00000001 01100110 01100001 00110110 11110001 01010110 00000001 01100110

CIO Insights

Managing a business-led cybersecurity strategy

‘It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you’ll do things differently.’ Warren Buffet

Cybersecurity, once an issue relegated to the confines of the IT department, now features on the front pages of newspapers and in boardroom discussions. In response, the UK offices of Robert Half Technology and Protiviti hosted a series of ‘IT Leaders Round Table’ events to highlight the challenges and issues faced by IT directors and to discuss best practice approaches and solutions.

Hosted by Robert Half Technology and facilitated by Jonathan Wyatt, managing director of Protiviti, and Ryan Rubin, leader of Protiviti’s UK Security & Privacy practice, the events were attended by chief information security officers (CISOs) from a range of private and public sector organisations.

So how are technology leaders coping?

+971 (0) 4 382 6700
roberthalf.ae

Robert Half®
Technology

Background to the cybersecurity threat

Cyber crime is estimated to cost the UAE economy $422 million a year in direct financial losses, and this figure is likely to be growing. A greater connectivity and reliance on information and communications technology and systems has put more businesses at risk, with the national security strategy categorising cyber attacks as a tier one threat to national security, alongside international terrorism.[1]

For businesses, this means protecting any form of digital asset, whether it is stored on a server, a laptop, a USB stick or in the cloud. The breakdown of boundaries between personal and business use of data means that cybersecurity should also cover all types of data accessed by individuals, including personal and corporate information.

A Protiviti survey of the top business risks for UK executives shows that cybersecurity is among the top concerns for 2014, alongside regulatory change, economic conditions and political uncertainty. More boards recognise that cyber threats have the potential to disrupt core operations, bringing what was previously a low-level IT concern to the senior decision-making table.

Awareness is being driven not just by high-profile cases such as attacks on major brands but also by communications from governments, including the UK Government Communications Headquarters (GCHQ). A recent missive from GCHQ to corporates, for example, states that it now sees 'real and credible threats to cyber security of an unprecedented scale, diversity and complexity … The magnitude and tempo of those attacks, basic or sophisticated, on UK and global networks pose a real threat to the UK's economic security. The mitigation of these risks and management of these threats – in other words, cyber security – is one of the biggest challenges we all face today.'[2]

An increase in breaches and their complexity has made dealing with cyber attacks more difficult and costly. According to a Robert Half Technology survey, nearly half (49%) of CIOs/CTOs said that the number of security incidents detected in their firms increased over the past year. Only 8% said they have decreased.

CIOs/CTOs were asked to rank the following cyber threats in order of concern to their organisation. Their responses:

1. Network security
2. Email (phishing, social engineering)
3. Viruses and malware
4. Physical (tampering, theft and/or environmental attacks)
5. E-crime and fraud (internal or external)
6. Insider threats (staff or third party)
7. Data leakage
8. Competitor threats (industrial espionage)
9. Privilege user abuse
10. Social media

Source: UK survey of 100 CIOs/CTOs.

[1] http://gulfnews.com/business/technology/uae-loses-422m-due-to-cybercrime-in-past-year-1.1086337

[2] Source: Iain Lobban, Director GCHQ: *10 steps to cybersecurity* – executive companion

The profile of individuals involved in cyber attacks has changed: today's criminals are clever, organised, well funded and passionate and tend to target people more than systems.

'Traditional approaches need to change to reverse the trends and help mitigate risk,' said Ryan Rubin. 'The average cost of a data breach is $250 per record – and there are mounting expectations that a company will do something for customers whose information has been compromised. As well as reputational damage, companies can face costs that escalate quickly.'

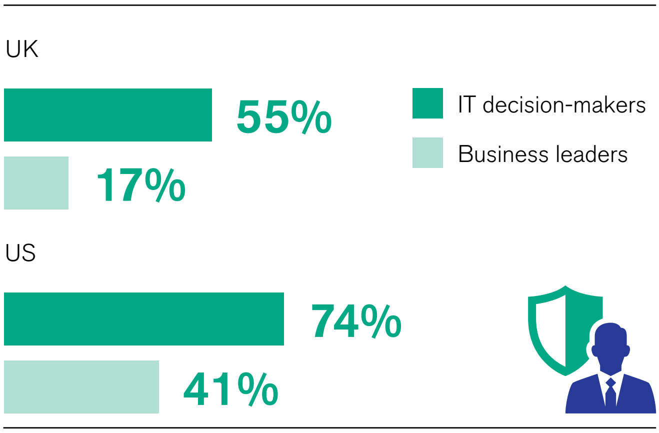
Where attacks were once focused on systems and IT, increasingly they are targeted at people. Criminals look at how employees access the data – for instance, socially engineering a user screen that has access to a system to obtain sensitive information – instead of breaking into the system itself.

'There has long been this concept of the head of security sitting in an ivory tower guarding IT systems and telling everyone what to do,' adds Rubin. 'That kind of concept doesn't always resonate or work very well in today's world. You also have to remember that the perimeter of your organisation is now in your employees' pockets on their mobile devices.'

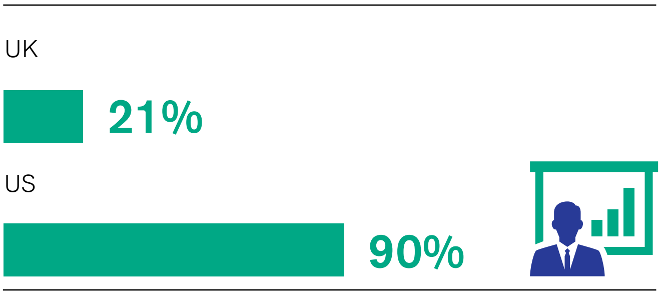
Another challenge for organisations when considering an approach to cybersecurity is the shortage of relevant skills. According to a recent survey, 90% of CIOs say it is now either 'somewhat' or 'very' challenging to find technology professionals with the requisite skills. Of these, 32% cited security as the scarcest skill set.

Further research from BT provides insight into the difference in attitudes towards the importance of cybersecurity measures, comparing perspectives from IT and the wider business. Compared with their American counterparts, British respondents are not grasping the importance of cybersecurity. Nine in 10 (90%) of the organisations in the US saw a clear return on investment in cybersecurity measures compared with just 21% of organisations in the UK, for example.

Cybersecurity importance



ROI on cybersecurity measures



Source: Survey of 500 IT decision-makers coordinated by Vanson Bourne on behalf of BT.

The indicators suggest that current approaches taken by organisations towards cyber attacks need to be rethought. In particular, the traditional way of managing cybersecurity in which organisations attempt to shut down access for end-users is no longer a sufficient response.

‘It sometimes helps to think through an analogy with the way in which we physically protect our houses,’ said Jonathan Wyatt. ‘We all understand that locking doors and installing CCTV will not defend us against a targeted attack. We put in place basic controls and rely on insurance for most of our assets.

‘Next we identify the precious items that definitely need to be protected, often focusing on sentimental items that could not be replaced, and adopt alternative measures, such as keeping them in a fireproof safe or in a safety deposit box at a bank.

‘While homeowners are good at prioritising when protecting assets in the house, companies are not very good at doing this, adopting more of a one-size-fits-all approach. A lot of corporations have put virtual locks on the doors and implement security policies and standards which they then apply to all assets. Few have identified the assets that they really care about and put in place measures that would defend against a sophisticated, targeted attack. Criminals have learned that once they get past the perimeter, it’s easy to find what they want to steal. If it ever did, this one-size-fits-all approach no longer works,’ concludes Wyatt.

WHAT DOES THIS MEAN FOR THE UAE?

The cyber threat to the UAE is credible and real. According to research by PwC, one in four (27%) UAE businesses have experienced cyber crime within their organisations and nearly six in 10 (56%) reported losses between USD 100,000 and USD 5 million. Like their global counterparts, UAE businesses still struggle with understanding the potential risks and mitigating damages, and are seeking effective ways to detect and prevent fraud.

Three in four (75%) respondents indicated that cyber crime was perpetrated by internal staff, a full 19 points higher than the global average. This suggests that stricter controls are needed – not only to hire lawful employees but to source people who understand both the technical and business requirements needed in an effective cybersecurity programme.

Reference for above: http://www.pwc.com/m1/en/publications/gecs2014reportuae.pdf

Governance and risk

Information exchange between IT security and the board

When asked about the quality of information exchange around cybersecurity between IT and the board, round-table participants reported that this was mostly limited and reactive, rather than ongoing. One company reported that it is taking a more proactive approach, holding monthly one-and-a-half hour meetings between IT security and the board to highlight particular issues.

'We've put together a dashboard that shows ongoing threats and where we are with different metrics. Not only do the meetings help to build confidence that we know what we are doing, but they are also good for securing funding when budgets are tight.'

Another company highlighted the fact that cybersecurity needs to be positioned as a business risk, rather than a pure IT issue: 'Information security is part of IT, but is actually a business issue across the board. It's a matter of financial risk and control, especially when you consider the impact of a security breach on reputation and financial performance.'

One company that had been taken over by a US firm found that risk management reporting was noticeably tightened up: 'All of this comes down to the risk management framework that organisations have in place. We operate in financial services, and our new parent company operates in a market that can expect punitive fines and jail terms for directors when data is breached.'

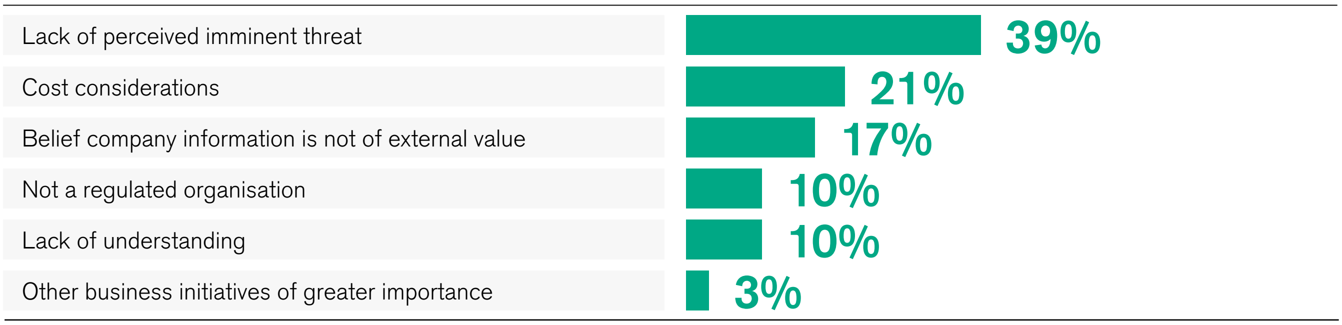
Board-level engagement with cybersecurity

Boards of directors are becoming more engaged with cybersecurity for a number of reasons, including greater regulatory scrutiny and stronger risk management generally. In fact, nearly three-quarters (72%) of CIOs/CTOs surveyed by Robert Half Technology said that cybersecurity is being prioritised by senior management.

This is often the result of a lack of understanding. While nearly four in 10 (38%) IT leaders cited 'lack of perceived imminent threat' as the top reason why cybersecurity isn't being prioritised, often this assertion is misguided. The threat is real, the evidence of the threat is real, and IT leaders need to find a way to convey this to senior management.

'Security is seen as a risk to revenue, not a way of protecting it,' said one round-table participant. 'The CFO agenda is what pushes the board agenda, and security is often seen as a cost. Cybersecurity is IT's problem.'

What is the primary reason why cybersecurity is not being prioritised by senior management?



Source: UK survey of 100 CIOs/CTOs.

One of the challenges is that people responsible for cybersecurity speak in technical language and use terminology that is unfamiliar to the board.

Jonathan Wyatt explained: 'IT functions find it hard to avoid using technical jargon. This is particularly true of IT security specialists. It's easy to dismiss information that is difficult to understand or that paints a picture of security risks that sound like something from a movie. Communications need to focus on the potential business impact, value of assets at risk and level of exposure, and not the technicalities of vulnerabilities or how weaknesses in systems might be exploited.'

Ryan Rubin adds, 'Recognising that technology underpins everything that a business does can be a differentiator as well as an enabler, but brings with it significant risk. Businesses need to ensure that they have people with a good understanding of technology represented at the most senior levels.'

However, delegates at the events felt that board directors were suffering from fear, uncertainty and doubt (FUD) fatigue. Many communications from IT to the board relating to cybersecurity budget discussions are centred on products. 'Our directors have toughened up to the FUD threats and ask why they should be worried about something that has never happened to them.'

The key is to make sure that the whole risk profile of an organisation is understood and that it's not just about IT systems. 'The board doesn't need to have a deep understanding of the technicalities of security risks, but they do need to know which risks they need to worry about and have a clear understanding of potential exposures,' adds Jonathan Wyatt. Most high-profile cyber attacks are not actually that technical in any case, but it's up to IT security to explain potential exposure to risk in a language the board understand.'

Getting the board to think in terms of assets and risks

One way to approach this is to talk assets rather than IT security in terms of hardware and software. 'Board members tend to be owners of particular assets, so it can make sense to run through asset reviews to check how happy they are with the level of protection in place rather than talk about cybersecurity in general terms.'

This capturing of business requirements and risk appetite is another area that can be fraught with difficulties. Delegates felt that talking about cyber risks should not be generic, but instead match the objectives and risk appetite of different parts of the business.

'You've got to get the conversations started to find out what's important to the business. For one company, it could be a secret recipe; for another, it could be more general sales and marketing data. But just ticking a box from a regulatory point of view is not enough – it's all about finding out what really matters to the organisation and protecting that. What are our most precious assets, where are they held and how do we protect them?'

This means that it is even more important that the communications gap between IT and business must be bridged. Delegates felt that the biggest recruitment challenge they faced was to find IT and security professionals with the right business engagement skills, who understand technology but can also explain how to make it effective within the business.

'Some of the best CIOs don't come from IT at all but from the business side of the organisation – they are less likely to be someone from the world of networking and infrastructure. It's easier to put technical skills into a job description than the ability to engage with non-technologically minded colleagues.'

> 'The board doesn't need to have a deep understanding of the technicalities of security risks, but they do need to know which risks they need to worry about and have a clear understanding of potential exposures.'

Round-table conclusions

One size does not fit all: traditional approaches are not working, and organisations need to stop thinking that they can plug every security gap. Instead, they need to prioritise the assets that they definitely need to protect and make sure that data is safe. A risk-based approach needs to be applied, and this should include identifying sensitive data, assessing potential threats, capturing risk appetite and mitigating risk threats.

People are the weakest link: cyber attacks have moved on from being simple attacks on IT systems to social engineering that targets people to gain access to data. Cybersecurity strategy needs to change to reflect that shift in emphasis, and all staff need to be trained in how to adjust their behaviour.

Communication breakdown: the disparity between the technical knowledge of IT security and business risk managed by the board is a major problem that needs to be addressed. The danger is that boards with 'FUD fatigue' lose sight of the reputational and financial impact of cyber attacks, which continue to grow exponentially in complexity and volume. Effective information security teams may require a different mix of skills than traditional teams have had available to them.

About Robert Half Technology and Protiviti

Founded in 1948, Robert Half pioneered the concept of professional staffing services and is the worldwide leader today. Robert Half Technology specialises in the placement of high-calibre IT professionals on a permanent basis.

Robert Half also is the parent company of Protiviti, a global business consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit.

Connect with us at Robert Half Half Middle East:

+971 (0) 4 382 6700
roberthalf.ae

Robert Half® Technology