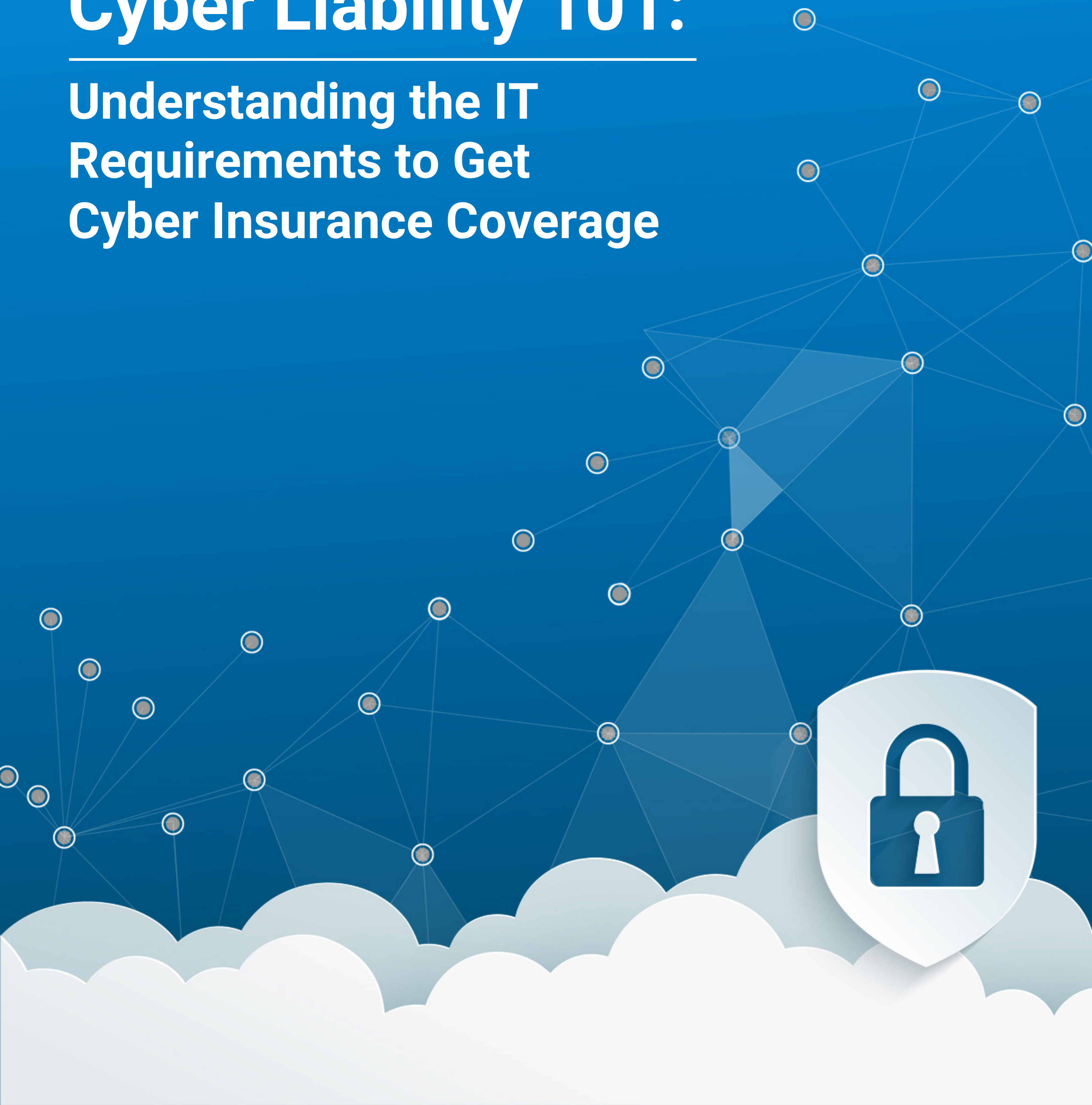
TPX®

Cyber Liability 101:

Understanding the IT Requirements to Get Cyber Insurance Coverage



Key Takeaways

☑ **Cyber Liability Insurance Protects Businesses From High Breach Costs**
Cyber liability insurance, also called cyber security insurance, protects businesses from the high costs of a data breach or malicious software attack. It covers expenses such as customer notification, credit monitoring, legal fees, and fines.

☑ **Storing Sensitive Data Puts You More at Risk**
You should have cybersecurity insurance if you handle customer data or store information about your business online.

☑ **Cybersecurity Must Be Regularly Updated and Monitored to Minimize Risk**
Cyberattacks can happen when the network security at a business is not up to date, or the employees lack the training or knowledge to recognize phishing attempts, ransomware, and other cyber hacking red flags.

☑ **Cyberattacks are Constantly Evolving and Capitalize on Stealing Data**
Phishing emails, malware, security breaches, network security issues, and computer system breakdowns are just a few examples of the kinds of cyber risks that could cause serious liability or losses.

☑ **Getting Cyber Liability Insurance Requires Certain Cybersecurity Requirements to be Met**
You can purchase cyber security insurance through most business insurance providers, but cyber insurers consider organizations with poor security practices as an unwanted, and potentially dangerous, liability to their business model. Improving your cyber defenses will improve your chance of qualifying for cyber insurance coverage, as well as obtaining the best rates.

To Obtain Cyber Insurance You Must Be Cyber Secure

Cyberattacks are on the rise. They make headlines when it involves high-profile targets, but everyone with an internet connection is at risk.

The number of attempted and successful attacks has increased in recent years. These attacks did not slow down amid the COVID-19 pandemic; in fact, bad actors stepped up their efforts and businesses of all sizes must prepare a better defense to mitigate risk and keep operations running smoothly.

Consider findings from the Identity Theft Resource Center's (ITRC) 2021 Annual Data Breach Report[1]:

Ransomware-related data breaches doubled in each of the past two years.

2x

45%

There were 45% more cyberattack-related data compromises (1,603) in 2021 than all data compromises in 2020 (1,108).

Compromises increased year-over-year in every primary sector, except for the military (there were no publicly disclosed military data breaches). The Manufacturing & Utility sector saw the most significant percentage increase in data compromises at 217% over 2020.

217%

190%

The number of data breach notices that don't reveal the root cause (607) has grown by more than 190% since 2020.

The Cyber Insurance industry has grown in recent years as hacks, ransomware and other cybersecurity threats have increased. Businesses are opting to add Cyber Insurance policies and what was a $7.8 billion industry in 2020[2] could grow to $20 billion by 2025[3], according to Insurance Business.

What is Cyber Liability Insurance?

Cyber Insurance mitigates losses businesses experience from internet-based and information technology infrastructure crimes. It covers your firm's balance sheet in the event of network security failure, which can include a data breach, malware infection, ransomware, or a phishing attack. Keep in mind data breaches can involve employee data as well as customer data.

Many businesses assume it's included in the insurance they already hold. However, considering the increased risks, **most traditional General Liability insurance policies exclude cyber exposure.** While General Liability insurance protects businesses from third party claims for Bodily Injury and Property Damage, it only covers physical property and not digital assets.

If businesses want to be covered for cyber exposure to protect their digital assets, they must have a separate Cyber Insurance policy.

Cyber Insurance Benefits Businesses of All Sizes

Companies are becoming more aware of increased cyber risks with the media regularly highlighting high-profile cyberattacks. But many low-profile attacks and attempts often don't make the news. The fact of the matter is, all businesses that operate computer systems need cyber liability insurance because all businesses are at risk of a cyberattack.

According to Hiscox[4], an international cyber insurer, roughly a quarter (23%) of small businesses suffered at least one cyberattack in the past year. Cyber crime is a growing threat that does not discriminate on company size or industry. **There are more than 4,000 ransomware attacks every day in the United States** since 2016, according to the FBI. If you handle or use digital information, you need to mitigate your cyber risks and protect your company, your employees and your customers.

A single cyberattack attack costs companies of all sizes an average of **$200,000**[5]

Security attacks increased **31%** from 2020 to 2021[6]

43% percent of attacks are aimed at SMBs, but only 14% are prepared to defend themselves[6]

The Importance of Cyber Liability Insurance

Cyber liability insurance can protect you from several first-party, third-party and additional costs that your company can face following a cyber-attack, depending on what your insurance policy covers. Cyber Insurance is as dynamic as the companies it protects and is consequently far from standardized. However, some things that it typically covers include:

- Cyber extortion
- Data loss, recovery, and recreation
- Computer fraud
- Business interruption/ loss of revenue due to a breach
- Loss of transferred funds
- Digital asset management

First party cyber liability insurance addresses the financial fallout associated with cybersecurity breaches on your own network and can include:

- IT Forensic Costs: To determine what information may have been breached and how it was breached.
- Notification Costs: To notify all individuals and businesses affected
- Credit Protection Costs: To provide credit monitoring services to all parties affected.
- Crisis Management Costs: For media relations for reputation management.

Third party coverage helps pay for lawsuits caused by data breaches on a client's network systems and can cover:

- Privacy lawsuits brought by customers or employees who allege that you were responsible for the data loss.
- Regulatory fines if you have to pay the authorities as a result of the loss.
- Claims that allege a breach of contract or negligence on your part.

Understanding the IT Requirements to Get Cyber Insurance Coverage

There are unique criteria that companies must meet to be eligible for coverage and maintain it annually depending on your insurance provider and your specific policy. This criteria continues to evolve with changes within the cybersecurity risk landscape, and businesses need to be proactive to ensure they meet the changes in policy requirements.

Often, insurance providers will require companies to secure a third-party assessment — a risk assessment or a cybersecurity gap assessment — to ensure they do the basic "block and tackling" tactics. **Before you seek out Cyber Insurance, completing a third-party assessment can help identify vulnerabilities and risk within your organization.** The information you gain will not only help your organization strengthen your security posture, but it can also help you get coverage under a Cyber Insurance policy.

Insurance providers can deny coverage to companies that do not meet minimum standards to prepare for and defend against cyber threats. Specific standards may vary slightly by provider, but typically four types of security controls are required:

Multi-factor Authentication (MFA): MFA protects data or applications by requiring a user to present two or more credentials to verify user identity at the time of login. These credentials typically consist of something you have like a token, something you know like a password, and something you are like a fingerprint. By enabling MFA, it is much more difficult for cyber criminals to hack into applications with stolen passwords.

Security Awareness Training: Nearly 90% of successful breaches are caused by human error. User training is important to educate staff on proper cyber hygiene and the ways to identify cyberattacks that may be encountered via email and the web. It is recommended that companies use continuous training techniques versus only training employees once or twice a year to ensure cyber best practices stay top of mind.

Encrypted Backups: In the event of a systems crash, natural disaster or security event, businesses need encrypted backups to minimize downtime. With backups hosted both on-premises and in a secure cloud location, rebooting a single server or an entire office can be done seamlessly with the click of a few buttons.

Endpoint Detection and Response (EDR): As hybrid and remote work become increasingly common in business, companies must protect their infrastructure at their endpoints (computers, laptops, servers, etc.). With EDR, you can monitor, detect, and mitigate any threats regardless if your employees are in the office or working remotely.

TPx can help make sure you have the right technology and protection in place to get coverage and keep it when it comes time to renew your policy.

Mitigate Your Risk with a Strong Cybersecurity Program so You Can Rest Easy

The security landscape continues to change with new vulnerabilities and malware constantly emerging. Having a strong cybersecurity program in place can help businesses reduce their exposure to cyberattacks and become more insurable to cyber liability insurance vendors.

A security program should not be created without taking into consideration industry standards as outlined by National Institute of Standards and Technology (NIST) or Cybersecurity & Infrastructure Security Agency (CISA). Both agencies have detailed guidelines of what private and public sector organizations can do to protect themselves against cybersecurity attacks.

Key Tactics to Include in Your Cybersecurity Program

Perform Monthly Vulnerability Assessments
Conducting monthly vulnerability assessments of the perimeter can help improve your posture and harden your environment. It can also identify weaknesses within your infrastructure and any new network holes created by system updates and router/firewall changes.

Perform Continuous Security Awareness Training
As previously mentioned, security awareness training is similar to other "healthy habits" and must be done systematically and consistently to see improvements. Through short monthly training content and regular phishing exercises, users, over time, become more vigilant.

Ensure All Systems Patch Levels are Current
Patches are used to update, optimize, and improve security for the software running in your infrastructure. When a provider makes a patch available, the purpose is to fix vulnerabilities. If a business isn't current on all patch levels, they are more vulnerable to cybersecurity attacks.

Enable Multi-Factor Authentication
The password alone isn't enough to protect your infrastructure from cybersecurity attacks. By enabling MFA, businesses can strengthen their security posture and provide more secure login access for their employees.

Ensure Endpoints are Using Current Antivirus and EDR
EDR not only needs to be part of your cybersecurity program to get cyber liability insurance, but it can also help keep your environment protected with 24/7 monitoring and alerting. Running a Next-Generation Antivirus (NGAV) can also go a long way to improve your endpoint security.

Validate Backups are Working Properly and Protected from Ransomware
Most businesses have a backup, but unfortunately, many aren't backed up or tested regularly to ensure a proper restoration and recovery of your data is possible. A managed backup solution can help ensure your backups are working properly, so in the event you need them, you won't have to experience any data loss.

Be Prepared. Ask the Right Questions.

Many policy requirements are changing with providers requiring more cybersecurity in place to get or renew a Cyber Insurance policy. You need to assess your risk and understand if your security posture is strong enough to be eligible for Cyber Insurance. Here are a few questions that you need to ask yourself – and that TPx can help you solve for.

☑ Does your company perform regular risk and vulnerability assessments?

☑ Does your company have MFA enabled on all applications where it is available?

☑ Does your company perform continuous security awareness training?

☑ Do you have an Incident Response Plan in place that is regularly reviewed and updated?

☑ Do you have next-gen antivirus installed on all computers and servers?

☑ Are you up to date on all available patches across systems and software?

☑ Do you have Endpoint Detection and Response monitoring all your devices?

☑ Do you have a Disaster Recovery and Business Continuity Plan that outlines how to restore data from a backup?

The threat of cybercrime is growing, and with it, the cost of combating cyberattacks. When cyberattacks like data breaches and hacks occur, they can result in devastating damage. It is important to remember that no organization is immune to the impact of cyber crime. Taking the appropriate steps to protect your company against cyber threats and getting the right coverage can protect your business and help you recover.

Resources:

1. ITRC 2021 Annual Data Breach Report
2. Security.org
3. Insurance Business Magazine
4. Hiscox
5. Hiscox Cyber Readiness Report
6. Accenture's State of Cybersecurity Resilience