DIY GUIDE TO CYBER INSURANCE

SOLVE IT

CYBERATTACKS ARE A GROWING THREAT FOR BUSINESSES OF ALL SIZES, AND IF YOU'RE MANAGING YOUR OWN IT, IT'S ESSENTIAL TO STAY AHEAD OF THESE RISKS. WHILE MANY BUSINESSES RELY ON MANAGED SERVICE PROVIDERS (MSPS) TO HANDLE THEIR IT SECURITY, WE UNDERSTAND THAT SOME PREFER A MORE HANDS-ON APPROACH.

Cyber insurance is an important safety net for any business, helping to cover financial losses and transfer risk to an insurance carrier in the event of a cyber incident. But securing that insurance can be tricky, especially if you're managing your own IT. This guide is designed to help you navigate the process, from understanding the necessary security controls to making sure you're compliant with insurer requirements.

We'll walk you through key steps, including a pre-assessment to identify potential gaps in your IT security, common pitfalls to avoid, and how to ensure you're fully prepared to meet the demands of cyber insurers. While DIY IT management can be empowering, a little guidance can go a long way in keeping your business safe and secure.

WHY IS CYBER INSURANCE IMPORTANT FOR BUSINESSES MANAGING THEIR OWN IT?

69% OF RANSOMWARE ATTACKS HAVE COST COMPANIES BETWEEN $100K-$500K, WHILE 20% REPORTED A LOSS OF OVER $500K.

Client protection: A data breach can be devastating for any business, whether you manage your own IT or work with an MSP. Cyber insurance can help cover the high costs associated with data recovery, customer notification, and even regulatory penalties, offering a vital safety net in the event of an incident.

Rising costs of ransomware and cyberattacks: Ransomware is becoming more costly every year. In fact, 69% of ransomware attacks have cost businesses between $700,000 and $1.2 million, with 20% of companies reporting losses over $500,000. Having cyber insurance can significantly reduce the financial burden.

Enhanced security posture: Obtaining cyber insurance encourages a proactive approach to security, as insurers often require certain security measures to be in place. This can lead to smarter investments in cybersecurity, improving your overall defenses and reducing the likelihood of a breach.

Competitive advantage: Understanding cyber insurance can set your business apart, even if you're managing IT yourself. By gaining knowledge about cyber insurance and integrating it into your security strategy, you position yourself as a more informed and valuable player in your industry. This can give you an edge when it comes to client trust, as you demonstrate a proactive approach to risk management and cybersecurity.

A growing market: The demand for cyber insurance is on the rise. In North America alone, the cyber insurance market is projected to reach $77.8 billion by 2027. Being well-versed in cyber insurance not only strengthens your IT defenses but also aligns your business with a growing trend, ensuring you're prepared for the future landscape of cybersecurity.

CYBER INSURANCE IS MORE THAN JUST FINANCIAL PROTECTION—IT'S A CRUCIAL PART OF A COMPREHENSIVE APPROACH TO IT SECURITY. IF YOU'RE HANDLING YOUR OWN IT, IT'S WORTH EXPLORING HOW THIS COVERAGE CAN BOLSTER YOUR SECURITY EFFORTS.

UNDERSTANDING CYBER INSURANCE COVERAGE

$11.8B - IN NORTH AMERICA, THE CYBER INSURANCE MARKET IS EXPECTED TO REACH $11.8 BILLION BY 2027.

Common coverage areas vary but often include:

Data breach: Cyber insurance can help cover the costs of dealing with a data breach, including forensic investigations, legal services, notification of impacted individuals, and credit monitoring to protect them after the breach.

Cyber extortion: If you're hit by ransomware, cyber insurance can provide financial assistance for ransom payments (within policy limits) and offer support for negotiating with attackers.

Network security: Cyber insurance can also help with costs tied to network security breaches, such as removing malware and restoring your systems to normal operation.

Business interruption: If a cyberattack disrupts your business operations, cyber insurance can reimburse you for lost revenue during the downtime.

Regulatory fines and penalties: In the case of non-compliance with data privacy regulations, cyber insurance can help cover legal fees and any penalties imposed.

Public relations and marketing: Should a breach occur, cyber insurance can help pay for notifying affected clients or employees and hiring a PR firm to manage reputational damage, helping to maintain your business's credibility.

GETTING STARTED

Pick a cybersecurity framework: Whether you're managing your own IT or providing guidance to others, choosing a cybersecurity framework is a crucial first step. Popular options include CIS Controls, ISO 27007, and NIST CSF. Select one that suits your business needs, implement it in your organization, and then align your cybersecurity tools and practices with that framework. Doing so will not only strengthen your own security posture but also help you ensure that your approach aligns with best practices when working with cyber insurance requirements.

CREATE A CYBER INSURANCE “PRE-ASSESSMENT”

Create a list of commonly required risk mitigations.

Examples include:

- Firewalls at all locations/workstations/servers Advanced EPP, EDR or MDR
- Email protections (OLP and Spam Filtering) Centralized logging (Like a SIEM)
- MFA for all cloud applications and admin users Password management
- Vulnerability management Risk management plans
- Phishing/cybersecurity awareness training
- Software and asset inventories Privileged access management
- Business continuity and disaster recovery plans Incident response plans

Build a comprehensive cybersecurity stack: Your stack should be able to cover most cyber risk insurance requirements and fit within your chosen cybersecurity framework. This includes people (roles and responsibilities), policy (governing documents), processes (plans and workflow) and tools (MDR, firewalls, MFA, etc.).

Have a conversation: Begin a self-assessment campaign to review your own cyber insurance needs. Take the time to evaluate your current coverage and ensure that you're meeting all the requirements set by your policy. This proactive approach will help you verify that your cybersecurity measures are aligned with what your insurer expects, reducing the risk of any gaps in coverage or compliance.

- **Review business contracts:** If your business engages in B2B contracts, it's important to review them to ensure you're meeting any cyber insurance requirements. Some contracts may stipulate that you carry a certain level of cyber insurance to protect against incidents. Make sure your coverage aligns with these contractual obligations to avoid potential legal or financial issues down the road.

PICKING A CONTROL FRAMEWORK

Getting started with security can be overwhelming. It's tempting to try and tackle every aspect at once, but that's a recipe for wasted time and resources.

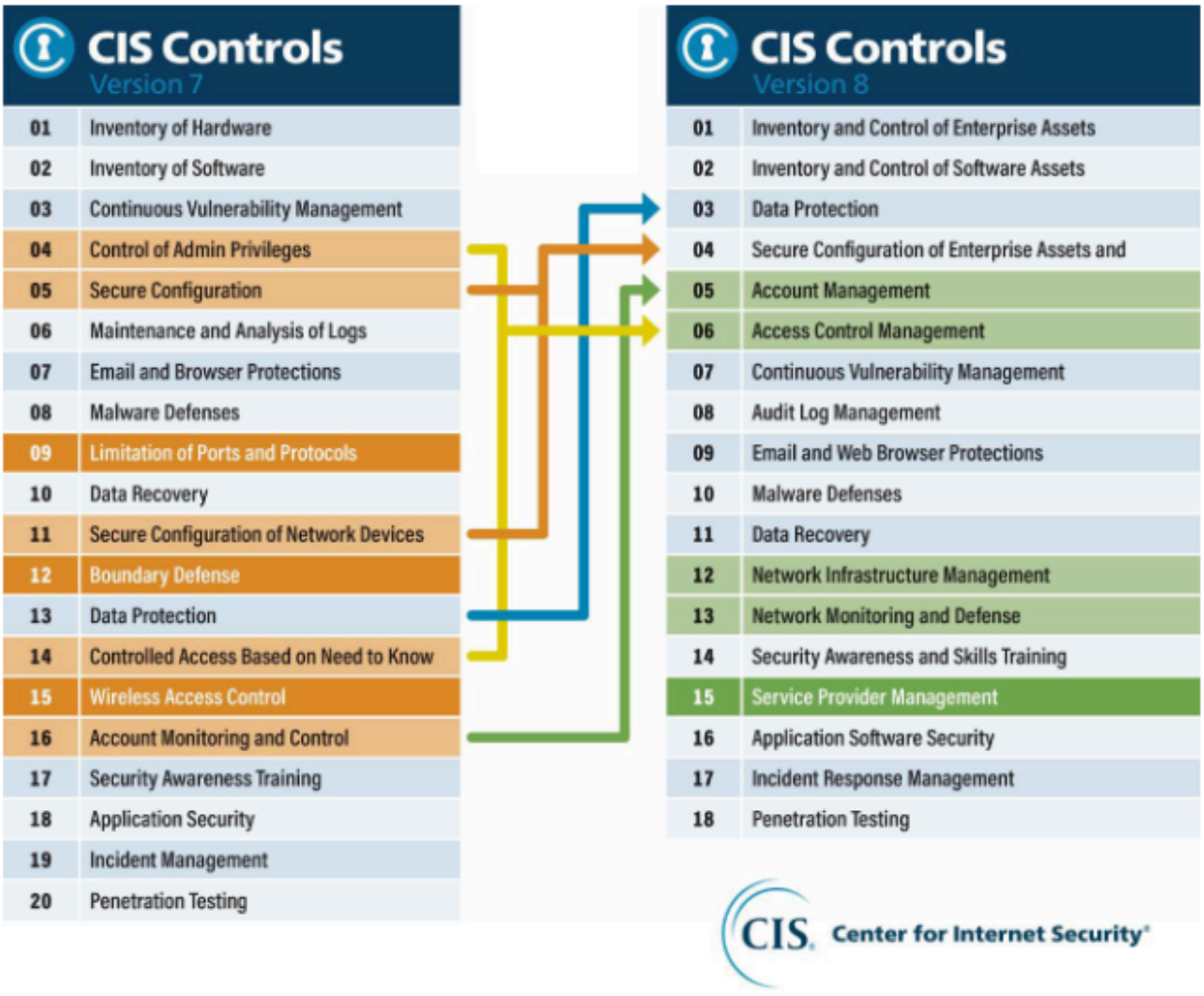
Security frameworks offer a much more efficient approach. They act as a roadmap, providing clear steps to establish foundational security measures. This not only saves time and effort, but also ensures you're prioritizing the most critical areas first, effectively jumpstarting your organization's security journey. So, how do you implement one?

Step 1

Choose a framework: When selecting a cybersecurity framework for your business, consider whether it aligns with your specific needs, as well as any regulatory or compliance goals you must meet. It's crucial to fully implement one framework before introducing another. If you find that you need to work with multiple frameworks, look for cross-mappings (also known as crosswalks) that allow you to map controls from one framework to another, ensuring consistency and reducing overlap in your security efforts.

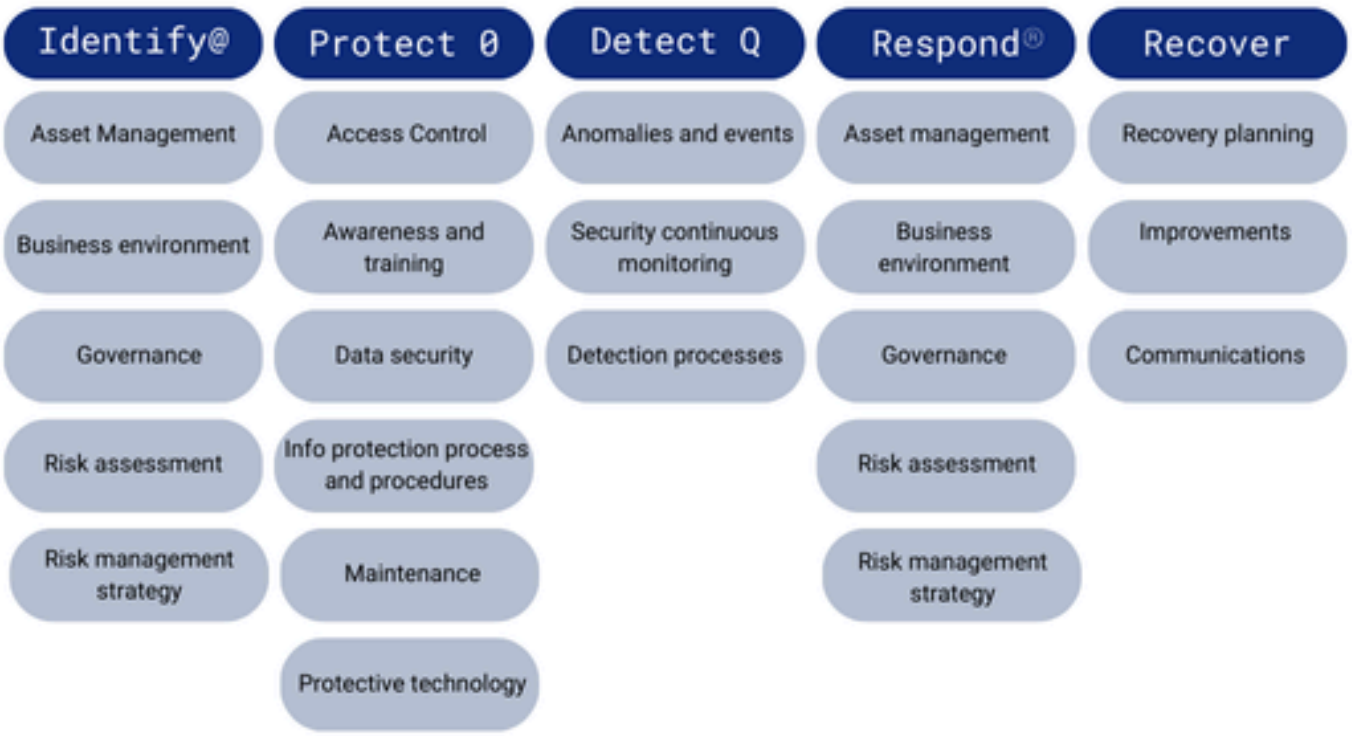
Some popular frameworks include:

CIS Controls



Source: SANS Institute: CIS Controls v8 (https://www.sans.org/blog/cis-controls-v8/)

NISTCSF



SOLVE IT

ISO 27001

The 14 Domains of ISO 27001

- Information Security Policies
- Human Resource Security
- Access Control
- Physical and Environmental Security
- Operations Security
- Supplier Relationships
- Information Security Aspects of Business Continuity Management
- Organization of Information Security
- Asset Management
- Cryptography
- Operations Security
- System Acquisition, Development, & Maintenance
- Information Security Incident Management
- Compliance

Step 2

Identify which controls you currently meet in your organization and potentially which controls do not pertain to your business.

Step 3

Identify the stakeholders and people responsible for implementing the controls. It may be worthwhile to use a matrix that outlines tasks and who is Responsible, Accountable, Consulted, and Included. Please see the attached RACI matrix, created for your use.

Step 4

Create a game plan with an end goal with 1-month, 3-month, 6-month, and 1-year milestones

Step 5

Review yearly. Determine which controls can be improved upon and which controls need to be implemented.

Cybersecurity frameworks have become the cornerstone of security for many organizations. These frameworks don't just offer a baseline level of protection, they also equip organizations to identify and understand the specific risks and threats they face. This allows them to tailor their security implementations to best address those vulnerabilities.

SOLVE IT

CREATE A CYBER INSURANCE “PRE-ASSESSMENT”

A strong first step toward securing cyber insurance is understanding your organization's current cyber risks. This process involves identifying, analyzing, and prioritizing these risks based on their potential impact.

Conducting a cyber risk assessment is a valuable way to pinpoint weaknesses in your cybersecurity defenses. Once you've identified and prioritized the most critical risks, you can focus on addressing them before applying for cyber insurance.

It's important to make cyber risk assessments a regular practice, as this not only strengthens your cybersecurity posture but also simplifies the renewal process for cyber insurance in the future. If you're managing your own IT, developing a structured approach to prepare for cyber insurance is essential, and it's advisable to treat this readiness process as a project.

To assist you in this effort, we’ve created a risk assessment questionnaire and a vendor risk questionnaire to help ensure you’re prepared for cyber insurance. Be sure to update these regularly as you encounter new cyber insurance requirements or as your organization evolves.

BUILDING YOUR STACK: BASICS

Endpoint Detection and Response (EDR)

- Sophos Intercept X Advanced
- SentinelOne
- Bitdefender
- Trend Micro
- ThreatDown

Multi Factor Authentication (MFA)

- BitWarden
- Keeper Security
- SSO/Entra ID with MFA
- LastPass MFA

Cybersecurity awareness training

- Proof point
- Breach Secure Now
- Phin

Domain Name System (DNS)/Web filtering

- BitDefender DNS/WebContent

Sophos

Patch/Vulnerability management

- NinjaOne
- ConnectSecure
- SentinelOne Network Discovery
- Cavelo
- ThreatDown - Vulnerability Assessment
- ThreatDown - Patch Management
- Bitdefender - Windows and Third Party Patching

Email filtering/security

- Sophos Central Email
- Proof point
- M365 Defender

Backups

- Axcient
- Dropsuite (Cloud) Veeam
- Acronis

BUILDING YOUR STACK: ADVANCED

include the basic stack, then expand to:

Endpoint Detection and Response (MDR/XDR)

- Sophos MDR Complete
- SentinelOne
- Bitdefender
- Acronis CPC
- Trend Micro
- ThreatDown

Privileged access management

- CyberFox
- CyberQP

Data loss prevention

- Sophos DLP
- Microsoft Purview
- Bitdefender DLP

Security Information and Event Management (SIEM)

- Microsoft Sentinel
- Blumira

Secure Access Service Edge/Zero Trust Network Access

- Sophos ZTNA
- Todyl
- Cloudflare

FOR BUSINESSES WITHOUT CYBER INSURANCE

It's important to understand cyber risks before diving into premiums and coverage options. Many businesses might not be aware of their vulnerabilities or the existence of cyber insurance solutions. We've prepared some helpful questions and talking points to guide you.

“DOES OUR ORGANIZATION STORE ANY SENSITIVE OR PROTECTED INFORMATION”?

Storing personally identifiable information (PII) like credit card numbers or health data comes with significant responsibility.

A data breach, whether caused by malicious hacking or a simple human error like a lost laptop or misplaced email, can trigger legal repercussions. Businesses are obligated to notify impacted individuals and potentially offer credit monitoring services. Furthermore, regulations regarding PII collection, use and storage can lead to hefty penalties if not followed (including severe legal consequences beyond simple financial fines).

Cyber insurance offers a safety net in these situations, covering the costs of legal counsel, notifying affected parties and any potential regulatory penalties incurred due to a data breach

“DOES OUR ORGANIZATION HAVE REMOTE WORKERS?”

A remote workforce introduces new cybersecurity challenges. Cybercriminals can exploit weak passwords or steal login credentials to gain remote access, potentially launching ransomware attacks or facilitating funds transfer fraud.

Phishing scams are also more effective when employees lack colleagues to verify suspicious emails. Additionally, lost or stolen work devices can lead to data breaches.

Fortunately, cyber insurance can safeguard your business against these financial losses, covering the costs associated with ransomware, fraudulent transactions, and data breaches - all potential consequences of a remote work environment.

"DO WE SEND OR RECEIVE ELECTRONIC PAYMENTS"

Electronic fund transfers are a common target for cybercriminals. They hack into email accounts, impersonate trusted senders, and issue fraudulent payment instructions.

These scams are difficult to detect as they often originate from legitimate email addresses and mimic real communication patterns. Recovering the stolen funds is unlikely as they're quickly transferred elsewhere. Banks rarely offer compensation, leaving businesses vulnerable to significant financial losses.

Fortunately, cyber insurance can help recoup these losses, with funds transfer fraud being a major component (around 25%) of global cyber insurance claims.

"CAN OUR ORGANIZATION RECOVER FROM AN EMPLOYEE'S MISTAKE?"

Even the most robust cybersecurity measures can't fully eliminate cyber risk. Humans are often the unintentional entry point for attacks. Employees might click malicious links in phishing emails, share login credentials with scammers, use weak passwords, fail to verify new fund transfer requests or even lose devices containing sensitive information.

Cyber insurance helps mitigate these risks by covering financial losses from such human errors. It also provides access to technical experts to help with recovery efforts.

“HOW LONG CAN OUR BUSINESS BE DOWN DURING A CYBER INCIDENT?”

Many businesses underestimate their vulnerability to downtime caused by cyberattacks. Modern businesses heavily rely on computer systems for day-to-day operations, making them prime targets for ransomware attacks where criminals encrypt crucial data and demand a ransom for decryption.

Unfortunately, most small businesses lack the internal resources to combat these threats and recover quickly. Downtime can last for weeks or even months, leading to lost revenue and potential reputational damage.

Cyber crime insurance offers a safety net in these situations. It provides access to technical experts to expedite recovery, covers financial losses caused by the interruption and even helps with restoring corrupted data. More importantly, it can help mitigate the reputational damage from lost contracts and customer trust.

FOR BUSINESSES WITH CYBER INSURANCE

Cyberattacks are on the rise, and even small businesses are not immune. These attacks can cripple operations, result in data breaches and cause significant financial losses.

Ensure your organization is currently meeting cyber insurance coverage requirements and that you have the correct coverage in place. This proactive approach can give you peace of mind and ensure that the insurance company will pay out in the event of an incident. Here are a few questions to ask:

"CAN WE REVIEW THE CYBER INSURANCE REQUIREMENTS?"

It's critical to actively ensure your business is meeting all coverage requirements. Organizations often mistakenly believe they're fully compliant, only to discover gaps after an incident. Here's where a proactive approach is key:

First, you need a comprehensive understanding of all assets to ensure proper coverage. This includes physical devices, cloud storage, and any software applications that hold sensitive data.

Second, security awareness training for employees is crucial. Not only does it fulfill policy requirements, but it also empowers employees to identify and avoid cyber threats.

Finally, documented security policies with clear enforcement procedures are essential. These policies should outline acceptable online behavior, data handling procedures, and incident response protocols.

By taking these steps, you can not only fulfill insurance requirements but also significantly improve your overall cybersecurity posture, minimizing the risk of a costly and disruptive cyberattack.

“DO WE HAVE ENOUGH COVERAGE?”

It's essential to ensure you’re fully prepared for a potential attack. Often, businesses underestimate the financial devastation an incident can cause, unaware of the true cost of downtime, data recovery, and legal repercussions. Being aware of coverage limits for specific claims like ransomware payouts or regulatory fines helps to fully understand your financial safety net.

Furthermore, delving into business operations is key. Do you handle large financial transfers (like mortgage brokers) or sensitive regulated data (medical or classified information)? These factors significantly impact their risk profile and required coverage.

Involving the insurance provider in these discussions from the outset is vital. They can tailor the policy to address specific risks and ensure the terms and conditions align perfectly with your organization’s needs. This approach ensures you have the right level of protection and minimizes surprises in the event of an attack.

IWhether your organization has existing coverage or not, it's important to understand the risks involved in their business and the role cyber insurance plays in making their company whole again after an incident. Cyberattacks are a constant threat, and even small businesses are vulnerable. These attacks can be devastating, leading to data breaches, operational disruptions, and crippling financial losses.

Cyber insurance acts as a shield for your business, protecting you from these unforeseen costs. It covers legal fees, data recovery and even helps repair reputational damage. Most importantly, it provides access to expert technicians who can get you back up and running quickly, minimizing downtime.

REVIEWING CONTRACTS

Reviewing business-to-business contracts for cyber insurance requirements is crucial for both parties involved. For your company, it ensures you comply with the terms of the agreement. Failing to meet these requirements, like adequate coverage or proper employee training, could open your company to more liability and loss of business with the other party.

Not only do these contracts sometimes spell out which security controls need to be in place, but they can also specify the amount of cyber insurance coverage you should have. You may also find that incidents involving shared information may have to be handled by a third-party security team.

All these considerations should be considered as you can increase liability and the need for more cyber insurance coverage.

CHALLENGES TO BUSINESSES

Comprehensive asset inventory: Building a complete picture of your environment -software, hardware, vendors, network devices, user roles and cloud services is a complex task. Without this foundation, achieving cyber insurance readiness and navigating specific requirements becomes difficult. Fortunately, automated inventory tools can streamline this process.

Automating deficiency remediation: Maintaining compliance with cyber insurance requirements involves continuous detection, alerting and remediation of security gaps. Tools like Robotic Process Automation (RPA) platforms like Rewst or custom scripts via your RMM, Active Directory Group Policy or Intune can automate tasks like removing local admin rights, deploying and reporting on required security software (EDR/MDR), ensuring patching schedules are met and enforcing password policy.

Backup and recovery readiness: While data backups are common, restoration capabilities are often overlooked. Regularly test data recovery, disaster recovery plans and business continuity procedures. This could involve spinning up servers in cloud environments (Azure or AWS), restoring cloud based software (e.g., Exchange mailboxes or SharePoint sites) and verifying access methods for recovered data (VPN, Remote Desktop, etc.). Rapid business restoration after a cyberattack is crucial.

Multi-factor authentication (MFA) hurdles: Enforcing MFA across all systems presents challenges. User resistance can lead to delays or attempts to circumvent setup. Additionally, some legacy applications and cloud services may not fully support MFA. For cloud environments, explore Single Sign-On (SSO) solutions like Microsoft Entra ID, allowing you to enforce MFA via conditional access policies. Legacy on prem apps might require isolation on dedicated networks, remote desktop setups, or virtual desktops.

Demonstrating compliance: Having the right security measures in place is essential but proving it to insurers requires robust evidence collection. RMMs and Governance, Risk, and Compliance (GRC) platforms can automate evidence gathering during audits. Additionally, ensure a system for documenting employee policy acknowledgment and security awareness training completion. This might involve sign-off processes or knowledge tests following training videos.

Audit log retention: Cyber insurance providers often mandate audit log retention for a minimum period (typically 90 days). A Security Information and Event Management (SIEM) system can help with log collection and retention from various sources, including cloud services, workstations, servers, network devices, endpoints and firewalls.

Carefully follow insurance company specifications regarding log collection and retention periods as it is important for forensics.

CONCLUSION

Securing cyber insurance has become essential for businesses of all sizes. While you can certainly navigate the process on your own, it can be complex, requiring a deep understanding of your security posture and risk profile.

You can take a DIY approach by gathering the necessary information, reviewing the technical aspects of your IT setup, and making informed decisions about the coverage you need. However, teaming up with a Managed Service Provider (MSP) can simplify the process. MSPs can guide you through information gathering, recommend actions, and help ensure that your systems are ready for insurance.

Whether you go it alone or work with an MSP, establishing a process for ongoing security monitoring and documentation is critical. This proactive approach can improve your risk management and potentially secure you more favorable insurance terms.

With the ever-evolving cyber insurance landscape, new threats and changing policies are always on the horizon. By staying informed or partnering with an MSP, you can ensure your business is well-prepared to navigate these challenges and secure the coverage you need, either on your own or with expert help.

THANK YOU!

NOW IS YOUR TURN TO DECIDE TO DO IT YOURSELF OR TO GET THE ASSISTANCE OF SOLVE IT

BOOK A TIME TO LEARN MORE

Solve iT

218 WESTINGHOUSE BLVD, STE 207, CHARLOTTE NC 28273

2925 WILLIAM PENN HIGHWAY, STE 100, EASTON PA 18045

980-505-7658

APPENDIX: CYBER INSURANCE CONTROL LIST

Cyber insurance requirements (Technical)

Cyber insurance requirements can vary by insurer, but here are common technical controls an MSP may provide to help businesses meet them. They are listed in order of most commonly asked.

Access controls

1. Multi-Factor Authentication (MFA) for all user accounts
2. Strong password policies and enforcement
3. Disabling unused accounts
4. Remote access restrictions (e.g., VPN with MFA, Conditional access policies, SASE or ZTNA)
5. Endpoint access controls (e.g., limiting USB usage)
6. Privileged access management (PAM) for high-risk accounts
7. Segmentation of networks to isolate critical systems
8. Regular review and updates to access control policies
9. Physical security measures for devices that store sensitive data (i.e., locked cabinets/doors)
10. Least privilege access controls (granting only necessary permissions)
11. User activity monitoring and logging

Filtering Tools

1. Email security with spam and malware filtering
2. Webfiltering to block malicious websites
3. DNS filtering

Vulnerability management

1. Prioritization and patching of critical vulnerabilities
2. Automated vulnerability scanning of systems and applications
3. Configuration management to ensure consistent security settings
4. Regular vulnerability assessments by qualified security professionals
5. Vulnerability scanning for web applications and mobile devices (if applicable)

Data security

1. Regular backups with offsite storage
2. Data encryption at rest and in transit
3. Data loss prevention (DLP) to prevent sensitive data leaks
4. Classification and labeling of sensitive data
5. Data access restrictions based on user roles

Endpoint security

1. Next-generation antivirus (NGAV) with real-time threat detection
2. Endpoint detection and response (EDR) to add context to your AV/audit logs
3. Managed detection and response (MDR) for advanced threat hunting
4. Application whitelisting to restrict unauthorized software
5. Endpoint security management with centralized controls
6. Regular patching and updates of endpoint security software

Security awareness and training

1. Security awareness training for employees on phishing attacks, social engineering, etc.
2. Phishing simulations to test employee awareness and response
3. Security policy education and enforcement
4. Training on secure password practices and data handling procedures

Incident response

1. Regular testing of incident response plan (i.e. tabletop exercises)
2. Log retention and forensic analysis capabilities
3. Partnership with an incident response team for advanced support
4. Breach notification procedures in accordance with regulations
5. Regular security assessments and penetration testing

D

CYBER INSURANCE REQUIREMENTS: ADMINISTRATIVE

Be aware that administrative controls reduce cyber risk and are becoming more common in cyber liability questionnaires. Here are some common administrative controls you may want to consider as part of your cyber insurance readiness.

Policies

1. Written information security policy (WISP)
2. Risk management plan
3. Incident response plan with defined roles and procedures
4. Disaster recovery and business continuity plans
5. Password management policy
6. BYOD (bring your own device) policy
7. Acceptable use policy
8. Log management policy
9. Data retention policy

Procedures

1. New user provisioning
2. Employee termination procedure
3. Wire transfer/bank transfer process
4. Identity verification for release of sensitive information

Governance

1. IT steering committee (quarterly, bi-annually)
2. Board of Directors reporting
3. Quarterly business reviews/ quarterly risk reviews
4. Change management
5. Vendor risk management