

## Why security is a leader's problem

*Protecting the IT system and data is a key business issue.*

*So bosses who dismiss it as technical could be putting their companies in jeopardy*

*By Paul Bray – (from the Guardian Security Supplement – April 2011)*

If information security isn't firmly on your boardroom agenda or you think it's something that can safely be left to the technicians, watch out.

"The single biggest threat to most businesses is that they still fail to see information security as a business need that should be centrally funded and business focused rather than a series of largely technical fixes," says Mike Gillespie, managing director of security consultancy Advent IM.

"You're facing a broad business risk not a technology one and the head of risk or the chief operating officer should have ultimate responsibility," agrees Malcolm Marshall, head of information security services at consultancy KPMG.

There needs to be an open dialogue between business leaders and their security experts, says Mark Chaplin, spokesman for the Information Security Forum, a membership organisation for major ICT users. The chief security officer shouldn't wait for the board to ask about the risks of, say, cloud computing or consumerisation: they should go in and explain them.

On the other side, says Chaplin, business leaders need to listen to their security people and not just regard them as traffic wardens who hand out penalties for breaking the rules.

A new breed of security leaders with mainstream business experience is taking a much broader, risk management-based approach to information security, says Mike Maddison, head of security and resilience at consultancy Deloitte. Instead of concentrating on keeping the

technology infrastructure up and running, there's a shift towards looking at the intrinsic value of the information and focusing on protecting this rather than the systems that hold it.

Of course, protecting the data will also involve protecting the systems. But organisations need to define what their key data assets are – customer data, intellectual property, commercial information and so on – and where they are held before they can design a strategy to keep them safe. This, says Chaplin, means understanding the whole 'information lifecycle': when and where it's created, where it's stored (within the network perimeter or on portable devices), when it goes to the printer, when it's archived or deleted, and so on.

A vital element of good security planning, say the experts, is classic three-part risk analysis: what could go wrong, how likely this is, and how serious the consequences would be.

Information on the type and likelihood of threats can be gleaned from many sources, including media reports, trading partners, trade associations, professional bodies, government and the police.

"People used to undertake a risk assessment on a one- or two-year cycle but now the threat landscape changes so fast that every three months would be sensible," says Marshall.

The organisation also needs to listen to its own heartbeat, says Gillespie. Is it recording a greater level of attempted intrusions at the internet firewall? Is it about to make people redundant who might steal data or damage systems?

Risk assessment isn't intrinsically difficult, says Gillespie. But it's a mistake to let a single risk manager do the whole thing. Instead, line-of-business people should be asked about the risks in their areas and the consequences if a breach occurred. This also helps to get business stakeholders to buy into the whole security process.

Third party relationships should also be taken into account, say the experts, especially now that strategic outsourcing, smart sourcing and cloud computing may have sprayed the organisation's data around dozens or even hundreds of trading partners and their own supply chains.

"There's quite a high level of investment in data assurance programmes and in getting a more fundamental understanding of where the organisation's data is going and who its third party relationships are with," says Maddison. That could be the bike courier carrying a back-up tape as well as a smart-sourcing supplier on another continent.

Large organisations such as banks and telecomms are imposing contractual obligations on suppliers to follow specific data security procedures, says Marshall, sometimes backing this up with on-the-spot compliance checks and education programmes for the supplier's staff.

The aim of any information security strategy is ultimately to guarantee three things: confidentiality, integrity and availability. There's a tendency to associate security issues primarily with the first of these, especially since the most worrying trends this year relate to the co-ordinated theft of data and the risks of it being lost or stolen from portable devices.

But integrity – protecting data from loss or corruption – is equally important. Integrity can be compromised by events that may have nothing to do with malicious activity, such as fire, mechanical failure or human error, so contingency planning and business continuity should also be factored into the security strategy.

As for availability, the most common complaint of users is that information

security gets in their way. Sometimes it's simply irksome, but at its most extreme it may affect productivity or competitiveness – preventing someone from taking work home in the evening or emailing an urgent document requested by a client, for example.

Thus it's important to have a 'feedback loop' to assess the impact of security on the ground, says Anthony Robinson, UK security practice lead at consultancy Accenture. "An information security policy should be informed by the business strategy that says what the organisation wants to achieve and how it wants to operate."

It's one of the reasons why the policy should be owned by business risk experts who are used to balancing different needs within the business, he adds.

Beneath the overarching security strategy sit a whole slew of detailed policies and procedures: who can access what data, how often should passwords be changed, what data can be held on mobile devices, what emails should be encrypted, can staff discuss work problems on social media websites, and so on.

Like the security strategy, policy issues have as much to do with the needs and culture of the business as with technical measures. The ISO standards 27001 and 27002 are useful templates, although they need to be tailored to the individual organisation. Finally, there is the issue of incident management: what action to take if you do suffer a security breach. "Anyone who says they have very few security incidents is probably wrong," says Marshall. "So you need incident response teams who can quickly identify the root causes and secure systems as soon as possible. Organisations are building up their response capability."

Robinson adds: "If a member of staff knows there's been a breach or potential breach it's important they know who to tell." This could be because they've lost their smartphone, they've noticed a problem with some data, or even because they suspect a colleague of doing something wrong. The best security leaves nothing to chance.

## The Human Factor

A high proportion of information security incidents are caused by people within the organisation, usually because they've done something daft. It's a depressing statistic, but it does have a silver lining: it's within the organisation's power to put it right.

"The biggest return on any security investment comes from getting people to behave in the right way," says Malcolm Marshall, head of information security services at KPMG. This is partly because of the potential losses if they get things wrong, but also because technology can't protect you from everything. "It's no use having a security policy and not telling people it exists," says Mike Gillespie from security consultancy Advent IM, adding that you have to tell them in their own language, not technobabble. If they understand the reasons for changing passwords regularly or not copying data on to memory sticks, they'll be much more likely to toe the line. User education is vital. "High performance organisations have information security training as one of their assurance and compliance metrics," says Anthony Robinson, UK security practice lead at Accenture. He recommends users should receive training at least annually on issues such as appropriate use of data, how to secure their laptop and safe use of social networks. Such training can be brief, but it needs to be relevant and memorable, says Marshall. One plc even commissioned a set of short stories with security-related morals, like a modern-day Aesop's Fables. Another initiated a personal responsibilities programme, giving every staff member a list of 10-20 security responsibilities and confirming annually whether they could fulfil these or whether they need further training.

To gauge whether a security policy will work, says Professor Kevin Jones from the Centre for Software Reliability at City University, try asking two people: the CEO and their PA. If both can understand and follow it the rest of the organisation probably will, too. PAs can also make excellent departmental security champions who can help to identify risks, train colleagues and cajole them into compliance.

A major issue is having a policy but not policing it, says Jon Fell, partner in information, communications and technology at law firm Pinsent Masons. "You need to ensure people understand the policy and also what the sanctions are if they break it." On the other hand, if your IT security people are able to read staff's emails or monitor which websites they've visited, this should be made clear, too. The organisation's approach must be consistent, and senior managers should lead by example, Fell adds. If bosses don't log off at lunchtime, for example, why should their juniors?

"You can only achieve good security if everyone in the business has bought into it," Gillespie concludes. "Security is everybody's responsibility."