

NOTICEBORED

Innovative information security awareness programs

Human factors in information security

White paper by Gary Hinson, IsecT Ltd.

Introduction

This paper lays out the case for managing the human side of information security just as carefully as the technical side. It is our contention that technological controls alone simply cannot deliver sufficient information security in practice, and awareness is *the* most cost-effective form of security control.

The problem with technology

Some organisations view "technical solutions" as the immediate answer to their information security problems. This attitude is promoted by several suppliers of - you guessed it - those very same "technical solutions". Security products such as firewalls, antivirus software, PKI systems and VPNs are very valuable weapons in the security manager's armoury, but there are severe drawbacks to a pure technological approach:

- Firstly, technology is fallible. Despite the best efforts of the software quality engineering movement, hackers, testers and users continue to find unchecked buffers, unexpected exceptions, backdoors and other gross vulnerabilities in commercial and in-house developed software. This problem is compounded by the complexity of modern IT systems. Organisations that employ multi-layered security have the right idea but we find it extremely hard to believe that every layer of armour is near perfect. Worse still, ever since mediaeval days, attackers have been known to bypass castle defences by taking an alternative approach. This kind of attack definitely occurs on the web too.
- Secondly, very few organisations understand their information security problems in sufficient detail to ensure that they specify appropriate technical solutions. Typically, they recognise the need for standard information security packages (such as antivirus software) to address individual concerns, but seldom have they a comprehensive view of their requirements. They buy "plug and play" firewalls with no regard to monitoring the security alarms, updating attack signatures, or responding to new forms of network traffic. They virus-scan EMAILs but ignore JavaScript.
- Thirdly, the term "technical solution" usually implies significant expense. Bespoke security technology is particularly costly, whilst standard off-the-shelf packages are often sub-optimal and offer little competitive advantage.
- Lastly, someone invariably has to implement and operate the technology ... and this opens a massive can of worms. This paper considers the importance of the last aspect, the human element of information security.

Copyright © 2003 IsecT Ltd. All rights reserved.

NoticeBored is a service from IsecT Ltd.

1 The Coppers, Holmbury St. Mary, Dorking, Surrey RH5 6LQ

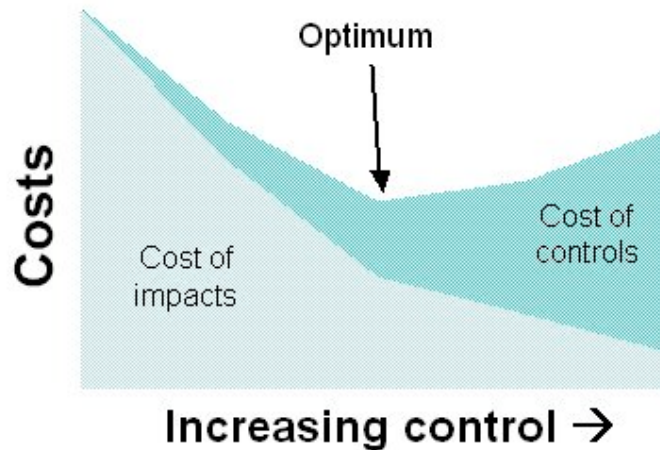
Registered in England № 4476358

www.IsecT.com and www.NoticeBored.com

Tel: +44 1306 731 770 EMAIL: info@NoticeBored.com

Optimising control investment

Organizations with limited or ineffective security controls suffer relatively more information security breaches and higher losses than their peers with better controls. However, beyond a certain point, procuring and running additional controls becomes more costly than the security breaches you are seeking to avoid. This is shown diagrammatically below:



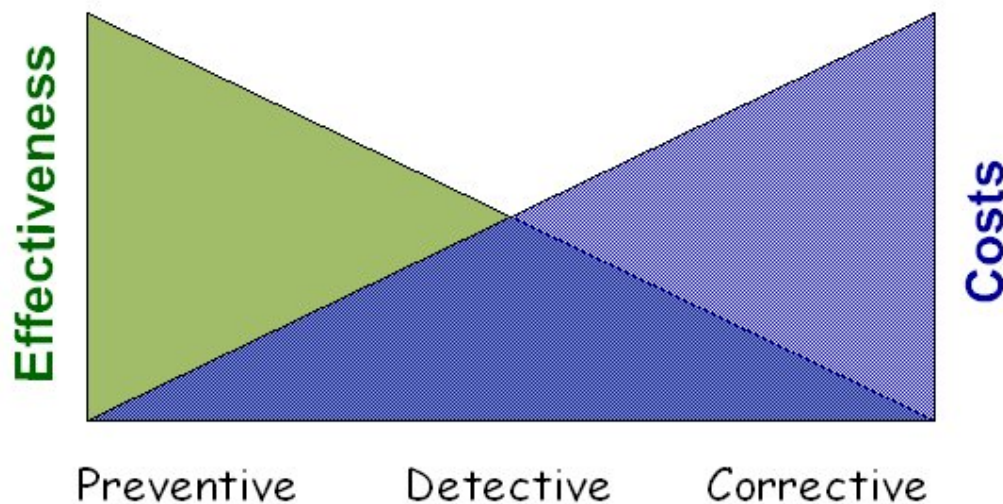
Although the problem of finding the optimum level of control investment is not directly solved by this graph, wherever we are on the graph, we clearly should not invest in additional controls unless we are convinced they are truly cost-effective *i.e.* the new controls cost less than the impacts they address. This then begs the question: which controls are cost-effective?

Cost-effective controls

Implementing additional controls has several associated costs, some of which are obvious and easily measured but many remain hidden and/or unmeasured:

1. There is usually a price to pay up-front when we purchase something, whether that is a product (such as a firewall) or a service (such as security management). The purchase price can be one-off (an invoiced charge) or periodic (*e.g.* license fees, maintenance). However, there are hidden costs to procurement, including the effort required to identify the requirement, select suitable products/services and complete the purchase transactions. The internal costs are generally absorbed largely by the Procurement function as an overhead across all purchases.
2. Controls have to be implemented and managed. In this case, the internal man-hours and change management costs can be more significant. Complex technical controls such as intrusion detection systems, for example, are relatively expensive to implement properly and may well be packaged up into an implementation project (investment).
3. There are costs associated with using/operating the controls. A trivial example concerns password-protected screensavers: users can no longer return to a dormant PC and just carry on working until they have unlocked the screensaver with a password, which causes slight delays and inconvenience. Someone has presumably made the value judgement that the accumulating delays and inconvenience are less costly than the breaches that might otherwise occur by unauthorized network access to non-password-protected dormant PCs. The operating costs are seldom calculated or tracked.

Secondly, we recognize that costs and effectiveness vary according to the types of control:



This diagram demonstrates the old adage “Prevention is better than cure”. As a general rule, controls designed to prevent breaches from ever occurring are more cost-effective than those designed to identify and/or correct breaches after the fact - the main reason being that preventive controls reduce or eliminate the impact costs. However, we acknowledge that no controls are perfectly effective, so there is still a need to invest in detective and corrective controls to contain the costs of breaches.

When considering investment in information security controls, there is one more factor to consider: should we invest in technology, processes or both? It is our firm belief that organizations need to work on both aspects. Anyone who believes they can simply install a technical control out-of-the-box and ignore the manual processes to configure, manage and operate it correctly is deluded. It seems to us that technology and people are complementary not alternatives.

Human factors

Thinking personally, have you ever entered a value in the wrong field on a form, or put the decimal point in the wrong place? Deleted the wrong file by mistake? Pulled out the wrong plug? Simple mistakes like this are so commonplace, we mostly just accept them as inevitable and do our best to spot and correct the problems before it is too late. In the context of information security, simple configuration mistakes can leave network ports open, firewalls vulnerable and systems completely unprotected. We contend that human error is far more likely to cause serious security breaches than technical vulnerabilities.

One could even argue that technical flaws are themselves the product of human errors: do you remember the case of the radiotherapy machine that delivered ten-times the stated dose? This was traced to an obscure bug in the program that somehow escaped rigorous testing. Human beings were to blame for the machine’s faults.

There is a field of science called "human factors engineering" that seeks to address the problem. In some cases (e.g. power station control systems), 'pressing the wrong key' can have such disastrous effects on safety that special controls are required to reduce the risk. There are system interlocks, dual controls and automatic programmed responses. Whole banks of monitors keep a constant check on the systems and their operators, and respond dynamically to alarm conditions. Safety-critical systems such as these are designed, developed, tested, operated and maintained with human safety very much in mind ... and yet mistakes still occur. Power station operators sometimes press the wrong buttons, shut down the wrong systems and cause safety incidents. Sports car drivers sometimes turn off their sophisticated traction control systems to 'have more fun', and occasionally exceed the capabilities of the anti-skid braking systems.

On another tack, Kevin Mitnick has demonstrated just how easy it is to persuade naive helpdesk staff to give out sensitive information over the phone to complete strangers. Users choose weak

passwords and resent having to change them regularly. They share IDs. They forget their smartcards. Whilst system controls can sometimes help (e.g. enforcing long alphanumeric passwords), users still have to play their part (e.g. not using simple keyboard patterns).

In a nutshell, information security is **both** a human **and** a technological problem.

Assessing the problem

Let's say you are serious about information security, and your organization is broadly keeping up with best practice. You probably have an information security manager, possibly even a small team. Management has endorsed a set of information security policies and standards. Your systems require strong passwords, maybe even smartcards and PKI, and users have guidance on choosing good passwords. You've installed good firewalls and comprehensive antivirus software. Your organisation might even be considering ISO17799 certification. The question is: how secure are you? Let's break this down a bit further:

- How competent is your information security management team? Are they technically qualified and experienced at managing information security? Do they have the respect of technical staff, management and staff in general? Are they given sufficient resources to do the job well?
- To what extent do management support the organization's information security policies, objectives and controls? Are security breaches routinely reported up the line, trends monitored and serious incidents investigated further? When was the last time a senior manager specifically referred to information security in a staff presentation?
- Do all your staff understand and follow the information policies and standards rigorously? Do the policies and standards cover all the organisation's information security requirements comprehensively? Are they up to date? Do new starters and temporary workers follow the same rules?
- Do users understand the need to choose strong passwords, keep them secret, and change them often? Does anyone actually check that they follow the guidance? What about all your other policies, standards and management edicts? Oh and don't forget the industry regulations and laws!
- Do the staff who configure and maintain the servers, firewalls, antivirus software *etc.* keep up to date with the latest threats, vulnerabilities and impacts on all the systems (including desktops, portables and network devices)? Do they routinely implement vendor-released security patches as a matter of urgency? Do they test the security of new releases before implementing them on the production network? Does anyone independently check that the systems remain secure, and if so how thoroughly and how often?

These questions relate concern the people rather than the technology. Sure, it's important to implement strong firewalls, but given that most commercially available firewalls are reasonably competent, isn't it more important to be sure they are properly configured, monitored and maintained - by the people? The same argument applies to antivirus protection, PKI and all the other security technologies. Despite what the vendors may say or imply in their marketing bumph, none of them are really "plus and play" or "fire and forget" - they all need to be properly configured and actively managed to keep up with the continuously-evolving threats.

Computers alone don't implement information security policies and standards - human beings purchase and configure the systems, switch on the control functions, monitor the alarms and run them. Whatever way you look at the problem, it is just as important to invest in your people as your technology.

Proactive risk management

We've seen in the previous section that asking "How secure are you?" raises a load of supplementary questions about the security of your technology and people. Most organisations assess their technology for information security risks, typically by evaluating new products and periodically testing the systems (e.g. pre-release testing and regular network vulnerability scans). In our experience, however, very few make a serious attempt to assess risks relating to their employees.

In risk management terms, people create threats, vulnerabilities and impacts:

- Staff or outsiders who deliberately try to breach system controls are clearly threats - typical examples are fraudsters, hackers and virus authors. Careless, slapdash and incompetent staff are another form of threat as they inject garbage data into your systems and cause damage, but even diligent and careful staff sometimes make mistakes.
- Staff who choose weak passwords, share user IDs, give out sensitive information *etc.* create vulnerabilities that may be exploited by others. Managers that don't bother to check the details before authorising expenses claims create another form of systematic vulnerability. There are many more real-life examples.
- Information security breaches cause human as well as organisational impacts. Staff naturally tend to distrust systems that often produce meaningless data, even if those data errors are the result of data entry mistakes by users. They resent the effort required to choose and remember good passwords, and try to follow simple patterns. Information security managers lose respect, and may even lose their jobs, if the organisation suffers serious information security breaches.

You need to check that your staff understand and follow policies ... that management authorisation processes are being followed correctly ... that helpdesk staff don't give out passwords ... that security patches are checked and applied consistently ...

Conclusion

If you are serious about information security, you *must* tackle the human factors as well as the technology. Proactively managing the risks involves assessing and reassessing all the threats, vulnerabilities and impacts and successively improving controls. This is not a one-off 'fire and forget' operation, just to get your '7799 certificate or whatever. Information security is an ongoing management process. Make sure your people get on board and stay on board.

Further information

The [NoticeBored](#) service delivers high-quality creative materials for corporate awareness programs, covering a different information security topic every month. [Contact us](#) to find out how NoticeBored specifically addresses the human elements of information security, and why we target end-users, executive managers and technologists.