A Guide to

Cyber-risks

for Directors and Officers

provided by Hazelton Mountford

HM
Hazelton Mountford
Chartered Insurance Brokers

Keeping workplace technology up and running is vital to any organisation's success. While this task may seem feasible, it's growing more difficult each year as cyber-criminals expand their reach. It's not enough to protect workplace technology with only software and security protocols. Instead, every member of an organisation must educate themselves on and protect against cyber-exposures related to ransomware attacks, social engineering scams and similar threats.

This is especially important considering that organisations of all sizes and sectors face increased cyber-security risks year after year. In fact, cyber-related disruption was rated the number one risk for businesses in 2023 by global insurer Allianz. What's more, approximately £2.4 million is lost to cyber-crime every minute; cyber-crime is projected to cost the world an estimated £8.7 trillion annually by 2025, according to a report by software company RiskIQ.

Simply put, every organisation that stores or handles data is at risk of a cyber-attack. As technology advances, companies are collecting, storing and transferring more personal information about their customers and employees than ever before. Not only does this put a target on an organisation's back, but it also means that just one breach can affect thousands or even millions of individuals.

Many wrongly assume that IT departments are solely responsible for managing data risks and ensuring cyber-security across an organisation. **In order for businesses to protect themselves, management must also play an active role.** Involvement from leadership not only improves cyber-security but also reduces liability for directors and officers. When cyber-attacks occur, legal action against directors and officers often follows. Specifically, stakeholders affected by a cyber-attack may allege that senior leadership failed to adequately address cyber-security threats or establish a plan for responding to an attack.

To reduce the likelihood of such claims, it's imperative for senior leadership to be actively involved in monitoring an organisation's unique cyber-risks. This means implementing proper cyber-security practices to prevent potential attacks, ensuring compliance with all applicable data security standards and establishing an effective cyber-incident response plan to minimise any damages in the event of an attack.

This guide is designed to help directors and officers, and other senior leaders of an organisation, plan for and respond to cyber-incidents.

Contents

This guide is for informational purposes only and should not be construed as legal or professional advice.

The Anatomy of a Cyber-attack

Before examining what senior leadership can do to manage cyber-risks, organisations need to understand who cyber-criminals are, what they want and what's at stake. In today's hyper-connected world, nearly every business has some form of cyber-exposure. Whether you process payments or store sensitive customer information, chances are cyber-criminals have already placed a target on your organisation and are primed to strike.

Common Threat Actors

Cyber-criminals are often much more sophisticated than they are given credit for. Examine the most common threats to your business:

Insiders

Employees are some of an organisation's best assets, but they can also be some of its greatest threats. In some cases, well-meaning employees accidentally put confidential information at risk through careless cyber-security practices. Other times, disgruntled current or former employees with access to the business's system will compromise assets or steal proprietary data to get back at an organisation. But it's not just data that's at risk. A cyber-attack can lead to an IT failure that disrupts business operations, costing the organisation both time and money.

Organised cyber-criminals

Cyber-crime has become increasingly organised and lucrative, even surpassing the drug trade to become one of the most profitable illegal industries. In fact, cyber-crime costs the UK billions of pounds each year. Given how much they are able to steal, it makes sense that organised cyber-criminals are primarily interested in money. These groups often seek personally identifiable information like National Insurance numbers, health records, credit card details and banking information. They then hold this information hostage through ransomware or sell it outright on the dark web to turn a profit.

Hacktivists

"Hacktivists"—a portmanteau of "hacker" and "activist"—operate with a political agenda, often carrying out high-profile attacks to distribute propaganda or damage organisations they disagree with. Hacktivists typically fall under the category of cyber-vandalism and look to damage reputations or steal incriminating information. Many hacktivists work alone, which can make their attacks more difficult to predict.

Government-sponsored Groups

It may sound like something from a movie, but government-sponsored attacks and cyber-espionage are real threats. These cyber-criminals are well-funded and are typically motivated by political, economic, technical or military agendas. Government-sponsored attacks are often very sophisticated, and these groups target highly sensitive and competitive proprietary data. In some instances, these groups have set their sights on energy facilities and other critical infrastructure systems, which can cause significant disruptions to organisations or even entire cities. These types of attacks often use multiple hacking strategies over a long period of time to gain prolonged access to a company's network.

What's At Risk

Businesses, both large and small, need to be proactive to protect themselves against growing cyber-threats. As larger companies take steps to secure their systems, smaller, less-secure businesses are becoming increasingly attractive targets for cyber-criminals. With this in mind, organisations must know what cyber-criminals might be after and what it could cost to recover from a breach. To help you avoid litigation and other costs associated with a cyber-attack, examine five examples of at-risk assets:

❶ **Productivity and operations—**Just one cyber-event can wreak havoc on an organisation and cause significant disruptions. Following a cyber-event, a business may lose its ability to service its customers. Additionally, employees may be unable to work altogether, leading to significant downtime. It is easy to see how any of these events might leave your company scrambling to do business. Unfortunately, many businesses don't have the resources available to detect and resolve the problem, which only increases the length of an interruption.

❷ **Banking credentials—**If there's one thing every thriving business has, it's a payroll. Financial information like this is an attractive target for cyber-criminals, especially considering how easy it is for malicious parties to impersonate your business or employees by using stolen banking credentials. In fact, cyber-criminals can drain entire accounts in a matter of minutes with this information.

❸ **Sensitive data—**Nearly every organisation works closely with vendors, staff and customers, storing sensitive information on their behalf. Things like credit card numbers, names, addresses, National Insurance numbers, emails and login credentials are common targets for cyber-criminals. In just one cyber-attack, criminals can gain access to financial accounts or information they can sell to other malicious parties. Not only do these types of attacks severely damage your reputation, but they can lead to expensive litigation, notification costs and potential compliance fines—expenses that can quickly sink an unprotected business.

❹ **Proprietary information and trade secrets—**As part of senior leadership, you work hard to differentiate your business from the competition. In fact, many organisations have designs, products and plans that are unique to them and a key component of future growth. Cyber-criminals understand the value of trade secrets and can earn big money selling proprietary information on the dark web. Following a loss of this kind, organisations can irreversibly lose their standing in the marketplace.

❺ **Physical assets—**Many wrongfully assume that the steep monetary burden of a cyber-attack is exclusively tied to damaged digital assets, lost records and the price of investigating and reporting a breach. While those expenses represent a significant hit, damage to an organisation's physical assets can be just as harmful. Cyber-attacks that cause physical damage typically occur when a hacker gains access to a computer system or app that controls equipment at a business. They can then control that equipment to cause damage to it or other property. As more traditionally offline items like homes, vehicles and heating, ventilating and air conditioning systems become a part of the Internet of Things, the potential for physical damage following a cyber-attack will increase.

While this list doesn't represent every cyber-exposure your business may have, it accounts for the most common targets.

In 2020, approximately **9 million** Easy Jet customers had their personal data unlawfully accessed by third parties in a sophisticated cyber-attack.

Consequently, law firm PGMBM issued a claim in the London High Court seeking damages of up to **£18 billion** on behalf of impacted customers.

Spotlight on Board Member Risks

In order for organisations to truly protect themselves from cyber-risks, all of senior leadership—including boards of directors—must play an active role. Involvement from leadership like you both improves cyber-security and can reduce liability for directors and officers.

As just one cyber-attack can result in significant damages, including reputational harm, financial losses, legal action and even regulatory action, efforts to improve cyber-security from boards of directors are crucial. In some instances, a cyber-event can negatively impact an organisation's share price, which could cause directors and officers to be sued for a breach of their fiduciary duty.

Further complicating matters, global regulators are increasingly concerned regarding the consequences of a cyber-attack. As a result, senior leadership—directors and officers especially—are being challenged to play a greater role in managing cyber-risks for the businesses they represent. In particular, boards of directors are being asked to sign off on an overall cyber-security plan that accounts for risk management considerations, delegation practices and cyber-risk escalation procedures, among other matters.

Should a board of directors fail to do their due diligence, they are not only endangering the well-being of the company, but they're also putting their finances on the line should they be sued.

General Responsibilities of Directors and Officers

While it's important for management to provide adequate oversight, carrying out cyber-security initiatives is ultimately up to a company's appointed leadership. Above all, senior leadership must ensure that everyone clearly understands their roles and responsibilities. At a high level, directors and officers must complete the following:

Policies

- Adopt written cyber-security policies, procedures and internal controls.
- Implement tools that detect cyber-security events.

Appointments

- Discuss (at the management and board level) the hiring of a chief information officer, chief security officer or similar role. Hiring a chief information security officer or creating a new cyber leadership role is not practical for every business. In these instances, organisations should identify a qualified, in-house team member and roll cyber-security responsibilities into their current job requirements.

Reviews and Reports

- Review budgets and IT security programmes on a regular basis.
- Receive and review reports on any data incidents.
- Remain well-informed on cyber-security trends that could impact the business.
- Create and oversee a team of individuals who are responsible for cyber-security oversight.

Direction

- Assess cyber-security risks.
- Determine which risks can be mitigated directly and which may be transferred using cyber liability insurance or other coverage.

Integrating Cyber-risks Into the Board's Objectives

Given the potential burdens a cyber-attack can put on directors and officers (eg legal action and compliance fines), the importance of board member involvement in cyber issues cannot be understated. Cyber-security must be accounted for in organisational decision-making, especially when considering its impacts on nearly every aspect of a business.

Poor cyber-security practices can create:

Operational risks should a business get hacked and lose access to digital services used to communicate with employees and customers (eg, email or websites).

Legal risks should a cyber-attack lead to a breach in contract or result in regulatory fines.

Financial risks, as a cyber-attack can lead to legal action, business interruptions and costs related to mitigating the damage from a breach.

One of the best ways boards can play an active role in cyber-security is to incorporate managing and mitigating cyber-risks as a part of their overall business strategy. This helps the board of directors remain invested in cyber-security measures, which, in turn, allows them to build a more cyber-safe culture.

Simply put, cyber-security is more than having good technology in place to address threats—it's about having the right culture and putting the right people and processes in place to manage cyber-risks effectively. For instance, to protect against data threats, boards must ensure their organisations have solutions that account for storing and handling data as well as managing the way the organisation accesses that data. These types of considerations need to be reflected in the organisation's structure.

Further, cyber-security shouldn't be the responsibility of one person. Instead, protecting company data and preventing a cyber-attack must be the goal of the entire board of directors. A board of directors should understand the potential impact a cyber-attack can have on all aspects of the business and empower technical experts to assess and mitigate cyber-exposures.
To better integrate cyber-risks into their objectives, boards of directors should ask themselves the following:

- Do board members understand the value of cyber-security?
- Has the board chosen an individual or entity to oversee the organisation's cyber-security practices? What are this individual's/entity's objectives? How does the board communicate with this individual/entity and provide updates on cyber-security initiatives? What does the reporting structure look like, and does it encourage communication?
- Does the individual/entity responsible for cyber-security have access to key stakeholders throughout the company to ensure all aspects of the business are considered in regard to reducing cyber-exposures?
- Are risk assessments and defensive priorities regularly reviewed and updated?

Growing Your Cyber-expertise

As part of senior leadership, you have a responsibility to build a team of experts that will ensure your organisation is adequately prepared should a cyber-attack occur. Having such a team also gives organisations the ability to draw upon the experience of proven professionals when it comes to assessing and responding to potential cyber-threats. When building out this expertise, there are specific duties for board of directors to consider.

For board members, growing the organisation's cyber proficiency involves auditing current practices. Essentially, senior leadership should understand the cyber expertise your organisation has access to today so they can plan for tomorrow. From there, it's a matter of determining what professionals, positions or processes are needed to strengthen the organisation's cyber expertise. For instance, this could involve hiring a chief information security officer.

It's important to note that directors and officers must determine if cyber experts are needed not only organisationally but also on the board. This ensures the board is making the best strategic decisions in the event of a cyber-incident.

Making the Most of Existing Talent

It can be difficult to attract and retain cyber professionals, particularly during a challenging hiring market. As a result, building out an organisation's cyber expertise isn't always about recruiting and instead involves upskilling. When creating a team of cyber experts, it's important to remember that the skillsets you need will vary from role to role. While you may need networking or infrastructure professionals, it's equally necessary to secure staff who can understand cyber issues and train others on complex concepts.

A report from cyber-security vendor Tessian found that **43%** of employees are "very" or "pretty" certain they have made a mistake at work that had security repercussions.

Creating Clear Training Policies

Every cyber-security programme must address employee training and create cyber-security policies. The content of these policies will differ depending on the size and type of the organisation, but it typically includes similar elements. Here are some questions the board should ask themselves:

- Does our organisation have a cyber-security policy in place?
- Is our organisation's cyber-security policy enforced?
- Does our organisation's cyber-security policy include provisions regarding privacy?
- Does our organisation have a system in place for checking the background of employees and contractors who have access to computer systems and sensitive data?
- Are employees and contractors required to wear ID badges?
- Does our organisation ensure the physical security of its computer systems?
- Does our organisation have a process for notifying IT personnel if a device is misplaced or stolen?
- Are staff informed regarding the importance of computer security?
- Does our organisation provide employees with cyber-security training on a regular basis?
- In the event of a cyber-attack, do our staff know how to respond?

Leveraging External Expertise

Not every business will have the time or ability to train and upskill their employee base to build out their cyber expertise. In these instances, seeking third-party assistance can effectively improve an organisation's cyber authority. Some options to consider include:

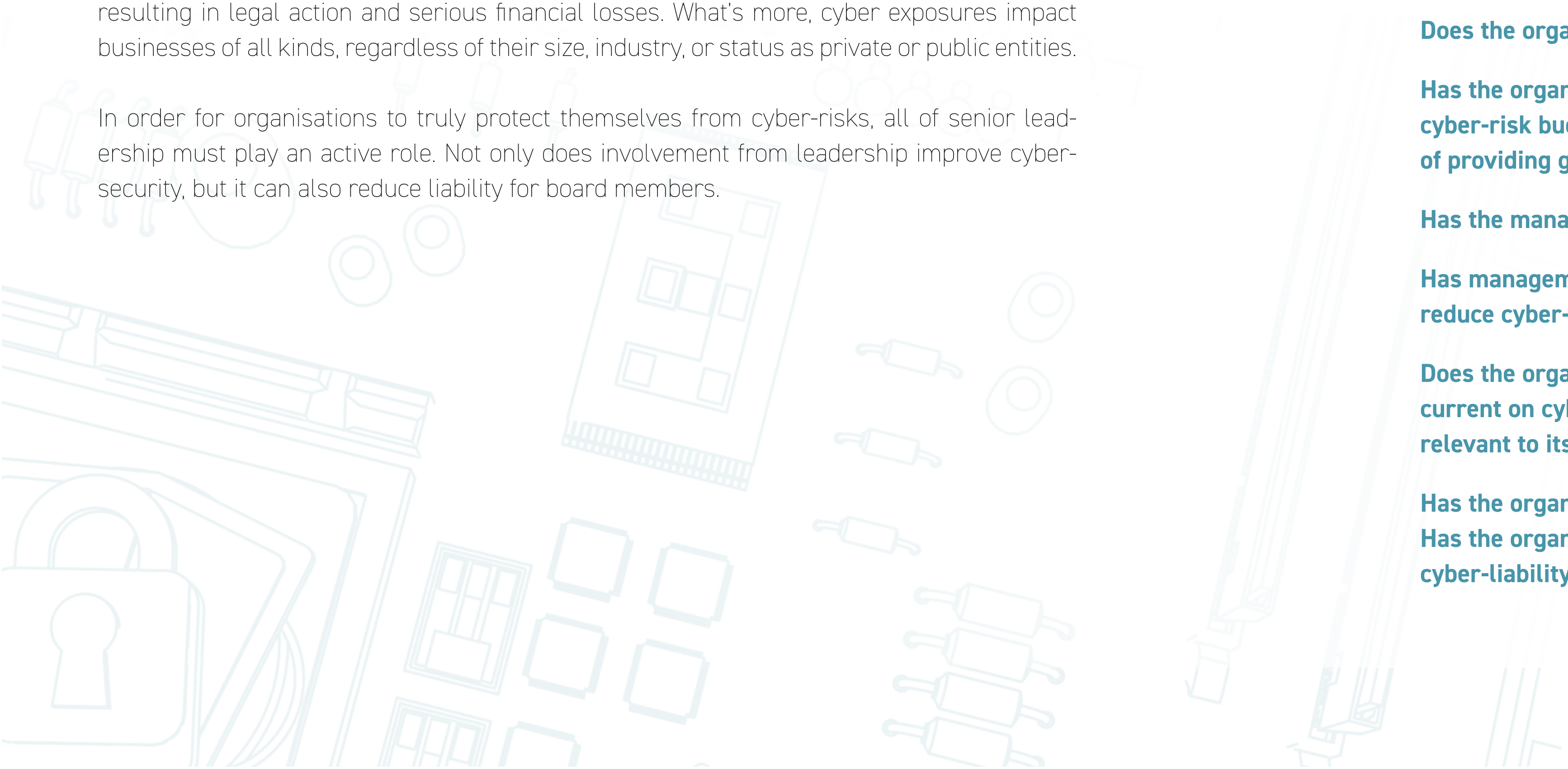
- Recruiting a skilled, non-executive director to the board
- Employing a cyber-security consultant
- Identifying the specific cyber-security services the organisation is lacking and seeking the help of a third party to address any gaps
- Recruiting employees who already have the skills the organisation needs

Above all, assessing the cyber expertise you have access to ensures you are agile in building resilient systems and keeping pace with evolving technology.

Assessing Your Organisation's Cyber-risks

When a data breach or other cyber-event occurs, the damages can be significant, often resulting in legal action and serious financial losses. What's more, cyber exposures impact businesses of all kinds, regardless of their size, industry, or status as private or public entities.

In order for organisations to truly protect themselves from cyber-risks, all of senior leadership must play an active role. Not only does involvement from leadership improve cyber-security, but it can also reduce liability for board members.



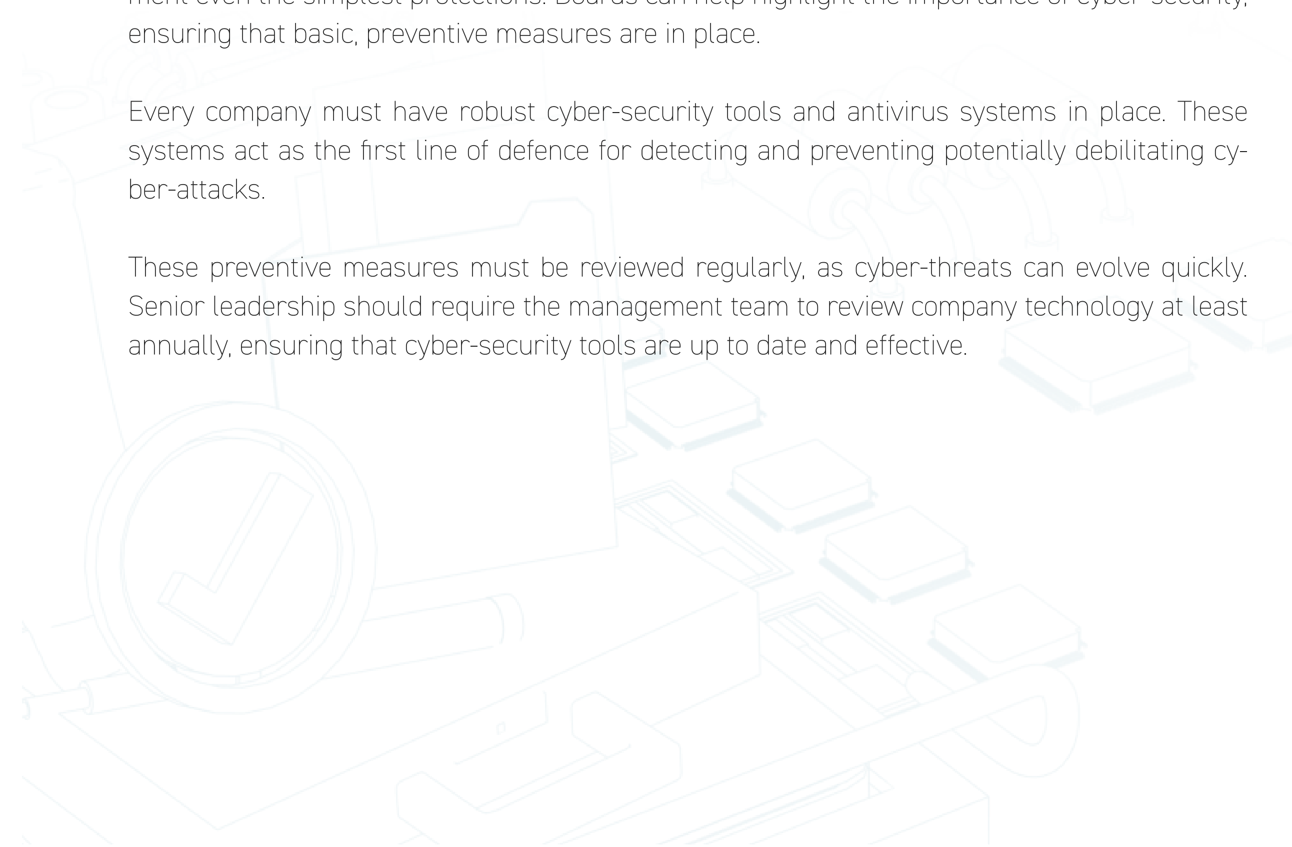
To help oversee their organisation's cyber-risk management, directors and officers should ask the following questions:

Does the organisation utilise technology to prevent a cyber-attack?

While it may sound obvious, many organisations fail to take cyber-threats seriously and implement even the simplest protections. Boards can help highlight the importance of cyber-security, ensuring that basic, preventive measures are in place.

Every company must have robust cyber-security tools and antivirus systems in place. These systems act as the first line of defence for detecting and preventing potentially debilitating cyber-attacks.

These preventive measures must be reviewed regularly, as cyber-threats can evolve quickly. Senior leadership should require the management team to review company technology at least annually, ensuring that cyber-security tools are up to date and effective.



Has the board or the company's leadership team identified a senior member to be responsible for organisational cyber-security preparedness?

Organisations that fail to create cyber-specific leadership roles could end up paying more for a cyber-attack than organisations that do. This is because, in a cyber-incident, fast responses and clear guidance are needed to contain a breach and limit damages.

When establishing a chief information security officer or similar cyber leadership role, directors and officers need to be involved in the process. Cyber leaders should have a good mix of technical and business experience. These individuals should also be able to explain cyber-risks and mitigation tactics at a high level so they are easy to understand for those who are not well versed in technical terminology.

It should be noted that hiring a chief information security officer or creating a new cyber-leadership role is not practical for every organisation. In these instances, organisations should identify a qualified, in-house team member and roll cyber-security responsibilities into their current job requirements. At a minimum, senior leadership must ensure that their company has a go-to resource for managing cyber-security.

Does the organisation have a comprehensive cyber-security programme? Does it include specific policies and procedures?

It is essential for companies to create comprehensive data privacy and cyber-security programmes. These programmes help organisations build a framework for detecting threats, remain informed on emerging risks and establish a cyber-response plan.

Directors and officers should ensure that cyber-security programmes align with industry standards. These programmes should be audited regularly to ensure effectiveness and internal compliance.

Does the organisation have a cyber-response plan in place?

Even the most secure organisations can be impacted by a cyber-attack. What's more, it can often take days or even months for a company to notice it has been compromised.

While cyber-security programmes assist with securing an organisation's digital assets, cyber-response plans provide clear steps for companies to follow when a cyber-event occurs. These response plans allow organisations to notify impacted customers and partners quickly and efficiently, limiting financial and reputational damage. A quick response to a cyber-event also limits prolonged disruptions to the organisation's operations.

Senior leadership should ensure crisis management and response plans are documented. Specific actions noted in response plans should also be rehearsed through simulations and team interactions to evaluate effectiveness.

In addition, response plans should clearly identify key individuals and their responsibilities, eliminating confusion in the event of a breach and ensuring your organisation's response plan runs as smoothly as possible.

Has the organisation discussed and formalised a cyber-risk budget? How engaged is the board in terms of providing guidance related to cyber-exposures?

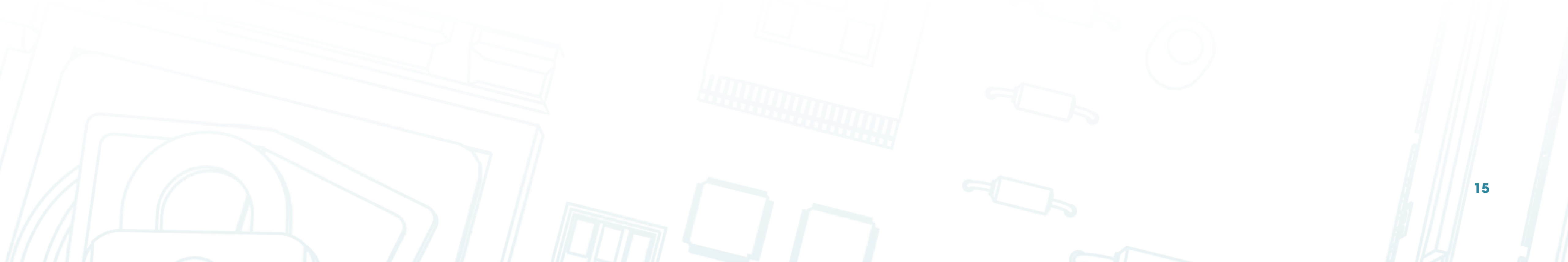
Both overpaying and underpaying for cyber-security services can negatively affect an organisation. Creating a budget based on informed decisions and research assists companies in investing in the right tools.

Senior leadership can help oversee investments and ensure they are directed toward baseline security controls that address common threats. With guidance from the chief security officer or a similar cyber leader, boards should also prioritise funding. That way, an organisation's most vulnerable and essential assets are protected.

Has the management team provided adequate employee training?

Employees are an organisation's first line of defence when it comes to preventing a cyber-attack. As such, organisations must provide thorough employee cyber-security training. Directors and officers can assist with overseeing this process and instruct management to make training programmes meaningful and based on more than just written policies.

In addition, senior leadership should make sure education programmes are properly designed and foster a culture of cyber-security awareness.



Has management taken the appropriate steps to reduce cyber-risks when working with third parties?

Working alongside third-party vendors is common for many businesses. However, when an organisation entrusts its data to an outside source, there's a chance it could be compromised.

Senior leadership can help ensure that vendors and other partners are aware of their organisation's cyber-security expectations. Directors and officers should work with the company's management team to draw up a standard third-party agreement that identifies how the vendor will protect sensitive data, whether or not the vendor will subcontract any services and how it intends to inform the organisation if data is compromised.

Does the organisation have a system in place for staying current on cyber-trends, news and data security regulations relevant to its sector?

Cyber-related legislation can change with little warning, often having a sprawling impact on the way organisations do business. If organisations do not keep up with both local and international data security regulations, they could face serious fines or other penalties.

Senior leadership should confirm that the chief information security officer or similar leader is aware of their role in upholding cyber compliance. In addition, directors and officers should be sure there is a system in place for identifying, evaluating and implementing compliance-related legislation.

Additionally, senior leadership should constantly seek opportunities to bring expert perspectives into boardroom discussions. Often, government authorities, the police and cyber-security agencies can provide invaluable advice. Building a relationship with these types of entities can help organisations evaluate their strengths, weaknesses and critical needs when it comes to cyber-security.

Has the organisation conducted a thorough risk assessment? Has the organisation purchased or considered purchasing cyber-liability insurance?

Cyber-liability insurance is specifically designed to address the risks of using modern technology—risks that other types of business liability cover usually won't include.

The level of cover your business needs is based on your individual operations and can vary depending on your range of exposure. As such, directors and officers, alongside the company's management team, need to conduct a cyber-risk assessment and identify potential gaps. From there, organisations can work with their insurance broker to customise a policy that meets their specific needs.

Implementing Cyber-security Measures

Even the most secure organisations are at risk of a cyber-attack, often taking days or even months to notice their data has been compromised. Cyber-attacks are no longer a matter of if but when, and reacting to a breach takes more than just threat neutralisation. When it comes to containing the damage caused by a cyber-attack, having a response plan in place is crucial.

While cyber-security programmes secure an organisation's digital assets, cyber-incident response plans provide clear steps for companies to follow when a cyber-event occurs. This type of plan allows organisations to notify impacted customers and partners quickly and efficiently, limiting financial and reputational damages.

Most organisations have some form of data protection in place. Although these protections are critical for minimising the damages caused by a breach, they don't provide clear action steps following an attack. That's where cyber-incident response plans can help.

Cyber-incident response plans are written guides comprised of instructions, procedures and protocols that enable an organisation to respond to and recover from various data security incidents. Companies must have the ability to defend against evolving threats, and cyber-incident response plans give organisations the tools they need to further enhance their data protection practices as well as assist with:

1. Anticipating cyber-security incidents before they occur
2. Minimising the impact of cyber-security incidents
3. Mitigating threats and vulnerabilities while a cyber-attack occurs
4. Improving cyber-security response overall, encouraging buy-in at a management level
5. Reducing the direct and indirect costs caused by cyber-security incidents
6. Maintaining business continuity in the face of significant threats
7. Preventing the loss of data critical to their business
8. Improving the overall security of their organisation
9. Strengthening their reputation as a secure business, thus increasing partner and customer confidence
10. Devoting more time and resources to business improvements, innovation and growth

Creating a Cyber-Incident Response Plan

The following checklist is a set of general recommendations organisations should keep in mind when creating a cyber-incident response plan. Select yes or no to help identify areas where you may need to focus cyber-response efforts.

Yes	No	
○	○	Your plan is part of a larger cyber-security programme that identifies tools and resources for incident handling. This programme helps prevent incidents from occurring by ensuring that networks, systems and applications are sufficiently secure.
○	○	Your plan establishes mechanisms that outside parties can use to report incidents.
○	○	Your plan takes into account the periodic auditing of critical IT systems.
○	○	Your employees understand what normal network, system and application behaviour looks like. They are trained to report any suspicious activity.
○	○	Your plan accounts for data retention and allows you to create and store information about any and all breaches.
○	○	Your plan allows you to record and track information regarding a breach the moment one occurs.
○	○	Your plan allows you to assess cyber-incidents quickly and prioritise them accordingly.
○	○	Your plan establishes strategies and procedures for containing incidents.
○	○	Your plan provides specific steps to restore system and network integrity.
○	○	Your plan accounts for privacy and payment card industry compliance, and competent legal advice or legal opinion is involved in the creation and management of your plan.
○	○	Your plan includes a cyber-incident analysis phase that allows you to evaluate the success of your response plan.
○	○	Your plan establishes an incident response team with clearly defined and documented responsibilities. These individuals are properly trained and understand their roles following a cyber-security event.
○	○	Your plan establishes a method for facilitating communications, internally and externally.
○	○	Your plan is practicable.
○	○	Your plan is regularly updated.
○	○	Your plan makes a note of safeguards, including cyber liability insurance.
○	○	Your plan provides information on who to contact following a breach, including law enforcement and government officials.

Moving Forward

Even if you have strong risk-management and cyber-security practices in place, you still can't eliminate the chance that a cyber-attack might occur and negatively impact your organisation. As a result, it's critical for the board of directors—and indeed all of senior leadership—to lead by example and take steps to protect the company and its assets.

To discuss more ways to assess and mitigate potential cyber exposures, contact us today.