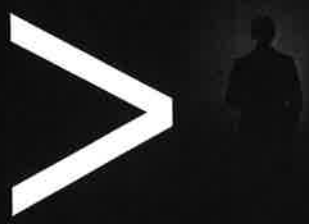

CYBERSECURITY AND THE MODERN DIRECTOR

Why cybersecurity is a board issue

Do you think cybersecurity is something that only concerns your IT department? It is certainly that, but cybersecurity is also something for which every person in your organisation carries some responsibility. As a director your responsibility is even greater, as cyber security is today recognised as a multi-disciplinary governance issue which goes beyond the ICT team and is a component of departments including human resources, communications, finance and legal.

But why has cybersecurity moved from what was essentially a fringe issue, to becoming a risk of such magnitude that it demands the attention of the board?

The simple answer is that we have become an information society, massively enabled by technology which makes the creation, exchange and transmission of information considerably easier than ever before.

That information is valuable has never been in question. However, what has changed is the volume of information available today, the systems which contain and convey it, and the enormous variety of information which can, if it falls into the wrong hands, constitute a risk to your business.

>_THE HEIGHTENED RISK OF ATTACK

While business today is enormously empowered by ubiquitous computing and connectivity, so too are the professional hackers who seek to profit from illegitimately acquired information. In much the same way that automation improves company productivity, it accelerates the ability of hackers to break into networks, databases, websites and applications. In the same way that the internet makes it easy to do business across the world, it makes it simple for hackers to operate from anywhere.

A recognised authority in tracking global cybercrime, the 2016 Trustwave Report examined cybercrime as a business model for the first time, detailing the methods that cybercrime organisations use to maximise profits from malicious attacks. "Cybercriminals have been congregating and organising for years, but 2015 showed a marked increase in the behaviour we would normally associate with legitimate businesses," said Trustwave Chief Executive Officer and President Robert J. McCullen.

The report also revealed that despite the hype around information security, companies today are still lackadaisical in their approach. For example, 97 per cent of applications tested by Trustwave had 'serious vulnerabilities'.

The work of the hacker, often working in an organised group structured like a legitimate business, is made infinitely more efficient with automated attacks, with bots crawling the web looking for vulnerabilities which they can exploit. It is your duty of care to ensure that when – not if – hackers target your systems, they are reasonably secured.

>_INFORMATION SECURITY AND GOVERNANCE: A LEGAL PERSPECTIVE

But what does 'reasonably secured' actually mean? Wellington firm Wigley Law provides a useful perspective on how the law is likely to treat information security as a board issue. The company points out that as with any other risk 100 per cent mitigation is usually not required – and nor is it possible. Instead, cybersecurity risk should be managed and balanced. Each company's risk profile differs: for example, some companies make 100% security promises in their contracts with customers (although that is something that should be fixed).

What is required, however, is for directors to determine how far to go in relation to categories of data. Wigley Law points out that those on the board have an obligation under the Companies Act to exercise the care, diligence and skill of a 'reasonable director' in the circumstances. They conclude that, if the board is not complying with the Institute of Directors' Cyber-Risk Practice Guide, or equivalent, they are unlikely to be legally compliant, giving directors' exposure to damages claims.

The law firm points out that 'companies with good corporate governance have robust board practices to manage risk to meet these duties...what is clear is that cybersecurity should become well entrenched in regular board reviews, given the risk and very real prospect of successful attacks.'

>_THE DUTIES OF A DIRECTOR

There is no question that effective cybersecurity is, to a degree, a technical issue (and a complex, multifaceted one at that). But the question for many directors is a simple one: what should I (and the board) do?

On a recent visit to New Zealand, GE's Chief Security Officer Tim McKnight provided something of a checklist which every director should consider. At the top of the list is to add cybersecurity to the agenda.

It is necessary for every director to be aware of cybersecurity. McKnight advised directors to educate themselves on the topic, including understanding the legal issues; this will empower you to ask the right questions of the IT department (and

Scott Bartlett

others). Knowing which information is most valuable is essential, as well as the roles and responsibilities of those tasked with managing it. Directors should assess and know the company security posture.

Given the complexity of the challenge of achieving reasonable cybersecurity, it may be necessary to call on specialist expertise. Experts can conduct vulnerability assessments, including 'penetration tests'; as mentioned in the opening paragraphs, cybersecurity is everybody's concern.

While often vulnerabilities may be found in information systems, they are just as likely to be identified as personnel issues. People remain one of the weakest links in information security chains, so the education of users and the establishment of a stance of vigilance is essential. Risk assessment should even go straight out the door and up and down the supply chain: third party suppliers can be targeted too.

The bottom line is that cybersecurity is a pervasive issue today. For businesses, it is more than an operational challenge; it has become a strategic one. The recognised strategies for dealing with risk must be applied to cybersecurity: understand, mitigate and, because it is a moving target, routinely revisit it. And, owing to the potential for a weak point anywhere in the organisation, vigilance is necessary from the shop floor, right through to the board.