SAFE *and* SOUND

THREE IT LEADERS EXPLAIN WHY GOOD INFORMATION SECURITY IS AS MUCH ABOUT PEOPLE AND PROCESSES AS IT IS ABOUT TECHNOLOGY

CIOs are under pressure like never before to help the business derive value from IT investments. In some cases, technology chiefs might make the decision to reduce spending – but information security is one area where CIOs simply cannot afford to cut corners.

The second part of the feature reports from an exclusive forum in Monte Carlo, which highlights how IT leaders must address risk in order to deal with ever-increasing security threats.

But we first detail the approach of three technology executives to information security. What becomes clear through the article is that successful security requires dedication, both in terms of people and processes:

- Security needs to be physically, logically and culturally embedded, says Katherine Coombs, IT director and information security officer at buyingTeam
- Andrew Bover, head of ICT at 1st Credit, has shifted the focus from information security (IS) as a technology concern to a business risk issue
- Being able to share information when necessary is the driving force behind Bill Limond's approach to information security at the City of London

WORDS: **LISA KELLY**

Name:
Katherine Coombs
Position:
IT director and information security officer
Organisation:
buyingTeam

More than simply IT director at buyingTeam, Katherine Coombs is also the firm's information security officer (ISO) – and it is a new role that she takes very seriously. Coombs is conscious of the fact that, as a smaller firm, the procurement outsourcer and solutions provider does not have the same budget or security staff numbers as she had in her previous role as CIO at Lloyds Banking Group.

"The question I ask is how small businesses can manage security as well as larger organisations?" she says. "Lloyds Banking Group has an entire IT team with dedicated security personnel, but I think SMEs can do security as well by ensuring everyone takes responsibility and by making security ingrained in the culture through education and training."

Coombs says information security can be a selling point in regards to the outsourcing of professional services. Sensitive data, such as suppliers' quotations and credit card information, must be protected.

"Customers do not want their data in the public domain and we receive requests for proposal questions around information security, and regulated organisations are particularly inquisitive," says Coombs. buyingTeam has ISO 27001 accreditation in regards to how it keeps data protected, including the physical security of data and access to information. Coombs' attitude is that security has to be much more than simply ticking the compliance box.

"I live and breathe what I am responsible for, and take a hands-on role because I am directly accountable for information security," she says. Coombs says the lack of a dedicated security team is not necessarily a bad thing.

"Security is embedded in all the IT teams' roles," she says, but the emphasis on responsibility for security filters throughout the organisation via a thorough education programme. "It is important that everyone has accountability for security, not just for the people within the IT team who deal with data, but also for people out there at the perimeter who must understand their responsibilities, our corporate policies and our acceptable use guidelines."

The embedded nature of Coombs' security approach is apparent when an employee first joins the company, as each new recruit must undergo training, including via video-based tutorials. "The technique was developed in-house and is maintained by us. We use scenarios which are applicable to the buyingTeam environment to bring the message home, so people know what they should and shouldn't be doing," says Coombs.

Footage includes ways to enter the building and sweeps of desk areas to spot possible security risks, such as passes left on desks. Coombs says it is often the little things that lead to the big breaches: "Security, like business continuity, is usually not about a worst-case scenario. It is often an everyday event that can cause a problem," she says.

Employees are asked to complete a security quiz every 12 months and undergo a refresher course if they give incorrect answers. "We are delivering a service to clients and security is part of that service," says Coombs.

In terms of mobile devices, buyingTeam issues staff with standard equipment depending on the employee's role. "We are mainstream in that respect and look at the entire lifecycle around equipment, including support issues. If we ever allow employees to opt out entirely, and bring in their own devices, it will be their responsibility to maintain them securely," says Coombs.

"I am also interested in the software-as-a-service delivery model because of the potential for maintenance and support. As a delivery model, I like it in principle as smaller organisations can leverage the expertise of larger infrastructure providers - but security is an issue. Cloud delivers on some challenges brilliantly, such as physical security, multi-layer security and intrusion detection, but it does open up other challenges around the Data Protection Act and the fear of information leaving the European Union."

Coombs does use third parties for security services, such as penetration testing, but she rotates the experts frequently to receive a fresh perspective. She also uses a subscription service to ensure that buyingTeam is kept up-to-date with security concerns. "We must keep abreast of new regulations that come out and compliance issues," she says.

"No firm can be lackadaisical or ambivalent about security. It should be at the forefront of any IT director's mind. Security needs to be physically, logically and culturally embedded, because no single piece of technology in isolation can guarantee your information integrity."

"Security, like business continuity, is usually not about a worst-case scenario. It is often an everyday event that can cause a problem"

Name:
Andrew Bover
Position:
Head of ICT
Organisation:
1st Credit

Andrew Bover, head of ICT at 1st Credit, has shifted the focus from information security (IS) as a technology concern, to a business risk issue, in an attempt to ensure the topic receives the attention it deserves at board level, and to improve IT governance and business alignment.

"The concept of IS on the c-level agenda can be a challenge, as some CEOs and CFOs believe that is the role of the head of IT," says Bover, before pointing out that the debt purchase and collection company simply cannot afford to treat technology as an add-on.

"We have 4.8m people's personal details on our system and IS is critical as we work in a regulated industry and our clients have to be comfortable, as technology is as core to the business as anything else we do. The issue of data integrity is a hot topic in our industry, across both debt collection agencies and regulators alike, and the last thing customers want is a call chasing a debt they don't owe."

Bover's business risk approach draws on the support of a pragmatic chief executive who understands the importance of IS. "Someone can lose a paper contract in the same way they can lose a laptop. By placing IS on the business risk agenda, it is looked at in a different light and conversations are about business risk problems and not IT problems," says Bover.

Explaining IS in terms of business concerns means looking at the potential cost of something bad happening, which then informs decisions about how the risk is managed. "Many IT heads will talk about security vulnerabilities and they struggle with such an approach to engage the business," says Bover, who has created a register which lists all the potential risk in IT.

"The first time I talked to the risk director about this approach when I started the job, he almost fell off his chair, because he was used to working out what the business risks are as opposed to being proactively approached by IT with the information," says Bover.

"A risk register is a good communication tool and gives the business a view of the concerns that IT is managing on its behalf. C-suite executives have so many business issues that they are trying to manage at any one time and the risk register gives them something to cast their eyes over, which gets the message across."

Bover says the register has focused capital resources on systems projects to ensure the business's appetite for risk is understood. "On the back of looking at IS as a risk, we have used the ISO 27001 compliance standards because one of the risks identified was a lack of data ownership in a few functional areas of the business. The framework will help bring structure and identity to areas where we could make improvements," he says.

That standards-based project began in June and is 40% complete. "From a business governance point of view, it is a great thing to do as it gets the owners of information to take responsibility,' says Bover.

Information, he says, then ceases to be an IT issue and becomes a business concern, as owners are given ownership of their specific assets. The standards-based approach can also help reduce costs and make IT more efficient.

"We can have discussions around data retention, which have to reflect the information's value to the business," says Bover. "Conversations around the value of information assets to the business define the level of security and can help reduce costs, such as storage and back-up."

The company is investigating whiteboard and electronic note-taking technologies, which will be automatically erased daily as an additional security enhancement. In fact, 1st Credit has already won awards for its compliance capabilities - and the training of staff forms an integral part of Bover's approach to continuous service improvement.

"Having the right executive support makes rolling out an ISO 27001 project much easier than in organisations where a framework needs to be developed as a pre-cursor to the implementation of the project," he says.

"Someone can lose a paper contract in the same way they can lose a laptop. By placing IS on the business risk agenda, it is looked at in a different light and conversations are about business risk problems and not IT problems."

Name:
Bill Limond
Position:
CIO
Organisation:
City of London

Bill Limond, CIO at City of London, is a member of the CIA; not the Central Intelligence Agency, but he is signed up to the three-pronged principle that security is all about confidentiality, integrity and accessibility.

"There can be a trade-off between confidentiality and accessibility and you must protect the information you are in charge of, but the key thing is quality and access, so you can find the right information at the right time in the right place," says Limond.

Being able to share information when necessary, and to have one version of the truth, is the driving force behind Limond's approach to security. He recently set up an information governance board (IGB) at the organisation to focus on the quality of data and its governance.

"The IGB was set up in May and looks at standardisation, governance principles and guidelines, because it is too easy to lose the plot, when managing information, and we need to put in place asset ownership," says Limond. He says the aim is for the IGB to help IT move up the value chain.

Limond is the chair of the board and other members include the chief executive of the built environment, the head of libraries and the head of archives. He says the seniority of members indicates the seriousness of information governance at the City of London.

"Like all local authorities and government departments, the City is aware of the need to keep information secure. We are currently putting people on training courses on information security management," he says.

Limond says that having a better grip on information organisation prevents wasted effort in regards to knowledge management and he gives the example of dealing with Freedom of Information Requests. The City is a high-profile organisation and that position comes with a responsibility to ensure information is accurate and secure.

"World-class businesses are located in the City and, when we try and encourage them to stay or establish themselves here, we must respond quickly and securely if they want information," says Limond.

Microsoft's SharePoint technology is at the heart of Limond's information-sharing strategy and provides the City's knowledge-management platform. Although the organisation has not been using SharePoint for a long period of time, Limond says there is value in moving cautiously and ensuring projects are carried out scrupulously.

"We have moved the old intranet onto SharePoint and are now developing a portal. We are also looking to move business intelligence onto the software. It will be the focus for collaboration, and file and document management. Other people may be ahead of us, but we can learn from their experience," says Limond.

"The City will be offering more services online, which can be completed faster and cheaper with the supply of information directed to where it is most easily located.

PHOTO BY MARTIN BURTON

The security on this approach is tight and Microsoft Office 2010, which we have also migrated to, fits with the SharePoint environment and helps improve security and information management," he says.

Some security constraints cause additional adherence concerns for the City. For example, the Cabinet Office has locked down standards in its Code of Connection, a mandatory set of requirements that must be demonstrated before local authorities in England and Wales can connect to the Government Secure Intranet.

"It is fairly stringent because of the risk of the fallout from security leaks, and devices are locked down, mobile data sticks are encrypted and we have firewalls, and we use the secure extranet standard to send and receive emails," says Limond. PCs, laptops and devices are encrypted. Limond, however, does not let security act as an inhibitor and is currently trialling iPads.

"Elected members are very busy people and we do try and help them by not throwing tonnes of paper at them," says Limond. "Information is often more acceptable if it is stored electronically and we are looking at how we can create a secure environment on the iPad by using Good Technology, which allows you to create a secure area on a device or a tablet."

Limond also says citizens, as well as businesses, are entitled to accurate and secure information: "We can respond to business requests, much quicker and more confidently, when we know it's the right information. Security really is key to all information," he says. ●

"World-class businesses are located in the City and, when we try and encourage them to stay or establish themselves here, we must respond quickly and securely if they want information."