Cybersecurity and the Board

Part 1 of 2: Where Should Cybersecurity "Live" and Why?

Steven Bowman
Managing Director
Conscious Governance

Monica Schlesinger
Principal
Advisory Boards Group

For years, cybersecurity has largely been seen as an IT responsibility, with the CIO and their team dealing with attacks from geeks and hackers seeking bragging rights, or disgruntled former employees who knew their IT infrastructure's weaknesses and security blind spots.

But over the last 10 years, things have become more serious, with highly damaging data breaches, intellectual property theft, compromised financial systems, stolen records sold on the "dark" markets, ransomware attacks and more. These factors have brought cybersecurity to the CEO's desk.

Today, the worst cyberattacks can shred an organisation's reputation and even destroy its business. Enter the board of directors.

Today, boards have an inescapable legal and fiduciary duty to protect their corporation's assets and shareholder value against all business risks, including the risk of cyberattacks.

Where, then, does cybersecurity fit into the board agenda? Are boards part of the solution or part of the problem? And what can they do to transform cybersecurity from something they don't even oversee to something they can exploit for competitive advantage?

CONSCIOUS GOVERNANCE

Advisory Boards Group

Diligent

THE STATE OF PLAY: WHAT BOARDS ARE DOING AROUND THE WORLD

Board consulting firm Conscious Governance surveyed 145 CEOs and board directors around the world about their experience of cybersecurity. The survey responses pointed to an all-too-familiar disconnect that exists in many boardrooms:

Q1. What has your experience of cybersecurity been like at the Board level?

Responses could be sorted into three categories:

- **87% had no idea,** even though three respondents had already suffered breaches or ransomware attacks.
- **8% had some discussion** or had heard about it.
- **4% had talked about it** or had considered it in their risk register.

One of the survey respondents reported having experienced multiple cyberattacks. Following the most recent attack, their organisation needed six months to recover. Very few of the organisations surveyed stated that they were well informed and had a cybersecurity strategy in place.

Q2. What do you believe is your greatest risk related to cybersecurity?

Over 12% of the respondents admitted candidly that they did not know or understand their cyber risks.

Around 30% referred to loss of reputation and branding, 40% to loss of sensitive information (with some specifying privacy breaches), and 40% mentioned operational and financial loss (including going out of business).

Q3. What are your top two questions about cybersecurity that the Board needs to continually consider?

Again, 12% of the respondents gave no answer or admitted that they didn't know. Risk management was referred to by 20%, with another 20% talking about policies.

Directors also thought of bringing an expert on the board (a 'Cyber Director'). Around 25% felt that the responsibility lies with the IT department and that they must do something to defend the organisation.

So it seems boards are aware of cybersecurity, but few have had strategic conversations on what to do about it.

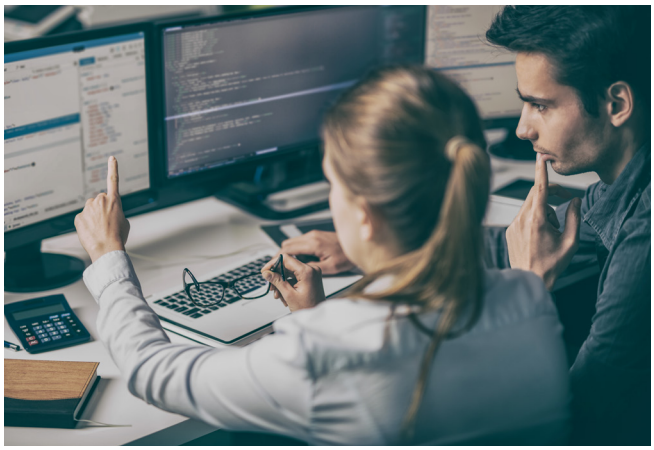
Significantly, about 20% of survey respondents said that they just didn't know where to start as directors, but they realised cybersecurity was a significant risk.

"Every board member should recognise it's not a matter of 'if', it's just a matter of 'when'. I can pretty much guarantee most directors that their organisations have either been hacked and they didn't know about it, or they will be hacked very soon," said Steven Bowman, MD, Conscious Governance.

THE STATE OF PLAY: WHAT BOARDS ARE DOING AROUND THE WORLD

How are boards thinking about cybersecurity, and how do they assess their own level of preparedness? Before we can answer this question, we must explore three areas of concern which are affecting many boards' overall attitudes toward cybersecurity and, ultimately, who is believed to be responsible for its governance.

First, many directors believe cybersecurity is only an information technology issue. Second, they are concerned about the onerous regulatory environment. Third, they underestimate the speed of the impact of a cyberattack and its potential consequences.



CYBERSECURITY IS NOT JUST ABOUT IT

Cybersecurity governance is much wider than IT security because often the issue isn't about technology at all. Boards should approach cybersecurity as a cultural issue as well as a management and governance issue.

"Directors must understand that cybersecurity is not an IT issue," said Bowman. "It's much bigger than that – it's a business continuity issue."

Boards often don't consider cybersecurity because they don't see themselves as a target, but it's not the case that only large or profitable companies get attacked – even charities and not-for-profit organisations have been targeted. "Hackers don't care," said Bowman. "They don't even know who you are. They're just looking for computers and networks they can get into."

A recent example is WannaCry, a computer virus that infected 545,245 computers[1] around the world. WannaCry was indiscriminate. It hit Britain's National Health Service and universities throughout China. For boards, your 'new normal' is that your organisation is in the crosshairs.

CYBERSECURITY-RELATED REGULATION IS YOUR FRIEND

Every board has a charter. One of a board's main duties is oversight of its organisation's finances and operations. This includes regulatory compliance.

Around the world, legislation demands a duty of care from directors. Whether it's Australia – sections 180 and 181 of the Corporations Act – or the US, UK or Europe, all boards must show due diligence.

"There is an enormous amount of national and international legislation and regulation starting to appear that will have a major impact on directors' liability if they continue to ignore cybersecurity. You should get ahead of the game and be prepared," said Bowman.

For example, Australia's mandatory data breach notification scheme, in force from 23 February 2018, applies to all companies subject to the Privacy Act.

Companies with European clients or EU citizens as clients must also deal with the incoming General Data Protection Regulation (GDPR) – a much tougher regime than what we have in Australia. If companies do not comply with the GDPR, the penalties are severe – €20 million or 4% of annual revenue, whichever is greater. It comes into effect on 25 May 2018.

CYBERATTACKS ARE FAST AND DANGEROUS

A cybersecurity event will likely come with little warning and can quickly bring down an organisation, whether corporate, government or not-for-profit. The speed of a cyberattack – and its potential impacts – put cybersecurity outside the 'normal' risk register.

"You must treat cybersecurity as a very, very different and special risk," said Monica Schlesinger, Principal, Advisory Boards Group. "Why? Because things can happen so fast. You can lose your entire company within the space of a few weeks."

The organisations doing cybersecurity well treat it as an issue in its own right – not as a subset of enterprise risk. They know that attacks can happen quickly and that the consequences can be dire.

WHO SHOULD BE RESPONSIBLE FOR CYBERSECURITY?

There is a tendency for boards to place cybersecurity under their finance or risk management committees. However, we're starting to see more boards give cybersecurity to a security sub-committee, rather than subsume it under risk management.

Today, cybersecurity is everyone's business. It is a mission-critical function. Touching every corner of an organisation – public or private sector – the natural home for the security of any organisation's information systems is with those people who are ultimately responsible for that organisation.

WHAT NEEDS TO CHANGE?

It's time to move the conversation from one of compliance – "What are we going to do about cybersecurity?" – to one of governance – "What do we need to do to govern cybersecurity from a strategic perspective?"

For boards, this means overcoming fear. "The fear of asking questions when you don't know about something. It's like the fear of trying to say something in a new language," said Schlesinger.

"You've got to start somewhere. If you don't know where to start, haul in your management."

Attitudes are starting to change. Cybersecurity must get out of the 'fear and risk' category and become a strategic play. In practical terms, this means understanding what motivates hackers and cyber criminals, and making strategic investments in the teams and technologies to secure your business.

MOVE WITH THE TIMES

There are already efforts to create more diversity on boards – trying to attract people who are younger and more comfortable with technology. This means boards will have a better general awareness of cybersecurity and its impact.

But it's also important to talk about the drivers and the evolution of cybersecurity.

Thirty years ago, we talked about hackers who were causing mischief for bragging rights, or about disgruntled employees seeking revenge on a company.

Now, hacking is a business. On the dark web, hacker services can be hired to compromise any network. It costs about $A300 to hack somebody's email address. There are denial of service attacks for hire that bring websites down by bombarding them with thousands of requests. Hackers want to make money; the tools are easy to find, simple to execute and cheap to hire; and they find many networks easy prey[2].

"It's an arms race," said Schlesinger. "We must keep up with everything that is happening and understand the motivations and methods of these hackers to stay safe."

INVEST IN INFRASTRUCTURE AND PEOPLE

Today, companies collect terabytes of information on millions of people. Often, these organisations – especially government and not-for-profit enterprises – have not been funded to maintain the infrastructure necessary to make sure they can keep the data secure.

That's starting to change, particularly with the not-for-profit sector, where there are some multimillion-dollar organisations with millions of personal and business-related records.

These organisations' boards should view cybersecurity from a governance perspective, not from a management perspective. This also means investment – in infrastructure and in people.

If the organisation wants to not only manage cybersecurity, but also turn it to their advantage, then the board must set the agenda.

"Imagine if you had the world's best cyber-tools and cybersecurity protocols – both the technology and the people," said Bowman.

"You could do things other organisations would not have thought possible because you understand the space and you have the people and the systems to go after contracts no one thought you could."

There is no reason boards shouldn't see cybersecurity as an opportunity to create strategic advantage, rather than simply manage it as a risk and compliance issue.

Cybersecurity is here to stay. And boards have a choice. They can do the minimum and simply comply, or they can go a step further in their defence strategy to protect their businesses.

WHAT TO DO NEXT

How do boards implement change?

First, by thinking about cybersecurity as more than just a risk – it's a game changer. This is why cybersecurity shouldn't sit under the usual risk level; it should sit alongside risk – finance, audit, risk management and security risk – elevated at board committee level.

The International Organisation of Securities Commissions (IOSCO), of which ASIC is a member, recommended in its April 2016 report *Cybersecurity in Securities Markets – An International Perspective*[3] that cybersecurity be elevated and treated differently from other risks:

"In many respects, cyber risk is not 'just another risk'. Cyber risk is a highly complex and rapidly evolving phenomenon. And the human element of cyber risk, combined with rapidly evolving technologies, gives it some unique characteristics: as organisations upgrade their defences, criminals continuously develop new and more complex approaches.

"Ultimately, in a highly interconnected and interdependent financial ecosystem, cyber-attacks may have systemic implications for the entire financial system, and also affect over time the trust on which financial markets are built."

TEST YOUR RESPONSES

Every organisation will have a disaster recovery plan. It should include cyber risk. However, a disaster recovery plan is useless unless you test it every six months – or at least annually – to make sure it works.

Boards should identify their key cyber risks and put in place what they need to minimise the potential for any of them to occur. Then, put measures in place that will minimise the impact if any of them do occur.

"It's like a fire drill. Everyone has fire wardens and they know what to do if there is a fire in the building. Think of cyberattacks as the fire of today's business environment," said Schlesinger.

COSTS – AND OPPORTUNITIES

Boards also need to view cybersecurity from a revenue perspective. If you look at everything from a cost perspective, then you'll only ever see costs. If you see cybersecurity as providing strategic opportunities or strategic advantage, then you'll start to unearth opportunities to create other revenue streams.

It's a question of intellectual and cultural awareness more so than of resources and money. It's about people and their habits. This is the cultural issue boards must address.

How much should boards invest in cybersecurity? What value do you place on the things you are trying to protect from cyberattack, such as your organisation's intellectual property, or your customers' privacy?

Think of what you could lose – and think about the consequences of a cyberattack. Put the right governance in place and you'll not only ensure your organisation's survival, you may even create a new competitive advantage.

PUT CYBERSECURITY ON THE AGENDA

The simplest technique is to put cybersecurity on your board agenda as an ongoing discussion item. You can bring people in to start educating the board – not about the IT aspects of cybersecurity, but about governance and due diligence.

"I was on a board for many years and at every board meeting we would invite one of the managers in the business to tell us what they were doing," said Schlesinger. "We were educating ourselves. We knew the pulse of the organisation."

You can start with your IT manager or CIO, then bring in an independent contractor for a discussion at the board meeting. Allocate some time – even 10 or 15 minutes is worthwhile. The key is to place cybersecurity in a larger business context, and to emphasise that it's not just an IT matter; as Bowman noted, "The last thing you should do is bring in an IT expert to get everyone bored with the IT component of cybersecurity because that's only one component."

Some organisations bring in the chair of another board who has put time into this matter and who is willing to share their experience.

In fact, getting outside people to come in and talk about the governance and strategic aspects of cybersecurity is worth including as a standing agenda item for your finance, audit and risk committee. This committee should become a finance, audit, risk and security committee, so that at least it has a focus on cybersecurity, and it's not lost under the risk umbrella.

It can be as simple as finding out what others who have been successful with cybersecurity are doing.

For example, many organisations in the health and finance sectors have become leaders in cybersecurity, given the nature of their businesses. Ask them what conversations they had in their boardroom.

The board has a duty to ensure learning and development at all levels in the company – including for the members of the board.

Board members should know what cybersecurity means for directors, what regulatory compliance is, what directors should do, what questions to ask, and how to institute a cybersecurity strategy. They must know what to do to make sure their organisation is cyber-secure?

"If you're not sure where to start, get your finance, audit, risk management and security committee to develop a cybersecurity governance policy," Bowman suggested. "That policy should include everything you need to be aware of. You can work backwards to develop the infrastructure you need to support your policy."

LOOK AT CYBERSECURITY FROM A PEOPLE PERSPECTIVE

Do you have strong processes and a strong culture in place? Do people in your organisation know what they're doing when they click on email attachments or share their passwords with a 'work' colleague?

Do you have the right policies in place for hiring and firing? Do you give employees the minimum access to your network? Have you done anything about your third-party contractors?

Most breaches happen through human nature – the social conditioning that dictates what we do with technology. Unless your board is clear about the culture it wants to create, and it makes that desired culture a KPI for the CEO, then cybersecurity just becomes an IT issue rather than a whole-of-organisation issue.

Elevate cybersecurity from a standard risk management and compliance issue, and turn it into something that has strategic implications and potential leverage.

DEFINE THE RISK LEVEL YOU ARE PREPARED TO LIVE WITH

The Australian Signals Directorate recommends measures that will protect the organisation against 85% of the attacks, on average, though this can be restrictive for the employees. Whitelisting applications (limiting the number or type of applications you can run on a computer) is such a measure.

A great American author once said, "A ship in harbour is safe, but that is not what ships are built for."

At board level, you need to gauge how much control you want to put in place against how much risk you're prepared to take to grow – yet still protect – your organisation. It's part of your risk appetite, which is part of the risk strategy.

No board should remain in a state of inertia. The only approach is to be prepared so you can minimise the potential of a cyberattack happening, and minimise the impact when (not if) it does.

1. https://blog.barkly.com/wannacry-ransomware-statistics-2017
2. https://securityledger.com/2017/02/hacker-for-hire-survey-finds-most-networks-easy-prey/
3. https://www.iosco.org/news/pdf/IOSCONEWS423.pdf

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.

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

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

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

WP0040_ANZ