Sensible security

Good information security is about risk awareness as well as sensible investment in automated controls, as **Mark Story** explains.

Over the past 10 years, threats to corporate information security from identity theft, viruses, email and web threats, hacking tools or countless other data security breaches have exploded in both their volume and the degree of nastiness. Based on Symantec data, there were around 500,000 new malicious software, or malware, threats in 2007 alone.

In addition to limiting access to the network or host via firewalls, other information security technologies commonly deployed by organisations include content security, intrusion prevention, end-point security, access-in and access-out, and data loss prevention.

While the motivation behind security threats used to be more about hacker bragging rights, the endgame of today's security breaches is preoccupied with stealing specific intellectual property (IP) and re-selling it for profit.

Having witnessed heightened levels of security breaches, and the damage inflicted on corporate victims, notably offshore, most Australian companies are now spending proportionately more to protect themselves against potential attacks.

But as Rob Goldberg, Partner with KPMG points out, throwing money at the problem doesn't necessarily make companies any more secure. Despite the increased spend on security technology, he claims that most local firms still operate with an insufficient 'duty of care' regarding the protection of their IP.

Missing management link

Goldberg attributes the misuse of funds to a missing link that exists between IT and other business departments in an organisation. "Sadly, information security still lives primarily in the IT space, and the list of security requirements typically doesn't get developed with the same level of commitment from the other side of the organisation," says Goldberg.

The wider the alignment gap between IT and business objectives, he says, the more likely companies are to rely on vendor-based solutions. While these solutions will address glaring symptoms, Goldberg says they typically overlook the root cause of their information security problems.

Greg Murray, Rio Tinto's Vice President, Information Security, says that rather than blaming vendors for selling their wares, companies would be better served understanding risk. He cites recent studies that suggest Supervisory Control and Data Acquisition (SCADA) and process control networks could be vulnerable to attack.

"Companies that read these studies without actively reviewing their own internal environments might go out and spend big money on it, while the issue may only be specific to particular areas," says Murray.

Before companies can achieve this minimum duty of care, Murray says they need to answer three key questions: "What do our shareholders, customers, business partners and employees inherently expect us to do in terms of security?"; "Do we understand the security risks we face and their impact on our businesses?"; and, "Are our priorities, spending and resourcing sufficiently aligned to mitigate risk to an acceptable level?".

Before companies can answer these questions, Tim Smith, Director of IT security consultancy, Bridge Point Security, says they need to identify information that is important to the organisation. Only then can they work out how to categorise it according to its value and sensitivity.

Piecemeal compliance

According to Smith, it's only once they've addressed these key questions that organisations can establish the appropriate information security strategy. If the minuscule uptake (only 50 companies in Australia) of certification to information standard ISO27001 is any barometer, too few companies approach information security strategy development with anything closely resembling a scientific discipline.

To Smith's reckoning, no more than 10 per cent of Australian firms have adopted anything close to overarching frameworks like SABSA (Sherwood Applied Business Security Architecture), the IT enterprise architecture classification structure the Zachman framework, or similar, to develop strategy and process. In fairness, he says, while many organisations recognise ISO27001 as the benchmark for their information security framework, they have moved towards the compliance to the standard rather than formal certification.

While industry at large is progressing towards compliance standards for managing information security, some sectors, like banking, are mandated to report according to certain standards. For example, PCI, a payment card industry standard for merchants, dictates that credit card data must be encrypted.

Smith suspects around 60 per cent of firms have a loose correlation between information security strategy and technology. That's why they tend to cherry-pick systems they think will complement their needs. While these organisations are by no means immune to security threats, Smith says the even more ad hoc approach of the remaining 30-plus per cent of firms exposes them to information security risk.

According to Murray Goldschmidt, Security Consultant at Sense of Security, overarching frameworks should help companies put steps into place to mitigate risk exposures. Risk assessment, the first step, identifies the key technologies on the network the organisations couldn't function without, advises Goldschmidt.

Only when companies have done this, adds Goldschmidt, can they establish a strategic road map

»

IMAGES: ISTOCKPHOTO

for where the company needs to head over time, and the building blocks required to get them there.

Leading edge security

So what are the characteristics of leading-edge information security? To KPMG's Goldberg, it comes down to how well information security strategy is formulated based on how well the company knows what business it's in. Assuming it has been done properly, he says the company should be able to draw a straight line from its business strategy (aka its mission statement) to its information security policy.

What separates the strategic from the ad hoc approach, explains Bridge Point Security's Smith, is the ability to justify expenditure on security applications. He says, by validating these controls ahead of IT spend, companies can avoid allocating too much or too little. In other words, by drawing out the business requirements and extrapolating the technology needs, Smith says companies have got the justification for putting certain technology into place. "It may mean justifying why there's a dual firewall in an area of high availability," he says.

What surfaces within 80 per cent of the reviews conducted by Bridge Point Security is a lack of policy and procedure. The second overarching trap, advises Smith, is security considerations not being built into the technology during the development phase. He says it's not uncommon for 'go-live' dates to be severely delayed while technology is re-coded or re-written. "I've seen situations where a developer at the end of a build process has said: 'You didn't ask for security; who is going to pay for it?'."

Another failing, says Goldschmidt, is insufficiently defined best practice baselines for specific applications. He says this could include security guides for database servers, web servers, routers and firewalls. While the strategy should dictate that a network must be auditable, it's the process that stipulates how this is done, adds Goldschmidt.

Key security principles

According to Goldschmidt, the key outcome of information security is knowing how, when and why deployment has strayed from prescribed strategy.

"If you don't have strategy that mandates for regular compliance audits, you can't guarantee that the technology deployed will operate anywhere near optimal capacity," he says. "The goal is to reduce the unknown hidden spend."

As most companies have limited resources for information security, Goldschmidt recommends a back-to-basic-principles approach, with layers of security control so that there are multiple control points. "This could mean controls at network, operating system and application levels, which remain invisible to the end user."

Ultimately, Smith advises that the net effects of having security in line with risk and asset value are fewer breaches, knowing what assets to protect, and where technology spend should be made. MT

Mark Story is a freelance writer from Western Australia.

To take away

- money spent on security technology may be misused owing to an alignment gap between IT and business objectives
- a good security strategy starts with identifying what information is important to an organisation
- the net effect of having security equal to risk and asset value is knowing what's worth protecting and where technology spend should be made.

>> Patch management

According to Tim Smith, Director of IT security consultancy, Bridge Point Security, the greatest vulnerability trap most local organisations experience is due to insufficient patch management for either viruses, operating systems or other applications.

And even if there is adequate patch management, he says companies often overlook the more obvious risks, like putting an infected laptop back on the network after it has been used offsite. "Many companies also become too dependent on the person in charge of specific IT projects rather than implementing mandatory security controls," explains Smith.

Ironically, these traps aren't the domain of small business. Due to failures in security governance, Ohio's Davis-Besse nuclear power plant became infected by the Microsoft SQL Server 2000 worm in January 2003. This made the Plant's Safety Parameter Display System (SPDS) and process computer inoperable for several hours.

The primary cause was an unprotected high-speed T1 connection to the corporate network that was established by a contractor whose company's network allowed use of User Datagram Protocol for data transfer. A second cause of attack was the lack of awareness of a security patch released by Microsoft approximately six months earlier. A little scary.