A Guide to

Cyber Risks

for Boards of Directors

provided by Autumn Insurance & Benefits

autumn
insurance & benefits

Keeping workplace technology up and running is vital to any organization's success. While this task seems feasible, it's growing more difficult each year as cybercriminals expand their reach. It's not enough to protect workplace technology with only software and security protocols. It's critical for organizations to educate themselves on and protect against cyber exposures related to ransomware attacks, social engineering schemes and similar threats.

This is especially important when you consider that organizations of all sizes and sectors face increased cybersecurity risks year after year. What's more, **$2.9 million** is lost to cybercrime **every minute**; cybercrime is projected to cost the world **$10.5 trillion annually** by 2025.

Simply put, every organization that stores or handles data is at risk of a cyberattack. 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 organization'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 cybersecurity across an organization. In order for businesses to protect themselves, management must also play an active role. Involvement from leadership not only improves cybersecurity but also reduces liability for directors and officers. When cyberattacks occur, lawsuits against directors and officers often follow. Specifically, stakeholders affected by a cyberattack may allege that your senior leadership team failed to adequately address cybersecurity threats or establish a plan for responding to an attack.

To reduce the likelihood of such claims, it's imperative for your senior leadership team to be actively involved in monitoring your organization's unique cyber risks, implementing proper cybersecurity practices to assist in preventing potential attacks, ensuring compliance with all applicable data security standards and establishing an effective cyber incident response plan to minimize any damages in the event of an attack.

This guide is designed to help board members and senior leaders of an organization plan for and respond to cyber incidents.

Contents

Contents 2

The Anatomy of a Cyberattack 3

Common Threat Actors 4

What's At Risk 5

Spotlight on Board Member Risks 6

General Responsibilities of Directors and Officers 7

Integrating Cyber Risks Into the Board's Objectives 8

Growing Your Cyber Expertise 9

Assessing Your Organization's Cyber Risks 12

Implementing Cybersecurity Measures 18

Creating a Cyber Incident Response Plan 19

Moving Forward 20

The Anatomy of a Cyberattack

Before examining what boards can do to manage cyber risks, organizations need to understand who cybercriminals 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 cybercriminals have already placed a target on your organization and are primed to strike.

Common Threat Actors 4

What's At Risk 5

Spotlight on Board Member Risks 6

General Responsibilities of Directors and Officers 7

Common Threat Actors

While cybercriminals may be commonly thought of as singular individuals bunkered in a basement, the truth is that attackers are often much more sophisticated. Examine the most common threats to your business:

Insiders

Employees are some of your best assets, but they can also be one of your greatest threats. In some cases, well-meaning employees accidentally put confidential information at risk through careless cybersecurity 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 organization. But it's not just data that's at risk. A cyberattack can lead to an IT failure that disrupts business operations, costing the organization both time and money.

Organized cybercriminals

Cybercrime has become increasingly organized and lucrative, even surpassing the drug trade to become one of the most profitable illegal industries. In fact, cybercrime costs the United States billions of dollars each year. Given how much they are able to steal, it makes sense that organized cybercriminals are primarily interested in money. These groups often seek personally identifiable information like social security numbers, health records, credit card details and baking information. They then hold this information hostage through ransomware or sell it outright on the dark web to turn a profit.

Hacktivists

Hacktivists operate with a political agenda, often carrying out high-profile attacks to distribute propaganda or damage organizations they disagree with. Hacktivists typically fall under the category of cybervandalism 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 cyberespionage are real threats. These cybercriminals 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 organizations 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 cyberthreats. As larger companies take steps to secure their systems, smaller, less-secure businesses are becoming increasingly attractive targets for cybercriminals. Knowing this, organizations must know what cybercriminals might be after and what it could cost to recover from a breach. To help you avoid litigation and other costs associated with a cyberattack, examine some examples of at-risk assets:

❶ **Productivity and operations—**Just one cyber event can wreak havoc on an organization 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 cybercriminals, especially considering how easy it is for malicious parties to impersonate your business or employees by using stolen banking credentials. In fact, cybercriminals can drain entire accounts in a matter of minutes with this information.

❸ **Sensitive data—**Nearly every organization works closely with vendors, staff and customers, storing sensitive information on their behalf. Things like credit card numbers, names, addresses, social security numbers, emails and login credentials are common targets for cybercriminals. In just one cyberattack, 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 a business owner, you work hard to differentiate yourself from the competition. In fact, many organizations have designs, products and plans that are unique to them and a key component of future growth. Cybercriminals understand the value of trade secrets and can earn big bucks selling proprietary information on the dark web. Following a loss of this kind, organizations can irreversibly lose their standing in the marketplace.

❺ **Physical assets—**Many wrongfully assume that the steep, monetary burden of a cyberattack 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 organization's physical assets can be just as harmful. Cyberattacks 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 HVAC systems become a part of the Internet of Things, the potential for physical damage following a cyberattack will increase.

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

In 2018, Yahoo settled a data breach-related securities class-action lawsuit for **$80 million**.

This marked one of the first times a shareholder lawsuit related to a data breach was successful from a plaintiff perspective.

Spotlight on Board Member Risks

In order for organizations to truly protect themselves from cyber risks, boards of directors must play an active role. Involvement from leadership both improves cybersecurity and can reduce liability for board members.

As just one cyberattack can result in significant damages, including reputational harm, financial losses, lawsuits and even regulatory action, efforts to improve cybersecurity from boards of directors are crucial. In some instances, a cyber event can negatively impact an organization'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 cyberattack. As a result, directors and officers 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 cybersecurity 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 wellbeing of the company, but they're also putting their finances on the line should they be sued.

General Responsibilities of Directors and Officers

Policies

Adopt written cybersecurity policies, procedures and internal controls.

Implement tools that detect cybersecurity 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, organizations should identify a qualified, in-house team member and roll cybersecurity responsibilities into their current job requirements.

Reviews and Reports

Review budgets and IT security programs on a regular basis.

Receive and review reports on any data incidents.

Remain well-informed on cybersecurity trends that could impact the business.

Create and oversee a team of individuals who are responsible for cybersecurity oversight.

Appointments

Assess cybersecurity 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 cyberattack can put on directors and officers (e.g., lawsuits and compliance fines), the importance of board member involvement in cyber issues cannot be understated. Cybersecurity must be accounted for in organizational decision-making, especially when considering its impacts on nearly every aspect of a business.

Poor cybersecurity practices can create:

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

Legal risks should a cyberattack lead to a breach in contract or result in regulatory fines.

Financial risks, as a cyberattack can lead to lawsuits, business interruptions and costs related to mitigating the damage from a breach.

One of the best ways boards can play an active role in cybersecurity 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 cybersecurity measures, which, in turn, allows them to build a more cyber-safe culture.

Simply put, cybersecurity 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 organizations have solutions that account for storing and handling data as well as managing the way the organization accesses that data. These types of considerations need to be reflected in the organization's structure.

Further, cybersecurity shouldn't be the responsibility of one person. Instead, protecting company data and preventing a cyberattack should be the goal of the entire board of directors. A board of directors should understand the potential impact a cyberattack 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 cybersecurity?
- Has the board **chosen an individual** or entity to oversee the organization's cybersecurity practices?
- Does the individual/entity responsible for cybersecurity 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

A board of directors has a responsibility to build a team of experts that will ensure they're adequately prepared should a cyberattack occur. This also gives organizations the ability to draw upon the experience of proven professionals when it comes to assessing and responding to potential cyberthreats. When it comes to building out this expertise, there are specific duties for the board to consider.

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

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

In general, it's critical for an organization to invest in their staff if they are to grow their overall cyber expertise. This can involve:

Making the Most of Existing Talent 10

Creating Clear Training Policies 10

Leveraging External Expertise 11

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 organization'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.

According to a report from Tessian—a cybersecurity vendor—**43%** of employees are "very" or "pretty" certain they have made a mistake at work that had security repercussions.

Creating Clear Training Policies

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

- Does our organization have a cybersecurity policy in place?
- Is our organization's cybersecurity policy enforced?
- Does our organization's cybersecurity policy include provisions regarding privacy?
- Does our organization 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 organization ensure the physical security of its computer systems?
- Does our organization have a process for notifying IT personnel if a device is misplaced or stolen?
- Is our staff informed regarding the importance of computer security?
- Does your organization provide employees with cybersecurity training on a regular basis?
- In the event of a cyberattack, does 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 organization's cyber authority. Some options to consider include:

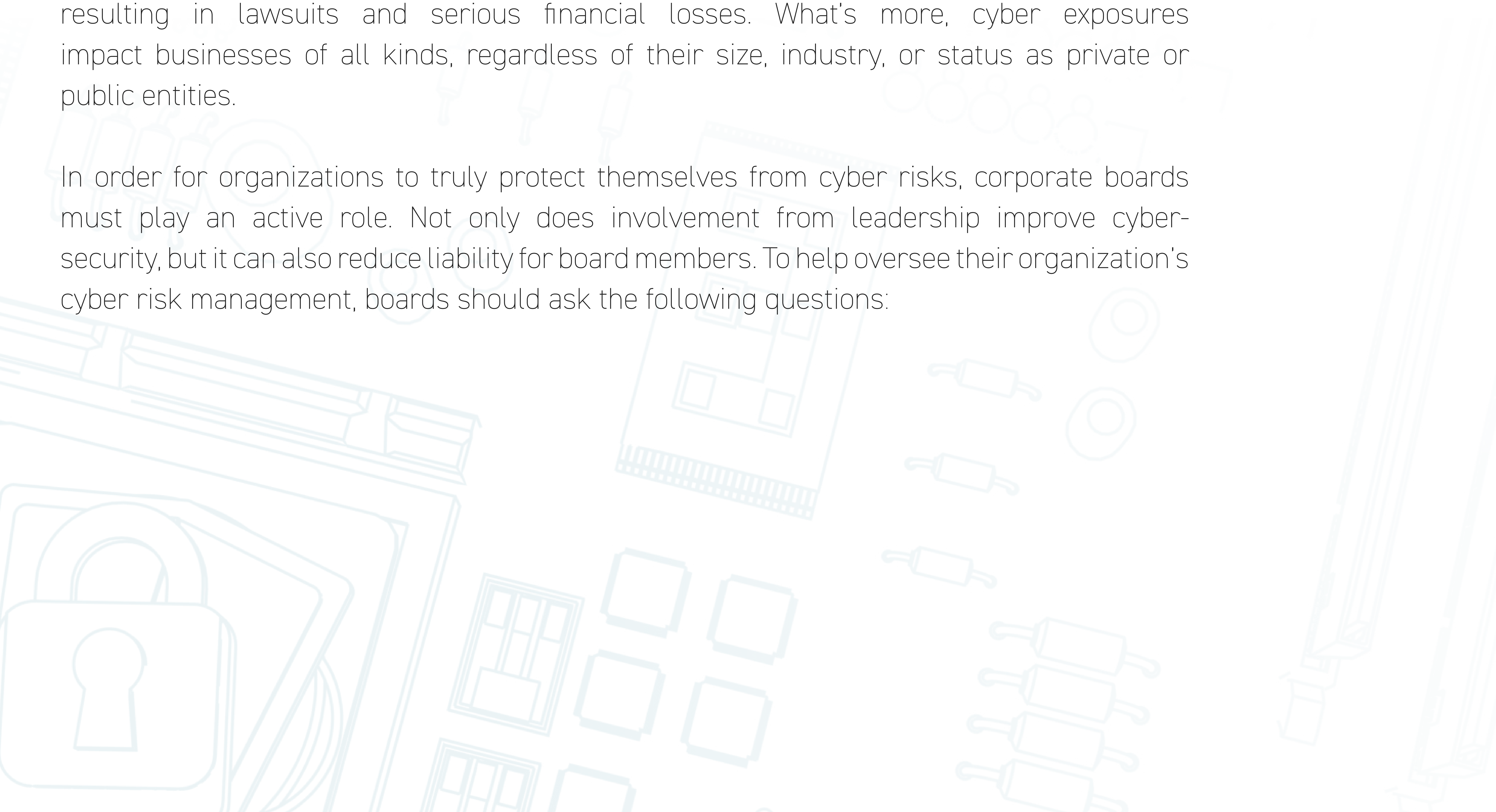
- Recruiting a skilled, nonexecutive director to the board
- Employing a cybersecurity consultant
- Identifying the specific cybersecurity services the organization is lacking and seeking the help of a third party to address any gaps
- Recruiting employees who already have the skills the organization 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 Organization's Cyber Risks

When a data breach or other cyber event occurs, the damages can be significant, often resulting in lawsuits 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 organizations to truly protect themselves from cyber risks, corporate boards 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 organization's cyber risk management, boards should ask the following questions:



Does the organization utilize technology to prevent a cyberattack?

Has the board identified a senior member to be responsible for organizational cybersecurity preparedness?

Does the organization have a comprehensive cybersecurity program?

Does the organization have a cyber response plan in place?

Has the organization discussed and formalized a cyber risk budget?

Has the management team provided adequate employee training?

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

Does the organization have a system in place for staying current on cyber trends, news data security regulations?

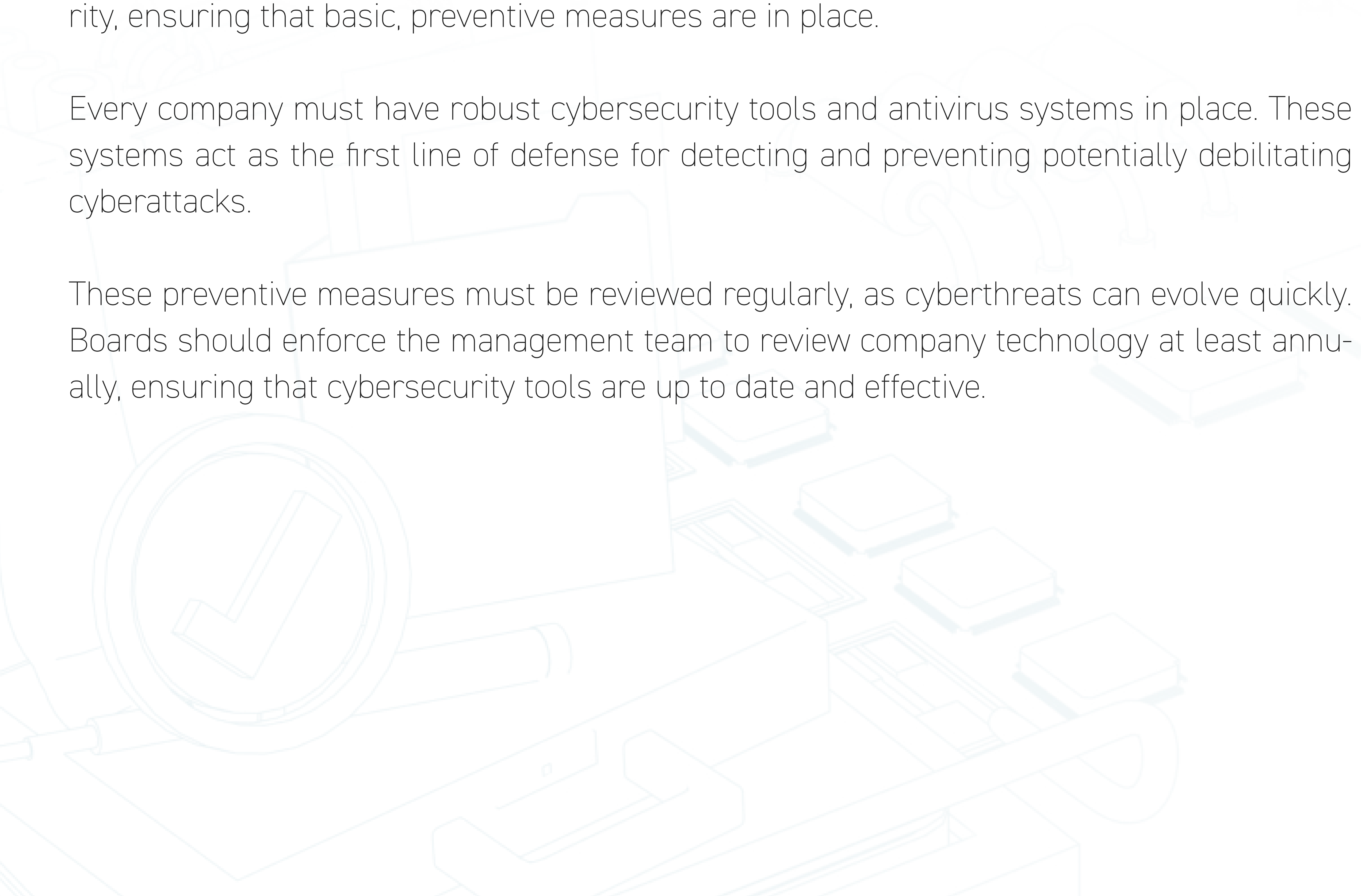
Has the organization conducted a thorough risk assessment? Has the organization purchased or considered purchasing cyber liability insurance?

Does the organization utilize technology to prevent a cyberattack?

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

Every company must have robust cybersecurity tools and antivirus systems in place. These systems act as the first line of defense for detecting and preventing potentially debilitating cyberattacks.

These preventive measures must be reviewed regularly, as cyberthreats can evolve quickly. Boards should enforce the management team to review company technology at least annually, ensuring that cybersecurity tools are up to date and effective.



Has the board identified a senior member to be responsible for organizational cybersecurity preparedness?

Organizations that fail to create cyber-specific leadership roles could end up paying more for a cyberattack than organizations 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, boards need to be involved in the process. Cyber leaders should have a good mix of technical and business experience. This individual 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 organization. In these instances, organizations should identify a qualified, in-house team member and roll cybersecurity responsibilities into their current job requirements. At a minimum, boards need to ensure that their company has a go-to resource for managing cybersecurity.

Does the organization have a comprehensive cybersecurity program?

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

Corporate boards should ensure that cybersecurity programs align with industry standards. These programs should be audited regularly to ensure effectiveness and internal compliance.

Does the organization have a cyber response plan in place?

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

While cybersecurity programs assist with securing an organization's digital assets, cyber response plans provide clear steps for companies to follow when a cyber event occurs.

These response plans allow organizations 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 organization's operations.

Board members 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 organization's response plan runs as smoothly as possible.

Has the organization discussed and formalized a cyber risk budget?

Either overpaying and underpaying for cybersecurity services can negatively affect an organization. Creating a budget based on informed decisions and research assists companies invest in the right tools.

Boards 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 prioritize funding. That way, an organization's most vulnerable and essential assets are protected.

Has the management team provided adequate employee training?

Employees are an organization's first line of defense when it comes to preventing a cyberattack. As such, organizations must provide thorough employee cybersecurity training. Boards can assist with overseeing this process and instruct management to make training programs meaningful and based on more than just written policies.

In addition, boards should make sure education programs are properly designed and foster a culture of cybersecurity 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 organization entrusts its data to an outside source, there's a chance it could be compromised.

Boards can help ensure that vendors and other partners are aware of their organization's cybersecurity expectations. Boards 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 organization if data is compromised.

Does the organization have a system in place for staying current on cyber trends, news data security regulations?

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

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

Additionally, boards should constantly seek opportunities to bring expert perspectives into boardroom discussions. Often, authorities from government, law enforcement and cyber-security agencies can provide invaluable advice. Building a relationship with these types of entities can help organizations evaluate their cyber strengths, weaknesses and critical needs.

Has the organization conducted a thorough risk assessment? Has the organization 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 coverage won't cover.

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

Implementing Cybersecurity Measures

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

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

Most organizations have some form of data protection in place. Although these protections are critical for minimizing 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 organization 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 organizations the tools they need to further enhance their data protection practices as well as assist with:

1. Anticipating cybersecurity incidents before they occur
2. Minimizing the impact of cybersecurity incidents
3. Mitigating threats and vulnerabilities while a cyberattack occurs
4. Improving cybersecurity response overall, encouraging buy-in at a management level
5. Reducing the direct and indirect costs caused by cybersecurity 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 organization
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 organizations should keep in mind when creating a cyber incident response plan.

Yes	No	
□	□	Your plan is part of a larger cybersecurity program that identifies tools and resources for incident handling. This program 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 behavior 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 prioritize them accordingly.
□	□	Your plan establishes strategies and procedures for containing incidents.

Yes	No	
□	□	Your plan provides specific steps to restore system and network integrity.
□	□	Your plan accounts for privacy and payment card industry compliance. Legal counsel 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 cybersecurity 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 cybersecurity practices in place, you still **can't eliminate the chance** that a cyber-attack might occur and negatively impact your organization. As a result, it's critical for the board of directors 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 Autumn Insurance & Benefits today.