Cybersecurity and the Board

Part 2 of 2: Ignorance Is Negligence – The Top-Five Questions the Board Should Ask About Cybersecurity

Steven Bowman
Managing Director
Conscious Governance

Monica Schlesinger
Principal
Advisory Boards Group

When it comes to cybersecurity, boards of directors struggle to ask the right questions. Even when they do, IT professionals often don't know how to respond in a way the board can understand. There is a language gap between the two, which leads to a knowledge gap at the board level. This communication misalignment begs the big question: How can your board assure itself that your organisation has the processes in place to address, report on and manage cybersecurity?

The answer starts with your board members themselves. As individuals, and as a group, your board needs to educate itself about your organisation's cyber risk.

The best boards adopt a 'nose in, hands off' approach to due diligence – they probe and query everything, but leave operational matters to management, according to Monica Schlesinger, Principal, Advisory Boards Group.

Simply put, they ask the right questions of the right people at the right time. Here are the top-five questions your board should ask about cybersecurity.

CONSCIOUS GOVERNANCE

Advisory Boards Group

Diligent

Q1. WHAT IS YOUR SECURITY FRAMEWORK?

“A cybersecurity framework for any organisation starts at board level,” said Schlesinger.

“The board must put in place a cybersecurity strategy. That doesn’t mean your directors need a 200-page document at a cost of thousands of dollars. You can create a cybersecurity strategy on a page. It should be simple and clear, and people in your organisation must understand what it means.”

Risk management – and that includes cyber risk – is part of any board charter. Your board must create the risk strategy. The risk strategy trickles down through the levels of your organisation, and the risk management moves upwards in a pyramid style.

> *“The vital aspects of any security framework are the technical plans you put in place, the risk management and the audit.”*

“At every level, people manage risk according to their delegated financial authority or delegated authority,” said Schlesinger.

“Anything outside their threshold they push to the next level. The CEO will manage risk up to a certain dollar amount, and anything above their remit they pass to the board of directors.”

Your board must understand and really know who the regulators are, and what they expect in terms of compliance. What are the laws and rules that govern your industry

If you generate more than $3 million per year in revenue; if you are a health services organisation – regardless of revenue; or if you are a contractor to any level of government, you are subject to the Privacy Act[1].

Starting in February 2018, you will also be subject to Australia’s new mandatory data breach notification laws[2].

Look at the current standards and methodologies to get a better idea of how to build a cybersecurity framework for your organisation.

This framework should contain the cybersecurity strategy, aligned to the overall governance framework, tactical plans and IT strategies; a risk management system; compliance; schedule of audits, etc.

Some organisations use the cybersecurity framework[3] of the National Institute of Standards and Technology, part of the United States Department of Commerce, for their IT security.

However, there are many other methodologies you can use as a guide, such as ISO27001[4] and ISO270005[5] and the other standards from the ISO27000 series, information security standards published by the International Organization for Standardization (ISO). COBIT is another IT governance framework that is used.

“You also need to look at the PCI Security Standards Council[6] standards if you have payment card information on any of your systems,” said Schlesinger.

“Finally, the vital aspects of any security framework are the technical plans you put in place, the risk management and the audit.”

There isn’t a one-size-fits-all approach and every organisation should employ a governance methodology that is tailored to their needs. But this governance should be overarching and enterprise wide and not limited to IT governance.

Q2. WHAT ARE YOUR TOP-FIVE RISKS?

Every organisation is different, so your risk profile will depend on your industry and line of business. However, an example of what we could call a set of risks common to most organisations would include the following.

1. Bring Your Own Device

Modern organisations want to give employees the best possible working conditions. This often includes the option for them to use the devices of their choice at work.

But have you considered the cybersecurity risks of a bring your own device (BYOD) approach? Do you even have a formal BYOD policy?

Allowing your employees to work from home or to access work emails and company data on their own devices is a real risk.

2. Keeping Data in the Cloud Without Implementing Security Measures

"There is a huge misconception about the cloud," said Schlesinger. "Many people believe their data is safe when they place it with a third-party cloud provider. It isn't."

All systems are vulnerable to attack, regardless of how and where they are set up, and there is always more your organisation can do about the security of the data that resides in the cloud.

3. Outsourcing to, and Relationships With, Third Parties

Most organisations consider their own vulnerabilities when it comes to managing cyber risk. However, many are not aware of the cybersecurity – or lack thereof – at the organisations they have a business relationship with, such as a third-party cloud provider.

Do you evaluate the cybersecurity measures employed by your partners, customers and suppliers? If so, how do you manage these risks? If not, how do you manage these risks?

Hackers and cybercriminals prey on the information network weaknesses they can find between organisations. For example, a relationship your organisation has with a vendor could be exploited by a criminal to gain access to your network and the information riches it holds.

And what if your partner's network is hacked? Will this give criminals access to valuable information about your business? The following steps will improve your security posture:

- Know who has access to your organisation's network, and to what extent. This list could include IT infrastructure providers, service providers and various contractors.
- Establish a list of your suppliers, with details about each one's services, access and security.
- Look at all of your organisation's service agreements with outsource partners and make sure you have in place contractual clauses that establish clearly how you will cooperate in the case of an attack through the third party.
- Restrict who has access to your information systems and make tough decisions about how much outside access you allow.
- Scrutinise your organisation's third-party relationships constantly.

Managing cybersecurity takes vigilance – of your own environment, and those of all of your outsource partners.

4. No Business Continuity Plan

More than 77 per cent of organisations have no capability to respond to a cyber incident, according to the 2016 NTT Group Global Threat Intelligence Report[7].

"This is madness," said Schlesinger. "You must have a business continuity plan and a backup plan. You have to know where your most important data is, and you have to know what you'll do if something goes wrong, like a data breach."

A sound recovery plan, one that has been stress-tested and rehearsed, will greatly assist response times in the event of an authentic data or security breach. It should describe the steps involved in isolating and responding to the threat, ultimately helping the organisation to resume business activities as soon as possible.

5. Human Behaviour

Finally, the most potent risk of all is human behaviour. To be blunt, any organisation's biggest cybersecurity vulnerability is its people. The need to incorporate an understanding of cybersecurity into the cultural norms and practices of an organisation cannot be understated. Vulnerabilities open when an organisation's employees are not adequately trained and tested regularly. Whether as a result of a disgruntled employee or someone's naiveté or negligence, even the most sophisticated security measures can't protect your organisation from human errors and frailties.

"Human beings make mistakes," said Steven Bowman, Managing Director, Conscious Governance. "And they are big targets for hackers."

"Even though many people believe they can detect a poisonous email or a threat-laden attachment, such scams are becoming more sophisticated."

Human error can leave information networks exposed through poor password protection, especially the networks of large enterprises or high-volume businesses, which can lead to illegal access of systems by people inside or outside the organisation.

“As we rely more and more on technology to do our jobs or organise our lives, we leave ourselves more vulnerable,” said Bowman.

Yet people will be the last line of defence, and they must be educated in how to deal with the threats.

Q3. ARE YOU RUNNING A PROGRAM OF CYBER EDUCATION AT ALL LEVELS?

In the world of cybersecurity, ignorance is negligence – or worse. Most organisations suffer from a lack of education about cyberattacks – what they are, how they happen and what to do when they happen.

When analysing cybersecurity, your organisation must brief all employees – from your most senior to your most junior staff. Cybercriminals are always finding new attack vectors, so it’s vital that everyone in your organisation is made aware of basic security and information hygiene techniques, such as not clicking on links from senders you don’t know, saving and backing up data, and keeping passwords to yourself.

This means constant education at all levels of your organisation, including instructions on what to do in a crisis.

Q4. DO YOU HAVE A CRISIS MANAGEMENT PLAN?

No matter how small your organisation, you can be hacked or attacked. Never think you’re not big enough to attract the interest of a criminal. The WannaCry virus happened by hackers scanning the internet for vulnerabilities. Its victims were just numbers in a huge pool of targets.

Have a crisis management plan and write down what you’re going to do if you are hacked. How are you going to recover from an attack? Will you have someone designated to tell your clients? Are you going to use your backup systems?

What do you do if your event is something more serious, such as a denial of service attack or a ransomware demand? Will you have a data breach response plan that you will send to the Office of the Australian Information Commissioner?[8]

“Incorporate your data breach response plan as part of your crisis management plan,” said Schlesinger.

“And test your crisis management plan – at least once or twice a year. Only when you test your plan will you realise that you did not envisage all the eventualities. You will be in a strong position to refine your plan and be better prepared, rather than panicking when something happens.”

Q5. DO YOU HAVE A DATA BREACH RESPONSE PLAN?

In 2012, then-FBI Director Robert Mueller stated, “There are only two types of companies in the world: those that have been breached and know it, and those that don’t.”

A data breach response plan will allow your organisation to confine, evaluate and respond to a data breach, such as the theft of customer information or business contract details.

A response plan names the individuals responsible for your organisation’s actions following a breach. The aim of a response plan is to react as quickly as possible, so your organisation can limit the damage and mitigate potential harm.

The Office of the Australian Information Commissioner publishes information on data breach response plans; however, the board must oversee the plans.

THE TRUTH ABOUT CYBERSECURITY

Boards of directors are faced with myriad topics and conflicting agendas during their regular course of proceedings.

Now, compelled by regulators, shareholders and customers, protecting information systems and the assets they hold has become one of a board’s most vital tasks.

It is impossible to eliminate all of your cybersecurity risk.

However, by asking the right questions and starting constructive conversations, your board can make sure that everyone in your organisation – from the C-suite down – is at least playing their part in minimising the risk of a cyber catastrophe.

1. https://www.oaic.gov.au/privacy-law/privacy-act/
2. https://www.oaic.gov.au/media-and-speeches/statements/mandatory-data-breach-notification
3. https://www.nist.gov/cyberframework
4. https://www.iso.org/isoiec-27001-information-security.html
5. http://www.iso27001security.com/html/27005.html
6. https://www.pcisecuritystandards.org/pci_security/
7. http://usdatavault.com/library/2016%20ntt%20global%20threat%20intelligence%20report.pdf
8. https://www.oaic.gov.au/about-us/

Diligent

Unleashing the value of information. Securely.

Diligent helps the world’s leading organisations unleash the power of information and collaboration – securely – by equipping their boards and management teams to make better decisions. Over 4,700 clients in more than 70 countries rely on Diligent for immediate access to their most time-sensitive and confidential information, along with the tools to review, discuss and collaborate on it with key decision-makers. Diligent Boards expedites and simplifies how board materials are produced and delivered via iPad, Windows devices and browsers. At the same time, Diligent Boards delivers practical advantages like cutting production costs, supporting sustainability goals, and saving administrative and IT time for leaders around the world.

Join the Leaders. Get Diligent.

For more information
or to request a demo,
please contact us by:

Tel: +61 2 9373 9601
Email: info@diligent.com
Visit: diligent.com

Download on the App Store | Get it from Microsoft | GET IT ON Google Play | AICPA SOC | ISO 27001 CERTIFIED BY BRIGHTLINE