CRITICALEYE

Beating Cyber Crime

It's inevitable organisations will experience cyber security issues. ***Malcolm Marshall****, Global Leader for Information Protection and Business Resilience at KPMG, talks to Criticaleye about how leaders need to adopt a robust approach to handle the threats they face*

Who is responsible for cyber crime and what data is being targeted?

There are four key cyber-crime players: governments, organised crime syndicates, hacktivists and insiders.

Governments typically target intellectual property or commercially valuable data, such as information on deals which can be passed onto one of their own country's companies.

Organised crime syndicates or gangs seek any data that can be converted into financial benefit. Hacktivists seek any data that suits their ideological beliefs, such as evidence of a company's wrongdoing, while insiders usually seek financial gain or revenge through intercepting or destroying the integrity of information.

What approach should senior executives take to manage cyber crime?

Companies need to know what their critical data assets are, what the impact of losing them is, and invest in protecting them. You can't protect all of your data to the same extent, so you have to be selective.

In most organisations, the decisions relating to what constitutes as critical data are made by the IT function and, though they are capable, they do not have the full picture of a company's business plans.

They often protect things that don't necessarily need protecting and fail to identify things that the CEO, COO or a market-facing executive will understand to be critical to the company's reputation and success.

> *“Sometimes it's difficult for senior executives to understand and articulate what cyber security means”*

Leaders need to think about their critical business processes: what are their key revenue streams? What's involved in supporting those key revenue streams? Who are their key suppliers?

Should cyber crime be a key board issue?

Yes, the board should be accountable for cyber risks. However, according to a survey we conducted, it's an area where they often feel uncomfortable in terms of their understanding and knowledge. Sometimes it's difficult for senior executives to understand and articulate what cyber security means to them.

How can this be overcome?

Firstly, the board needs to understand exactly what its role is when it comes to scrutinising the strategy around cyber crime.

Through workshop sessions and case studies, senior executives can identify which data needs to be protected in order for them to meet their business plans. Applying cases that have been in the news or ones which are relevant to their own organisation is incredibly useful. This triggers individuals to think about how they would respond in similar situations and brings the issue to life. Often, until you do that, they may think it's just something to read about in the newspapers.

They should also be aware that, as board members and individual leaders, they are likely to be targets of cyber crime themselves.

What about wider awareness across the organisation?

Building the right security culture within your organisation and encouraging the right attitudes is critical. Everyone has to fully understand why tackling cyber crime is so important.

Senior executives need to encourage – rather than enforce – the right attitudes, and emphasise the fact that security is not something to be feared or something that gets in the way of doing business. It enables you to do business more safely.

It is the responsibility of the board to ensure that employees understand the risks. Staff should be able to identify something that looks suspicious and know when to ask for help, and this applies to people within the company and to those who are external too.

Managing cyber crime is all about people – you can have all the anti-cyber-crime technology in the world and people will still get around it.

Make sure that all of your staff understand their responsibilities, know the risks ▸

and realise that security is not something to be feared. They should see it as something that's going to enable you to do business better.

How should cyber security measures be extended across an organisation?

The responsibility of cyber security needs to go across the whole company. An immature organisation will consider the cyber risks as being focused around the IT function, but increasingly technology is being embedded in people's products, especially as we see the emergence of 'the Internet of Things'.

For example, in the product development process, things like cars and radios, even vending machines can now be IT-enabled – they can now send maintenance requirements using the internet.

Is there any particular department that needs to be more vigilant when it comes to cyber security?

Companies will need to build more security and governance into their R&D, manufacturing and product processes.

Recently, a company launched a product with a security weakness, and despite being warned of the dangers it failed to pay an extra £1 to update and protect the product. Six months later, those weaknesses became a reality and the company is now in a position where it can't recall the product.

Building security into the product process is down to individual product teams who, typically, don't have a deep understanding of either risk or of the board's appetite for risk, which is a problem that needs addressing.

> *"We need to remember that technology and the internet are inherently insecure"*

What future trends will we see in the area of cyber crime prevention?

As people's understanding of cyber crime matures, we'll see growth in the cyber insurance space. This market is fairly immature right now – products don't necessarily cover loss of information, they usually cover the costs of a technical response or the costs of litigation for losing somebody else's personal data. But there are some good products available and this has the potential to develop as a market.

Cloud computing is another trending topic. Most people appreciate the benefits of using the cloud, such as the cost savings and added efficiency, but some questions need to be kept in mind, such as, where is your data? Which parts of your data are secure? Do you know which parts of your data are most valuable and should you put those in the cloud?

All the potential risks need to be managed appropriately. It could be through putting 95 per cent instead of 100 per cent of the company's data into the cloud. That 5 per cent could be the really critical data which you shouldn't let go of.

Should cyber security be handled with a long-term plan in mind?

Managing cyber-risk is always going to matter. The way organisations use IT is constantly evolving, while the market environment in which they operate and the associated risks are ever-changing. All of which non-executive directors and other executive board members need to feel comfortable.

We need to remember that technology and the internet are inherently insecure, and cyber threats happen over a prolonged period of time.

Managing and investing in these risks over the long-term, rather than seeing them as projects, is certainly the best approach. ■

Malcolm Marshall
Global Leader, Information Protection and Business Resilience, KPMG

Malcolm has over twenty years' experience in advising clients on information risk management. Clients include several of the world's largest corporations and central government departments. His recent work includes security improvement programmes, data breach investigations, identity and access management projects, privacy advisory and security compliance programmes.

Contact Malcolm through: ***www.criticaleye.net***