The growing requirement for information security awareness

2009

ENISA – The growing requirement for information security awareness 2009

The growing requirement for information security awareness

2009

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (*http://europa.eu*).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2009

ISBN 978-92-9204-024-6

doi:10.2824/1209

© European Communities, 2009
Reproduction is authorised provided the source is acknowledged.

Printed in Italy

PRINTED ON WHITE CHLORINE-FREE PAPER

Introductory Note

This volume presents selected results achieved by the Awareness Raising Section of the European and Network Information Security Agency (ENISA) for the year 2009. The white papers included have been produced as part of the Work Programme 2009 of ENISA.

This edition consists of one book containing the following publications: *ENISA's ten security awareness good practices, ATM crime: overview of the European situation and golden rules on how to avoid it, The ENISA Awareness Raising Community, Information security awareness in financial organisations – Guidelines and case studies.*

The information has been compiled based on studies, analysis, research and interviews conducted by ENISA.

The collection is published in English and it has been prepared for documentation purposes.

General Table of Contents

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and the private business and industry actors.

Contact details:

For contacting ENISA or for general enquiries on Member State awareness programmes, please use the following details:

e-mail: Isabella Santa, Senior Expert Awareness Raising - *awareness@enisa.europa.eu*

Internet: *http://www.enisa.europa.eu/*

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA regulation (EC) No 460/2004. This publication does not necessarily represent the state-of the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external web sites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise without the prior written permission of ENISA, or as expressly permitted by Law or under terms agreed with the appropriate rights organisations. Source must be acknowledged at all times. Enquiries for reproduction can be sent to the contact address quoted in this publication.

© European Network and Information Security Agency (ENISA), 2009

ENISA's ten security awareness good practices

July | 09

enisa
European Network and Information Security Agency

ENISA's ten security awareness good practices

July 2009

Contents

Executive summary

This booklet touches upon crucial and important issues of awareness of information and communication technologies (ICT) for organisations. It does so by providing security good practices to focus employees' attention on information security and allow them to recognise IT security concerns and respond accordingly.

Good practices can be used as guidance for the main steps to undertake when promoting information security awareness. ENISA has produced this booklet to sensitise employees to information security risks and remind them of the basic golden rules. It is available for use in any information security training programme, awareness activity and company website.

The ENISA's ten security good practices are part of the set of tools developed in line with the information security awareness campaign that the Agency has launched across Europe.

ENISA's ten security awareness good practices

Recent high-profile data breaches have raised concerns, leading private and public organisations to understand that policies and technologies must be put in place to secure sensitive corporate information. These controls have to ensure the ability to secure information on the network as well as the opportunity to manage data which enter and leave the company. While policies and technology are certainly a critical part of any information security programme, these measures alone cannot deliver sufficient information security in practice.

Awareness of the related risks and available safeguards is the first line of defence for security. Employees are the real perimeter of the organisation's network and their behaviour is a vital aspect of the total security picture. Protecting organisations begins with making sure employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources and assist the organisation in keeping computers and network safe.

To this end, ENISA is engaged in positively influencing employees' behaviour towards information security, changing the mindset of the human element in order to achieve greater information security self-awareness.

Thus, the Agency has produced this booklet containing ten security good practices. These good practices are a great tool which will sensitise employees to information security risks and remind them of the basic golden rules.

This document is intended to be used by any organisations which are tasked to run initiatives which help employees learn how to protect corporate information and assets proactively.

1. Use of password

Your password is the equivalent of the lock and key to your house on the Internet. Passwords are a major defence, and developing good password practices will help keep your sensitive personal information and identity more secure.

Use a strong password

- ✓ The password of your computer is the key to access all information — both corporate and personal — you have stored on your computer and online accounts. Use a strong password to protect your data: use at least eight characters; combine letters (capital and lowercase), numbers and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Don't use personal information — name, child's name, birthdates, etc. — that someone might already know or easily obtain and try to avoid common words: some hackers use programs that try every word in the dictionary.

Change your password regularly

- ✓ If you believe your system has been compromised change passwords immediately.

Keep your password secret

- ✓ Your password is unique and must not be shared with anybody.
- ✓ Whenever possible, try to commit your passwords to memory. Have a strategy to memorize them.
- ✓ If you write your passwords down, be careful where you store them. Do not leave these records of your passwords anywhere that you would not leave the information that they protect.

Use different passwords

- ✓ Use different passwords for each online account you access (or at least a variety of passwords). If you use the same passwords on mul-

tiple accounts, an attacker who gains the access to one account will be able to access to all of your accounts.

2. Protect your computer

- ✓ Lock your desktop when you leave your desk to go for a meeting, a break and/or lunch.
- ✓ Do not allow other people to plug their USB drive into your computer, especially personal non-secure drives.
- ✓ Don't install or use illegal and/or unauthorised software as you are compromising your data security and breaking the law. Unknown outside programs can open security vulnerabilities in your organisation's network.
- ✓ Don't connect any personal disk, music player and/or USB drive to your computer.
- ✓ Don't connect your personal laptop to the network of your organisation as it may contain viruses or malware.

3. Use e-mail and the Internet with care

- ✓ Don't open unknown e-mails and attachments.
- ✓ Don't click on any hyperlinks contained in a suspicious email.
- ✓ Forward e-mail whether it is appropriate. Consider deleting the history of the message before doing so.
- ✓ Share documents in PDF format to ensure that the files cannot easily be changed.
- ✓ Confidential information should be encrypted when sent by e-mail.
- ✓ Surf the Internet carefully.
- ✓ Do not share information about your organisation and duties on social networking sites.
- ✓ Avoid participating in blogs in which your views and opinions may be interpreted as those of your organisation.
- ✓ Don't download documents and material from untrusted parties.
- ✓ Do not access, download, store or send any illegal or offensive material.
- ✓ Remember that what you surf on the Internet using your workstation can be traced back.

4. Use of portable corporate devices: laptops, USB drives, mobile phones and BlackBerrys

Laptops

- ✓ Don't install or use illegal and/or unauthorised software as you are compromising your data security and breaking the law.
- ✓ Switch off wireless connections when not required.
- ✓ Connect your laptop to the network of your organisation regularly to update your security checks.
- ✓ Back up the information stored in your laptop.
- ✓ Lock your laptop when you leave your desk to go for a meeting, a break and/or lunch.
- ✓ Do not allow other people to plug their USB drive into your laptop, especially personal non-secure drives.
- ✓ Don't leave your laptop unattended.
- ✓ Don't leave your laptop on view in the car.

USB drives

- ✓ Use an encrypted USB drive.
- ✓ Limit the number of corporate data which you store on your USB drive, especially on personal non-secure drives.
- ✓ Attach USB drives to key chains/lanyards to avoid loss of media: the reduced size of USB flash drives makes these devices easier to lose or be stolen. Furthermore, the higher storage capacity increases the potential amount of data at risk for unauthorised access. USB flash drives are usually put in bags, backpacks, laptop cases, jackets, trouser pockets or are left on unattended workstations. The number of incidents has increased recently as USB drives get lost, misplaced, borrowed without permission or stolen.
- ✓ Invite users to put the USB flash drive in read-only mode using the physical switch to avoid virus transmission: some USB flash drives include a physical switch to put the drive in a read-only mode to avoid the host computer from writing or modifying the data on the drive.
- ✓ Scan USB flash drive after copying files from an untrusted and/or unauthorised machine to avoid virus transmission.

- ✓ Before plugging your USB drive into someone else's computer, delete all files which are not relevant for the purpose of that action.
- ✓ Backup information: be able to recover data residing on USB flash drives.

Mobile phones and BlackBerrys

- ✓ Switch off wireless connections (i.e. Bluetooth and WLAN) when not in use. Bluetooth technology enables electronic devices to communicate with each other by using a short-range radio link. Some Bluetooth mobile handsets suffer from software bugs which lead to the practice of Bluejacking and Bluesnarfing.
  Bluejacking is when someone sends an anonymous text by creating a message and then sending it to another Bluetooth activated mobile. Bluejacking can be used to send unwanted messages.
  Bluesnarfing is used to copy personal information such as the contacts list from a handset to another.
- ✓ Don't leave your mobile and BlackBerrys unattended. Otherwise, it could lead to data loss.

5. Handle information with care

- ✓ Mark any document with the appropriate classification code.
- ✓ Protect sensitive content with a password to help prevent someone from changing or deleting it.
- ✓ Clean desk policy: don't leave sensitive data lying around. Carefully dispose documents.
- ✓ Don't leave sensitive information in shared conference facilities or meeting rooms in order to prevent their exposition to anyone using the room after you.
- ✓ Secure printing: print, copy and scan information only if necessary. Remember to collect the document from the printer's output-tray.
- ✓ Always shred documents containing sensitive information and/or marked confidential.
- ✓ Don't store any information on your local drive.

- ✓ Ensure that any third party working with you has signed a non-disclosure agreement before providing any sensitive information.

6. Visitors

- ✓ All visitors should be registered and signed –in when they arrive and out when they depart.
- ✓ All visitors should be provided with a visitor identity badge that needs to be worn at all times while they are visiting the corporate building.
- ✓ Escort visitors around the corporate building at all times. Letting visitors roam around the office is not secure.

7. Report loss and/or damage to portable corporate devices and incidents

- ✓ Report loss and/or damage to portable corporate devices (i.e. mobile, PDA or USB drive) to the IT department of your organisation.
- ✓ Report any found portable corporate device to the IT department of your organisation.
- ✓ Report any security breaches and/or incidents, even if you are unsure.
- ✓ Report any suspicious activities on your workstation and unexpected unavailability of an application if not warned in advance by your IT department.

8. Protect information outside your organisation

- ✓ When you are outside your organisation, ensure you keep sensitive information and equipment secure at all times to prevent theft or loss. In particular when you are in public places handle information with care.
- ✓ Be aware that someone can overhear your conversation. Don't make your organisation's confidential information available to everyone.
- ✓ When travelling or working from a remote place protect yourself against shoulder surfing.

9. Comply with the corporate security policies and procedures

- ✓ Comply with implemented corporate security policies and procedures.
- ✓ Ensure the confidentiality, integrity and availability of data.
- ✓ Respect legal requirements such as copyright restrictions, intellectual property, privacy and software licences.
- ✓ If you see colleagues acting in breach of corporate security policies and procedures, report it immediately.

10. Provide feedback to further fine-tune enforced solutions and security policies

- ✓ Provide feedback to further fine-tune enforced solutions and security policies.
- ✓ Suggest the purchase of any additional software if necessary to carry out your tasks.
- ✓ Ask questions or make suggestions for improving solutions and security policies.

Conclusions

Information must be protected from unauthorised access and employees should understand their roles and responsibilities in safeguarding sensitive data and protecting company assets.

Employees should know what they can and can't take home (company laptops, etc.), what they can and can't do with company resources, and what, if any, role they have in making backups and using security technology.

To this end, ENISA is engaged in positively influencing employees' behaviour towards information security, changing the mindset of the human element in order to achieve greater information security self-awareness.

By keeping these security awareness good practices in mind, employees will focus their attention on information security and allow them to recognise the most common IT security risks and respond accordingly.

References

ENISA, *Secure USB flash drives*, June 2008, available at *http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf*

ENISA, *Secure printing*, April 2008, available at *http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing.pdf*

August | 09

ATM crime

Overview of the European situation and golden rules on how to avoid it

enisa
European Network and Information Security Agency

ATM Crime:
Overview of the European situation and golden rules on how to avoid it

August 2009

Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways. The information includes contributions from members of the ENISA Awareness Raising Community (AR Community).

ENISA wish to acknowledge the efforts of the members of the AR Community and their organisations, ADICAE, Arjen de Landgraaf of E-Secure-IT, Daniel Blander of InfoSecurityLab Inc., David Barroso of S21sec, Fabio Guasconi of @ Mediaservice.net S.r.l., Fabrizio Cirilli, Gerasimos Ntouskas of KPMG Limited, INTECO, Joao Brites Moita, Lachlan Gunn of European ATM Security Team Ltd, Neal Ysart of PwC, Sissel Thomassen of InfoSecure, William Beer of PwC, Yves Le Roux of CA, who provided valuable inputs, material and prompt support for the compilation of the paper.

Finally, we would like to acknowledge the individuals who contributed to this document with informal reviews, valuable insights, observations, suggestions, and fixes. In particular, we would like to thank the members of the European ATM Security Team. While this is undoubtedly not a complete list, this content would be incomplete and incorrect without their help.

Contents

Executive summary

The number of ATMs in Europe is raising every year. ATM's can increasingly be found in many remote site locations other than banks, such as convenience stores, airports, petrol stations, airports, railway stations, department stores and so on. With the rise in the number of ATMs in Europe there has also been a significant rise in the total number of reported ATM crimes with the total losses reaching EUR 485.15 million in 2008. Organised crime is behind many of these attacks and the recession is seen as a likely driver of this increase. As a result, the ATM industry has placed the safety of users and protection against fraud as a high priority in order to help protect user's confidence in the system.

This white paper aims to provide a set of recommendations to raise user awareness about the different types of risks faced when using an ATM, along with advice on how to identify and counter them. ENISA believes that increasing user awareness of the risks is the first line of defence when tackling ATM crime, and can result in a significant reduction in ATM attacks and fraud. Citizens need education and guidance on what they can do to reduce these risks, by taking the necessary precautions when using an ATM, such as shielding their PIN when entering it, and by being alert to any signs of tampering or suspicious activity at an ATM.

ATM crime is constantly evolving, as are the countermeasures required to control it. This document can not cover all risks associated with the use of ATMs, nor can it offer complete advice on how to safely use them. This document should instead be seen as a useful and necessary starting point to increase overall user awareness of the issues they face when using ATMs, both within the European Union and elsewhere in the world, of data security and industry good practices. ENISA is committed to providing educational information to ATM's users about potential vulnerabilities and urges further information and advice are provided nationally in EU Member States by banks, financial institutions, payment schemes and law enforcement agencies.

This document does not cover any matters relating to legal requirements for the installation, operation, and maintenance of ATMs, for the processing of ATM transactions or for the movement and dispensing of bank notes.

Lastly, this document does not provide any advice or guidance with regard to the suitability, availability and effectiveness of any systems or devices that can be used to prevent or deter attacks on ATMs.

PART 1: ATMs AND RELATED SECURITY IMPLICATIONS

ATM

A definition

An automated teller machine (also known as an ATM or Cash Machine), is a computerised device that provides the customers of a financial institution with the ability to perform financial transactions without the need for a human clerk or bank teller.

Most modern ATMs identify the customer by the plastic card that the customer inserts into the ATM. The plastic card can contain a magnetic stripe or a chip that contains a unique card number and some security information, such as an expiration date and card validation code (CVC). Authentication of the user is provided by the customer entering a personal identification number (PIN).

When using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and can check their account balances as well as purchasing mobile phone prepaid credit, paying bills and so on.

The use of ATM machines: the European overview

In 2008, the European ATM Security Team (EAST) estimated that there were 383,951 ATMs in Europe and more than 1.5 million ATMs around the world ([1]). Seventy-two percent of the total number of European ATMs is

([1]) *https://www.european-atm-security.eu/Welcome%20to%20EAST/*
According to an EAST poll relating to the use of ATMs, which was conducted in May/June 2009, 49 % of the respondents had a basic knowledge of likely risks and threats but needed more information, while 14 % of the respondents were unsure of the risks and threats and would value guidance in how to identify them.

located in five countries: UK, Spain, Germany, France and Italy. The total number of European ATMs has increased by 6 % from the previous year.

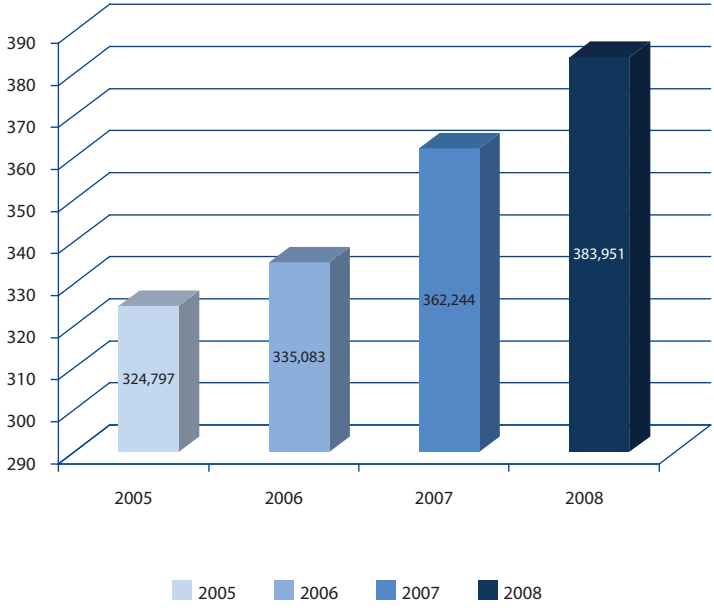


Figure 1: European ATM numbers. Source: EAST & EPC.

ATM crime and its financial impact in Europe

With the growth in the number of ATMs there has also been dramatic growth in ATM crime. A recent report released by EAST says that in 2008, fraud related ATM crimes in Europe jumped 149% when compared with the previous year. According to the report, this increase in ATM fraud is linked primarily to a dramatic increase of so-called ATM-skimming attacks. During 2008, a total of 10,302 skimming incidents were reported in Europe. However more disturbing are recent reports of attacks that are

leveraging readily available and advanced malware ([2]) that has infected the ATM networks and ATMS themselves.

According to the same report, physical attacks on users of European ATMs have fallen by 29 % mainly because of a decrease in the number of reported robberies. However cases of ATM physical attacks against the ATMs themselves have risen by 32 %. While the cash losses for such attacks are lower than other ATM crimes, these attacks continue to remain of great concern to the industry.

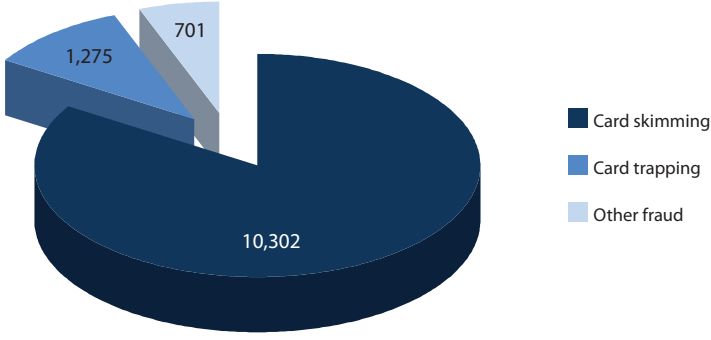


Figure 2: ATM related fraud attacks by number of incidents 2008 (full year). Source: EAST & EPC

Despite the dramatic increase of incidents, the actual losses due to fraud increased only 11 % when compared to the previous year. The losses due to ATM fraud were still significant and a total loss of almost EUR 500 million was reported last year despite the countermeasures taken in all European Countries. Figure 3 shows the loss breakdown in more detail.

Of this loss nearly EUR 400 million was due to international losses, which is the result of fraud committed outside national borders by criminals

([2]) Malware is software that is designed to infiltrate or damage a computer system without the owner's informed consent.

using stolen card details. These losses are mostly occurring outside Europe primarily due to the rollout of EMV ([3]) technology in Europe.

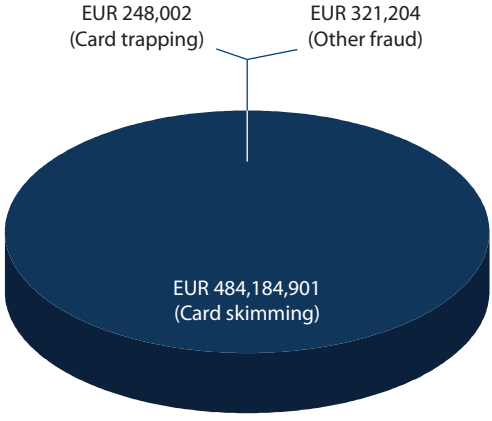


Figure 3: ATM related fraud attacks by total reported losses 2008 (full year).
Source: EAST & EPC

Estimated losses worldwide

The U.S. Secret Service estimates that annual losses from ATM fraud totalled about USD 1 billion or USD 350,000 a day in 2008.

In 2007, the cost of credit and debit card fraud in the UK soared to a record high of GBP 535 million. APACS reported that card fraud increased by 14 % in 2008 to almost GPB 610million. ATM specific fraud increased by 31 % and accounted for GBP 45.7million in losses in 2008.

([3]) EMV is a standard for interoperation of IC cards and capable POS terminals and ATM's, for authenticating credit and debit card payments. The name EMV comes from the initial letters of *Europay*, *MasterCard* and *VISA*, the three companies which originally cooperated to develop the standard.

Among recent incidents worldwide

Cases of ATM crimes continue to occur globally. Incidents have been reported not only in Europe but also in Asia-Pacific, the Americas, Africa, Russia and the Middle East. Some examples include:

- ✓ USD 500,000 were stolen from an Australian bank using a skimming device attached to an ATM in Melbourne ([4]);
- ✓ Devices capable of scanning bank and credit cards details were placed on cash machine outside a supermarket in UK ([5]);
- ✓ Ten ATMs were used to clone cards and steal more than USD 1 million from banking accounts in Melbourne ([6]);
- ✓ USD 500,000 were stolen from more than 250 victims in Staten Island by placing cameras directly onto the ATM keypad and filming victims typing in their PIN codes ([7]);
- ✓ Around 4,000 pages of data containing Cypriot credit cards were found on a computer belonging to thieves ([8]).

Types of ATM crime

A definition

ATMs are attractive to criminals because they provide direct access to currency, bank notes, and in some cases even user's personal information

---

([4]) 'ATM scam nets Melbourne thieves $ 500,000', 24 March 2009, available at *http://www.atmmarketplace.com/article.php?id=10808* (last visited on 20 April 2009).
([5]) 'Shoppers are targeted in ATM scam', BBC News, 11 March 2006, available at *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.stm* (last visited on 20 April 2009).
([6]) 'Australian police suspect Romanian gang behind $ 1 million ATM scam', 14 April 2009, available at *http://www.atmmarketplace.com/article.php?id=10883* (last visited on 20 April 2009).
([7]) 'ATMs on Staten Island rigged for identity theft; bandits steal $500G', 11 May 2009, available at *http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html#ixzz0J8qBVdar&D*
([8]) 'ATM scam targets hundreds of credit cards', New Europe, issue: 793, 4 August 2008, available at *http://www.neurope.eu/articles/89221.php* (last visited on 20 April 2009).

which can be used for identity theft. While an ATM may contain a significant amount of currency, bank cards themselves can give thieves access to customers' bank accounts which can easily exceed the value of the money contained in a single ATM. A stolen card, provided that the PIN has also been obtained, can be used by criminals to withdraw money from a bank account until the daily withdrawal limit is reached, or the card is blocked by the issuer. While thieves continue to attack ATMs and the currency they contain, they have increasingly focused on ways to collect bank card information and expand their gains.

There are three basic types of ATM attacks:

- ✓ Attempts to steal a customer's bank card information;
- ✓ Computer and Network attacks against ATM's to gather bank card information;
- ✓ Physical attacks against the ATM.

Theft of customer's bank card information

The main focus of ATM crime is the theft of the data stored on the bank card. Until recently bank cards used a magnetic stripe to store information to identify the customer and a PIN code to authenticate them and allow them to perform transactions at an ATM. Unfortunately the magnetic stripe information is simple to copy and counterfeit. As a result thieves have focused on methods of collecting this information.

This weakness has been partly addressed by the introduction in Europe of EMV smartcards (also known as Chip and PIN cards or Chip cards). According to EAST, 90 % of European ATMs are now EMV compliant.

While these cards also have magnetic stripes, the magnetic stripe alone is not sufficient to allow a transaction to take place at an ATM with a card reader that has been modified to read an EMV Chip (unless the card issuer allows such a transaction takes place). Thus counterfeit copies of these EMV cards cannot be used to withdraw cash from EMV compliant ATMs.

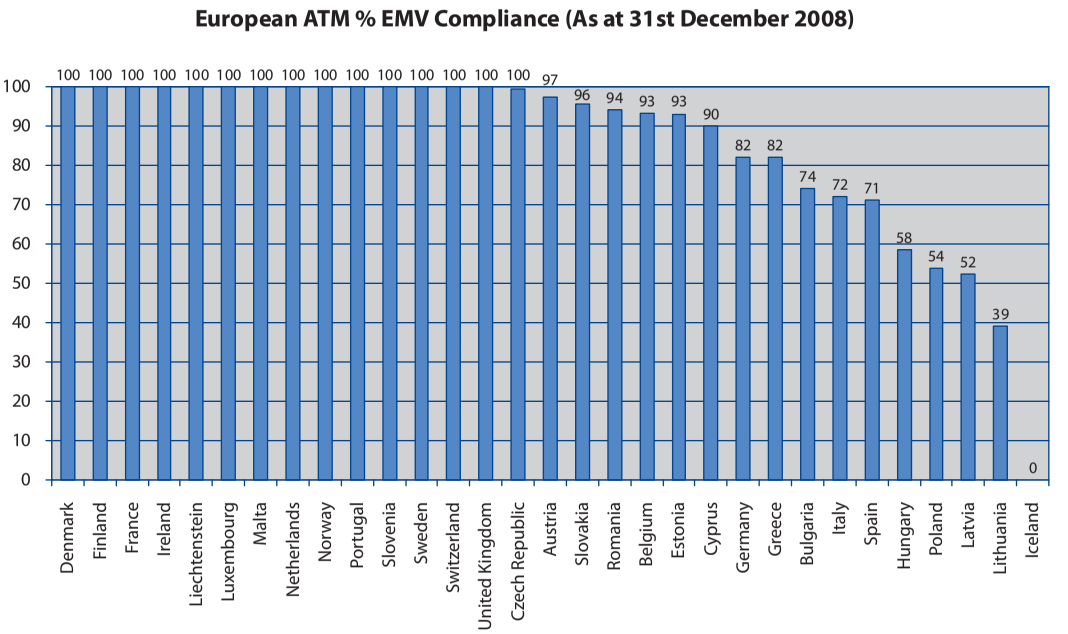


Figure 4: European ATM % EMV compliance. Source; EAST & EPC.

As most of Europe will have EMV compliant cards by the end of 2010, this means that criminals will have to use counterfeit cards outside of Europe and in countries where ATMs do not have EMV compliant ATMs. Until that time, however the threat of counterfeit bank cards still exists.

Card Skimming

This is when the card magnetic stripe details and PIN are captured at the ATM by a modified card reader known as a skimming device. The skimming device is placed on the ATM in such a way that disguises its presence but allows it to capture the information on the magnetic stripe of the card and the input of the customer's PIN. The customer inserts their card into the ATM that has been modified with a skimming device, performs a normal transaction, and retains the card. The customer leaves the ATM unaware that their card has been compromised. The captured information is then used to produce counterfeit cards for subsequent fraudulent cash withdrawals. The customer will only become aware of the fact when unauthorised cash withdrawals/transactions are made from their bank account. Because the skimming devices are very sophisticated, and often difficult to detect, multiple cards are compromised.

Several different methods are used by criminals to do this, and the PIN is obtained either by the usage of a small spy camera, or by a PIN pad overlay (false PIN pad). Increasingly blue tooth wireless technology ([9]) is used to transmit card and PIN details to a laptop at a remote location. This information can then easily be sent anywhere in the world to allow the fast production of counterfeit cards.

Typical methods used to skim cards

A small skimming device placed over the mouth of the card reader (or a false panel over the card reader), with a fake PIN pad overlay (or a small spy camera) to capture the PIN.

([9]) Blue tooth technology enables electronic devices to communicate with each other by using a short-range radio link.

Figure 5: Image is Courtesy of EAST

Figure 6: Image is Courtesy of EAST

A complete false front panel is placed over the fascia of the ATM.

Figure 7: Image is Courtesy of EAST

A skimming device placed in a card reader designed to open the door of a bank lobby (typically the camera used to collect PINs will be located above the ATMs in the bank lobby).

Figure 8: Image is Courtesy of EAST

Skimming devices can also be mounted beside the normal ATM card slot with a sign that says, 'slide card here first', although this is not so common in Europe.

Figure 9: Image is Courtesy of Naples Police Department

Fake ATM machines

Criminals have been known to place fake ATM machines in and around shopping centres and other public locations. These look like real ATM machines, and some have even been known to dispense cash. All cards used at these machines are copied, and the PIN information is obtained from the PIN pad. As these machines are not connected to a network, the criminals can place them anywhere there is a power source.

Recent ATM skimming incident

In April 2009, a 33-year-old Microsoft employee, who lives in New York City, stopped in the closest Chase bank to get some cash to pay his barber. When he inserted his ATM card in the machine, he noticed a bit of resistance. The screen said the machine was unable to read his card. So he tried again. But a second time, the machine gave him an error message.

Figure 10: Skimming incident.

He was about to give up and try another machine, when a thought popped into his head. He had heard about devices that fraudsters attach to the outside of card readers on ATM machines and, though it seemed unlikely, wondered if that was the source of his problem. He tried to pull on the green plastic surrounding the card slot and found that it peeled right off. Behind an extra mirror attached to the machine, he also found a hidden camera positioned right over the key pad, to capture the PIN codes as victim's type them in ([10]).

Card trapping

This is when a card is physically captured by the ATM combined with any number of methods used to capture the customer's PIN. When the customer leaves the ATM without their card, the card is retrieved by the thieves and used to make fraudulent cash withdrawals or to make other purchases (either in store, telephone, or online). Typically only one card is lost in each attack. The criminals have to withdraw the whole device each time a card is trapped, although recently a card trapping device has been seen that can stay in place for a period of time and that allows removal of trapped cards without the removal of the device.

The most common variant is known as 'Lebanese Loop'. Thieves place a device fitted with a loop of tape, wire, or strong thread over an ATM card reader. This allows a card to be inserted and read by the ATM, but not returned. The criminals obtain the PIN by watching the user entering the PIN (shoulder-surfing), and retrieve the card after the victim has left the ATM under the impression that the card has been retained by the ATM for other reasons.

There are multiple techniques used to capture the customer's PIN including the use of video cameras, offering advice and distracting the customer while they input their PIN. Another variant of card trap is known as the Algerian V.

([10]) *http://abcnews.go.com/Technology/Business/story?id=7434509&page=1*

Distraction theft or 'manual' skimming

This is similar to card trapping, the difference being that instead of a trap capturing the card it is actually removed from the card reader by the criminals. Having observed the entry of the PIN, a group of criminals distract the user and cancel the transaction. While two criminals keep the user busy (often by dropping a bank note and asking the user if belongs to the user) another criminal hits the stop key and takes the customer's card. When the user turns back to the ATM they are informed that the ATM is faulty and will not return their card.

Shoulder surfing

This is a method used by criminals to obtain a PIN, typically when trapping cards, or when stealing cards by distraction theft. Standing behind the victim, a criminal reads the PIN as it is entered and either memorises it, writes it down, or enters it straight into a mobile phone.

Leaving transaction 'Live'

This when a criminal completes an uncompleted transaction after the victim has left the ATM. This is typically done by making the victim believe the ATM is out of order while they are in the middle of a transaction, or any other means of moving the victim away from the ATM while in the process of withdrawing funds.

A recent incident in the USA

Two men robbed unsuspecting customers of USD 1800 in cash within half an hour of stealing their ATM cards in the middle of a transaction. In one of three known robberies, police believed the criminals walked less than two metres to a neighbouring ATM and withdrew USD 900 in three separate transactions, all before the victims made it into the bank to cancel their card. On another occasion, the pair stole USD 900 through credit card transactions and cash withdrawals within half an hour of stealing a bank card.

Police believe the first offender watches a bank customer enter their PIN into the machine and keys it into a mobile phone. The second offender then distracts the customer by dropping a USD 20 note at their feet and tapping their shoulder, while the first offender steals their card as it is ejected from the ATM. The stolen card is used in another machine, leaving the ATM customer to wonder why the machine has not returned his card ([11]).

Cash trapping

Criminals fix a device to the cash-dispensing slot, causing notes to get stuck inside when customers attempt to do a withdrawal. The customer leaves assuming that the machine is out of order or goes inside the bank to report the incident and the thieves return to retrieve the notes.

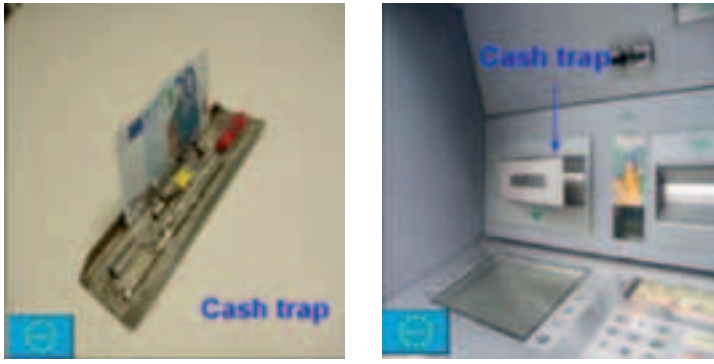


Figure 11: Images are Courtesy of EAST

([11]) Robinson G., 'Bondi banks scam: ATM alert', *The Sydney Morning Herald*, October 2008, available at *http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950* (last visited on 2 July 2009).

Computer and network attacks

The Internet provides world-wide access and connectivity. It provides each of us access to individuals around the globe. It also provides thieves with access to systems and people. This threat manifests itself the same way.

Network attacks against ATMs

ATMs communicate with the banking systems through a network connection. Some of these connections use private networks and proprietary network protocols but more often these connections now occur via the Internet and using standard network protocols. Thieves will use computer programs (malware) to attack the ATM in order to gain access through a software or computer flaw. Once they have gained access to the ATM, the thieves will install software that collects card information and PINs. An ATM that has been compromised is not physically recognisable from one that has not and often users will be unaware of the danger.

Viruses and malicious software

ATMs often now use publically available operating systems and off the shelf hardware and as a result are susceptible to being infected with viruses and other malicious software. The malicious software is injected into the ATM through network attacks, or through other infected devices. Once installed on the ATM, the malicious software will collect card information and PINs.

Recent incident

In April 2009, ATMs in Russia were discovered to have been infected with sophisticated malware. The malware was able to not only collect card details but also the PIN. While one specific ATM vendor's machine was successfully targeted, intelligence reports received in March indicated attempts were made to infect other vendors ATMs ([12]).

([12]) *http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html*

Phishing

Fraud and scams using mail communication have existed for many years. With the advent of email and the Internet this scam has quickly spread worldwide and earned the name 'Phishing'. Phishing scams are designed to entice the user to provide the card number and PIN for their bank card. Thieves will send an email representing them as a bank and claiming that your account information is incomplete, or that the user needs to update their account information to prevent the account from being closed. The user is asked to click on a link and follow the directions provided. The link however is fraudulent and directs the user to a site set up by the thieves and designed to look like the user's bank. The site directs the user to input sensitive information such as card numbers and PINs. The information is collected by the thieves and used to create fraudulent cards, withdraw funds from the user's account and make purchases.

PIN cash-out attacks

Thieves use sophisticated programming techniques ([13]) to break into websites which reside on a financial institution's network. Using this access, the thieves access the bank's systems to locate the ATM database. The thieves collect card numbers, and if necessary, alter the PIN for the cards they are planning to use. The thieves then sell the cards and their data to other thieves. Those thieves create ATM cards using the stolen information, and use the cards to withdraw cash from the accounts. The original thieves usually receive a percentage of the proceeds.

Recent incident

During January and February 2008, the US Secret Service has revealed that they were investigating two breaches - one against OmniAmerican Credit Union and the other against Global Cash Card. In April and May of 2008, it is also known that there were breaches of this nature against

([13]) *Thieves use SQL injection techniques.*

Symmetrex, a transaction processor, and 1st Source Bank. Symmetrex cards were used by MetaBank. Actual losses of more than USD 4 million were experienced just by those brands ([14]).

Physical ATM attacks

ATM physical attacks are carried out with the intention of gaining access to the cash within the ATM safe or the ATM security enclosure. Some of the most common methods include ram raids, explosive attacks (gas and non-gas) and cutting (e.g. rotary saw, blow torch, thermal lance, diamond drill). Robbery can also occur when ATMs are being replenished or serviced. Staff are either held up as they are carrying money to or from an ATM, or when the ATM safe is open and cash cassettes replaced.

Security implications

What happens when a customer's details have been captured?

Once criminals have captured card numbers and PINs, the information can be used in any number of ways. The details from compromised cards can either be used to make withdrawals from the customer's bank account, or the card details can be used to make purchases in retail outlets, over the Internet or over the telephone. Counterfeit credit and debit cards can be made for use by other individuals.

The criminals normally operate in highly organised gangs and can be acting on behalf of larger criminal syndicates. There has been a recent upsurge in criminal gangs coming from overseas to carry out such deception.

([14]) *http://garwarner.blogspot.com/2009/03/bank-hacking-exposed-analyzer-affadavit.html*

Risks and threats

Summarising the potential risks and threats that citizens could face following a successful ATM crime is a significant task. This is mainly because a successful ATM crime may not only result in unauthorised access to a victims' bank account but it could also equip the criminal with the information and tools to commit a broader variety of offences ranging from simple impersonation frauds to more complex identity related frauds such account take over.

This is perhaps best illustrated by considering the growing range of services that are available via the typical ATM served bank account. If, for example the details of your debit card were compromised together with the PIN, the criminal may then have the ability to access, not only funds from your account but they could potentially perform a range of account management functions specifically directed at the commission of further offences.

As a result, the number of risks and threats are almost infinite, however at the highest level there are two broad categories of risks and threats to be considered.

The first risk category centres around more immediate forms of attack such as note traps, the Lebanese Loop where the victim's bank card is immediately obtained by the criminal, or direct physical attacks on either ATM users or the ATM's themselves for example pick pockets or ram raids.

The second risk category is focused on longer term damage and is arguably the most prevalent due to the broad range of attack signatures. This type of crime invariably results in the subsequent exploitation of the information and identity of the victim although there are also often primary gains such as immediate access to funds. A range of frauds including identity theft, account takeover and extortion may result and for the victim, apart from the financial losses, there are often undesirable impacts such as impaired credit ratings or adverse court judgements.

Looking ahead, ATM crime is likely to become even more attractive to the criminal, as the types of services and products that are delivered via the

latest generation of ATM's continue to develop and evolve. As well as increasing numbers of ATM's being designed to take a variety of different types of deposit for example cash and cheques, many are now being used to dispense other products which will also be attractive to the criminal, such as postal stamps. In these circumstances it is reasonable to expect that the variety of attacks will also keep evolving and ATM crimes in all their different forms will continue to be a cause for concern thus making the need for public awareness all the greater.

Security implications for ATM cardholders

ATM fraud has become more technically sophisticated and criminals have found new and innovative ways of withdrawing money from cash accounts using fake or counterfeit cards with real cardholder data on them. Although the criminals' methods of getting to the money have become more advanced technically, the issues for the cardholders are still the same as they were when ATM fraud first became a major issue.

The main aim for account holders is to keep their money safe in the bank. Information security has, for too long, been focusing on technical solutions to maximise protection. With regard to ATM security incidents over the recent years, the human element has increasingly attracted more attention. Cardholders must be aware of the risks they are exposed to and how to prevent fraud occurring, or what to do to minimise the damage should their card details fall into the wrong hands. ATMs are used by criminals both to gather card information and to fraudulently withdraw money from customer accounts. Cardholders must constantly be aware of both issues when using their cards, when observing people withdrawing money, and when checking their own bank statements.

Card protection

Cardholders must be aware of the risk to their cards, and also of how they can help to prevent money being withdrawn fraudulently from other cardholders' accounts.

The first sign of something not being quite right is when a cardholder visits the ATM. It is important for cardholders to be aware of their surroundings; to stand close to the ATM and shield the key pad to avoid anyone seeing them enter their PIN. The best way for cardholders to protect their own card and card details is to be alert when using an ATM. For example, using the same ATM regularly will make cardholders aware of how the ATM should look and to observe normal, expected behaviour. Should there be anything unusual with the machine, cardholders must ensure that they don't use the machine and notify their bank of their observations and suspicions.

Personal protection

If cardholders see suspicious behaviour around ATMs, then it is important that they immediately notify the bank if possible. It is important that they never try to further investigate a suspicious looking ATM or one that is not behaving as expected; fraudsters are often close by, and may try to intervene, should anyone start to investigate the ATM more closely. There are examples of situations where ATM cardholders have been physically assaulted when trying to find out what may be wrong with the machine. Be aware of other people around the ATM; if you see someone is behaving suspiciously or it feels uncomfortable to be using an ATM, then pass your suspicions and observations on to the bank and use another ATM.

Protecting your PIN

Fraudsters use many different methods to get to card details, and the first line of security to protect cardholders from being defrauded is to ensure nobody knows the PIN. When fraudsters get to know the PIN they can easily get to the money. ATMs do not have the same security measures all over the world, and it is a good rule for cardholders to change their PIN

every time they've been abroad. Fraudsters will also try the PIN they have to access accounts on other cards, so a good rule is always to have a different PIN for different cards.

ATM card details and the Internet

Another way of gaining access to personal banking and authentication details e.g. PIN numbers is via the Internet. Once this information is obtained duplicate cards can be produced. Phishing incidents, where cardholders receive an email asking them to click on links and provide bank and personal details, are on the increase. The emails often come from sources that look legitimate, because the fraudsters have found very sophisticated ways of simulating correspondence between cardholders' banks such that it may sometimes be difficult to spot a fraudulent message. A good rule is never to click on hyperlinks received by email asking to confirm bank details. Another good rule is to use good anti-virus and firewall software on the PC used for Internet banking.

Other security precautions

Another security precaution might be to investigate the use of rechargeable banking cards that have limited amounts of money put on them. This will prevent the fraudsters from withdrawing a huge sum of money that a cardholder may have deposited in a bank account.

Moreover, consumers should also be vigilant when providing bank details over the phone as someone nearby may be listening in. Always try to find a quiet area when contacting your bank using the phone.

To enable to spot a fraudulent withdrawal, a cardholder should regularly check his bank transactions and account balances.

Keep the bank's emergency number at hand

The fraudsters will try to withdraw money as quickly as they technically can, after they have gained access to card details and PIN numbers. It is

important to notify the bank and sometimes the local law authorities as quickly as possible after a cardholder suspects that his PIN and/or card details have been disclosed, to enable the bank to put a block on the account(s) thus preventing fraudulent withdrawals. Keeping the bank's emergency line details always to hand is crucial; remember that with when a card has gone missing, the emergency number will also be lost if it is not written it down somewhere safe. Also, find out which number to call from abroad, as the number used at home may not work from a hotel switchboard.

PART 2: GOLDEN RULES

Golden rules to reduce ATM crime

These safety tips draw on analysis of data and available research. This section of the paper is intended to provide, in one convenient place, recommendations to raise awareness about the various types of crimes being carried out, with advice on how to spot them.

These rules offer maximum protection for the least amount of effort. By following these rules interested parties will increase their protection when they using an ATM.

Category	#	Recommendations	Description
Choose a safe ATM machine	1.	Don't use ATMs with excessive signage or warnings	Don't use ATMs with excessive signage or warnings posted on the machine as they are often used by fraudsters to try and assure the public that ATMs that have been tampered with are safe. Be especially cautious of unusual instructions on how to operate the ATM.
	2.	Use ATMs inside banks	When possible use ATMs inside banks, other buildings and enclosed areas, rather than on the street. ATMs on the street are easier for criminals to access.
	3.	Don't use free standing ATMs	Avoid free standing ATMs that are in the open. Avoid ATMs that are not bolted to the side of a building or secured inside a facility. If the machine offers no fees but it is attached to a building and everything processes properly, you are probably fine.

>>>

Category	#	Recommendations	Description
Observe your physical surroundings	4.	Be aware of the surroundings	Always be aware of your physical surroundings. Use an ATM which is in clear view and well lit. Be extra careful of machines in dark areas or in places that don't look well guarded and monitored.
	5.	Check that people in the queue are at reasonable distance	Check that other people in the queue are a reasonable distance away from you. Be cautious if strangers offer to help you at an ATM, even if your card is stuck or you're having difficulties. Do not allow anyone to distract you.
	6.	Protect your PIN by standing close to the ATM and shielding the key pad	Shield the keypad with your hand as you enter your PIN to prevent a hidden camera or a person from capturing your information. Never reveal your PIN to anyone.
Observe the ATM	7.	Pay attention to the front of machines	If the front of the machine looks different from others in the area (for example, it has an extra mirror on the face), has sticky residue on it (potentially from a device attached to it) or extra signage, use a different machine and notify bank management with your concerns.

>>>

Category	#	Recommendations	Description
Observe the ATM	8.	Pay close attention to the slot you slide in your card	If you're visiting an unfamiliar ATM machine that is not inside a bank, examine it carefully for devices. Even if you are familiar with an ATM machine, pay attention to any differences or unusual characteristics of the card reader. If the slot looks strange or bulky, try to push on it with your hand. If something has been stuck over the real reader it will wiggle or even come off. Card or cash trapping devices need to be glued or taped to the card reader or cash dispenser. If the ATM appears to have anything stuck onto the card slot or keypad, do not use it. Cancel the transaction and walk away. Never try to remove suspicious devices.
	9.	Pay close attention to the ATM's PIN pad	Even if you are familiar with an ATM machine, pay attention to any differences or unusual characteristics of the ATM's PIN pad. If a fake PIN pad has been stuck over the real pad it will appear 'incorrectly attached' when being moved a bit back and forth.
	10.	See if there are extra cameras	Look for 'extra' cameras beyond the basic and generally obvious ATM security camera.

>>>

Category	#	Recommendations	Description
Observe the ATM	11.	Report confiscated cards immediately	Report confiscated cards immediately. If you can, don't leave the machine. Instead call the bank from the ATM where your card was taken. Never rely on the help of strangers to retrieve a confiscated card. In addition notify your local law enforcement.
	12.	Beware if the ATM does not dispense cash or charge fees	If you use an ATM that doesn't dispense cash, it is much more likely to be a fake and you should notify your bank of the potential risk to your account. If you are using an ATM that is not associated with a bank (often in service stations and bars) beware if it does not charge you a fee. Private ATMs that are not associated directly with banks make their money through fees. Not charging a fee is an indication that the ATM may be fraudulent.
Review your statements	13.	Frequently review your account statements	Review your card statements frequently for any activity you do not recognise. While most fraud happens quickly, some may not occur for weeks or months after your card information is captured. Frequent reviews will help reduce the potential impact of any fraud.

>>>

Category	#	Recommendations	Description
Report suspicious activity	14.	Report confiscated cards immediately	Report confiscated cards immediately. If you can, don't leave the machine. Instead call the bank from the ATM where your card was taken. Never rely on the help of strangers to retrieve a confiscated card. In addition notify your local law enforcement.
	15.	Report any suspicious activity immediately	If your bank card is lost or stolen, or if you notice fraudulent activity in your account, report it immediately in order to prevent any further loss.

Conclusions

ATMs are an important part of commerce throughout Europe and provide a valuable service to customers. With the growth of the use of ATMs there has also been a dramatic increase in ATM attacks and fraud. Techniques such as skimming, phishing, and network attacks against ATMs have caused nearly EUR 500 million in losses in Europe last year. These techniques have become more sophisticated over time, and have resulted in a 149 % rise in ATM attacks during 2008.

This paper has presented numerous ways that ATM attacks are carried out, as well as simple techniques and guidance that ATM users can use to detect and prevent against these attacks.

ENISA believes that an important step to reducing ATM fraud and attacks is to raise the awareness of likely threats and ways in which to counter them. This information can significantly reduce the incidence and financial impact of ATM attacks, and result in improved confidence in the use of ATMs.

APPENDIX

ATM usage and fraud: case studies

ENISA gathered some case studies and experiences from a few European countries dealing with different ATM usage and fraud, to enable readers to identify key problems, issues and solutions, making the suggested rules more effective and presented in concrete ways.

Cyprus

Currently on the island (in the part that is controlled by the Republic of Cyprus), about 560 ATMs are installed. There is no information about the number or type of ATMs installed in the Turkish Occupied area of the island. The majority of the 560 ATMs are installed as through-the-wall. A number of 2-3 ATMs are installed as cash-kiosks. A significant number of ATMs installed on the island are equipped with special plastic shields at the card slots, plus an anti-skimming device to prevent the placement of skimmers (and the subsequent capture of Magnetic Stripe information), which could play a significant role in eliminating the card skimming cash machine fraud ([15]).

Recent incidents occurred in Cyprus

The following information was captured by the JCC Payments System Ltd Fraud Monitoring System.

Case No. 1

Some individuals were using counterfeit, top up and re-encoded cards at ATMs. 26 cards were used and EUR 2,310.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. One fraudster was arrested at the airport.

([15]) All the information disclosed are provided by the Risk Management department of JCC Payments Systems Ltd, the sole acquirer/processor of Cyprus for VISA, MasterCard, AMEX and Diners.

Case No. 2

Two individuals were using counterfeit, top up cards at ATMs. 131 cards were used and EUR 15,830.00 was withdrawn. The individuals were arrested by Police while using counterfeit cards and after the fraud monitoring system identified them.

Case No. 3

An individual was using counterfeit top up cards at ATMs. 43 cards were used and EUR 1,860.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. The fraudster was arrested.

Case No. 4

Two individuals were using counterfeit top up cards at ATMs. 76 cards were used and EUR 7,950.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. The fraudsters were arrested.

Case No. 5

Several individuals were using counterfeit top up cards at ATMs. 53 cards were used and EUR 10,700.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. One fraudster was arrested.

Case No. 6

Two individuals were using counterfeit top up cards at ATMs. 122 cards were used and EUR 21,980.00 was withdrawn. The individuals were arrested by Police while using the counterfeit cards and after the fraud monitoring system identified them.

Case No. 7

An individual was using counterfeit top up cards at ATMs. 41 cards were used and EUR 28,340.00 was withdrawn. The individual was arrested by Police while using the counterfeit cards and after the fraud monitoring system identified him.

Case No. 8

An individual was using counterfeit top up cards at ATMs. 82 cards were used and EUR 12,330.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. The fraudster was arrested.

Case No. 9

Two individuals were using counterfeit top up cards at ATMs. 21 cards were used and EUR 10,980.00 was withdrawn. The fraud monitoring system identified the fraudulent activities and informed the Cyprus Police. The fraudsters were arrested.

Risks and threats

ATM fraud development

ATM fraud activity is steady and decreasing in 2009 mainly due to the EMV chip rollout within Europe and the effective and proactive fraud counter-measures as used in Cyprus.

An increasing number of fraudsters have been identified. The main reason for that is they wrongly assume that Cyprus is a country with limited technological advancement (Limited EMV terminals and Weak Card Monitoring Systems) and it is Europe's most distant island which is consider by fraudsters as a place in which they cannot be caught. In fact there is only one acquirer so it is much easier to get caught in Cyprus, whereas in the UK or Greece where there are 5-6 different acquirers that do not share data between them it is much more difficult to get caught.

ATM fraudsters capabilities

Fraudsters identified on the island were characterised by an intelligent approach during the commitment of fraud and showed great ability to circumnavigate the banks' security defences. They also act resourcefully and seem much organised. Furthermore, fraudsters' skimming technologies are superseding vendors' technologies (e.g. 'Jitter', 'FDI').

ATM fraud impact

Fraud is currently affecting the 'brand integrity' and cardholder confidence; however it is compensated by the Card Systems' actions as these effectively counterattack the fraudsters' actions during a credit card fraud case.

Italy

In Italy the ATMs are mainly used with debit cards, which allow the immediate withdrawal of cash from the bank account and also payment and query features such as telephone charges, information retrieval on the personal account, donations, etc. The BANCOMAT circuit (main Italian debit card circuit) and its protocols were designed more than twenty years ago and, even though today they are evolving towards new concepts, security issues are still present related to design choices and solutions applied to technologies that nowadays are dismissed in favour of more modern ones.

The first cards of this type, still widely used, are based on a magnetic strip on which various information are stored. Authentication is based on a PIN code of 5 digits, which is given directly by the bank. However, in the recent years, the companies managing the circuit are trying to replace these cards with the new chip-based generation ones (smart cards), more robust with regards to cloning attempts. The whole environment is evolving: the old ATMs based on proprietary systems are being replaced and the new ones provide advanced functionality, such as multimedia content, payments with the automatic recognition of notes,

touch screen, keyboard and more extensive opportunities for customisation of the operational software.

All ATM devices are controlled by closed circuit video surveillance equipment to avoid physical attacks like using cranes to uproot the ATMs from their basement, using stolen cars as rams or placing explosives. Sophisticated systems of attack are using a false front-end with a 'skimmer' to clone the card. Italian Banks, to limit the damage of theft (in addition to the cost of the ATM system, which is still high), supply ATMs with only the strictly necessary cash amounts, and with devices that permanently alter the notes (colour ink, etc.).

Until today, those frauds carried out in Italy were mainly limited to the categories described above, since there have not been any documented logical attack on the ATMs. Nevertheless, it is possible to assume that in the near future this trend will dramatically change.

One of the main problems encountered while working on the security of ATMs, is related to the number of players in the field: often the communication between these parties is weak and it is not easy to understand if a bug is due to the hardware manufacturer (ATM vendor), to the software manufacturer, to the protocols being used or to the configuration of the ATM infrastructure itself.

Methodologies used during attacks

The latest generation ATMs are basically industrial PCs with specific serial connections or USB devices (PINPAD, dispenser for notes, keyboards more or less customised, etc.) communicating with the bank via IP or via SNA protocols (now encapsulated over IP). Banks have also saved money by reducing investments in dedicated data lines decreasing the secu-

rity of the ATM systems themselves. It has often been pointed out that these devices are directly connected to the internal network (LAN) of the bank or to the branch network and are rarely separated from the network segment where there are other corporate systems (from the workstation to the server systems).

Generally speaking, ATM systems are used as industrial equipment and not as ordinary computers. This also means that, once installed, are rarely updated and poorly managed. Furthermore, as industrial products, patches of the operating system (mainly Microsoft Windows) first have to be tested, licensed and distributed by the manufacturer, introducing an additional obstacle. This choice exposes ATM systems to various types of well-known threats, such as worms and viruses, which could compromise the infrastructure, resulting unavailable (e.g. the mass crash of Diebold ATMs in 2003, due to the Slammer worm). An agent of external or internal threat to the bank could also attack the systems by exploiting vulnerabilities in the operating system, software or password management (often, 'known') to access the ATM and modify the software in order to provide more cash, if specific conditions are met.

Moreover, the analysed communication protocols have revealed numerous security problems. Although in the recent past newer and safer-considered specifications have been released, usually are not fully implemented. For example, communications between the ATM and the back. end (mainframe, etc) are often not encrypted and there are no features that will ensure the legitimacy of the data. During some attack sessions it has been demonstrated how it is possible to intercept and edit these notifications, allowing the attacker to withdraw more money than the account current availability, or modify the amount of withdrawn money.

From the different analysis carried out, another serious problem was found (that also exacerbates what done before), which is the placement of ATM systems: in case of mobile ATMs located in unprotected areas, the power connections and network links are often accessible by the end-user (even if the ATM is located inside the bank). An artificial lack of power would cause a reboot of the system, providing several information to the attacker; on the other hand the possibility to reach network cabling

could allow installing a TAP system able to intercept network traffic and forward through a wireless network.

In order to better understand how many security issues are possible, not just related to technology, we can think about how ATM systems are deployed. They are spread throughout the country, often not transiting the banks headquarters and being installed directly at branches or at other points of interest by external parties that are provided with encryption keys.

Management procedures for those systems are usually less detailed than the ones of IT systems, even if they are now using more and more similar platforms: we are speaking about security tests after deployment, password management, security monitoring and alerting, vulnerability and patch management, malware protection and so on.

It has to be repeatedly pointed out that many of these attacks are not just aimed to debit cards but can also be effective with credit cards being used through ATMs, even if the specific impacts still have to be fully assessed.

Security issues related to the ATMs are too often not recognised, very few if no banks have conducted a formal and complete security risk assessment to their ATM infrastructures. The use of the concept of 'security through obscurity' that has long gone along with dedicated devices is conceptually wrong, and is proving to be so as the global trend of bank fraud rises. More and more people are studying such infrastructures to find security issues, which could provide access to cash dispenser and to the real final aim of these new forms of organised crime: notes.

In the future logical attacks to the ATMs will almost certainly grow: overlooking these risks during this delicate, transition stage, will mean, in practice, starting to lose a definitely critical fight, much important to the national security of every country and economical system of the world.

Portugal

Portugal has one of the highest penetration rates of ATM machines *per capita* in Europe. This is, in most part, due to the advanced functionalities that are available to the population in general, including the payment of public and private services (such as gas, water, taxes or mobile phone services) or the possibility to buy tickets for concerts, apart from the more traditional financial services such as withdrawing money or consulting the balance.

In the following paragraphs, we will present an overview of the ATM network in Portugal, the main threats and types of frauds, as well as what is being done and what needs to be done in order to improve the security of the ATM environment.

The ATM network

The ATM network in Portugal is managed by SIBS, a company owned by the majority of banks that have a presence in the market. SIBS ranks as the sixth biggest automated clearing house (ACH) in Europe, processing over 2.000 million transactions / year totalling about 6.000.000 million Euros, and has been responsible for the development of an integrated ATM and POS network, common to all the banks in the market.

Regarding the usage of credit and debit cards, the Portuguese indicators are above the average in the EU, both in cards, ATM machines and POS terminals *per capita*. Also, Portugal has the highest level of card usage in Europe, when compared to other forms of payment, representing over 60 % of the transactions.

All the ATM machines in the country are now EMV compatible (Europay, Mastercard and Visa), as well as 83 % of the POS terminals. An effort is also being made from the financial institutions to make available EMV compliant credit and debit cards, representing about 44 % of the cards in the country as of 2008.

In terms of communications, the ATM network is supported by dedicated communication lines (VPN) through SSL, with additional security mechanisms in place such as 3DES encryption and MAC (Message Authentication Code). In addition to that, the philosophy behind the development of the ATM network takes a security approach into consideration, where no equipment can initiate a communication directly with an ATM machine; instead, is the ATM machine that communicates with other equipment (including SIBS systems).

PayWatch

In late 2008, a new company was formed – Paywatch – with the responsibility to monitor 24/7 the ATM network, identify card usage patterns, and detect fraud patterns at ATM and POS terminals. This will allow Paywatch to identify frauds perpetrated with Portuguese cards and/or at the ATM / POS network in real time and rapidly limit the damages. This is only possible due the abovementioned fact that the network is integrated and can be seen as whole as opposed to a fragmented network. Not so long ago, these monitoring activities were seen by the population in general as some sort of a 'Big Brother', and people could not understand why someone was looking to his/her own transactions. However, probably due to the fact that more cases are made public every year (not only in Portugal, but all over the world) the mentality has changed in the last couple of years and people now see this as an advantage to the system and as a protection to themselves and to their own money.

PayWatch is able to detect in real-time where a cloned card is being used in the ATM network, through the analysis of cryptograms – this is limited to Portuguese cards and ATM machines. Basically, if a card is supposed to be an EMV card, but only the magnetic track is being used (fallback), the card is most likely a clone, and the transaction is rejected.

PayWatch has an overview of all the usage of Portuguese credit / debit cards, both in the Portuguese ATM network, as well as abroad. This makes it possible for PayWatch and SIBS, to block the usage of certain cards, or

even block transactions from a certain area in the world, in case a surge on the fraudulent usage is detected – for example, transactions from any Portuguese card made from, say, the city of Barcelona, can be blocked.

If PayWatch detects a cloned card or other fraudulent usage in real time, SIBS or the bank can contact the client immediately and proceed with the appropriate actions in order to mitigate the risks.

Threats and fraud levels

Fraud levels in the country are generally low, with one to two situations reported a year. Physical attacks to ATM machines are the biggest threat, which grew significantly in 2008, due to the specialisation of a group of people from Eastern Europe in this type of attacks.

However, the number of unsuccessful attacks is also growing at a faster rate. This is due to the fact that an increasing number of ATM machines now have banknote ink/dye staining systems and are fixed to the ground.

In terms of attacks on cards, skimming is still the #1 threat. The copy of the card occurs at the ATM machine itself, or at the lobby of the banks where some ATMs are installed where citizens have to swipe the card to open the door, the latest representing 10 to 20 %. The PIN is usually captured through the use of a camera placed on top of the ATM machine, through a fake keyboard or through shoulder surfing.

All ATM machines in the country have now some sort of anti-skimming mechanisms. The most common is the use of a reader that slows down the entrance of the card, making it more difficult for the card to be read by a fake reader.

From a technological point of view the ATM machines could have a camera incorporated in order to try to detect if someone was placing fake equipment on top the ATM, but that is not possible in Portugal due to privacy issues, as stated by the National Commission of Data Protection.

Although the relationship between SIBS and the police is very cooperative and with mutual trust, the same cannot be said about the Justice. People, who commit fraud repeatedly, are sometimes condemned only for one particular action, and the fact that they are re-incident is not taken into account. Also, the Portuguese legislation only condemned people caught with cloned credit cards, and not debit cards which is seen as a problem given the number of this type of cards (Visa Electron) in the country.

In terms of trends, since the introduction of EMV cards, it is foreseen an increase on the usage of cloned Portuguese cards abroad, in countries where EMV is not yet fully deployed.

Towards a more secure environment

SIBS has on its website the precautions that citizens must have when using ATM or POS terminals, including, but not limited to, not losing the card from sight, do not repeat operations unless the terminal presents a message stating that the first try was unsuccessful and do not transmit the PIN to third parties. With this respect, the ATM terminal itself shows a message to the user to protect and hide the introduction of PIN from third parties.

The introduction of banknote ink/dye staining systems helped on preventing physical attacks to ATM machines, and awareness is being made to merchants that an inked banknote is a robbed banknote – up until now, only one case has been detected of an inked banknote being used at a merchant.

Given the mechanisms that are being implemented at the ATM machines, attackers are focusing on the doors at the lobby of the banks where ATM machines are located. Any card with a magnetic stripe opens the door, making the mechanism useless in regards to controlling access to the lobby, while introducing a new vulnerable point for skimming. A button to open the door, which provides the same level of control as the one that exists today, could eliminate this vulnerable point. While the

card is needed to access the lobby, people are advised to use a card to open the door, and a different one to make the transaction at the ATM machine.

Also, people are advised to use, whenever possible, the same ATM machine every time, in order to detect abnormal things (such as fake keyboards or card readers).

An increase of fraud levels at the virtual world is also foreseen. In order to tackle this issue, SIBS developed a system – MBNet – which allows for people to associate an MBNet account to a bank account, operation that can be performed at the bank. From here, when someone wants to pay for something online, it is possible to access MBNet website and generate a virtual visa card number, which has a limited amount of money available, and an expiration date due in one month.

References and sources for further reading

'ATM scam nets Melbourne thieves $ 500,000', 24 March 2009, available at *http://www.atmmarketplace.com/article.php?id=10808* (last visited on 20 April 2009).

'ATM scam targets hundreds of credit cards', New Europe, issue: 793, 4 August 2008, available at *http://www.neurope.eu/articles/89221.php* (last visited on 20 April 2009).

'ATMs on Staten Island rigged for identity theft; bandits steal $500G', 11 May 2009, available at *http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html#ixzz0J8qBVdar&D*

'Australian police suspect Romanian gang behind $ 1 million ATM scam', 14 April 2009, available at *http://www.atmmarketplace.com/article.php?id=10883* (last visited on 20 April 2009).

http://abcnews.go.com/Technology/Business/story?id=7434509&page=1

http://cert.inteco.es

http://garwarner.blogspot.com/2009/03/bank-hacking-exposed-analyzer-affadavit.html

http://www.adicae.net/

http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html

http://www.computerworld.com/securitytopics/security/story/0,10801,111158,00.html

http://www.denverpost.com/headlines/ci_12276447 (last visited on 5 May 2009).

http://www.europol.europa.eu/index.asp?page=news&news=pr090731_2.htm

http://www.mydigitallife.info/2006/09/25/atm-hacking-and-cracking-to-steal-money-with-atm-backdoor-default-master-password/

http://www.theregister.co.uk/2006/11/18/mp3_player_atm_hack/

http://www.wired.com/threatlevel/2009/04/pins/

https://www.european-atm-security.eu/Welcome%20to%20EAST/

Marks P., 'Cash machines hacked to spew out card details', *NewScientist magazine*, issue number 2713, available at *http://www.newscientist.com/article/mg20227135.700-cash-machines-hacked-to-spew-out-card-details.html?full=true* (last visited on 8 July 2009).

McGlasson L., 'ATM Fraud: 7 Growing Threats to Financial Institutions', *BankInfoSecurity*, available at *http://www.bankinfosecurity.com/articles.php?art_id=1523* (last visited on 9 June 2009).

Peretti K. K., 'Data Breaches: What The Underground World of "Carding" Reveals', *Santa Clara Computer & High Technology Law Journal*, volume 25, issue 2, available at *http://www.chtlj.org/volumes/v25* (last visited on 2 July 2009).

Reuters, '*Cyberthieves steal millions from banks*', May 2009, available at *http://uk.reuters.com/article/idUKTRE54I6CK20090520* (last visited on 20 May 2009).

Robinson G., 'Bondi banks scam: ATM alert', *The Sydney Morning Herald*, October 2008, available at *http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950* (last visited on 2 July 2009).

'Shoppers are targeted in ATM scam', *BBC News*, 11 March 2006, available at *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.stm* (last visited on 20 April 2009).

SIBS, 'Relatório e Contas 2008', *SIBS*, 2009, available at *http://www.sibs.pt/export/sites/sibs_publico/pt/documentos/relatorioecontas/Contas_SA_2008.pdf* (last visited on 5 May 2009).

Sydney Morning Herald, October 2008, available at *http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950*

Trustwave, *Automated Teller Machine (ATM) Malware Analysis Briefing*, 28 May 2009, available at *https://www.trustwave.com/pressReleases.php* (last visited on 13 July 2009).

VISA Business News, *Data Security Alert – Compromise of ATM PIN Transactions*, 3 June 2009.

Zetter K., 'ATM Vendor Halts Researcher's Talk on Vulnerability', *WIRED*, June 2009, available at *http://www.wired.com/threatlevel/2009/06/atm-vendor-halts-talk/* (last visited on 8 July 2009).

The ENISA Awareness Raising Community

August | 09

enisa
European Network and Information Security Agency

The ENISA Awareness Raising Community

August 2009

Contents

Executive summary

This paper presents the ENISA Awareness Raising (AR) Community that aims at sharing and analysing information security good practices across Europe.

The AR Community builds on a diverse range of skills and knowledge of information and communication technologies (ICTs) and differing interests and levels of expertise and priorities.

Shared awareness practices have been deemed critical to the success of the AR Community. Leveraging upon the AR Community members can greatly enhance the way awareness raising activities evolve within private and public organisations when it comes to information security.

The establishment of the AR Community marks the beginning of a deep engagement not only with sharing but also with analysis of information security good practices across Europe.

This paper presents basic facts and figures about the AR Community and its members.

The cut-off date for data used in this publication was August 2009.

The Awareness Raising Community: a success story

The Awareness Raising (AR) Community is a subscription-free community open to experts who have an interest in engaging in raising information security awareness within their organisations (see Figure 1). The AR Community was launched in February 2008 and is designed to engage with ENISA in its mission to foster a culture of information security.

Figure 1: Awareness Raising Community logo

As a point of contact for matters related to information security awareness, the AR Community has grown now to 46 nations, comprising 325 members. All European Union (EU) and European Economic Area (EEA) countries are represented. The AR Community welcomes membership applications from any European or non-European country.

Though members have a diverse range of skills and knowledge of ICTs, and differing interests and levels of expertise and priorities, they are united in helping the AR Community become the intellectual backbone of the exchange of information security good practices. Thus, the establishment of the AR Community marks the beginning of a deep engagement not only with sharing but also with analysis of information security good practices across Europe.

History

ENISA began building an AR Community in late 2006. To enhance the capacity of such a Community, promote knowledge sharing and dialogue within Member States and stakeholders, ENISA created a new way of coming together and sharing information. Monthly conference calls were organised from March 2007 and were joined by about twenty participants from eight European countries: Austria, Belgium, Germany, Ireland, Italy, Luxembourg, the Netherlands and the United Kingdom.

During 2007, following the positive feedback received by stakeholders and the common willingness to create a recognised and established information security awareness community, ENISA included the creation of such Community in the framework of the multi-thematic annual programme of the Agency.

Later in 2007, the work programme of ENISA was approved, thus laying the foundations of the AR Community.

Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Ireland, Italy, Malta, the Netherlands, Norway, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, the United States, and Vietnam joined in February 2008, followed by Egypt, Luxembourg, Morocco, New Zealand, and Turkey in April 2008, Australia, Latvia and Cyprus in May 2008, Lithuania and Poland in June 2008 and Bulgaria, Czech Republic and Sierra Leone in July 2008. From January to June 2009, the AR Community grew by 60% and got its first members from China, Canada, Malaysia and Mexico (see Figure 2).

Figure 2: AR Community worldwide

Membership growth

Most of the AR community's population growth is due to a common recognition of the importance of information security awareness.

Recent events have raised concerns, leading private and public organisations to understand that policies and technologies must be put in place to secure sensitive corporate information. These controls have to ensure the ability to secure information on the network as well as the opportunity to manage data which enter and leave the company. While policies and technology are certainly a critical part of any information security programme, these measures alone cannot deliver sufficient information security in practice. Awareness of the related risks and available safeguards is the first line of defence for security. Employees are the real perimeter of the organisation's network and their behaviour is a vital aspect of the total security picture.

Moreover, the good work of the AR Community members and its recognition has attracted considerable interest and attention of other experts.

As shown in Figure 3, the AR Community counts 325 members.

The AR Community covers five continents – Africa, Asia, Europe, North America and Oceania – and a large number of countries. The largest membership is from Europe.

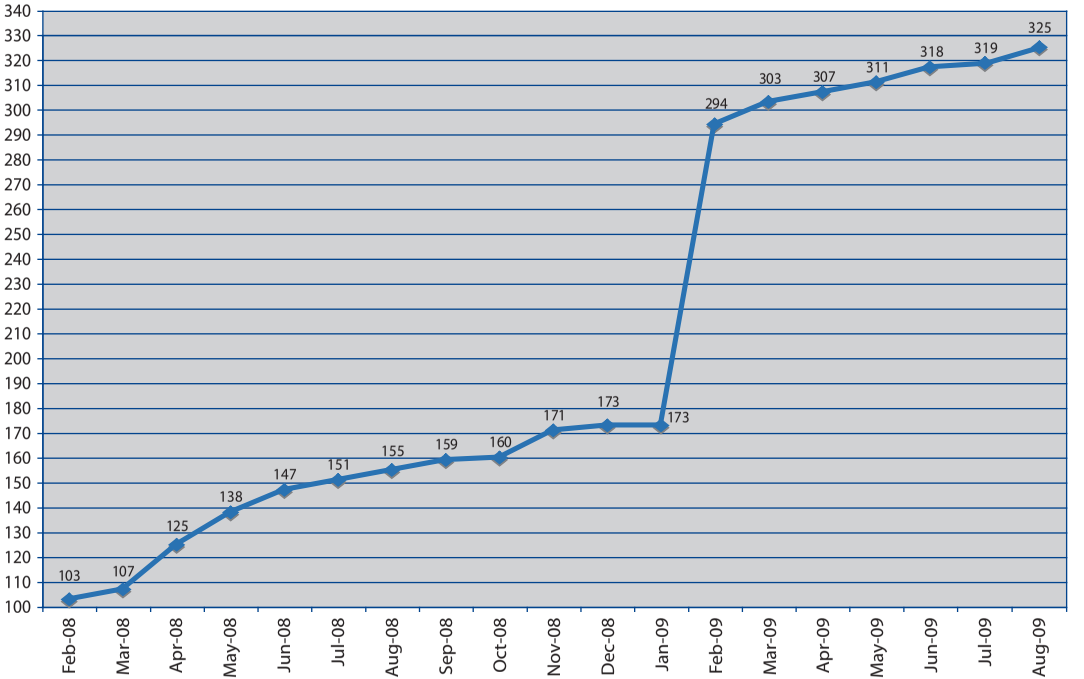


Figure 3: AR Community membership growth

Members at work

Though members have a diverse range of skills and knowledge of ICTs, and differing interests and levels of expertise and priorities, they are united in helping the AR Community become the intellectual backbone of the exchange of information security good practices. Members are a point of contact for matters related to information security awareness in general or related to their countries, industries, or areas of activity.

The AR Community's work increases through a combination of activities which show the continuous involvement of members of the Community. ARNews and a calendar of events are prepared using inputs received by experts and then distributed to Community members who wish to receive periodic correspondence. Along with this, the AR Community offers the chance to participate in presentations at events and to attend and contribute to monthly conference calls. The AR Community hold regular conference calls for sharing emerging good practices, discussing cutting-edge topics and key issues in the information security field.

Furthermore, the members contribute by participating in discussions and drafting white papers on specific security topics, taking part to virtual working groups (VWGs).

Achievements

In 2008 and 2009, some AR Community members participated in VWGs which enable the preparation of white papers on obtaining support and funding from senior management while planning an awareness programme, organising awareness programmes in financial organisations and ATM crime.

Obtaining support and funding from senior management

Gaining management support and sponsorship for the awareness programme was recognised as the most crucial aspect of the entire initiative. It is vital to build consensus amongst decision-makers that the awareness programme is important and worthy of funding. Even though many managers express their desire to support security initiatives, putting it into action is another story. This is the reason why ENISA addressed private organisations staff and decision-makers providing an introduction on the importance of gaining support and funding from senior management of companies. Moreover, it provided a valuable tool to take the first steps towards the preparation and implementation of an information security awareness initiative.

Figure 4: 'Obtaining support and funding from senior management while planning an awareness initiative'

The paper '*Obtaining support and funding from senior management*' (see Figure 4) seeks to raise awareness among senior management on the importance and criticality of endorsing information security awareness within an organisation ([1]).

([1]) ENISA, *Obtaining support and funding from senior management while planning an awareness initiative*, September 2008, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/obtaining_support_and_funding_from_senior_management.pdf*

How organising awareness raising programmes in financial organisations

A more in depth analysis was conducted for the financial services industry such as retails and wholesale banks, investment firms, insurance companies and so on.

Data security is a key risk for these organisations by the nature of their business. They are generally hold lots of personal and financial data and their safeguard is crucial responsibility for them.

A set of twenty recommendations were included in the paper '*Information security awareness in financial organisations*' (see Figure5) to provide a valuable tool to understand the importance of data loss for this industry sector and prepare awareness raising and training programmes ([2]).

Figure 5: 'Information security awareness in financial organisations'

([2]) ENISA, *Information security awareness in financial organisation*, November 2008, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf*

ATM crime: Overview of the European situation and golden rules to avoid it

The number of ATMs in Europe is raising every year. ATM's can increasingly be found in many remote site locations other than banks, such as convenience stores, airports, petrol stations, railway stations, department stores and so on. In 2008, with the rise in the number of ATMs in Europe there has also been a significant rise in the total number of reported ATM crimes. As a result, the ATM industry has placed the safety of users and protection against fraud as a high priority in order to help protect user's confidence in the system.

Figure 6: 'ATM crime: overview of the European situation and golden rules on how to avoid it'

A set of recommendations to raise user awareness about the different types of risks faced when using an ATM, along with advice on how to identify and counter them, were included in the paper '*ATM crime: overview of the European situation and golden rules on how to avoid it*' (see Figure 6) to provide a useful and necessary starting point to increase overall user awareness of the issues they face when using ATMs, both within the European Union and elsewhere in the world, of data security and industry good practices ([3]).

([3]) ENISA, *ATM crime: Overview of the European situation and golden rules on how to avoid it*, August 2009, available at *http://www.enisa.europa.eu/doc/pdf/publications/ATM_crime.pdf*

Conclusions

The AR Community was created with the aim of sharing and analysing information security good practices across Europe. Being a member of the AR Community gives the opportunity to create a point of contact between countries which can easily promote knowledge and share information security awareness.

To this end, ENISA makes efforts to enhance knowledge and to increase the number of its AR Community members, to positively influencing public behaviour towards information security and to provide any private and public organizations with the good practices and the key issues in the information security field.

References

ENISA, *Obtaining support and funding from senior management while planning an awareness initiative*, September 2008, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/obtaining_support_and_funding_from_senior_management.pdf*

ENISA, *Information security awareness in financial organisation*, November 2008, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf*

ENISA, *ATM crime: Overview of the European situation and golden rules on how to avoid it*, August 2009, available at *http://www.enisa.europa.eu/doc/pdf/publications/ATM_crime.pdf*

Information security awareness in financial organisations

Guidelines and case studies

September | 09

enisa
European Network and Information Security Agency

Information security awareness in financial organisations
Guidelines and case studies

IV

September 2009

Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways. The information includes contributions from members of the ENISA Virtual Working Group (VWG) on 'How to organise awareness raising programmes in financial organisations'. This VWG and its members are part of the ENISA Awareness Raising Community.

The initial publication drafted in 2008 was updated in 2009 with valuable insights from recognised players in the financial institutions arena.

ENISA wishes to acknowledge and thank Mr. Thomas Schlienger of TreeSolution Consulting GmbH, whose initial support and co-operation have influenced some prevailing aspects of this project, Ms. Kate Dodds of Sai Global, Mr. Mathieu Gorge of VigiTrust, Mr. Jorge Pinto of Banco Credibom, Mr. Thomas Schlienger, Ms. Paula Davis of Sai Global, Ms. Sissel Thomassen of InfoSecure, Mr. Stefan K. Burau of Clariden Leu, Mr. David Prendergast from AIB Group, Mr. Mark Logsdon from Barclays Bank and Mr. Jan Wessels from Rabobank for their prompt support, valuable input and material provided for the compilation of this paper.

Finally, the author would also like to acknowledge Ms. Colette Hanley of Betfair, Ms. Isabel Milu of Banco Credibom, Mr. Luke O'Connor of Zurich Financial Services and Ms. Tone Thingbø of Norges Bank who contributed to this document with reviews, valuable insights, observations and suggestions. The content would be incomplete and incorrect without their help.

Contents

Executive summary

This report targets decision-makers and staff involved in developing information security awareness programmes in financial organisations, a sector which is increasingly threatened by information security breaches. The average loss caused by theft of customer information is on the rise, as is the cost of responding to security incidents. Security breaches in financial organisations not only damage reputation but also cause heavy financial losses, which can be difficult to recover from.

According to the 2008 report of the UK Financial Services Authority (FSA), financial services firms could significantly improve their controls to prevent data loss or theft. Moreover, employees are now considered the single most likely cause of security incidents as confirmed by many international surveys including the 2007 Global State of Security and the 2008 BERR survey. Technical solutions are no longer the panacea that they might have been in the past. The effort to mitigate the security risks evolving around the human element is growing, and constitutes an important financial commitment for any organisation.

The objectives of this publication are to explain the importance of information security awareness in financial organisations, to analyse the environment and the business drivers which may impact such programmes, and to provide a communication framework to better organise an awareness initiative. Case studies and recommendations are given to help as a starting point for the awareness raising professionals and teams.

The first part of the report is an assessment of the environment of financial organisations and their main business drivers. In these environments, information security awareness must integrate with the ongoing information security and compliance requirements set by legal and industry mandates. It is extremely challenging to run information security awareness training initiatives and at the same time ensure business continuity and disaster recovery in such a demanding operational environment. This is because the flow of data, apart from requiring high levels of protection, cannot be stopped or reduced even for short periods of time in this type of business.

The paper then focuses on the landscape of international standards, fundamental legislation in place and certification objectives together with major risks, threats and end-user behaviour with regard to information security. Several parameters define the awareness strategy to be followed in addition to those mentioned above, such as audience segmentation, roles and job functions, geographical location, multiculturalism and so forth.

The second part covers the different phases of implementation of awareness raising programmes in financial organisations and the assessment of results. To ensure that information security awareness corresponds to the objectives of a financial institution, it should be a continuing and ever-evolving process. Factors to be taken into account in the planning, designing, implementation phases are presented in this chapter together with tools for measuring the success of awareness raising initiatives.

The third part includes practical advice, recommendations and case studies provided by a number of private organisations. It is worth noting that the paper was updated in 2009 after receiving valuable feedback and case studies of large national and international financial institutions.

ENISA hopes that this paper will provide financial organisations with a valuable tool to improve understanding of the importance of data loss and prepare and implement awareness raising and training programmes. Providing information security awareness is a huge challenge in itself for any company; awareness raising in this targeted industry sector is an important first step towards meeting that challenge.

PART 1: BUSINESS ENVIRONMENT AND MAIN DRIVERS

Introduction

Governments and regulators have attempted to address information security threats through the implementation of a range of legislation and regulation such as the Data Privacy laws, Computer Misuse laws, Sarbanes Oxley and so forth.

Failure to ensure the appropriate use and adequate protection of an organisation's information assets may well result in a breach of one or more of these requirements and may also result in adverse publicity relating to the misuse of information or resources - with an associated potential loss of consumer and shareholder confidence. Penalties are increasingly draconian and varied in form; for example SOX fines can be up to $15m with accompanying actions against company officers and Basel II has the potential to result in increased capital adequacy requirements with costly implications for profitability.

Most security risks are driven in practice by the lack of a well-defined and managed information security culture, with errors and breaches frequently caused by human error and a failure to follow procedure. The UK Department for Business, Enterprise and Regulatory Reform (BERR) reported in their 2008 Information Security Breaches Survey that 47% of UK large businesses suffered from staff misuse of information systems ([1]).

Metrics in themselves are compelling - the average loss from theft of proprietary information is on the increase as is the cost of responding to security incidents. The 2008 BERR survey reported that 77% of UK businesses spent their information security budget on protecting customer information and 72% on maintaining information integrity. The average

([1]) BERR, 2008 Information Security Breaches Survey, 2008, available at *http://www.security-survey.gov.uk* (last visited on 22 July 2008).

total cost of a UK company's worst incident is between £ 10,000 and £ 20,000, with direct financial loss (such as loss of assets, fines etc.) between £ 500 and £ 1,000.

In 2007 the Financial Crime and Intelligence Division (FCID) of the Financial Services Authority in the UK handled 187 financial crime cases, of which 56 involved data loss. Due to the nature of their business, mismanagement of data security could constitute a significant risk to financial organisations They generally hold large volumes of personal and financial data about their customers, such as names, addresses, dates of birth, bank account details, transaction records, PINs, national insurance numbers and so on ([2]). Safeguarding this personal and financial data is a key responsibility of the financial services industry.

Additional technology alone will not solve these issues; a more holistic approach is needed that incorporates behaviour and culture, as well as technology. While policies and technical controls are certainly a critical part of any information security (IS) programme, these measures alone cannot deliver sufficient assurance that information is protected in practice. In order to be effective, information security awareness programmes are reliant on the actions of individuals within the organisation. Employees are, of course, the real perimeter of the organisation's network and their behaviour is a vital aspect of the total security picture.

Research and analysis conducted by ENISA suggest that effective employee awareness, where employees not only understand their obligations but routinely act upon them, is one of the most effective ways of managing the information security risk faced by any large organisation today.

Purpose

ENISA considers the poor state of data security as a serious and widespread issue. It recognises that effective employee awareness for man-

([2]) Financial Services Authority, Data Security in Financial Services, United Kingdom, April 2008.

aging information security risks is crucial, especially within financial organisations. This white paper aims to provide an introduction to the importance of information security in this specific industry sector. It also aims to provide valuable tips on preparing and implementing information security awareness initiative.

The document is structured in three parts covering the following issues:

- ✓ Assessment of the financial organisations environment and main business drivers.
- ✓ Awareness raising programmes in financial organisations.
- ✓ Practical advice in the form of recommendations and case studies provided by a number of private organisations and models.

Objectives

The objectives of this publication are for ENISA to:

- ✓ Explain the importance of information security awareness in financial organisations.
- ✓ Analyse the environment and the business drivers which may impact such programmes.
- ✓ Present case studies and recommendations to be used as starting points by the awareness raising team.
- ✓ Contribute to the development of an information security culture and promote knowledge sharing between Member States.

Audiences

This white paper is for use by staff and decision-makers in financial organisations, when undertaking information security awareness raising programmes. It also seeks to raise awareness of the importance and criticality of endorsing information security awareness within their organisation.

Background

The Awareness Raising (AR) Community is a subscription-free community open to experts who have an interest in raising information security awareness within their organisations. The AR Community was launched in February 2008 and is designed to engage with the Awareness Raising Section of ENISA in its mission to foster a culture of information security — with the aim of supporting the Section in its activities.

Contributors to this paper offer a diverse range of skills, and knowledge, as well as differing interests, a range of areas of expertise and a variety of business priorities. Their combined analysis allows the AR Community to play a key role in the exchange of information security good practice across Europe.

Being a point of contact for matters related to information security awareness, the AR Community invited members to take part in Virtual Working Groups (VWG) to explore in further detail relevant topics aiming at producing white papers.

This paper relies on studies and analyses conducted by the ENISA VWG 'How to organise awareness raising programmes in financial organisations', ENISA staff and through information that is publicly available or has been supplied to ENISA by appropriate organisations.

Financial organisations: a definition

This paper targets financial organisations, in particular decision-makers and staff involved in developing information security awareness programmes, to ensure the ability to secure data and to assess related risks as well as to plan effective training and awareness initiatives in order to prevent information security breaches and incidents.

We refer to financial organisations in a generic way to indicate retail and wholesale banks, investment firms, insurance companies (life and gen-

eral), financial advisers, credit unions and payment service providers of any size.

Assessment of environment and main drivers

An introduction

There has been much talk of information security incidents and data breaches in financial organisations in the last year. Of course, most of us will have focused our discussion on the banks as they are the centrepiece of the financial world. However it is worth noting that due to the current regulatory climate, all financial organisations are currently reviewing their approach towards information security and especially towards security education for staff at all levels of seniority. This phenomenon includes credit card associations, merchants from the retail industry, payment service providers as well as insurance organisations.

These actors of the financial world are subject to multiple legal and industry frameworks regulating how they should educate staff on dealing with information and how to protect sensitive information. Whilst some frameworks offer clear guidelines as to why, how and how often information security education must take place, others remain vague. Financial organisations must all consider the following important questions:

- ✓ What legal and industry frameworks apply to my financial organisation and to our way of doing business?
- ✓ Does our current information security strategy allow the organisation to take a pro-active approach towards security in order to meet compliance requirements as well as industry security mandates?

- ✓ How do our information security awareness programmes and staff education initiatives compare with the demands of financial industry best practices?
- ✓ Is information security awareness approved and fully endorsed by senior management?
- ✓ Has information security awareness been positioned as a business enabler and, if not, how can my organisation turn information security awareness initiatives from a cost centre to a return on investment and productivity enhancement tool?

The challenge for financial organisations, however, is firstly to plan for IS awareness raising activities and to then deliver awareness programmes. This is due to the nature of their business. Staff are continuously engaged in guaranteeing data flows all the time as downtime cannot be afforded. The recent example of the London Stock Exchange being unable to function for an unprecedented period of time shows just how IT system failures can affect daily work. A way of dealing with this challenge is to extend existing generic induction and training programmes to include information security awareness. Information security awareness must, nevertheless, be part of an ongoing security and compliance process: education first, then remediation and, where applicable, official accreditation/compliance and, finally, accreditation maintenance through ongoing information security awareness initiatives. Maintaining this iterative process is very important for financial markets as they are fundamental to the world's critical infrastructure (CI) and therefore much scrutinised by consumers, businesses and Governments.

The financial industry is typically governed by two types of mandates: legal mandates and industry frameworks. Whilst there is some level of convergence between both elements, such that compliance with industry guidelines may become a legal requirement, most financial legal frameworks are independent of industry frameworks that regulate the design, development and implementation of information security awareness initiatives in financial institutions. Notwithstanding this aspect, one should however note that in the last five years, the industry has clearly seen common objectives between legal and industry frameworks emerge with regard to information security for financial institutions. This is due to the fact that the

number of identity theft incidents has soared and major breaches have occurred primarily in the UK and in the US. This is relevant as these two countries are the key global financial centres and have, as a consequence, been leading the way in developing legislation and regulation to tackle these problems. In addition, the requirement to notify security breaches has been imposed in many jurisdictions worldwide and is becoming the norm across the globe. For instance, the concept of Senate Bill 1386 in California (SB 1386), which details when and how consumers, authorities and the media need to be notified of data breaches, was used as a model for similar state legislation in the US where over 40 states now have notification laws. A number of countries in the EU, including the UK and Ireland, are exploring similar avenues. This is important to note because if notification of security breaches becomes a legal requirement, then more efforts are likely to be accorded to preventing breaches in the first place. This also means that all staff within financial institutions will need to become all the more aware of information security threats and will require formal education in the risks associated with processing financial data.

Review of business drivers

The main driver for compliance with legislation and industry mandate is the fear of penalties and prosecution for failure to comply (which may involve civil or criminal law suits). Whilst there is rarely any direct financial or legal ('safe harbour' type) rewards for compliance, it can result in reduced insurance costs in some cases.

Fundamentally, with regard to awareness requirements, financial organisations should be familiar with compliance and governance mandates and security frameworks in order to understand which apply to them globally or nationally and which impact the whole financial industry. The main business drivers revolve around demonstrating good governance

and compliance whilst actually increasing information security both for the financial institution itself and for its customers and suppliers. In other words, the financial organisations' ecosystem makes all of its actors interdependent and there are clear links between those responsible for promoting standards and those who must implement the standards down the chain, for example with Payment Card Industry Data Security Standard (PCI DSS) requirements. By complying with legal and industry mandates, we are making use of industry frameworks to protect sensitive data and ensure continuity of operations within this ecosystem. Technically, this is achieved by focusing on reducing legal exposure, protecting public relations and the reputation of the brand by protecting consumer financial assets and the identity of each individual customer. The Payment Card Industry Data Security Standard (PCI DSS) is probably one of very few security standards which actually dedicate a full control objective to information security awareness training (requirement 12.6). It includes requirements for information security awareness programmes and touches on multiple layers of the financial organisations industry from the card associations to other entities such as the acquiring banks, payment service providers, merchants and any third party in this chain which might store, process and transmit credit card information. As such, compliance to the requirements of PCI DSS will be expected from most high street retailers as well as any corner shop able to take credit card payment. The standard applies to all entities worldwide. It consists of 12 high-level requirements each associated with a set of policy, procedure, technical controls and skills transfer requirements. Requirement 12.6 states that an entity 'needs to implement a formal security awareness programme, and educate employees upon hire at least once annually on the importance of cardholder data security'. It also covers how compliance with the rule is to be checked for the most stringent level of PCI DSS (level 1) which requires an annual on-site audit to be performed by Qualified Security Assessors (QSAs). An entity 'needs to be able to demonstrate through training records that all staff in scope have been trained. In addition, you need to be able to produce the security awareness material and show that it has been updated on a regular basis to reflect changes in your own cardholder data environment as well as new requirements within the standard'. From a more holistic perspective, all entities are responsible for raising awareness levels of those downstream

in the PCI chain, such that acquiring banks are responsible for promoting the standard to all of its merchants which in itself requires a security awareness raising project.

ISO/IEC 27001, the international standard for information security originating from BS7799, and complemented by ISO/IEC 27002 and 27005, is also gaining traction and includes a provision for information security awareness programmes. Although the ISO/IEC 27001 framework can be applied to any organisation, it is not unusual to see financial organisations it as a benchmark for good information security practices with a view to complying with a wide range of legal and regularly frameworks, including PCI DSS (note: the UK Post Office delivered a presentation at a recent PCI DSS seminar stating how they used ISO/IEC 27001 as the basis for PCI DSS Compliance since implementing an information management system (ISMS) will go some way to cover a large number of PCI DSS compliance requirements).

At a more fundamental level, whilst some of the newer members are still refining their data protection and retention regimes, the European Directive on Data Protection of 1995 has been adopted in most EU countries. Whether you consider for example the Irish Data Protection Act, the UK Data Protection Act, the Portuguese Data Protection Law, the German Datenschutzgesetz or the French Act's, Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, most European legal frameworks governing data protection include clauses whereby organisations are required to 'take appropriate security measures to safeguard the good name of the company, its employees, affiliates and customers' and insists on protecting 'key data including any financial information' it may hold ([3]). The means recommended for achieving that goal is security awareness programmes.

([3]) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995. Also in the Irish Data Protection (Amendment) Act 2003, Article 2 '(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity', available at *http://www.dataprotection.ie/documents/legal/act2003.pdf*.

In Ireland, this has been very well communicated by the Office of the Data Protection Commissioner. A number of banks and insurance organisations have registered with the Office and developed security awareness programmes for staff and even for their customers, the end-consumers. Some banks, such as Ulster Bank, have rolled out basic education programmes for their merchants to help them with PCI compliance whilst others are actively engaging with employees in a bid to raise security awareness levels.

Traditionally, financial institutions have always tended to be ahead of the game with regard to information security awareness programmes, along with some government institutions, the IT and pharmaceutical sectors. However, initiatives have remained focused around ad hoc training seminars dealing with fraud and identity theft or on social engineering. This type of effort is no longer sufficient (if it ever was) to meet legal and industry mandates or to reassure consumers. Consumers expect that their financial information is kept safe as a matter of fact and that their financial assets are protected even in the event of a network information security breach suffered by the bank. In other words, whilst consumers may not fully understand the ramifications and demands of putting in place security strategies, controls and safeguards, they still expect financial institutions to protect the money they have entrusted to them. This is called trust.

Financial institutions have to provide a controlled and secure environment for consumers. However there are noticeable regional and industry variations in the way legal and industry frameworks mandating information security awareness training are applied to the target 'markets' of a given financial institution. This is often a major challenge for large international financial organisations who must understand the local regional legal mandates in order to incorporate them into a wider corporate information security awareness strategy which will allow them to ensure that

internal corporate security standards are met whilst compliant with national and country-specific legal requirements.

Best practice to develop such an awareness strategy within financial organisations usually involves several steps:

- ✓ Step1 – Categorise the business into country/zones subject to similar legislations and industry frameworks in order to make the project more manageable.
- ✓ Step 2 – Identify data protection and data retention frameworks applying to each category.
- ✓ Step 3 – Define a full specification for information security awareness mandates for each category.
- ✓ Step 4 – Perform a gap analysis against existing awareness programmes and update programmes to address legal/industry mandates.
- ✓ Step 5 – Deliver updated programme to all categories.
- ✓ Step 6 – Make steps 1 to 5 an ongoing process subject to annual reviews (at least).

The development of such strategies and programmes take it as given that an Acceptable Usage Policy for corporate communications tools is in place and that a data classification schema has also been approved by the board governing what constitutes confidential, sensitive and public data for the financial organisation.

Most financial institutions will include key topics in their programmes: protection of personal data, details of monitoring techniques used by the organisation (which is a requirement under the EU Data Protection Directive), and guidelines for data transfer (such as from EU to US). Attention may also be given to notification mechanisms whereby notification for incidents taking place in the US will be mandatory and notification in the EU will be internal to the security team first. The team will then work with the local data protection enforcers to ensure they notify when required.

Financial organisations are also typically good at measuring success rates of information security awareness programmes. They tend to use matrix-based measurements which include reach (has the organisation reached

out to all its staff across all territories?), understanding (has the target audience fully understood what is required of them, why and how to improve security?) as well as behavioural change (ensuring that bad security habits are no longer in use and that all staff are fully security aware).

It is also worth considering the fact that most large financial organisations are in a position to take a holistic approach towards information security awareness. Senior decision makers who must become involved in this process remain the prime point of contact/target for government and industry frameworks enforcers and as such will want to foster a culture of information security using the measurable and long term vision for information security awareness described above. This means that they will be looking to ensure that the programmes are sustainable (i.e. a long term programme that will evolve as the financial organisation's business model may change and reflect on emerging threats as well as new legal and industry mandates), consistent (always and fairly applied to all staff regardless of seniority or rank), efficient (measured for effectiveness and improved on an ongoing basis) and transparent (fully communicated to all staff including penalties for non compliance with information security requirements as detailed in the awareness programme).

Focus on the US – Latest news in Awareness Raising Requirements: ID Theft Red Flags Rules

This new requirement for US financial institutions is coming into effect on 1 November 2008. It is worth noting that it demands that banking institutions strengthen, document and implement new awareness programmes for employees and customers alike. Training, including that of board members, is a major part of achieving this compliance.

The Red Flags Rule is part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. Under this rule, financial institutions and creditors with covered accounts must have identified theft preven-

tion programmes in place by 1 November 2008, in order to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft ([4]). Banking regulatory agencies are working with their institutions to ensure compliance. Meanwhile, the Federal Trade Commission oversees compliance by the rest of the covered entities identified as creditors.

The State of Banking Information Security 2008 – Survey executive overview

According to the 2008 State of Banking Information Security survey, customer education remains insufficient ([5]). The survey argues that 'To secure this trust, they must demonstrate proactive efforts to educate customers about online banking safety and the risks of identity theft – including phishing, which occurs via email and telephones outside of the institutions, but still can cause untold damage and erode customer confidence'.

This shows that education and awareness raising for financial organisations needs to be carried out internally as well as externally to foster a platform of trust and allow for compliance and governance mandates to be adhered to on a pro-active basis.

Financial organisations' concerns

Following the research and analysis conducted by ENISA it was possible to identify some of the major corporate concerns relating to data security.

- ✓ Market confidence: maintaining confidence in the financial system ([6]).

([4]) See McGlasson, Linda, 'ID Theft Red Flags Rule: How to Help Your Business Customers Comply', BankInfoSecurity.com, 8 September, 2008 *http://www.bankinfosecurity.com/articles.php?art_id=960andrf=090908eb*

([5]) See 'The State of Banking Information Security 2008 - Survey Executive Overview', BankInfoSecurity.com, available at *http://www.bankinfosecurity.com/whitepapers.php?wp_id=143* (last visited 20 November 2008).

([6]) Financial Services Authority, Data Security in Financial Services, United Kingdom, April 2008.

- ✓ Consumer protection and awareness: data loss could have a significant impact on individuals.
- ✓ Data leakage: to limit data leakage, organisations could, for example, establish information security policies and regulate the use of mobile devices.
- ✓ Lost data and support costs: an information security policy could help financial organisations recuperate stolen or lost data, which can occur even when security measures are in place, decreasing the costs of ownership and support.
- ✓ Challenges of complying with regulatory and security standards: having enterprises take care of data security will help in complying with the three aspects of information security (confidentiality, availability and integrity) and some security standards and/or compliance framework (such as ISO/IEC 27001, PCI DDS and so forth).
- ✓ Reduction of financial crime.

Risks and threats

Given the structure of financial organisations, the procedures they are required to follow, the frequent use of third parties to provide specialised services (for sending bulk mailings, providing IT services and so forth) and the ability to access, store and transmit sensitive information quickly, easily and efficiently, the number of possible risks and threats is almost infinite. The following can be identified.

- ✓ Data leakage ([7]): it is not possible to estimate the effects of valuable data leaking out of an organisation, but the problem is growing.

([7]) Heiser, Jay, Understanding data leakage, Gartner, 21 August 2007; 'Data-leak security proves to be too hard to use', Infoworld.com, available at *http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html* (last visited on 2 June 2008).

- ✓ Information loss: it is most likely when sensitive information (for instance customer and/or employee data) falls into the wrong hands, it is kept and eventually re-used for personal use, even when marked as confidential. This can possibly result in legal liability.
- ✓ Information confidentiality: when information falls into the wrong hands, the financial institution suffers a much greater loss than simply the replacement of the cost of, for example, the drive the information was stored on.
- ✓ Information integrity: when content is modified.
- ✓ Corruption of data: when unintentional changes are made to data
- ✓ Data security: smuggling information out of the business. There is a risk that the data will be used or sold for criminal purposes.
- ✓ Damage to company business/reputation/image: when data is stolen the resulting publicity can be extremely damaging to the reputation of the company and therefore negatively impact business.
- ✓ Market leadership loss.
- ✓ Malware: when malicious software code is introduced to the network, being a virus, worms, spyware or trojans.
- ✓ Fraud/deception:
  - Extortion.
  - Identity theft: for example in the UK, a laptop with data of some 2,000 people with individual savings accounts (ISAs) was stolen from a HM Revenue & Customs employee; HM Revenue & Customs lost personal details of 6,500 private pension holders; nine NHS trusts lost patient records kept on disk ([8]).
  - Theft of intellectual property, trade secrets, proprietary information.
- ✓ Money laundering.
- ✓ Market abuse.

([8]) ENISA, *Secure USB Flash Drives*, 2008, available at *http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf*

Audience segmentation: a definition

A large part of the planning of a training and awareness campaign in an organisation is to ensure that the programme is delivered efficiently and effectively and that the content is easily understood. It must be in a format everybody can understand.

A corporate programme may be difficult to apply across an organisation where the message may have to be changed to fit the country's culture, laws and regulations. Local customisations are often required for any corporate message however the programme must be delivered in the recognised company style to have the same look and feel.

- ✓ What is already in place across the corporation/locally?
- ✓ What other initiatives are in place (link in with current initiative)?

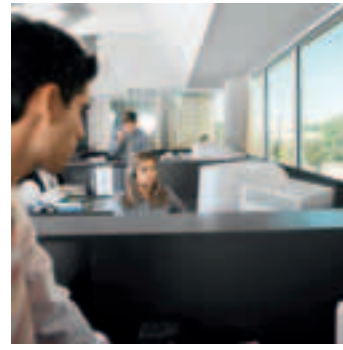
Job functions

Staff need to be divided into target groups depending on job function. Each target group will have different requirements for training and awareness. Applicable content needs to be arranged in modules and delivered efficiently. Their availability and place of work (i.e. mobile workers, home workers and so on) must be considered when defining the content.

To allow a targeted training programme, it is necessary to group people into different job functions/target groups and define the business risks for the different target groups to enable appropriate training.

To prevent wasted time and frustration, it is important that an awareness initiative is targeted and only applicable training should be provided. By delivering applicable training in the correct format, an organisation will have motivated their staff by providing them with a relevant message

and will prevent unnecessary use of time and funds by avoiding hours of inappropriate training.



Because information security is a pervasive issue, different groups of employees have different needs of education. Besides regular awareness for employees in general which should include, among other topics, proper usage of organisation resources, alert procedures, business continuity responsibilities, compliance and ethics issues, the following specific groups are a small example of the different types of training that can exist:

- ✓ Employees with access to internal client information in direct or indirect contact with the public, such as call centre employees and tellers, should have access to information regarding issues like social engineering and privacy regulations due to the fact these employees have access to client information and could unwillingly provide it to unauthorised parties.
- ✓ Employees with access to internal business information in contact with the public like salespeople and account managers should be made aware of the need for information confidentiality regarding internal business processes, partnerships and control mechanisms within the company that directly or indirectly affect the strategy of the organisation.
- ✓ IT staff should have training that include the regulations the company is subjected to, internal control and auditing mechanisms in place as well as the organisation strategy regarding best practices for computer and network security management.
- ✓ C-Level staff (CEO, CFO and so forth) are in charge of the organisation and are, ultimately, responsible for it, so a specific training/awareness programme should be developed in order to identify and maintain awareness in respect to existing regulations and how they can affect the organisation (in both a positive or negative way).

When designing an awareness programme, it is imperative that all the roles are clearly defined and match them to information security topics. The tables below provide a list of roles and related description and a sample of a model with the roles down the left-hand side and across the top the information security topics that they may need to be aware of:

Figure 1: List of roles and related description. Illustrative only.

Role	Description
Senior Executives	Need to be aware of information governance issues as well as the legal frameworks, risks and liabilities (including personal liabilities). They are typically time-poor and unwilling to undertake the same awareness activities as the general population. Short and much focussed awareness activities are best with clear links between information security and the protection of the organisation's reputation.
Clerical and administrative staff in back office and support functions	These employees often work to strict transaction processing schedules and targets. Careful consideration may need to be given to the organisation and scheduling of training in these areas. It is be important to liaise with managers regarding the scheduling of training and facilitated group training sessions may not be appropriate as there would be too big an impact on 'business as usual'. Most staff in these areas do not work outside of the office and do not make extensive use of portable devices. This narrows the range of information security topics that need to be covered and, therefore, reduces the duration of the overall training requirement.
Call centre staff	As with clerical and administrative staff, the scheduling of training is likely to be critical in a call centre environment where prompt response to customer calls is of prime importance. Again, liaison with call centre management will be important. Again, most staff in these areas don't work outside of the office and do not make extensive use of portable devices thus reducing the scope of the training requirement. Data protection and confidentiality, as well as awareness of social engineering is, however, likely to be vital.

Role	Description
Branch staff for retail financial services	Many employees in branches do not have access to their own dedicated workstation and in some retail banks tellers do not even have intranet access. Access to technology-based training is often via shared PCs or managers' PCs and, therefore, requires careful scheduling in order to maintain service levels whilst achieving training objectives. In retail banking, it is also common for more geographically remote branches to have limited bandwidth and challenges accessing the corporate intranet – consideration may, therefore need to be given to optimising delivery of web-based training for this environment.
Sales staff and remote workers	These employees are likely to access the corporate intranet remotely from portable computing devices. They have some particular training needs over and above those in the general population including: ✓ Information security out of the office (security of mobile devices and so on) ✓ Remote access procedures ✓ Travel Security.
Investment banking	Investment banks tend to have performance and compensation-orientated cultures. Presenting the rationale for the training is critical in this group. It is also important to ensure that the training is of the minimum duration possible, that it can be studied in manageable chunks and that the training can be bookmarked so that learners can return to the point where they left the training without needing to repeat any content. Senior management sponsorship from within the business unit is typically critical for the success of an information security training programme within this audience group.

>>>

Role	Description
Marketing	Marketing personnel are in charge of public relationships as well as the institution image. They need to know what types of information they can and cannot use whether it's preparing a campaign or interfacing with media in case of an incident.
IT Staff	IT staff should be made aware of the organisation security strategy and what types of controls are mandatory as well as what type of evidences need to be generated in order to insure compliance.

Some of the information security topics mentioned below may vary for each role depending on the policies of the financial organisation. A bank may permit home working for certain clerical staff, for example. Thus there could be variations in policy that would change the awareness required by that role.

Also, certain topics may be broken down into subsections ('handling customer data' is an important subset of handling sensitive information and may be worthy of its own section) or topics may intersect with other topics ('equipment security' would be present in 'mobile working' awareness, for instance).

Figure 2: Roles match to security topics. Illustrative only.

	Senior Executives	Clerical & administrative staff in back office and support functions	Call centre staff	Branch staff for retail financial services	Sales staff & remote workers	Investment banking	Marketing	IT Staff
Physical security	✓	✓	✓				✓	✓
Workplace security (for example office, branch and so forth)	✓	✓	✓	✓		✓	✓	✓
Equipment security	✓				✓	✓	✓	✓
Internal controls	✓	✓	✓	✓	✓	✓	✓	✓
Recognising & reporting security breaches	✓	✓	✓	✓	✓	✓	✓	✓
Privacy							✓	
Business continuity	✓	✓	✓	✓	✓	✓	✓	✓
Mandatory regulations						✓		
Data protection & privacy	✓							
Retention, storage & disposal of sensitive information	✓	✓	✓	✓	✓	✓	✓	✓

>>>

	Senior Executives	Clerical & administrative staff in back office and support functions	Call centre staff	Branch staff for retail financial services	Sales staff & remote workers	Investment banking	Marketing	IT Staff
Handling customer data		✓	✓	✓	✓	✓	✓	✓
Portal devices	✓				✓	✓	✓	✓
Removable media	✓			✓	✓	✓	✓	✓
Software (licensing)	✓	✓		✓	✓	✓	✓	
Passwords	✓	✓	✓	✓	✓	✓	✓	✓
Back ups	✓	✓		✓	✓	✓	✓	✓
Malicious code	✓	✓			✓	✓	✓	✓
Mobile & home working	✓				✓	✓	✓	✓
Use of Internet & Email	✓	✓		✓	✓	✓	✓	✓
Third parties (i.e. vendors & visitors)	✓					✓		
Social engineering	✓	✓	✓	✓	✓	✓	✓	✓

Geographical location

Implementing an information security awareness programme for staff in different geographical locations is challenging with regard to both the content and the method of delivery. The key challenge is to deliver the training across the organisation and ensure that it is in a format that is recognised and accepted by the different audiences consistently. The following should be taken into consideration:

- ✓ IT Systems/methods for delivering awareness training: in organisations that are spread over a wide geographical area where a common approach is not possible, various alternatives for delivering awareness training are considered. Different parts of the world have limitations due to the available infrastructure. Where e-learning or computer-based training (CBT) training is the preferred method, it is important to identify existing limitations before planning the design of a central or distributed solution. Undertaking a pilot implementation often will ensure that the programme can support the different system requirements and will prevent delays in the implementation process. Key system tests need to be included for:
  - Network bandwidth.
  - Web server limitations.
  - End user systems limitations (audio/video etc).
  - Different Intranet styles.
- ✓ Laws and regulations/legislations vary in each country: data protections/privacy laws vary between different jurisdictions and the following must be considered ahead of producing content in an awareness programme:
  - Ensure that content complies with local laws and regulations.
  - Use local partners and specialists for content where may be insufficient internal knowledge.
  - Customise parts of the programme to cater for local laws and regulations and legislation.
- ✓ Organisational structure
  - Complicated reporting lines: each part of the organisation may have different or unclear reporting lines. Therefore, senior management support is an absolute necessity in every implementa-

tion of information security awareness initiatives. In this regard, the project needs to consider:
- Who to engage with.
- Management support.
- Funding.
- Planning.
- Development/customisations.
- Delivery/roll-out.
- Evaluation.

✓ Head Office initiating the awareness campaign: most implementations of awareness programmes have been initiated by the organisation's Head Office with varying degrees of global acceptance. It's important to gain senior management acceptance in each country/region thus ensuring a successful adoption of the programme throughout the organisation. Equally, this approach will ensure that, local requirements are identified at an early stage and programmes customised accordingly.

Mergers and acquisitions

The awareness programme must be constructed to meet the challenges associated with acquisitions and mergers. Programme design must be modular to prevent having to change large portions of content while exploiting opportunities to improve the programme overall. The following should be taken into consideration:

✓ Different company cultures: the company may have a variety of cultures and the content may have to be adapted slightly to cater for new requirements.
✓ New companies/other processes/other business risks: the risk profile may change because of business merger, and parts of the awareness content may need to be changed or amended.
✓ Company profile: intranet style and logos may change. The awareness programme must be sufficiently flexible to adapt content to the new company profile.
✓ Management: the awareness programme must be acceptable to new senior and line management. It is, therefore, important that a mes-

sage from the board accompanies the programme showing senior management commitment and stakeholder commitment to it.

Multicultural environment

Implementation of an information security training and awareness programme in a multicultural environment is a major challenge both between organisations and also internally within each organisation. The differences are on more than one level and the fundamental issue is to recognise them and deal sympathetically with each one, while retaining the integrity of the whole.

Cultural differences within an organisation must also be taken into account during the planning phase. Parts of the organisation may have different organisational cultures, especially where companies have inherited processes and systems as a part of a merger. The following should be taken into consideration:

- ✓ Cultural issues.
- ✓ Gender issues.
- ✓ Religious issues.
- ✓ Racial issues.
- ✓ Attitude to humour (verbal and non-verbal).

Media channels/Method of delivery

The media channels and method of delivery, as well as the message and its sender, must be influential and credible. Otherwise the target group may be less inclined to listen. To engage the audience successfully, more than one communication channel must be used.

The following section details some of the main media channels and method of delivery available to help raise users' awareness as part of an

information security related initiative. Moreover, it suggests using a blend of approaches:

- ✓ Targeted modular training: see Audience segmentation above. It is important that the awareness programme is built up using individual modules. This will allow appropriate training to different target groups, at the same time as some of the content can be re-used in different programmes.
- ✓ Use of workshop/e-learning: experiences with implementations show that the best approach for encouraging discussion, and subsequent adoption of the learning in the operational environment, is to run departmental workshops so that the content of the awareness programme can, under the line managers' control, form part of a departmental work plan developed during workshop. This way the employees will have the opportunity to discuss the local business risks and related awareness content with one another and the line manager at their work place.
  Use of e-learning has proven to be more effective where staff are physically located in different areas and where e-learning is already in use within the organisation. The e-learning version should support the workshop awareness programme using the same content to ensure all employees throughout the organisation have a consistent level of information security awareness training. E-learning has also proven to be effective where specific training is required for defined target groups.
- ✓ Use of different content: using a combination of film clips, right/wrong scenarios, learning material, games and self-test questions, has proven to be successful in delivering information security awareness training. Showing film clips of incidents helps people to associate rules with the more practical elements of their jobs. Where a lighter approach and format is offered, people feel more relaxed and will not need a lot of additional learning material in order to understand business risks, how to deal with incidents that happen and, more importantly, how incidents can be prevented from happening in the first place.
- ✓ Awareness vs. Training: Awareness is defined in NIST Special Publication 800-16 as follows: 'Awareness is not training. The purpose of awareness presentations is simply to focus attention on security and understand why security is important. Awareness presentations are intended to allow individuals to recognise IT security concerns and re-

spond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance' ([9]).

Investment bank - to change behaviours, training needs to be interactive

An investment bank explained that its primary objective is to achieve regulatory compliance in a cost-effective way.
This is not possible without the creation of clear policies that set out what individuals should and should not do. Without this foundation, enforcement and discipline become hard if things break down. The bank has, as far as possible, included information security points in existing policies and training, rather than creating new ones.
Policies themselves are not effective unless staff understand them. The bank's security team gives induction presentations to all new joiners that explain the bank's security policies. This face-to-face contact gives staff an opportunity to discuss possible issues with the security team. Feedback from the training shows that interaction is critical to challenging people's attitudes and helping them learn. If people are asking questions, they are thinking and considering the information. A room full of silent people is unlikely to be learning much. Sharing war stories and relevant experiences helps staff see how security threats might affect them.
The bank has found that induction training alone is not enough. It is important that staff receive frequent reminders that reinforce key messages in a coherent way. Critical to this reinforcement has been getting senior management to lead by example; they, rather

([9]) NIST, Information technology security training requirements: A role- and performance-based model, NIST — SP 800-16, USA, 1998, available at *http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf* (last visited on 21 July 2008).

than the security team, are the best people to promote the importance of the messages.

The security team uses a variety of techniques to reinforce awareness messages on an ongoing basis. Quizzes and prizes get a good response level from staff; they get people thinking, and are well received within the business. Again, interaction with staff is vital. For example, posters that are passive reminders and ultimately require no individual action are often ignored in practice. Intranet articles and sites are good ways to promote messages to those that already actively use them. However, for people who do not visit them (the majority of staff), they are not an effective mechanism.

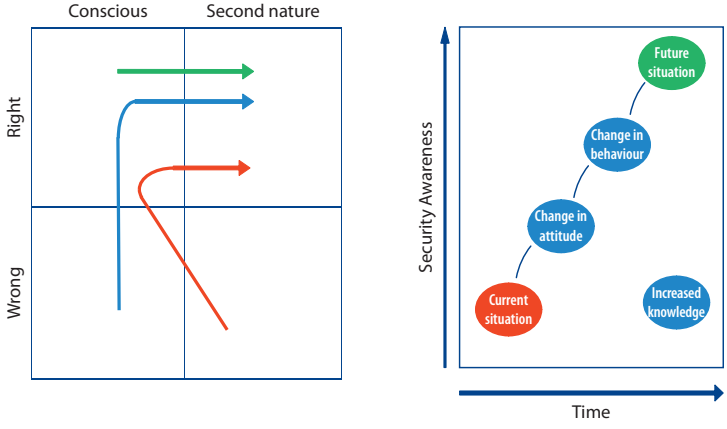


Figure 3: Information security as second nature.

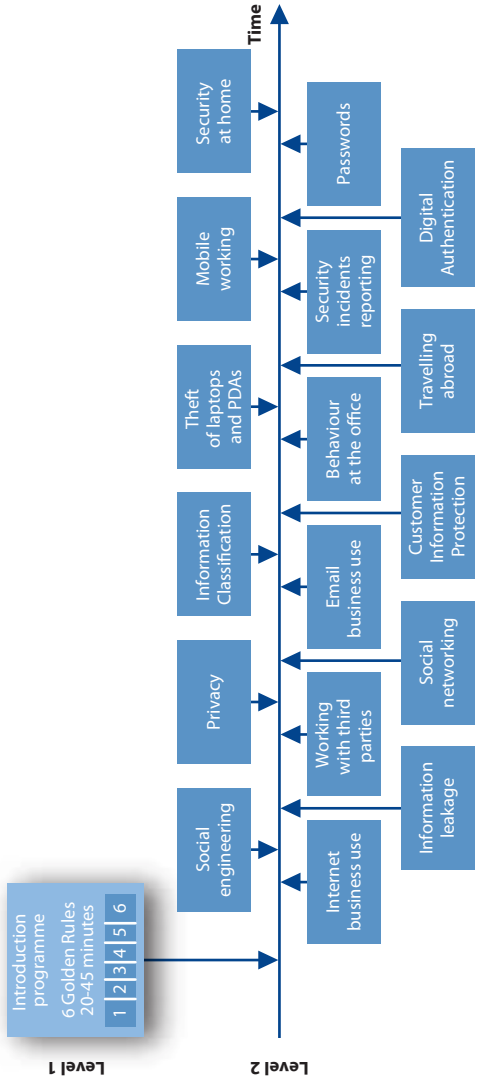


Figure 4: Illustration of continuous awareness programme.

Training is one of the 'how' components to implement information security. A training programme should be designed and developed according to the learning objectives set by the organisation. Thus the training seeks to teach skills which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. The skills acquired during training are built upon the awareness foundation, in particular upon the information security basics and literacy material ([10]).

Awareness programmes start with awareness, build eventually to training, and evolve into education (see Figure 4). They should be customised for the specific audience they are targeting. Thus it will be very important to define the users who will attend both programmes. Different methods could be used to define the target audience. ENISA developed a simple tool to identify better a target group and capture the related data, as described in the section 'Define target group' ([11]).

Scalability

The issue of scalability is fundamental to successfully reaching a growing global audience. It might further encourage the modular approach to awareness (segmentation of the audience and the message).

Languages

Getting a message through to people and making sure they understand the message presents another challenge. The formal business language in a company may not be sufficient and understood by all employees and the most effective way of delivering a workshop and e-learning content

([10]) NIST, Information technology security training requirements: A role- and performance-based model, NIST — SP 800-16, USA, 1998, available at *http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf* (last visited on 21 July 2008).
([11]) Herold, Rebecca, *Information security and privacy awareness program,* Auerbach Publications, USA, 2005; NIST, *Building an information technology security awareness program*, NIST — SP800-50, NIST, 2003, available at *http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf* (last visited on 17 July 2008).

is to do it in their local languages. Therefore it is very important to consider that in one geographical location there may be several languages. The following should be taken into consideration:

- ✓ Different languages within the same country
  - One country – several languages
- ✓ Different languages between countries
  - International operations
- ✓ Corporate language
- ✓ Different variations of the same language
  - For example business English vs. plain English

International insurer – senior management commitment makes a big difference

An insurance company explained why information security is important to their business. They collect, store, and process significant amounts of financial, medical, and personal information. This information is their number one asset; confidentiality breaches could put their reputation at risk, as well as exposing them to harmful litigation. Unfortunately, the threats (such as identity theft and scams) are rising; this makes staff awareness vital.
The main challenge has been to develop an approach that is suitable for over 10,000 employees speaking many different languages. To counteract this, the company engaged an external provider to help them build suitable training plans and materials. To create the greatest impact with staff, training materials were translated into the local mother tongues of the countries concerned.
There is a continual programme to adjust and promote the key messages. The objectives of this are to try to change people's behaviour and perception of risk. Numerous techniques are used to reach the audience, since different people learn by different mechanisms. The most effective technique has been face-to-face time with staff through workshops and training sessions. Being able to put

a face to a name or function is more personable and people are more receptive to messages being face-to-face. The training is mandatory. Senior management actively support the awareness schemes, making sure training events are at convenient times for the business and promoting them to staff. There is good attendance at sessions since missing the events results in escalation to the employee's manager. This senior management support across the business has proved to be critical to the success of the awareness programme.

Other non-interactive mechanisms, such as intranet articles, emails, posters and publications, are used to reinforce important messages. However, it has proved difficult to gauge how many people have read or understood the messages and people can easily ignore them. So, they are used as a complement to, rather than a substitute for, classroom training.

The main measure of the impact of the awareness training is feedback and questionnaires completed on or shortly after training sessions. This feedback gives a good insight into the impact of the training on the individual. Generally this has been positive, with the vast majority saying that they have learned something new and will try to change their behaviours.

Other ways to test awareness, such as checking the strength of passwords or mocking up social engineering type situations to gauge responses, have been considered. However, these are not used, due to concerns about dependence on other variables (such as the mood of the person), privacy and entrapment.

The company is now focused on ensuring that training continues to engage people; e-learning modules are being developed to add variety. A continual process is underway to enhance the relevance of the material to staff, so they can see the benefits and understand the risks more clearly.

International Financial Group – Awareness Raising in red carpet style

In response to recent incidents that have attracted national and international press attention steps were taken to initiate a Group wide global Privacy Program and to improve the general Information Risk Management (IRM) awareness material.

The Privacy Programme Awareness Raising

The Programme goal is to move the bank to a position where it can actively demonstrate its compliance to privacy laws and regulations and proactively manage its privacy risk profile. This includes producing materials for measurable awareness and training campaigns, and developing a two-year communications plan for each Business Unit.

A critical success factor was to ensure that they could effectively communicate privacy messages to more than 150,000 staff to drive cultural change across the Group. To achieve this they worked with an external strategic communication agency, to create and release a global awareness campaign. The 'Think Privacy' campaign has been translated into multiple languages and distributed across our global business. Awareness materials were used all over the Banks buildings, including in the toilets, lifts, on the security barriers, on desks and being handed out on a 1-2-1 basis in lift lobbies, all carrying the key privacy messages.

To drive the adoption of the 'Think Privacy' campaign the programme created a Training and Awareness Toolkit.

This toolkit acts as an implementation aid outlining the process for creating privacy messages, planning a campaign, producing material and measuring the effectiveness of the campaign.

Measuring the effectiveness of the campaigns is key to the success of the pro-

gramme. To ensure behavioural change is taking place following the implementation of the new privacy practices they have used both pre and post campaign surveys, focus groups and are monitoring the performance of privacy metrics. Early results have confirmed a steep rise in awareness across the Group.

Information Risk Management (IRM) Awareness Raising

The IRM Awareness Raising campaign has three elements: a film, a mandated training package and an awareness raising package for third party suppliers.

They already had produced an awareness film that had become dated so it was decided to produce a new film that was fresh, innovative, and entertaining in order to keep the attention of the viewer whilst delivering the key messages:

- ✓ *Be aware of Information Risks*
- ✓ *Use technology and software appropriately*
- ✓ *Protect Group's integrity*
- ✓ *Protect Group's information and data*
- ✓ *Understand personal responsibilities*

The new film, subtitled in 5 languages, and associated campaign materials were based around a 'Corporate Security Drama' and included references to a wide variety of film genres. These separate genres which the film incorporated are viewable independently as modules on the Group's Intranet, along with the main film, which was also distributed on DVD.

A series of posters and e-shots were designed as film posters to reflect each genre and promote the issues raised in that genre-specific film. These were released at various times and places to remind people about the messages within the film and to direct people to their IRM Intranet site.

Building on the success of the film and the central character in it, a mandated computer based training (CBT) package was created. It was more conservative in its approach, but was of the same length – 20 minutes - the maximum length advised by e-learning experts.

It is as interactive as possible in order to make the training process a more enjoyable and effective experience when compared to the 'click next' type CBT packages. To ensure consistency it uses very similar messages to those used in the film. The CBT is delivered to the desktop via their Learning Management System.
Despite all this work they were acutely aware that there was a gap in their coverage, i.e. raising the IRM awareness of third party suppliers. The team identified an opportunity to work with colleagues who interface with third parties to create a CBT package that closes this gap.

Key Learning Points
The Group has identified a number of key learning points. In no particular order there is a list of their top 5:
Ensure your messages are simple and clear. Don't over complicate them with technical jargon or assume technical knowledge. Your messages must be short otherwise users won't read them.
If possible, make your messages and the way you deliver them stand out from the 'corporate crowd'. Avoid using colleagues in your material. At some point they'll leave and date your material, and your audience will spend more time looking at them and less time on the actual message.

- ✓ *Identify, engage and manage your stakeholders early. Consider giving some thought to including those who could make the delivery of the project difficult in your stakeholder list. Persuade them to provide input and agree the messages.*
- ✓ *Identify your delivery channels early and engage with the key stakeholders in those areas to avoid delays in delivering your product. Don't make assumptions about technology and technology builds especially in large companies.*
- ✓ *Think holistically about your campaign. If making a film, consider producing other materials to support it and the messages it contains.*

PART 2: AWARENESS RAISING PROGRAMMES

Awareness raising programmes

Raising information security awareness is not a one-off exercise. In the same manner, an awareness raising programme cannot then be relied on indefinitely in an organisation without further action or modification. To ensure that the programme continues to correspond with the targets of a financial organisation and that information security is incorporated in the organisational culture, awareness must be maintained or raised continuously. It is an ongoing process, a cycle of analysis and change, as we find it in many quality management systems, such as ISO 9001 or ISO/IEC 27001. 'Taking [such] a change management approach to an awareness initiative is crucial as it helps close the gap between a particular issue and human responses to the need to change, even in the case of cultural change' ([12]).

The first step is to analyse the actual information security awareness and culture and to identify the main business drivers. If the culture does not fit with the organisation's targets, the culture must be changed. If it fits, it should be reinforced. The necessary controls such as an information security training programme or an awareness campaign must be chosen (planning and design) and realised (implementation). The success of the controls taken must then be evaluated and learning specified (measuring success and programme improvement). The process is illustrated in Figure 5.

([12]) ENISA, *A New Users' Guide: How to Raise Information Security Awareness,* 2008, available at *http://www.enisa.europa.eu/pdf/deliverables/new_ar_users_guide.pdf*

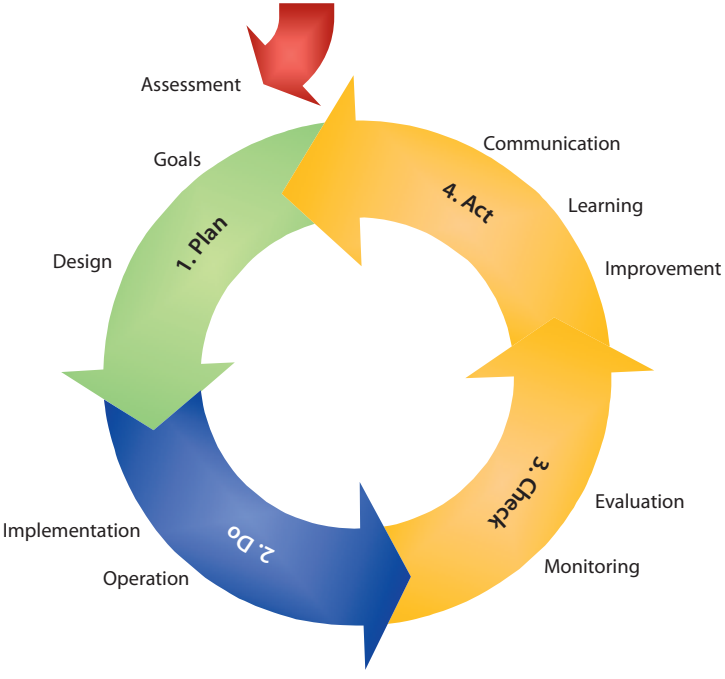


Figure 5: Overall Strategy for raising information security awareness in financial organisations.

Assessment

The need for information security awareness is widely recognised. In order to make a substantial contribution to the field of information security and to choose the appropriate controls, it is necessary to have a set of methods for its study. Despite the fact that information security awareness and culture can be measured, not many financial organisations have tried to quantify the value of awareness programmes.

According to Gartner, there are four main categories against which information security awareness can be measured ([13]):

1. Process improvement (development, dissemination and deployment of recommended information security guidelines as well as awareness training),
2. Attack resistance (recognition of information security event and resistance to an attack),
3. Efficiency and Effectiveness (efficiency and effectiveness with regard to information security incidents),
4. Internal Protections (how well is an individual protected against potential threats).

In practice, a wide variety of instruments targeting these four categories are used today to assess information security awareness, but there is little consensus on the most effective measures.

According to one ENISA study, the most popular source of information on actual behaviours is internal or external audit ([14]). The research shows that many survey respondents use their experience of information security incidents as a metric. Relatively few respondents find in-

([13]) ENISA, Information security awareness initiatives: Current practice and the measurement of success, 2007, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf*

([14]) ENISA, Information security awareness initiatives: Current practice and the measurement of success, 2007, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf*

put metrics (for example number of visitors to intranet site, number of leaflets distributed) helpful. The most used measures of this type are the number of staff receiving training and qualitative feedback from staff on the programme. Roughly a third of respondents used each of these metrics.

Given the ease with which process improvement measures can be captured, the number of respondents using them is low. Organisations also appear to find it very difficult to put effective quantitative metrics in place. For example, only one third of respondents included questions on information security awareness in staff surveys. They then measure awareness levels before and after initiatives take place. Respondents following this quantitative approach highlight issues with the complexity of collecting and processing this data. Given a carefully designed and tested questionnaire, a staff survey on information security awareness provides valuable insights into the factors driving secure behaviour including leadership behaviour, know-how, attitude and motivation. Some case studies report excellent results by using surveys in financial institutes ([15]).

Bearing in mind the difficulties in comprehending all human behaviour and culture, the use of a combination of measurement tools and methods, as proposed by experts in organisational culture, would seem advisable. These allow verification of the results obtained by other methods. The financial organisations are thus able to pick the appropriate methods to assess their information security culture.

A grounded analysis framework allows the financial organisation to systematically analyse its information security culture, to quickly identify weaknesses and improvement actions and also to prove progress when improving an information security culture.

([15]) Schlienger, T. and S. Teufel, *Tool supported Management of Information Security Culture: An application to a Private Bank*, The 20th IFIP International Information Security Conference (SEC 2005) - Security and Privacy in the Age of Ubiquitous Computing, Makuhari Messe, Chiba, JAPAN, Kluwer Academic Press, 2007.

Planning and designing phases

When planning an information security awareness programme there are several factors which should be taken into account. In this section we will look at the most important issues, why they are important and how to deal with them.

Approval from the board

The most critical success factor in any project with organisation-wide focus is to obtain executive commitment. This is one of the most powerful levers inside any organisation since executive support not only provides funding, but also provides an example to all levels of the organisation.

The board should appoint someone to formally sponsor the programme across the organisation. Doing so actively demonstrates to all employees that the programme is part of the organisation's strategy and also guarantees an alignment at all levels of the business.

International financial organisation – Information security awareness programme for all staff

An international financial organisation with substantial influence throughout Europe wanted to implement information security awareness programme for all staff. The aim was to make staff throughout the organisation aware of the seven most important information security rules to follow.

To demonstrate senior management's commitment, it was decided to make a management film featuring the head of the organisation. The management film is a direct message to all staff about the different information security threats and what the consequences would be if staff does not start making information security a part of their daily routines. In the film he also makes it clear that he, himself, will follow this work-shop and that he trusts all staff to do their best to cooperate with the initiative; a very strong message from senior management to staff on all levels of the organisation.
The use of different learning methods was also seen as vital to a successful awareness programme. An awareness programme with eye-opening business film clips, learning material and self-tests was selected. This was to make the programme more interesting and to show practical examples of how security incidents could occur.
It was decided that the awareness programme would first be delivered in departmental work-shops, utilising a face-to-face approach to engage staff directly and to encourage discussions.
The work-shop programme was supported with an e-learning version for staff not being able to participate in the work-shops and for all new staff entering the organisation. Initiation of local action plans as a part of the work-shop was seen as a way of making staff commit to including information security in practice in their place of work.
The test results from the self-test are recorded and MIS is available to show overall participation and the average scores achieved. It was decided not to measure individual results to avoid privacy concerns across the different countries.

Identify drivers

The main output of this activity is to understand exactly why the financial organisation needs an awareness programme. It is important to state the reasons behind a programme, so that it can be made more effective.

Among the most recent reasons for launching an awareness programme for information security we have the related controls imposed by regulations for example as SOX, BASEL II and other country-specific privacy laws.

It can also be a part of the organisation's strategy - several organisations are pursuing certification objectives such as ISO/IEC 27001 for Information Security Management and BS25999 for Business Continuity Management, which ask for a high level of commitment from every employee.

Some control frameworks, like CobiT, also emphasise the need for user training and awareness.

Other possible reasons for launching an awareness programme are changes in the institution's policies, implementation of new systems, employee know-how, corporate values, audit findings, results from risk analysis and so on.

It is important to remember that different areas of the organisation have different needs. The programme manager should meet with top management in order to identify what kind of information their employees should receive regarding information security. For example, if the employees are not aware of the organisation's information security policy that should be the first action of the programme.

The drivers should be included in the programme so that there is good general awareness of why the organisation is investing resources in the project.

Identify requisites and needs

There are different types of requisites, needs and constraints to be identified before programme design.

Depending on the size of the institution, the project managers might want to look at different geographical and cultural details, for instance country-specific laws and languages in the first case and cultural values in the second case.

International Swiss private bank – Information security culture assessment & awareness programme

Information Security (IS) is an important issue for private banks. A number of steps, such as staff information and clear desk flyers, have been and are being taken to address and improve the quality of information security. However, to ensure that the required level of security is maintained, staff trainings are a vital part of this process.

The management has requested suggestions on steps that can be taken to implement a security awareness programme and seeks assistance in a companywide rollout of this programme.

Firstly, the IS-culture was assessed by means of a quantitative staff survey. Different subcultures have been identified. This is the effect of a merger which resulted in the creation of one company.

Secondly, countermeasures were defined in order to raise the maturity level of IS awareness. These measures were realised within a global awareness programme.

The global IS awareness programme included:

- ✓ *CEO film demonstrating the commitment of the management to the IS programme.*
- ✓ *Definition of six golden security rules.*
- ✓ *An e-learning programme including a test.*
- ✓ *Management workshops.*
- ✓ *IS awareness promotional material like posters and flyers for all staff and locations.*
- ✓ *New IS awareness intranet presence.*

For the successful realisation of this IS awareness programme two factors were essential: first that key people from Marketing & Communications as well as from Human Resources were part of the project team; second that the executive board members were fully committed. Indeed, these two factors were crucial for the success of this IS awareness programme. In addition, it was important to use a unique IS awareness brand. A unique branding was created

for all communication measures such as the e-learning programme, posters, flyers, management workshops and the intranet portal. The branding was represented by a photo which was created thanks to the active cooperation of employees. It was a true eye catcher solution. While it perfectly represented the programme it also raised the consciousness for the project. Hence, the programme was very well perceived by the staff.
In a next step it is planned to evaluate the outcome of the IS awareness programme through another quantitative assessment approach. Furthermore an IS awareness management process is going to be installed to constantly optimise the IS awareness level at the bank.

The requisites and constraints relating to end users need to be identified and related to each other in order to build more effective training curricula that align with the institutions' objectives. All these points should be validated with the Human Resources department.

Budgetary and resource requirements must also be determined; different media and methods have different costs, and the organisation may be willing to invest different resources for different awareness methods.

Another provision which might impact on your planning or content is the requirements of regulations and standards. For example, if the organisation is planning to obtain certification against ISO/IEC 27001, there are two key factors to consider regarding the timing and the type of training. Firstly, new personnel need to understand the organisation's information security policies and expectations before being allowed to use the services or access the organisation's information and secondly the need to provide ongoing training programmes to ensure personnel continue to understand the organisation's information security controls.

Financial services group – reducing the training burden on staff

A large financial services company explained that information security awareness has a high priority. It is on the board's agenda; they see it as important to retaining the trust of customers.
One challenge is the high percentage of part time staff and contractors. Another is the existing mandatory training burden on staff (anti-money laundering, data protection, anti-fraud, etc.). Linking information security awareness training into other on-the-job training activities has proved vital. The company has recently restructured its security function to bring together physical security, information security and fraud prevention. The key awareness issues from each of these aspects are combined and distilled into a single set of training messages.
Staff show good understanding of some security issues, such as email and mobile devices (phones and lap top computers etc.). Getting messages across in other areas (such as Internet-related threats and instant messaging) has proved harder. The awareness training clearly explains each individual's personal responsibilities for information security. It then provides guidance on good practices the individual can adopt to discharge those responsibilities.
The business demands training to be available as required and in a cost-effective way. To meet these demands, there is a drive to deliver security awareness through on-line systems and self training. Completion of computer-based training (CBT) is now mandatory. Quizzes in the CBT provide statistics that measure the levels of awareness; the CBT itself records the extent to which staff have been trained. The speed, ease of use and consistency of the on-line training programme are seen as key benefits. While the set-up has involved some investment, the efficiency of training delivery achieved has maximised the return on this investment.

Other measures that have proved helpful in tracking staff awareness include the number of mobile devices lost, and the number of concerns and security-related incidents reported.
The content of CBT training is continually reviewed, so that it reflects emerging risks and staff continue to see the benefits. The next stage will be to target high risk groups for additional face-to-face security awareness training.

Design the programme

Having identified the factors that influence and impact the design of the programme, it is now time to begin building the programme itself.

At this stage and based on the identified education and training needs, identify the following:

- ✓ Target groups and their members. Some examples are the administration board, the CxO level, the operational risk team(s), IT teams, employees by role and so forth.
- ✓ Efficient delivery mechanisms, for instance computer based training (CBT), classroom training, intranet materials, posters etc.
- ✓ Timings. If the project has different phases it is very important to plan the right beginning and duration of each so that information overload to the employees can be avoided and the momentum of the programme maintained.
- ✓ Session performance evaluations and benchmarking. In order to assess the effectiveness of the programme, metrics should be defined at this stage in order to provide for monitoring and reporting on training effectiveness. One method for achieving this is to conduct a survey before and after the training sessions.
- ✓ Metrics for evaluating training content, quality, effectiveness, cost and value. These metrics will allow for future curriculum definition.

Review the design

After finishing the information security awareness programme it is time to present it to the board and top management for reviewing and final sign-off.

At this time, special care should be taken to show that the programme's objectives are directly connected to the organisation's objectives and explicitly support them.

Implementation phase

This section of the report covers how to deploy a successful awareness campaign and considers:

- ✓ Building a platform for delivery.
- ✓ Assigning project resources.
- ✓ Planning and executing the roll out.

Build a platform for delivery

One of the key challenges for any IS training project is the roll out, administration and management of the various learning solutions that will ultimately make up the full awareness programme.

Most organisations that are seeking to deploy comprehensive and ongoing awareness solutions implement a learning management system (LMS). These systems typically:

- ✓ Track employee usage of e-learning, recording progress, completion rates and other performance data such as test scores.
- ✓ Produce a range of management reports that can be accessed by administrators and managers at the centre and in the regions.
- ✓ Import and export data from and to other applications (for instance the HR system).
- ✓ Allow for user profiling in order that content can be assigned to users according to pre-defined characteristics (for example job role and/or preferred language).

- ✓ Manage the roll-out of learning solutions across the business in order to minimise impact on business and network resources.

A learning management system allows the organisation to deliver a range of awareness solutions to a variety of target audiences while allowing the system administrator to track usage and completion rates and to assign content to individuals based on, for example, their job role or department. These systems are purpose built and are particularly effective when large, complex and ongoing awareness initiatives are being implemented.

Although students can self-enrol in most LMSs, the full potential of the system is best realised when the database is pre-populated with appropriate student data. In particular, pre-population of the database allows the administrator to control the assignment of learning materials to predefined groups of students and hence to carefully manage the roll out of courses. Also, if the database is pre-populated, tracking and reporting (particularly of students who have been assigned to, but have not completed courses) is much easier.

Assign project resources

Adequate resourcing of large-scale information security awareness initiatives is critical for their success. Outlined below are some of the key roles and responsibilities that would typically be required for the completion of a project of this nature.

Figure 6: Key roles and responsibilities. Illustrative only.

Role	Tasks	Commitment
Project manager	✓ Monitors progress against plan. ✓ Co-ordinates internal resources. ✓ Manages the relationship with vendors.	Involved throughout the project – participates in regular progress meetings.

>>>

Role	Tasks	Commitment
Subject Matter Expert	✓ Agrees the overall approach to the content of the awareness programme. ✓ Approves content.	Involved in the early stages of the project in defining requirements and reviewing content Subsequently, occasional contact with instructional designers and developers to maintain relationship and identify any future developments that are required.
LMS Administrator	✓ Maintains the LMS. ✓ Produces management information and reports	The time commitment for the LMS Administrator depends upon how frequently changes to the configuration of the system are required and what the MI and reporting requirements are.
IT Help Desk	✓ Provides support to users once the programme is rolled out.	IT Help Desk should provide support to users regarding the operation of the LMS and any e-learning courseware as part of the routine Help Desk duties. It can be helpful to provide a short training session for Help Desk staff during the implementation.
Corporate Communications	✓ Provides support and advice regarding internal marketing issues, branding and so forth.	Involved in the early stages of each deliverable approving visual identity, styles etc. Can help to plan and execute internal marketing campaigns to promote awareness of the training initiative.

>>>

Role	Tasks	Commitment
Line of Business Representatives	✓ Provides liaison with key business lines.	Involved in supporting and promoting the internal communication campaign and the roll-out strategy May also be involved in user acceptance testing and piloting of learning tools to generate buy-in from specific businesses.
IT and /or HR Representative	✓ Provides interface to HR systems for pre-population of the LMS database.	Involved in the initial set up and pre-population of the LMS database and subsequent updates to the system for joiners, leavers and movers.

Plan and execute the roll out

There are several key factors to consider when planning the roll out of a comprehensive awareness programme:

- ✓ The roll out plan should include pilot testing of all materials before 'going live'. Pilot programmes should test the effectiveness of the content of the learning tools from an instructional perspective. Importantly, where technology-based training is being delivered, there needs to be pilot testing from a technical perspective to ensure that the training functions adequately in all of the proposed business environments.
- ✓ Where a learning management system is being used to manage any or all of the roll out, there should be sufficient time to ensure that it contains all of the required student data, and that invitation and reminder emails have been drafted, tested and approved. Roll outs can often fail because learners experience difficulty accessing the content via the LMS or because email invitations are not clear or helpful.
- ✓ A phased roll out (other than in the most urgent of circumstances) is usually preferable to a 'big bang' approach because:
  - o It minimises the impact on network resources for technology-based training
  - o It minimises the impact on 'business as usual' for the organisation

- It allows for issues to be identified and addressed on a rolling basis so that they are not experienced by large sections of the target population

✓ The roll out should prioritise any areas of the business that are considered high risk from an information security perspective.

✓ Consideration should be given, in global organisations, to the requirement for language versions of any training content. Ideally, the roll out strategy should allow for the full completion and testing of a 'base' language version (usually the main business language of the organisation) prior to the development of further language versions. This approach ensures standardisation and consistency across languages and minimises the management, administrative and financial overhead of maintaining multiple language versions during the development phase.

✓ The roll out should be planned around other known initiatives within the business (such as major training initiatives, product launches, financial year ends and so forth) so as to minimise competition for the attention of the intended audience groups. Liaison with Learning & Development, HR and internal communications departments will usually yield much useful information about other initiatives.

- The visible commitment of senior managers within the business units to the aims and objectives of the awareness programme is a critical success factor. Any awareness initiative should therefore begin with events (presentations, briefings and so forth) to engage the attention and active support of senior management. Many large organisations take a cascade approach to management communications, providing managers with their own presentation packs or 'meetings in a box' to drive the message down the management line.
- High quality learning tools often fail to have impact in organisations because of a lack of internal marketing and PR. Information security is not a topic of inherent interest to many employees yet their 'buy-in' to the key messages of any awareness campaign is critical to bringing about any meaningful behavioural change and embedding a culture of security. The active support of the Internal Communications department should be sought in 'selling' information security and security awareness to the target population. Typically this can be achieved using a variety of internal communication tools and channels to create the initial 'launch campaign' as well as ongoing communications to help maintain levels of awareness.

- If the planned programme included external vendors and suppliers it is important to ensure that they:
  - Have strong internal procedures and project management capabilities to ensure delivery of solutions on time, on budget and to the desired quality.
  - Have an appropriate combination of learning and development expertise and subject matter expertise to deliver effective learning solutions.
  - Consideration should be given to providing feedback to managers and the wider target audience about the successes and impacts of the training campaign so that individual employees are aware of the outcomes of their learning activity and can be encouraged to see the time investment as worthwhile.

Full service bank — Creating an enterprise-wide security training and awareness campaign covering both general users and technical specialists.

This project, for a global financial institution, was designed to bring about a step change in information security training and awareness at an enterprise level. With 50,000 employees in over a dozen countries, the brief was to reach all employees and deliver training customised to meet varying job roles and responsibilities. After a detailed consultancy phase a three-strand solution was recommended. This comprised general information security training and awareness for non-technical employees with concurrent training for managers and executives. The solution was delivered in several languages via a Learning Management System, complete with evaluation tools, and a follow up programme of refresher training. In addition, a detailed series of workshops and support materials was developed for technical and security employees, comprising a core curriculum covering secure application development, access controls and intrusion management for developers, technical architects and systems administrators. These were delivered across

several international locations, but with stranded material reflecting particular job roles and responsibilities. The training initiatives were combined with an overall internal marketing campaign. Deliverables included a detailed communication campaign with tag lines, newsletters, presentations 'in a box', executive briefings and a revamped information security portal for the corporation.

The Outcome…

Reduced vulnerability and heightened awareness of business critical security issues and responsibilities across the enterprise.

Measure the success and improve the programme

Measuring success provides valuable information about the efficiency and effectiveness of the controls implemented. It helps to evaluate the controls taken, to define necessary follow-up and also to legitimate investment in information security awareness. This is especially important in applying for the following year's budget. Evaluation of a campaign or training programme is essential to understand its effectiveness, as well as to use the data as a guide to adjust the initiative to make it more successful.

To highlight the changes achieved in a culture, the same measurement instruments as during the assessment should be used. They can be complemented by specific evaluation on the controls taken to reveal its effectiveness. If for example an awareness training programme was implemented know-how test can assess the learning goals reached.

International commercial bank – measuring is critical to targeting efforts

A large commercial bank has a central information security function. This team is responsible for driving awareness training across the world. They aim to get basic messages about security across to a large, geographically dispersed audience. They also need to send specific messages to smaller groups of staff with key roles in systems or security.
A big challenge faced by the bank has been how to measure awareness levels and the effectiveness of its awareness programme. Ideally, the bank wants to measure the change in people's behaviours. This is difficult to assess quantitatively. However, measurement is critical to targeting training efforts at weak areas, so the bank has invested in identifying practical metrics and key performance indicators.
A particularly successful technique has been the use of computer-based training (CBT). A centralised CBT library includes training courses and captures test results from the automated testing of staff. All new employees must complete the training as part of their induction. The training is updated regularly, and all staff must complete the updated training. Reports analyse the extent of completion of CBT training and the scores in tests; the central team monitor these and act on any significant trends.
Password scans provide a useful direct quantitative measure of the attitude and behaviour of staff. The bank periodically runs software that scans password files on key systems and analyses the strength of individual passwords. The number of staff using easily guessable passwords is a key indicator of security awareness.
Other techniques that have proved effective include simulated phishing emails and competitions. These have made the targeted staff think carefully about why they are asked to be secure. They have also provided helpful statistics for trend analysis.
There are plans to introduce a new survey to gauge the level of security awareness and behaviours within the bank. An independent third party will gather responses from a random sample of staff

(rather than self-select). This will enable the bank to use the survey results to draw statistically valid conclusions across the business. Initially, the bank monitored incidents to assess security awareness. However, root cause analysis has shown there are many different factors behind each incident, so the number of incidents is not a true reflection of security awareness. In addition, the frequency of incidents is so low that trend analysis is not meaningful. For these reasons, incident statistics are no longer used to measure awareness.

When measuring success, qualitative and quantitative instruments can be put in place. Regardless of the measure used, it is important that any organisation address these issues ([16]):

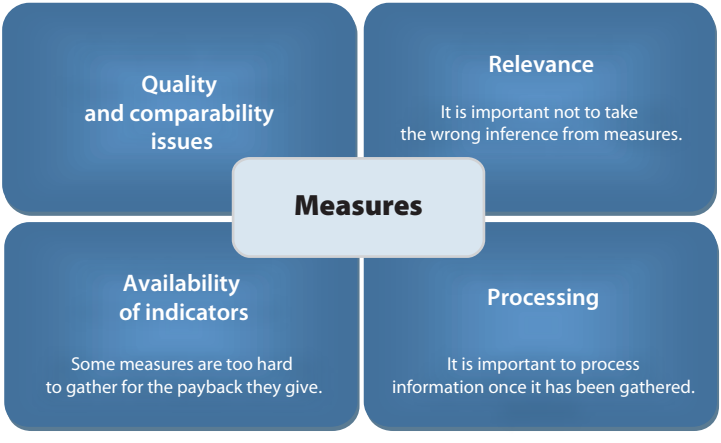


Figure 7: Measuring the effectiveness of awareness programmes.

([16]) ENISA, Information security awareness initiatives: Current practice and the measurement of success, 2007, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf*

Evaluation can evidence change and improvement in an information security culture and also reinforce organisational learning thereby encouraging continuous improvement and a strong information security culture.

International financial institution – motivation is the key word

Selling security can be a bit like selling insurance – who needs it until after a break-in? International Financial Institution is actually trying to prevent the break-in in the first place but people need to be sufficiently motivated to act in a secure way.

Policies – Standards- Contracts

Policies and Standards are fundamental but are rarely written in a language and tone that users would enjoy. Staff security responsibilities are stated in all contracts across the Institution, but these are quite general and they have a tendency to be written from a legal standpoint covering things like non-disclosure. These sign-offs apply to contract and temporary staff as well as permanent.
The Information Security department is developing their Information Security Standards consistently with ISO 27002 and BS 7799. These are very detailed and target primarily IT staff so the Standards for All booklet was created addressing the needs of non-IT employees. This booklet covers the main Do's and Don'ts around acceptable use of IT systems including their security expectations and supports a number of policies. As the name suggests this is developed for all staff to read.

eLearning / CBT

The Information Security department has put a lot of effort into their annual eLearning course which serves as an awareness initiative in its own right and includes a test of understanding at the end. It is mandated so they also have a record kept of each staff member's course completion which can be used, for example, in the

event of a disciplinary case to evidence whether the Institution's IS expectations have been explained to a user around specific topics. For new starters this eLearning option is much more effective in explaining the security culture than reading policies so it is also forming a key part of the induction process.

Intranet

Intranet provides fresh content each month which is flagged on the front page. Information there aims to be relevant, newsworthy and eye-catching to as many staff as possible. The IS department tries to make this useful outside of the workplace, where possible, such as risks associated with social network sites despite them being blocked from work. These have to be easy to understand and jargon-free as much as possible. Topics covered include for instance, 'financial scams & phishing', 'Security threats' and '10 things every employee should know'.

Presentations

Presentations are provided on a request basis to internal teams, but they also ensure that Information Security is a key part of the IT graduates induction process.

Other Controls

Cross-cut shredders are installed around offices replacing the old confidential waste bins.

Print on demand not only cuts down printing costs but it also reduces the amount of printed output left lying around. The user has to go to the printer and present or swipe their staff card before anything is printed and anything not printed is deleted. This has also proved useful in disciplinary cases showing who printed a document. Both the shredding and print on demand projects support the Clean Desk policy as well as recycling and 'green' initiatives.

Laptops have hard disk encryption and software which enforces encryption for permitted users to write to CD or USB, is employed.

Blackberry devices are policy managed so they have limited user configuration capability and the kill-pill functionality to wipe the device once we're notified of loss or theft. A voice biometric system is in place for automated password resets cutting the number of Helpdesk calls and is available 24 hours a day, 365 days a year.

Communication

Appropriate communication to suit different audiences – general users, IT staff and managers – is important especially when there are language & translation barriers too

As Security Professionals we need to recognise the different audiences we have and tailor our messages to suit each.

Competing for 'air-space' internally is one of the main challenges. Staff is bombarded with a number of financial, legal, regulatory and compliance messages, anti money laundering, general bank training, etc. Security may be everyone's responsibility but it's not everyone's main job or prime focus.

Targeted awareness training of key teams such as IT is top of the agenda. There are also call centres, postal and facilities, HR, and Management. The IS department of the Institution is currently developing a training program specifically for the IT Teams which will consist of a catalogue of presentations and handouts on key topics and are also looking to adopt the e-Learning mechanism.

Objectives

The long term aim is to get more specific details set in Staff Objectives so that all staff can show where they have contributed and are sufficiently motivated to comply. Motivation is key to this whole subject.

PART 3: GUIDELINES FOR GOOD PRACTICE

Good practice guidelines

Based on the information gathered and subsequent analysis, this section provides good practice guidelines that can help readers and their organisations while looking at data security and planning effective training and awareness activities.

Recommendations

Figure 7: Recommendations.

	#	Recommendations
Information security policies and procedures	1	✓ Define written information security policies and procedures to ensure data security. Define who has access to which type of document. Specify in which format documents can be accessed, either electronic or paper-based. ✓ Avoid giving access to all personal and financial information to all staff, including for example bank account and credit cards details, recording of telephone conversations. It is a quite common practice for financial call centres to record telephone conversations containing sensitive data. Particular attention should be given to this. ✓ Include a monitoring access mechanism to personal and financial data. ✓ Include a reporting mechanism in case of data loss including when and how to notify affected customers. Specify roles and responsibilities for financial organisations' employees. ✓ Provide laptops and mobile devices such as PDAs only to senior management and staff who work offsite regularly. ✓ Only give access to the internet and email to staff with a business need. ✓ Encourage the use of strong passwords.

>>>

	#	Recommendations
Physical security	2	✓ Regulate access to corporate premises including visitor access. ✓ Implement a clear-desk policy. ✓ Store personal and financial records in a locked cabinet when leaving the office. ✓ Dispose shredders.
Data security risks	3	✓ Personal and financial data security is a crucial responsibility for every organisation. Every piece of data can be of value to fraudsters as they can access multiple sources of information and aggregate it.
	4	✓ Review the quality of risk assessment and related processes.
IT controls	5	✓ Define access rights on recruitment, when employees change job or leave the organisation. ✓ Define individual user accounts. ✓ Back-up data on a regular basis. ✓ Encrypt data when necessary. ✓ Establish procedures for business continuity and disaster recovery. ✓ Explain to employees the importance of personal and financial data security and the risks associated with the use of mobile devices, such as laptops, PDAs and USB flash drives, the internet and email.
Controls	6	✓ Coordinate different business areas such as Human Resources, physical security, and information security so as to avoid focusing only on IT controls. ✓ Apply the same type of controls in all sites regardless of their geographical locations. This applies to offshore operations as well.

>>>

	#	Recommendations
Internal audit and compliance	7	✓ Conduct internal audit and compliance reviews of data security on a regular basis.
Staff recruitment and vetting	8	✓ While recruiting personnel, conduct high level vetting for all staff. ✓ Keep in mind that junior, temporary and call centre staff often have a wider access to personal and financial data. ✓ Even if under pressure to fill vacancies quickly to maintain a good level of customer service, ensure that appropriate vetting is always carried out.
Third parties	9	✓ Define within the corporate information security policy if third parties, for instance call centres, archiving firms and IT consultancies, can access personal and financial data and how.
Awareness and training initiatives' setup	10	✓ Most important is to get support and funding from senior management. The board must understand the organisation's dependence on information, recognise its value and importance as well as understand the regulatory and legal business environment.
	11	✓ Information security awareness is never an IT business only. The most important aspects of an awareness programme are communication, marketing and training. It is therefore strongly recommended to set up an interdisciplinary project group with members of the internal communication department, marketing department, human resources department, physical and information security department.
	12	✓ Keeping the pace during the project is an important success factor in every project. It may be good in some situations to plan different stages instead of committing to a more complex and longer plan.

>>>

	#	Recommendations
Customisation of the awareness programme	13	✓ The awareness programme must be customised to the needs of the organisation. Generic programmes most of the time fail because of the missing business link and non-specific content.
	14	✓ A tailored programme needs defined cultural values related to risk awareness. An information security document framework with an issued policy statement, guidelines and standards defines these values. The documents must be up to date, approved by the board and they also must reflect the way of working at the organisation. In many cases the policies are not up to date and do not reflect the implemented procedures. In this case it is recommended that the policies be reworked.
	15	✓ It is essential to understand the levels of awareness in the organisation. Workforce time is very precious. A training programme should be as short as possible and as long as needed. It is therefore wise to know the strengths and weaknesses of the information security culture and to tailor a programme targeting on the specific weaknesses of the organisation.
	16	✓ It is critical to tailor the programme to the specific needs of the target audience group. Not every user needs the same information. People will ignore the message if they receive too much or un-specific information.
	17	✓ Minimum recommended target groups for financial institutions are: ▪ Senior Management ▪ All staff ▪ Staff working with confidential data.
	18	✓ The programme must also respect the different cultures in different countries. Cultural surveys show that people in Europe, South America and Asia have a different perception and attitude towards information security.

>>>

	#	Recommendations
Change management process	19	✓ Never think that a one-off project will change information security awareness in the long run. Information security awareness follows the curve; at the beginning one can measure increased awareness and motivation, but then the curve flattens and even may drop to its original state. Awareness deals with changing the behaviour of people and that may need years.
	20	✓ It is therefore recommended to follow a change management process. Continuous awareness communication and training are good examples of how the attention on the topic can be kept high. It is also very important to evaluate each step and to adjust the goals and measures if needed. This requires you to take into account the feedback of your target audience.

Conclusions

Recent incidents involving data loss have forced many organisations to consider how they can significantly improve their data security. In particular, safeguarding personal and financial data is a key responsibility for the financial services industry. The mismanagement of data security is a significant risk for financial organisations due to the nature of their business as they generally hold large volumes of personal and financial data about their customers, such as names, addresses, dates of birth, bank account details, transaction records, PIN, national insurance numbers and so on. Thus, the financial services industry needs to pay close attention to how they handle this type of data.

Financial organisations are becoming more aware of the potential costs of losing data. However, corporate information security policies, procedures and controls are not enough to prevent data loss through lack of employee awareness about the risks related to handling information.

Effective training and awareness mechanisms are crucial in these organisations as the risks to which they are exposed, for instance identity theft, money laundering, market abuse may all result in considerable inconvenience and possible financial loss to the victims as well as damage to the organisation itself.

ENISA hopes that this paper will provide financial organisations with a valuable tool to understand the importance of data loss and prepare and implement awareness raising and training programmes.

References and sources for further reading

BERR, *2008 Information Security Breaches Survey*, 2008, available at *http://www.security-survey.gov.uk* (last visited on 22 July 2008).

'Data-leak security proves to be too hard to use', *Infoworld.com*, available at *http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html* (last visited on 2 June 2008).

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995.

ENISA, *A New Users' Guide: How to Raise Information Security Awareness,* 2008, available at *http://www.enisa.europa.eu/pdf/deliverables/new_ar_users_guide.pdf*

ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf*

ENISA, *Raising Awareness in Information Security – Insight and Guidance for Member States,* 2005, available at *http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cd_awareness_raising.pdf*

ENISA*, Secure USB Flash Drives*, 2008, available at *http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf*

Financial Services Authority, *Data Security in Financial Services*, United Kingdom, April 2008.

Heiser, Jay, *Understanding data leakage*, Gartner, 21 August 2007.

Herold, Rebecca, *Managing an Information Security and Privacy Awareness and Training Programme,* Boca Raton: Auerbach, USA, 2005.

Herold, Rebecca, *Information security and privacy awareness program,* Auerbach Publications, USA, 2005.

McGlasson, Linda, 'ID Theft Red Flags Rule: How to Help Your Business Customers Comply', *BankInfoSecurity.com*, 8 September, 2008 *http://www.bankinfosecurity.com/articles.php?art_id=960andrf=090908eb*

NIST, *Building an information technology security awareness program*, NIST — SP800-50, NIST, 2003, available at *http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf* (last visited on 17 July 2008).

NIST, *Information technology security training requirements: A role- and performance-based model,* NIST — SP 800-16, USA, 1998, available at *http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf* (last visited on 21 July 2008).

Schlienger, T. and S. Teufel, *Tool supported Management of Information Security Culture: An application to a Private Bank*, The 20th IFIP International Information Security Conference (SEC 2005) - Security and Privacy in the Age of Ubiquitous Computing, Makuhari Messe, Chiba, JAPAN, Kluwer Academic Press, 2007.

'The State of Banking Information Security 2008 - Survey Executive Overview', *BankInfoSecurity.com*, available at *http://www.bankinfosecurity.com/whitepapers.php?wp_id=143* (last visited 20 November 2008).

How to obtain EU publications

Publications for sale:
- via EU Bookshop (*http://bookshop.europa.eu*);
- from your bookseller by quoting the title, publisher and/or ISBN number;
- by contacting one of our sales agents directly. You can obtain their contact details on the Internet (*http://bookshop.europa.eu*) or by sending a fax to +352 2929-42758.

Free publications:
- via EU Bookshop (*http://bookshop.europa.eu*);
- at the European Commission's representations or delegations. You can obtain their contact details on the Internet (*http://ec.europa.eu*) or by sending a fax to +352 2929-42758.

European Network and Information Security Agency

The growing requirement for information security awareness

Luxembourg: Publications Office of the European Union

2009 — 171 pp. — 12 x 17.4 cm

ISBN 978-92-9204-024-6

doi:10.2824/1209

TP-78-09-929-EN-C

ISBN 978-92-9204-024-6