

Why take a pro-active holistic approach to Information Security

Information is the lifeblood of organizations, a vital business asset in today's IT-enabled world. IT systems and networks link every internal department and connect us with a myriad of suppliers, partners and markets. Access to high-quality, complete, accurate and up-to-date information makes managerial decision-making relatively easy by reducing the margin for error. This begs the question: how do we guarantee access to high-quality information? The answer: (1) we design and build information systems that are effective at gathering, analyzing and outputting the information we need. And (2) we secure our information systems against risks to their confidentiality, integrity and availability of information.

Protecting and enhancing the value of our information and IT systems has become a central objective in most businesses, second only to making profits. Information security is not just a simple matter of having usernames and passwords. Regulations such as Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, Basel II, Sarbanes Oxley Act and privacy/data protection laws impose a raft of obligations on us. Viruses, worms and hackers assault us on all sides.

Richard Menta, writing in Scmagazine (July 2005), commented on 'recent research of the top 350 UK companies listed on the Financial Times': "Four out of five investors indicated that a significant breach in security would have a major impact on share price. Two thirds said it would influence a decision to buy or sell shares. Nearly nine in ten expected board members to be aware of, and to be able to review, their company's infosec vulnerabilities, and 57 percent thought they should know about the company's information risk strategy"

Why technical security controls alone are insufficient

Many companies have invested in firewalls, antivirus systems and other security technology. Every one of those products was no doubt sold to them on the basis of its effectiveness but they still suffer severe information security breaches and the problems are getting worse, not better. What's going wrong? The answer according to Gartner (World's leading provider of research and analysis) is that "80% of unplanned downtime is due to people and processes." COSO makes the point that "Internal control is effected by people. It's not merely policy manuals and forms, but people at every level of an organization".

In May 2005, Verisign found that the majority of people asked were willing to reveal their passwords for a \$3 Starbucks coffee token. "According to the company, one executive who was too busy to respond to questions but still wanted a gift card sent his administrative assistant back to complete the survey. The assistant promptly revealed both the executive's password and her own." The survey team had no obvious/legal way to verify the passwords (which is presumably why this was labeled a "light-hearted and unscientific survey") but the take-home message in terms of a general disregard for information security is pretty clear. [A similar survey in 2004 (Ref: <http://news.bbc.co.uk/1/hi/technology/3639679.stm>) used chocolate bars to bribe people out of their passwords.

The value of and need for security awareness

The phrase 'To err is human ...' encapsulates a fundamental difference between people and computers. People often make mistakes, are sometimes lazy, forgetful or inattentive, and often misunderstand complex situations. We seek shortcuts to avoid boring, repetitive tasks and may cheat, bend or break the rules to get things done. Even perfectionists occasionally settle on being good enough. We react emotionally, sometimes irrationally. Computers, in contrast, slavishly and precisely follow logical program instructions. Boredom is not a factor - computers simply take longer to process more data or resolve more complicated problems. If we are to improve information security, we must take these fundamental differences into account. We need to think holistically: 'systems' are not just the computers but include the users and administrators plus the management and operational processes. ***"Errors are caused by faulty systems, processes and conditions that lead people to make mistakes or fail to prevent them."***

Ref: <http://www.iom.edu/Object.File/Master/4/117/0.pdf>

It is pointless to put stronger and stronger links in our security chain unless we address the weakest links. Technology alone is clearly not enough to ensure information security: it has to be implemented and managed professionally and of course it has to be used properly. The problem lies not so much with technology itself but with the people and processes in the organization. General staff, technologists and managers must actually use the security controls properly in order for them to be effective. People and processes are the weakest links. Until we measure and improve security awareness, this will inevitably remain true.

"Security is a Process not a Product"

~Bruce Schneier~

In 1993, Michel Kabay published a paper called "Social Psychology and Infosec" (ref: <http://catless.ncl.ac.uk/Risks/15.16.html>) exploring the psychological reasons why conventional approaches to security awareness are ineffective. Many companies lend merely lip service to the idea of security." Amongst Mich's conclusions were the following points:

- Presenting case-studies is likely to have a beneficial effect on participants' readiness to examine security requirements.
- Security awareness programs should include many realistic examples of security requirements and breaches.
- We must inspire a commitment to security rather than merely describing it.
- Emphasize improvements rather than reduction of failure.
- Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.
- Identify the senior executives most likely to succeed in setting a positive tone for subsequent security training.
- Security awareness programs should include repeated novel reminders of security issues.
- Build a corporate culture which rewards responsible behaviour such as reporting security violations.
- Develop clearly written security policies and procedures.

- Encourage social activities in the office ... Pay special attention to social outliers during instruction programs ... Work with the outliers to resist the herd's anti-security bias.
- Include small gifts in your security awareness program.
- Start improving security a little at a time and work up to more intrusive procedures.
- Bring in experts from the outside when faced with groupthink.

Total Information Security is now becoming a federal mandate

NIST Special Publication SP 800-53 recommend security controls for federal systems says "An effective information security program should include ... security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks". The draft NIST FIPS 200 published for comments in July 2005, notes: "Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. "

Conclusion:

With identity theft and system breaches spinning out of control, and so many respondents concerned with the lack of security and employee awareness, it is troubling that only 65% of organizations have trained their employees on how to identify and report suspicious behavior" Ref: Deloitte 2005 Global Security Survey.

Information security places a heavy emphasis on the judgment of individuals at all levels. However, uninformed judgment, even in the presence of genius or intuition, is no substitute for accurate and timely information about the threats that an organization faces.

Alastair Morrison (CEO of Kroll International Security) stated:

"If I were a terrorist or criminal who wanted to disrupt or steal from your company. I would look at your vulnerability through your staff."

So let's revisit the original question:

Why take a pro-active holistic approach to Information Security ?

Because if your information is not safe, your future and your business is in jeopardy.

"We must inspire a commitment to security rather than merely describing it"

~Mitch Kaybay~