The Key to Tackling Cyber Crime

Boards can't afford to ignore the threat of cyber crime. ***Criticaleye*** *speaks to a range of business leaders to find out what organisations must do to minimise the risks*

While organisations are spending significant amounts of money trying to keep cyber criminals at bay, financial investment alone won't be enough to deter governments, hacktivists or nefarious gangs, nor will it prevent carelessness among employees. Increasingly, it's apparent that senior executives need to step up and take the lead, and ensure everyone within the organisation knows the part they must play in creating a truly effective defence.

In other words, delegating responsibility to an IT specialist won't be good enough. Unless boards and executives understand the extent of the risks, it'll only be a matter of time before security weaknesses are exploited. Criticaleye spoke to a range of leaders and advisors to find out how organisations can beat cyber crime:

1 SCOPE OUT THE RISKS

If security structures are to be successful, leaders need to identify where the cyber threats to their company originate and what's being targeted. **Malcolm Marshall**, Global Head of Information Protection and Business Resilience at KPMG, comments: "You've got four key players: foreign governments typically [want] commercially valuable data... or intellectual property that they can pass on to one of their own country's companies.

"Criminals are after any data that can be converted into financial benefit. Hacktivists [look for] information that suits their ideological beliefs, such as evidence that a particular company is evil or unethical, and the insider [is usually out for]... revenge or financial gain."

Ian Bowles, CEO of workforce optimisation and corporate governance solutions provider Allocate Software, ▸

says: "I would encourage organisations not to simply adopt a fortress mentality and assume keeping the bad guys out is enough. Cyber security should be equally as focused on the inside... on rogue employees sending out confidential data."

However, insulating yourself from every threat is impossible. **Peter Shore**, Chairman of Arqiva, a provider of television and radio broadcast infrastructure, says: "You need to prioritise your systems and put a defence around them according to how critical they are...

"In some cases what you try to do is entirely segregate a system from others which are more widespread and, by nature, less secure."

2 CHOOSE A LEADER

Selecting the right person to lead the cyber security agenda is vital. Whether it's the CRO, CIO, COO or CFO, the specific responsibilities will vary considerably depending on the organisation and how threat levels are perceived.

What is clear is that the leader heading up cyber security needs to be constantly communicating with the executive committee and be thinking across the organisation, rather than about their own silo.

According to **Malcolm**, critical decisions can't be left solely in the hands of the IT function. "Capable though they are, they do not have the full picture. They'll often [prioritise] things that don't necessarily need protecting and fail to identify those that a chief executive, COO or market-facing executive will understand to be critical to their collateral success or reputational integrity."

> *"There has to be line of sight from the main board to wherever your key risks are located"*

A similar point is made by **John Lewis**, Chief Operating Officer at mobile communication provider Airwave Solutions: "Quite often you will get demands from the business to make things easier, which often means bringing in greater security risk. So, having someone who understands the risks in some detail but can then balance the risk/reward decision is important."

Whoever takes the lead must clearly identify the key action points, communicate them to their executive colleagues and ensure they're being executed. **Gavin Walker**, Chief Information Officer at air navigation service provider NATS comments: "My challenge is to make sure that those risks are owned by the business. I can create the right mechanisms, the right policies and the right standards to work to, but we need to be very clear that everyone takes responsibility for implementation."

3 ENGAGE THE BOARD

According to **Heather Savory**, Independent Chair of the Open Data User Group, which advises the UK Government on the value of the data it collects, boards are being short-sighted if they fail to treat cyber security as a priority.

"Too many organisations have strong governance around financial risk – primarily because they are required to report their financial status publicly – but pay little attention to IT risks until disaster strikes," she says.

Brian Stevenson, Criticaleye Board Mentor and Non-executive Director of the Agricultural Bank at China (UK), comments: "There has to be line of sight from the main board to wherever your key risks are located. It's about having the ability to probe an organisation and to satisfy yourself that its defences are adequate."

As with all fast-moving, specialist areas, organisations have a duty to ensure their non-executives are kept up-to-date. "We might get external speakers in to take the board through the wider national threats – that's something I would certainly recommend," says **John**.

For **Peter**, this is where the skills and experience of an IT executive can come in particularly handy. "Our board members can ask for a session with our CIO or chief IT guy if they feel it's necessary to get up to speed and fulfil their obligations as a director."

4 EDUCATE YOUR STAKEHOLDERS

Employees are potentially a company's biggest vulnerability when it comes to cyber security. However, for organisations that devote sufficient resource to informing them about the risks, staff can become a powerful asset. ▸

"We're having to raise the level of education that we provide to our staff," says **Alan Towndrow**, Group Information Systems Director at international asset manager, M&G Investments. "We're making sure our employees are aware of phishing emails and the social engineering that takes place. This is just as true in their private lives as it is at work."

Leaders need to communicate the security strategy and explain exactly why it's central to a business' success. **John** explains: "People get frustrated by the security measures because, naturally, they make things more difficult. Giving some exposure as to why... we have those processes in place helps make it real for them."

As is often the case, actions speak louder than words. **Gavin** says: "The executives at NATS lead by example because they understand how big the risk is. If cyber crime isn't being taken seriously by them, it's unlikely it'll stick with the rest of the organisation."

According to **Ruchir Rodrigues**, Managing Director of Digital for Barclays' Personal and Corporate Banking Group, UK and Europe, this education should extend beyond an organisation's employees. "An area of concern for us is that fraudsters use different methods to get information from customers.

"We need to reach a point where certain behaviours and practices are ingrained in customers' brains... so [if, for example, someone phones you], whoever is claiming to be on the call, do not give them any passwords [or sensitive bank details]. It's that kind of awareness you have to drive."

Collaborating with your competitors may be necessary for this because it's a job that's too big for any single business to tackle alone. **Ruchir** continues: "Banks are coming together to agree certain principles or frameworks that we will all have in place... This has to be industry wide."

5 CONTINUALLY REASSESS YOUR POSITION

Investment in cyber security should no longer be seen as a one-off, technical fix. Leaders have to regularly invest time and money into assessing the threats, their systems and cultural practices, or they'll quickly find themselves at risk.

The proliferation of internet enabled devices and mobile working, as well as an increasing reliance on cloud technology, is raising a number of questions. **Alan** comments: "There's a growing awareness that the infrastructure that businesses use can expose them to vulnerabilities, so work needs to be done to respond and to develop strategies that allow you to come up with higher levels of security."

Gavin says: "This isn't something you just pick up, put a bit of effort into and then put down again. It's here forever and it's just going to get worse or more complicated. So, it's a journey... that all organisations are going to have to live with for a long time."

Increasingly, companies rely on the integrity of their digital capability to maintain the way they operate and their reputation. That's why time invested in understanding the macro issues and how your company is responding is never wasted.

As **Malcolm** says: "Security is not something [that should] get in the way of doing business but enables you to do it more safely. Hopefully that means something to [you and] your customers." ■

Featuring Commentary From:

Ian Bowles
CEO
Allocate Software

John Lewis
COO
Airwave Solutions

Malcolm Marshall
Global Head
Information Protection & Business Resilience, KPMG

Ruchir Rodrigues
MD, Personal & Corporate Banking Group, UK&I
Barclays

Heather Savory
Independent Chair
Open Data User Group

Peter Shore
Chairman
Arqiva

Brian Stevenson
Non-executive Director
Agricultural Bank at China (UK)

Alan Towndrow
Group Information Systems Director
M&G Investments

Gavin Walker
CIO
NATS

Contact the contributors through:
www.criticaleye.net