Information Security and Employee Behaviour

How to Reduce Risk Through Employee Education, Training and Awareness

ANGUS McILWRAITH

GOWER
Introduction

It is clear that many security breaches are the result of human error or negligence resulting from weak operational practices. As any experienced hacker – ethical or criminal – will attest, it is more effective to focus on people errors and poor security practices than it is to try and crack today’s sophisticated technology solutions.

Deloitte – Global Financial Services Industry
2005 Global Security Survey

Information security ‘awareness’ has been promoted for years as being fundamental to information security practice. In reality, it is something that is often done poorly – so much so that I have seen very limited progress since I started in information security over 20 years ago. To improve this situation requires us (that’s you and me, the information security implementation community) to look at awareness in a different way. This book suggests that we are not solely in the security business – we are in the communications and corporate change businesses as well. Changing things is difficult, hence the well-worn quotation from the master:

It must be considered that there is nothing more difficult to carry out, nor more doubtful of success, nor dangerous to handle, than to initiate a new order of things. For the reformer has enemies and only lukewarm defenders. He must confront the disbelief of mankind, who do not truly believe in anything new until they actually experience it.

Niccolo di Bernardo dei Machiavelli (1469–1527)

We are fighting the entrenched perceptions of many people, and will suffer the problems Machiavelli\(^\text{1}\) states above. This book focuses on implementing lasting, perhaps permanent change within your organization.

There is also considerable emphasis placed on communication. The manner in which information security has been presented by the media has been poor

\(^1\) Machiavelli was the author of The Prince, a guide for politicians and tyrants written in the 16\(^{th}\) century. It remains fresh and valid to this day.
– perhaps understandably so in that journalists are by nature generalists and have to relate complex issues rapidly and succinctly. Some of the blame for this misrepresentation has to lie squarely within the information security profession itself. You can argue about why this is so, but the reality is simple. Our historic inability in this area has created a problem that this book seeks, in some part, to address.

Another element within the book is the concept of corporate culture and issues relating to changing it. The change processes relate as much to this area as any other. Culture is an oft-misused term. I hope that my ideas may help you find a way of understanding and then addressing your corporate cultural issues as they relate to information security.

Finally, I am keen to stress that there is no magic bullet to deal with information security issues. The work we are involved in crosses a large number of disciplines and fields, and we have, in order to be successful, to operate in many of them. You need to appreciate that an information security infrastructure is more than network links, servers and software. It includes buildings, documents and, most importantly, people. Messing up when you address people issues will make your professional life a lot more difficult. Dealing with them in a coherent, structured way will ease much of this pain.

**WHAT IS AWARENESS?**

For the purposes of this book, awareness is discussed in two parts. The first part is the practice of making people aware of the issues relating to information security. The second part involves encouraging (cajoling, bullying and threatening) them to act in a way that is appropriate to the value of the information they handle as part of their everyday work activities. It is different from training and education. What is apparent is that awareness, training and education practices are unavoidably interlinked.

Many people confuse awareness with publicity, and think that a yearly roadshow or the production of a mouse mat with a slogan printed on it will meet the bill: they will not. Such activities have a place in the panoply of other activities that need to happen if you are to make people truly aware, but they are by no means the total picture.

It is the second part (encouraging people to change the way they do things) that makes the difference. The core of the ideas in this book centres on behaviour. There are certain behaviours we want to happen, and others that we
do not want to happen. Knowledge is often not enough – we have to work on attitudes and perceptions, as it is these things that drive behaviour.

Behaviour is normally the result of a decision-making process. Decisions are made based on a wide variety of criteria – some seemingly logical, others, totally illogical. The criteria include:

- knowledge
- prejudice
- psychological make-up
- event specific conditions (the weather, the time and so on).

Many observers, when analysing behaviour, respond to certain actions with questions such as ‘Why the hell did he do that?’ A variety of these issues are discussed in Chapter 1 in the section called ‘The Psychology of Risk, or Why Do People Do Stupid Things?’. Many of the behaviours we don’t want to see happen are in fact predictable, but only if you take the time to analyse and understand how people come to make decisions.

Part of this analysis should concentrate on how people perceive risk. Perception forms a basic part of prejudice, and distorts knowledge. Chapter 1 discusses the issues relating to risk perception in depth, but it’s worth outlining some of them at this point.

If things are unfamiliar, outside your control and imposed upon you, they are automatically perceived as more risky than something that is known, in your hands and performed by you personally. This perception drives decision making on risk to such an extent that it has led to inappropriate risk management investment decisions. These inappropriate decisions waste time and money without addressing real risk efficiently or effectively. They have also led to the reduction of the credibility of information security as a practice, which in turn has lead to ongoing future problems obtaining reasonable investment to meet real risks. Examples of such inappropriate investment occur often. Most competently built e-commerce systems have extensive, expensive technology protecting them from external attack. This technology includes firewalls, complex cryptographic facilities and intrusion detection systems (IDS). Whilst these are necessary, not least to ensure basic legal and financial principles such as non-repudiation, there is often a parallel lack of investment in staff training, HR recruitment procedures and management control over contractors and similar short-term employees.
A further issue in dealing with inappropriate behaviour (in the context of how risk is perceived) is that of how to meet awareness needs. I have already asserted that awareness is more than publicity and giveaways (mouse mats, fluffy stick-on bugs, pens, drinks mats and so on, collectively known as ‘collateral’). You need to identify those behaviours you want (or don’t want), and then try to initiate (or stop) them. If these things are identified, then it becomes easier to focus one’s effort – indeed, it becomes possible to operate by setting measurable objectives. Such a technique forms the core of Part 2 of this book.

Having hopefully provided you with a way of taking awareness forward, I have also looked at another matter – that of how information security professionals and/or practitioners (in many circumstances there is a difference) are perceived. This perception drives many prejudices, which in turn affects the way security investment decisions are made. We have to address our own image – mainly because it has become tarnished.

**WHY AWARENESS?**

Raising awareness is the single most effective thing an information security practitioner can do to make a positive difference to their organization.

> The idea is the more lines of defense a company has in place, the less likely there will be a successful penetration, the more chance there is that an attack can be detected and the most likeliness an attacker will give up and move on to another more vulnerable target. In this light, many people might think of multiple layers of technology such as firewalls, networks, host and network intrusion detection systems, bastion hosts, and so on that would comprise this defense of depth. However, we know based on published surveys and analyses that the biggest threat to our technology environment is often ourselves.

> Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with enterprise-wide information security.
In addition, human error is often the root cause of problems in some of the most sophisticated technological implementations. This is why security awareness in your company is so critical.²

Security apathy and ignorance are the biggest threats to computer systems. . . . And the best way to achieve a significant and lasting improvement in computer security is not by throwing more technical solutions at the problem – it’s by raising awareness and training and educating all computer users in the basics of computer security.³

Too often awareness campaigns are run by people who are incompetent. They are incompetent not because they are fools or are lazy – incompetence occurs when you step outside the envelope of your own capability. I am an incompetent flute player but a competent guitarist. I was a competent (although never skilful) rugby player, but remain absolutely useless at golf.

Awareness for most information security practitioners is that small part of information security practice that they feel they have to do because someone has told them it’s worthwhile – and anyway, BS 7799 says they should do it. So the temptation is to try and run a campaign using your own current skills – and incompetence strikes.

This book aims at reducing your incompetence gap. Perhaps the most chilling quotation comes from the notorious convicted hacker Kevin Mitnick:

... the human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted, because none of these measures address the weakest link in the security chain.

Kevin Mitnick – hacker

You only have to read Mitnick’s material on ‘social engineering’ to understand fully what he means.

---

THE RATIONALE FOR SECURITY AWARENESS

STATISTICS

Statistics on the number and percentage of security incidents generated from inside an organization suggest that internal users are responsible for at least around 70 per cent, and that most of these incidents are the result of user error, mishap and ignorance. The statistics have remained reasonably consistent over a number of years. Many of these incidents could have been prevented by improved understanding and by changes in attitude to information security. Losses from information security incidents have been estimated as being up to 3 per cent\textsuperscript{4} of corporate annual profit, the effect of substantially reducing them could be immense.

The UK Government Department of Trade and Industry (DTI) Information Security Breaches Survey 2004 makes five high-level recommendations, of which the second states:

*Integrate security into normal business practice, through a clear security policy and staff education.*

One of the key findings of the 2003 Computer Security Institute (CSI)/FBI Computer Crime and Security Survey was:

*As in previous years, virus incidents (82 per cent) and insider abuse of network access (80 per cent) were the most cited forms of attack or abuse.*

The CSI/FBI Survey also reckoned that the biggest costs were associated with viruses, laptop theft and Internet abuse. All of these issues can be addressed positively through sound education and awareness.

In recent years there has been a swing in various surveys towards external attack; the numbers seem to be indicating that external criminality is increasing. Much of this change has been due to the increase in Internet connectivity, and that it is now relatively easy to detect (although perhaps not so easy to prevent) events impacting on outward-facing computer systems. This will lead to increased numbers of detected incidents generated externally. Many of these are small scale, and only recorded because they were external, and because they are easy to detect. See the ‘Perception of Risk’ section in Chapter 1 to find out why these externally generated events are often seen as more important than internally generated ones.

The statistics further suggest that some 55–70 per cent of incidents are the result of insiders making mistakes – either through ignorance or stupidity. Bearing in mind the fact that some 2–3 per cent of profit is potentially lost due to information security incidents, the potential for making a significant contribution to your organization is very great.

It is important to remember that the most effective security countermeasure is a balance of controls. You need a sound technical infrastructure – that is undeniable. You need sound internal governance. You need appropriate measures to deal with Corporate Governance. You need workable internal processes to deal with new people joining your organization, just as you need sound processes for dealing with leavers. This notwithstanding, you need measures to reduce the number of errors, and to rectify the damage caused by the incurably stupid.

STANDARDS

There are a number of drivers (other than common sense and statistics) that make pursuing security awareness very worthwhile. These include a number of international standards, although there is no single specific public standard published at present that defines security awareness practice.

OECD

The Organization for Economic Co-operation and Development’s (OECD) Guidelines for the Security of Information Systems and Networks – Towards a culture of security published in 2002 outline a series of nine principles. Awareness is the first of the nine, which states:

1. **Awareness**

   Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

   Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control.

   They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be

---

aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

The other eight principles are:

2. **Responsibility** – All participants are responsible for the security of information systems and networks.

3. **Response** – Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

4. **Ethics** – Participants should respect the legitimate interests of others.

5. **Democracy** – The security of information systems and networks should be compatible with essential values of a democratic society.

6. **Risk assessment** – Participants should conduct risk assessments.

7. **Security design and implementation** – Participants should incorporate security as an essential element of information systems and networks.

8. **Security management** – Participants should adopt a comprehensive approach to security management.

9. **Reassessment** – Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

The emphasis on awareness (particularly as it is the first of the nine) is strong. The other principles are fundamental, and this enhances the OECD view that awareness is extremely important.

**Information Security Forum (ISF)**

The Information Security Forum (ISF) is a member-based organization that draws membership from large organizations across the world. Most of its work and output is retained for member use only, but it has decided to publish the Standard of Good Practice (SOGP), a thorough set of control statements for information security. The SOGP states the following (in section SM24 Security Awareness):

*Awareness of information security should be maintained via effective awareness programmes covering all individuals with access to*
information or systems within the enterprise. Employees (including contractors) should be provided with guidance to help them understand information security, the importance of complying with policies/standards and to be aware of their own personal responsibilities.

**Formal awareness programmes should be:**

- coordinated by a designated individual or group run using structured education/training programmes and specialized awareness material supported by top management;
- kept up to date with current practices;
- applied to all individuals with access to information or systems.

The level of awareness within the enterprise should be measured and reviewed periodically.

The SOGP also states:

**Education/training should be provided to all personnel with control over, or access to, the organization’s information and systems.** This should equip all personnel with the know-how required to assess security requirements, propose security controls and ensure controls function effectively.

**Education/training should also be provided to ensure that:**

- business users use systems correctly and apply security controls;
- IT staff develop systems in a disciplined manner and run installations or communications networks correctly;
- information security specialists understand the business, know how to run security projects and can communicate effectively.

**ISACA/COBIT**

COBIT (the Control Objectives for IT) from ISACA (Information Systems Audit and Control Association), have made awareness one of the six main guidelines of their control framework.

**ISO 13335**

Part Three of ISO/IEC TR 13335, a standard often referred to as GMITS (Guidance for the Management of IT Security), contains excellent guidance to a number of information security practices, including awareness.
BS 7799

The mostly widely used information security standard, BS 7799 says in Section 8.2.2:

> Information security awareness, education and training

> All employees and the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant to their job function.

The standard also states that such initiatives should be ongoing and suitable to the roles and responsibilities of the people concerned.

Summary of standards

All these extracts from these various standards make a clear point; security awareness is a fundamental requirement if one is to even contemplate meeting best practice. Given that many industries (financial services for example) are driven by regulation, and that this regulation strongly recommends adherence to standards, in many circumstances security awareness is a prescribed requirement.

The Financial Services Authority (FSA) in the UK has strongly suggested that certification to BS 7799 is seen as meeting many of their regulatory requirements that relate to information security.

PARALLEL ACTIVITIES

Awareness is not a panacea; panaceas for information security do not exist. To make awareness effective, it is a given that other parallel activities have to take place if you are to succeed. The most important of these include:

DESIGNING OUT ERROR

It makes sense to idiot-proof your systems and processes. Take for example the electric plug used in the UK. You can't insert it in the socket the wrong way round. This book does not teach you how to design out error – I can merely tell you that by doing so you reduce risk.
Designing out error should start with the obvious. I have heard it suggested that the act of performing standard risk analysis on any system reduces risk without any formal intervention or action by the security practitioner. This may seem improbable, but the fact remains that risk is reduced simply because the person interviewed as part of the analysis exercise realizes just where the yawning gaps are in their control infrastructure, and puts them right immediately as part of business as usual. These control improvements are initially invisible to the security folk. The improvements form part of designing out error.

A well-designed system is normally a more secure system. A process developed by a high quality project management regime incorporates better controls and security practice. This is often because sound project management includes a risk analysis phase and it often communicates with those people most likely to be affected by the project – the poor users of the resulting system. They are by far the best qualified to design a set of controls, and are more familiar with the real risks that affect their work.

TRAINING

If your people aren’t trained, it should come as no surprise if they make mistakes. If there’s one thing you can do to assist your operations staff it is good training. Let them know what they are to do, and let them know what’s expected of them. Very few people know what their responsibilities actually are. Good training reduces error. Good training improves security because it reduces the error count. If people know what’s expected of them, they’ll normally carry it out.

Chapter 4 contains extensive discussion and analysis on training and how it relates to security awareness. It is a powerful tool that you need to take account of when initiating an awareness programme.

TECHNICAL MATTERS

Information security grew out of the IT profession. Many practitioners have a technical background (although this is changing). This legacy has led to a distinct technical bias to the profession. When you rely on one single control (or type of control) you can become exposed to risks that are not covered (see ‘The Maginot Line Syndrome’ and ‘The Potato Syndrome’ overleaf).

---

6 Sometimes known as the ‘bleeding obvious’ by Basil Fawlty – the character played by John Cleese in *Fawlty Towers*. 
You need a strong technical infrastructure – populated with appropriate tools. At the time of going to press such tools might include (in no particular order):

- access control facilities
- anti-virus software
• browsing controls
• e-mail filters
• event logging and monitoring capability
• firewall deployment
• intrusion detection.

There will no doubt be additions to the above list. To make awareness effective, you need to make the most of your technical controls.

Therefore, you need a combination of things to survive, just as you need a balanced combination of controls to address information security issues. To rely totally on technical controls is foolhardy.

MANAGEMENT

A sound management structure is needed to implement information security effectively.

Management is a very broad subject, but let me place it in some form of context. The subjects need to be covered include:

• internal governance (policy, standards, procedures and so on)
• intelligence (management information, including event logs, monitoring information and suchlike)
• education, training and awareness (ETA)
• risk management (including project based risk analysis)
• audit and compliance.

Internal governance

Without the rulebook that is internal governance, you will find it extremely hard to operate, particularly in complex organizations. Figure 1.1 outlines the sort of policies most information security practitioners would expect to influence.

Not all the published documents are written in the same manner or in the same style. It is established wisdom that the higher documents (policy and sub-policies) are reviewed occasionally (perhaps six-monthly or annually), but due to their relatively generic nature, and the fact that they often have to
Figure 1.1  Policy and standards hierarchy
be periodically revisited and authorized by very busy people, they tend to be fairly static in content.

Other documents are much more volatile, and require revisiting on a more regular basis. This is especially so of documents that provide specific technical guidance (such as the baseline guides to the building of secure server platforms illustrated above), as they tend to change whenever new technical vulnerabilities are uncovered. This can occur more than once a day.

There are many other documents that need to be put in place in an operational environment. Many of these are low level, covering processes and procedures. These have been omitted from the diagram for the sake of clarity.

**Intelligence**

In order to maintain the ‘manage by fact’ principle (a concept expanded upon in Chapter 4), you need to make use of trustworthy intelligence. Such intelligence feeds come from:

- access control software
- conversations in the pub
- direct reports from co-workers
- firewall logs
- helpdesk event logs
- incident management procedures
- intrusion detection systems (IDS)
- system audit trails
- system control files.

Some security managers take multiple feeds and use them to create ‘dashboards’. These are reports that indicate the status of devices, processes, controls and so on, using a RAG (red, amber, green) marker. Such reporting concepts can be used either for compliance checking (for example, indicating whether devices are built to specified company standards), or for indicating event status.

---

7 Managing by fact is the opposite of what usually happens. Most people manage by ‘myth’, conjecture, bias and guesswork.
If your security management information is missing or untrustworthy, you will not be able to provide reasonable assurance that your company is meeting policy, and thereby failing to reduce the potential for harm.

**Risk management**

Risk management means the practice of identifying, qualifying and controlling information risk as it affects an organization.

The process normally involves a practice called ‘risk analysis’; a formal process that often makes use of commercial methodologies (such as CRAMM, the UK Government approved method). There are others, including SARA/Sprint (from the Information Security Forum). The methods are built around a series of steps that include:

- **impact analysis** – calculation of the effects of an incident. This is normally expressed, but not in every case, in financial terms;
- **risk assessment** – estimation of the likelihood of an incident;
- **control selection** – a process to meet risks by avoiding, minimising, accepting or transferring them. Transferring risk normally involves the purchasing of appropriate insurance.

Risk analysis can also be less rigid, and use informal methods. What is clear is that these processes help practitioners focus on those potential events that are likely to cause the biggest problems. If you are not performing some form of risk management, your awareness initiatives will be considerably less effective. Risk analysis can be project based or part of an established systems development lifecycle (SDLC).

**Audit and compliance**

If your organization does not have a solid audit and compliance regime, awareness will be less effective.

**SUMMARY**

This book is not designed to help you become an all-round information security manager. That is why the previous few sections have been brief, and the list of potential parallel activities is probably incomplete. However, without them, security awareness would be much less effective. One of the main elements of a control infrastructure is balance. Too much emphasis on a single element and you’re likely to face a problem.
**HOW IDIOTIC?**

A considerable percentage of security incidents are down to errors. Many of these errors are a result of ignorance, which should normally be addressed by training. Other errors are simply down to stupidity. These can be addressed by such practices as designing out errors, but many cannot be legislated for. The ‘Piltdown Man Syndrome’ section below illustrates how human foibles can cause people to make big mistakes.

**PILTDOWN MAN SYNDROME**

The now mythic Piltdown Man is one of the most famous frauds in the history of palaeontology. In 1912 Charles Dawson discovered an apparently hominid skull and related jawbone in a quarry near Piltdown, Sussex, England. For many years palaeontologists had assumed the existence of a human ancestor who linked modern humans with more primitive ape-like relations. Finding this ‘missing link’ became the stated goal of many field palaeontologists. The bones unearthed by Dawson appeared to be the expected missing link, a mixture of human and ape, with the noble brow of *Homo sapiens* and a primitive jaw.

As with most scientific breakthroughs, you have to consider context and perspective. In 1912, the UK and Germany were locked in a terrifying arms race. Rivalry in all fields was huge, and any opportunity to beat and belittle the other was taken. In human palaeontology, the Germans had the upper hand. In 1856 the first Neanderthal fossil discovery was made in Germany. In the next 50 years finds were made in continental Europe and in Asia. Not in Britain. Given the animosity between Germany and the UK at the time, there was a perceived need for a British win. So, in 1912, the fossil remains of an ancient Pleistocene hominid found in the Piltdown quarries became fêted in London (although not in Paris or Berlin). During the years 1912 to 1915 the Piltdown quarries yielded (from the same stratified context) more skulls, a canine tooth, another jawbone, a tool carved from an elephant tusk, and fossil teeth from a number of Pleistocene animals.

Unsurprisingly, initial reaction to the finds was variable. British palaeontologists were enthusiastic; the French and American palaeontologists tended to be sceptical. The objectors held that the initial discoveries of a jawbone and skull were obviously from two different animals, and that their discovery together was simply an accident of placement. The report of the discovery of the second skull converted many of the sceptics; one accident of placement was plausible, two were not.
The hoax was revealed as a deliberate fraud as late as 1953 (41 years later)! The first skull was eventually dated as medieval, as was the second. The jawbone was from an orang-utan, whilst the other fossils were genuine, but from (probably) Tunisia, Malta and Central Africa. The bones had been deliberately aged using simple staining agents.

The fraud was successful because:

- the team finding the specimens had excellent credentials;
- some of the experts were incompetent;
- primitive analytical tools were used;
- the forgery was skilfully implemented;
- it matched what was expected from theory.

It is the final characteristic of this example that is important. When information, behaviour or evidence correspond to our expectations, we are likely to assume they are correct. Remember the old saying: ‘In any collection of data, the figure that is obviously correct, beyond all need of checking, is the mistake.’

Let’s relate this characteristic to information security.

SECURITY MANAGER’S ASSUMPTIONS

A former colleague who had a problem called me one day. An apparently deliberate attempt was being made to hack into his organization’s network. Initial analysis showed that at some point after a new user account was set up, an attempt was made to illegally access that user account. An automatic log record print out listed each of these illegal access attempts.

There was no geographic or chronological pattern to these attacks. Whoever was attacking knew exactly when a new user account was being set up, no matter where the user was based (it was a global network). Meetings were held, and no information was passed other than in neutral premises, avoiding the use of phones, mobiles, fax and e-mail. This clandestine approach was tiresome, inefficient but considered necessary. Still, the hacker ploughed on, testing the new accounts whenever they were created.

A very sophisticated sniffer device was placed on the network, tasked with looking for unauthorized devices. It was placed in a physically secure location,
without permission from anyone other than those involved in the project. A number of trips were taken to overseas locations, investigating rumours and checking out what were fruitless leads. There was no evidence, no joy and no luck.

Eventually, a test network was set up, remote from any external connection. This was to test the next generation of sniffers. As the system was populated with dummy user accounts, the hacker struck. The system log detected him trying to access the new dummy accounts. Given that the test network was in a single room, with no external connectivity, the hacker had to be something else. Just as the palaeontologists assessing the Piltdown Man finds had leaped on the missing link, the security managers had assumed that the alert log messages were genuine (because a classic hacking technique is to target new accounts, looking for default passwords and the like). They weren’t. There was a bug in the network operating system. It has since been corrected.

Stories of user stupidity are legion. I have heard of people folding a paper message in half prior to faxing it ‘to keep it safe’ – regardless of the fact that the recipient saw a facsimile of a blank folded sheet of paper.

**ATMs AND STUPIDITY**

Another example of stupidity involves a major UK retail bank. The incident happened at a time when ATMs (Automated Teller Machines) were extremely important to people who wanted to make large purchases. This was because credit card penetration was much lower than now, and the banks limited cheques to small amounts. Just about the only way to make purchases above £50 was to get cash out of the ATM.

The golden hour of 12:00 to 13:00 on Christmas Eve is the time when many men do their Christmas shopping. In this incident, such shoppers were out in force, and the ATM networks were taking a hammering. So much so that the operators in the computer room at the bank in question noticed that some devices (especially the customized computers used to check ATM user PINs) were beginning to hit capacity. These devices (often referred to as hardware security modules or HSMs) could, when being thrashed by massive throughput, start to heat up. In this incident, one (of three) was getting very warm, and was probably causing (or at least, likely to cause) a bottleneck, and could have reduced ATM service levels.

One operator had an idea. He had been working on a concept that is close to what is now known as ‘load balancing’. He decided that he could ease the
pressure on the HSMs by running a program that would balance the load between all three. He ran the program, and the whole system went down immediately, and remained down for six hours.

There are many lessons to be learned from this event, but the following year, the same person (who for reasons unknown had kept his job), when asked about the event, said ‘Yea. It was I. All I did was this….’ He then proceeded to do exactly the same thing, with the same results. He did not stay in the post long afterwards. You cannot legislate for this type of person, and you cannot legislate for a management system that allows operators to update live systems in such a way.

WHY DO ACCIDENTS HAPPEN?

My father always used to paraphrase Freud and tell me that ‘There’s no such thing as an accident.’ Freud’s interpretation of accidents is largely based on the premise that we subconsciously allow things to happen and consciously declare them to be accidental.

You may not be totally convinced by Freud, but there is no doubt that accidents are often the result of subconscious activity. There are myriad examples of people making mistakes even in circumstances designed to reduce the chances of error. Experts make errors all the time. Most transport accidents are due, in some degree or other, to driver or pilot error. If you think you would never allow your attention to waver in such circumstances, please consider the following question:

*Have you ever driven a car and arrived safely at your destination, and then realized that there were parts of the journey of which you have no memory whatsoever?*

Experienced drivers are ‘unconsciously competent’ which allows them to concentrate on other things (their tax bill, the song on the radio or last night’s curry) rather than the immediate process of driving a vehicle. It’s when you are in this state that accidents happen.

Norman F Dixon, Professor of Psychology, University College London suggests another reason we act irrationally and cause accidents is because our in-built survival mechanisms kick in, in situations for which they were not designed.
Information security awareness is a fundamental part of effective security management. It is not a panacea and requires competence and attention to be paid to a number of parallel activities. These include:

- empowering policies and standards;
- providing a sound technical infrastructure;
- helping ensure staff are competent in their main jobs;
- enabling an effective systems and process design environment.

People make mistakes and can sometimes be stupid. You have to recognize this rather than pretend it doesn't happen. This statement is neither malicious nor condescending – it is a statement of fact meant to make your task clearer. Once you recognize that we are all capable of making mistakes, you will be more able to try and help your organization avoid, reduce or transfer the impact of unwanted events.

**Survival Mechanisms Working Too Well**

In an aircraft crash the pilots became distracted by an important, but not necessarily fatal, event. A warning signal had triggered telling them that the aircraft’s front wheel had not locked itself into place for landing. The pilots spent some time trying to force the wheel down (even manually) and were so engrossed in the task that they failed to hear other alarms (such as the ground proximity alert). The plane crashed, killing all on board. The human survival mechanism that kicked in focuses nearly all attention on threatening situations. This is useful if confronted by a predator or an enemy, but actually is sometimes counterproductive in an aircraft cockpit. The pilots focused on the wheel lock alert, and in doing so actually blocked out other (more urgent) alerts.

The world is full of examples of people being presented with alarms and alerts, and ignoring them assuming that there’s been an alert error or malfunction. If your fire alarm keeps going off, it’s hard to persuade people to evacuate the building each time it does. At some point, there will be a real fire.
The majority of errors, security incidents and disasters have, as part of their foundation, an assumption. This assumption is normally a variant on ‘it’ll never happen to me’.

Remember that even the most experienced of professionals can make errors of epic proportions. Never assume that staff of great experience and competence cannot be subject to human foibles – they are and will continue to be.