



The IT Security Buck Stops Here

Sue Bushell, CIO

10/05/2004 11:58:31

<http://cio.idg.com.au/index.php?id=18384495>

Need to convince corporate leaders with objective measures of security's value? Start here.

US President Harry S Truman said in his farewell address in 1953: "The President has to decide. He can't pass the buck to anyone." Now that's an adage all executives might consider carving into their desks (if not their very souls) as the torrent of cyber attacks continues to highlight corporate vulnerability to IT security threats.

The days when executives could profess ignorance and happily pass all responsibility for security to their IT professionals are long gone. No executive can fail to be aware of the mounting toll data theft, virus and worm attacks and other security intrusions are taking on corporations struggling to keep up with the army of cyber villains intent on exploiting their technical knowledge to inflict maximum damage whenever and wherever they can.

In 2003 alone, the Australian Computer Crime and Security (AusCERT) Survey shows, 42 percent of corporations fell victim to one or more computer attacks that harmed the confidentiality, integrity or availability of network data and systems. Financial fraud, laptop theft and virus, worm and Trojan infections caused real losses, yet a dismal 11 percent of respondents felt they were managing all computer security issues reasonably well. This should worry those at the top, since all executives could find themselves potentially liable in the event of a catastrophic security breach.

Experts warn that increasingly, executives must consider themselves chief information security officers, and recognize that as with any other cause of business disruption, if IT security adversely interrupts business it is, ultimately at least, their responsibility.

Following are some of the things all executives must know, and some questions they all must ask.

You Are Where the Buck Stops

While no court in the land is likely to find you personally liable should your corporation choose the wrong firewall, liability for IT security is governed by precisely the same sorts of principles that govern individual liability of directors and officers for any failure to carry out their duty. It might take a significant failing in your duty to act in the interests of shareholders under sections 180 and 181 of the Corporations Act for you to be found culpable, says Sydney-based IT lawyer Chris Wood, but the risk is always present.

"IT security is a significant enough problem for business that if executives completely ignored it, they'd leave themselves exposed to claims by shareholders," Wood says. "In an extreme case of neglecting the issue of IT security, directors could have an exposure personally, because it might be said that they have gone so far down the track in breaching their duty to the shareholders that they create a personal liability."

Taking responsibility means being prepared to talk frankly to customers about any attack. In the US, the new California Cyber Security Law requires any corporation suffering a cyber attack to notify their customers, and other states in the US are looking at implementing similar laws. Likewise, says Invisus president James Harrison, new US federal laws regulating certain industries, including health-care and banking and finance, impose similar requirements. Not only must any Australian company eager to do business in the US take note, Australian law is likely eventually to follow suit.

Australian firms that choose voluntarily to ensure their security practices conform to the growing international standard ISO-17799 will have an easier time doing business abroad.

You need to make security an everyday part of IT, from daily operations, through design and architecture, policies, practices, configurations, event tracking and response, to training awareness and to driving improved risk-based metrics. Your entire management team must recognize that information is not just an IT matter, but a business matter, and therefore each business unit owner must understand how they contribute to the overall success of information security through simple, easy to implement security practices that benefit the company overall, says TrueSecure Asia Pacific vice president of operations Philip Dewar.

Information Security Is a Business Success Issue

Information security is all about managing and mitigating risk. What level of risk am I willing to accept? How do I avoid being compromised? What procedures do I have to reduce risk if I am compromised?

“Every executive needs to understand that information security should be addressed with risk-based thinking with exactly the same logic and methods that are used by executives every day to make financial, acquisition, launch, merger and other ‘non-security’ decisions,” Dewar says. “Unfortunately most technologists’ and security professionals’ thinking and activities tend to be reactive, tactical, binary, single computer-focused, and vulnerability-oriented.”

Executives must drive their organization’s information security programs to become information risk management programs where thinking and activities are proactive, strategic, synergistic, organization-focused and risk-oriented.

“A lot of the industry still talks about security as if it was a technology problem: put the right technology in place and your problems will go away,” says Darrell Ryman, technology fellow Asia Pacific for Avanade. “What people tend to forget is that the technology is just an enabler to solving a business problem. Processes and the people using them are what usually achieve results. This philosophy is applicable to everything we do. Rather than thinking that technology is going to solve the whole problem, you need to integrate technology to assist the people and processes to achieve the intended results.”

According to Ryman, you should think of security the way you think about insurance. People buy insurance for life, business, estate and assets. Information security is about buying insurance for your information systems. People also update their insurance policies to cover for changes. It is just as important to update and maintain information security as it is to update your insurance policy.

There is a very defined and very clear process you need to go through to ensure you remain aware of what your business is doing and how, and your risk exposure.

“I would suggest that everybody needs to do a security review of the technology every quarter, and from a business risk analysis they would want to do a security review of business process every year, as a baseline,” says BearingPoint head of managed services Bob Hay. “A lot of organizations clearly do not do that. And that clearly allows them to be somewhat more exposed, if there is in fact a business risk in the way that they are doing business.”

With so many organizations online and doing electronic processing in financial systems, that security profile should include a data classification that identifies what data is important to the business, what needs to be preserved, what events stand to damage that information, how sensitive information is to competitors and others, and what you need to do to preserve your business in the event of a catastrophic failure or an event that causes some damage to that environment or that data.

Mike Higgins, managing director of the Technology Risk Management Practice for Tekmark Global Solutions, poses some useful questions. When was the last independent assessment? What were the findings and how are they being addressed? When was the last IT security review of operations policy for the firm? How and who decides how new technologies are integrated into the business environment and why? What kind of training is the IT security staff attending each year?

“These questions, especially the training, will tell the executive how robust an IT Security program he or she has. Is it integrated into the business operations or is it merely a box checker?” Higgins says.

It’s the People, Stupid

A recent survey by the Computing Technology Industry Association (CompTIA) found almost a third of all the respondents indicated they had at least one to three major security breaches in the past six months, with human error the most likely cause. Some 80 percent of respondents believed this human error was caused by a lack of security knowledge, training or failure to follow security procedures.

Some 96 percent of those surveyed recommended security training for their IT staff and 73 percent recommended comprehensive security certification. Yet a staggering 69 percent of companies have trained less than a quarter of their IT staff in security-related issues, and 22 percent have trained none of their IT employees on security, even though 66 percent believe that training certification has improved their IT security by raising awareness and causing risks to be proactively identified.

These are mere statistics, certainly, but they give a clear direction: one focus should be to concentrate on the human side of security. Find out how many of your people have security certification that proves they have a minimal foundational knowledge of what IT security is all about.

“If you don’t have the right person, from a pure knowledge standpoint, behind the wheel, you’re not going to get to that destination, and that’s the most telling thing that I think that every executive needs to be looking at if they’re serious about implementing an IT security program within their organization,” says CompTIA COO Brian McCarthy.

Security is an ongoing process, not a one-time event. With new threats evolving every day, perhaps the most vital defence is to train staff effectively in how to watch out for certain threats, or to protect against threats. This training must be updated at least every six months.

“Part of an executive’s job is to make sure that everybody in their organization is aware of all the new threats and how to defend themselves against them,” Invisus’s Harrison says.

One of the biggest security threats comes from social engineering, the deliberate attempt to manipulate authorized users into helping you gain access to systems protected by IDs and passwords. One of the easiest ways for a hacker to find their way into a corporate network is to phone an employee pretending to be a systems technician and ask for their system password.

Social engineering works because most people in any computing environment are insufficiently aware or knowledgeable of IT security. You need to make sure everybody in your organization is aware of all the new threats

and how to defend themselves against them. How many of your people would know if they were being socially engineered? Are there training programs in place to alert them to the risks?

Ask Me No Questions (and you could end up in deep doo-doo)

In understanding risk, Ryman says, you also need to understand the impact of a compromise. What level of compromise is the business willing to accept? He says areas to focus on include:

- Assets, both IT and non-IT and possible vulnerabilities
- Potential threat vectors and the chance of using a threat vector to compromise an asset
- The cost of a security breach
- Is there a business continuity plan in place? If so, how often is the plan updated? Moreover has the plan been tested? (Usually they are never tested.)

According to Dewar, you must also be aware of what is being done to incorporate information security into the culture of the organization to ensure that there are effective practices and processes in place to expand the hardware security controls and act as contingency safeguards for the areas where unanticipated security failures will occur. For example, everyone in the organization needs to understand the risk to the company of unsanctioned technologies.

Dewar says you should also ask:

- ~~///~~ How do we know how much value each security purchase, decision, activity, configuration et cetera brings to the organization?
- ~~///~~ Which exact risk is improved by performing a given activity, with a given policy or purchase?
- ~~///~~ How can we reduce both the risk and the cost of our security activities?
- ~~///~~ How can we use simpler and less expensive and less intrusive countermeasures and controls together in a way that both reduces total costs and more reliably and extensively reduces risk?
- ~~///~~ How can we efficiently get the right security information to the right IT employee in the right time frame so they have time to plan and time to be strategic, and have minimal interruptions and emergencies?
- ~~///~~ How are we evaluating our information security through a continuous program to keep us informed and current, and helping us be proactive in a pragmatic and holistic approach?
- ~~///~~ How are we measuring the effectiveness of our risk management program?
- ~~///~~ How does our information security measure up against regulatory standards, against other companies, and are we being efficient and effective in our efforts?

Good Security Starts with Good Policy

Information security policies underpin the security and wellbeing of information resources, and should be considered the bottom line of information security within an organization.

Yet CompTIA found less than half of organizations have a comprehensive written IT policy, even where they have experienced an unauthorized user security breach. And 7 percent of those with a written policy in place say it is “never” updated by C-Level, director or equivalent level staff.

“Even in my own organization when I look at my responsibility, I think the general executive needs to be asking of their IT security policy, do they have a written IT security policy in place — a comprehensive plan,” CompTIA’s McCarthy says.

A comprehensive security policy can act as an action plan when an attack takes place, Harrison says. “What does each employee at every level of the company do when a new virus or worm has attacked the company? How do you alert everybody in the company? When MyDoom came out, how did every person who was using a computer in that company become aware of MyDoom and what were they told to do to prevent being attacked themselves?”

The security policy should cover both technical and procedural matters, and be robust enough to ensure that the instant the organization comes under attack the action plan kicks into place, warnings and alerts are pushed out, and personnel with identified responsibilities for security begin following well-defined procedures. “Those are some of the simple things when you’re attacked: How to recover from it, and how to move on quickly,” Harrison says.

The policy should also spell out procedures for notifying customers of the attack or security breach.

Passwords Won’t Do It

One critical piece of information that every executive needs to know about information security is that the cost-effectiveness and protection provided by password-based networks are decreasing, says Zvetco Biometrics founder and CEO Zavi Cohen.

“Passwords are easily lost or deciphered, and there is significant cost associated with password maintenance. According to the US IT research firm Aberdeen Group, the labour costs for configuring and maintaining password systems range anywhere from \$US100 to \$350 per user per year, depending upon company size,” Cohen says.

This has given rise to a new class of network logon devices that use biometrics — human characteristics such as fingerprint authentication, optical scanning and voice recognition — to secure physical and network access in the workplace. In 2002 and 2003, revenue for biometric technologies grew more than 50 percent, to \$US928 million, and is expected to continue at this pace with annual revenues forecast to exceed \$US4 billion by 2007. Desktop fingerprint authentication readers are the most common type of biometric device used for network security, accounting for more than 60 percent of the market.

Outsourcing Adds Risk, Opportunity

One of the newer security risks to Australian companies is the outsourcing of business operations, warns Tom Patterson, a partner emeritus (Security Services) at Deloitte Touche Tohmatsu Germany, whose new book, Mapping Security, is coming to bookstores later this year. “There needs to be an understanding that while you are outsourcing the processes, you still own the risks and responsibilities,” Patterson says.

“On the other side of the outsourcing coin, as some of the developing nations stumble with their own growth, Australia’s stable political environment, solid technology infrastructure, strong commitment to global security standards, and an educated English-speaking workforce will start to make it a preferred spot for co-location of globally outsourced operations.”

And that — if Australia's executives are canny enough to capitalize on the opportunity — could be very good for Australia's long-term security indeed. v

Test Your Security

A new tool created by CSO Magazine and the Software Engineering Institute's CERT Coordination Centre lets security professionals determine which practices are repeatable, documented, and regularly reviewed and updated — characteristics that enhance security strategy and policies. <http://www.csoonline.com/surveys/securitycapability.html>

Raising the Bar

It's time CEOs take information security seriously. IT CAN BE TOUGH to define what it means to be a global leader in quality, ethics, safety, or corporate security. Nevertheless, the lessons that companies have learned from seeking to improve their performance in any of these or other intangible business values will be applicable as companies seek to improve their corporate security. These include:

- ✍ Success requires a significant long-term commitment of resources from the organization. These resources include capital, people, training, time, and most importantly executive attention.
- ✍ The CEO cannot, on his or her own, ensure the success of the endeavour, but they can, by their lack of commitment to the process, personally ensure the failure of the process.
- ✍ As with the black belts in the Six-Sigma quality program, the leading organizations will be comprised of countless individual leaders within the company who drive the company forward. In the world-class organization, these leaders will be evangelical zealots for the cause.
- ✍ The tools of the continuous improvement process will be leveraged to move the organization forward. This means that progress will be measured, root cause analysis will be employed against failures, and benchmarking used to gauge success.
- ✍ There will be no absolute measures of success and the bar will continuously be moved. Peer organizations will continuously redefine world-class (as has happened in quality, customer service, and operational effectiveness) while the government and regulators will continuously redefine minimal acceptable standards (as has happened with environmental, health, and safety issues)."

Source: Extracted from "The Evolving Standard of Corporate Security" — Glen Hastings, Online Security