CYREBRO

Cyber Insurance Coverage Checklist 2023

13 SECURITY ESSENTIALS FOR BUSINESSES OF ALL SIZES

TABLE OF CONTENTS

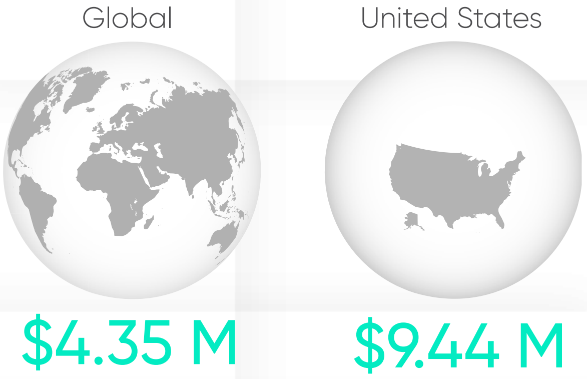
A Game of Chance

Attaining the proper insurance policies to reduce financial uncertainty in the event of a damaging incident has always been a cost of doing business. Now, in addition to property insurance, liability, and automobile insurance, businesses must add cyber insurance to their coverage portfolio. That's because you have a higher chance of experiencing a cyber-attack than a fire or natural disaster. In fact, the likelihood of a data breach involving a minimum of 10,000 records was estimated at 29.6% over a two-year time horizon. The chance of ransomware is even greater.

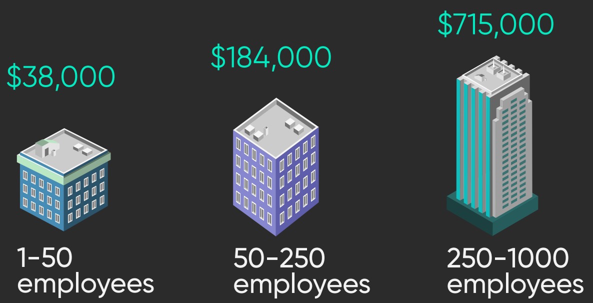
Based on a Sophos State of Ransomware Report 37% of small and midsized organizations reported suffering a ransomware attack over a twelve-month period. Perhaps the most troubling statistic is from a 2022 report by the World Economic Forum which showed that 6% of organizations do not even know if they have been affected by a possible cyber incident in the past two years.

According to the Ponemon Cost of a Data Breach Report 2022, the global average cost of a data breach has reached a record $4.35 million in 2022. For organizations in the United States, the average stands at $9.44 million.

Average Cost of a Data Breach



According to a Kaspersky Lab Study, the average direct cost of a cyber incident for a small business is $38,000. For companies with 50 to 249 employees, the cost rises to $184,000, and sky rockets to $715,000 for companies with up to 1,000 empolyees.



While the actual costs for a small business are much less, they can prove equally daunting for the typical small business.

The Indirect Costs of a Cyber Attack

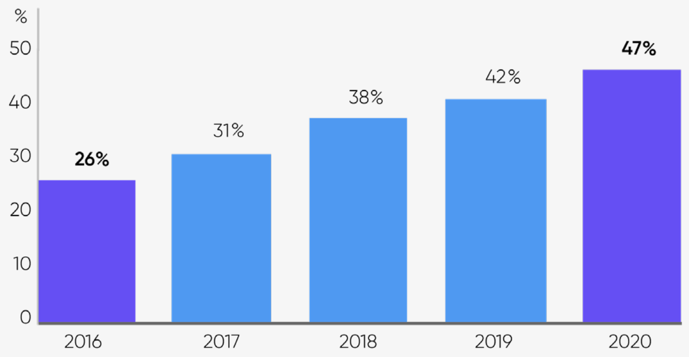
Direct costs are only part of the equation. Cybersecurity incidents involve both direct and indirect costs that can span weeks, months, even years after the event. For instance, the ransom is only one of the incurred costs involving a ransomware attack. Other costs can include the following:

- First response IT services
- Legal services
- Negotiation team
- Public relations team
- Restoration costs
- Business disruption and lost opportunity costs
- Fines and penalties
- Legal settlements

As a result of the increased frequency of attacks and the surging costs associated with them, businesses have turned to insurance companies to lessen the cost burden of a cyberattack. According to the U.S. Government Accountability Office, the number of clients opting-in for cyber coverage rose from 26% in 2016 to 47% in 2020 and that number has only risen since.

Cyber insurance adoption rate from **2016** to **2020**, showing clear signs of significant change.

Cyber insurance take-up rates from a large broker's clients



What Cyber Insurance Offers

Homeowner's insurance is designed to get you back on your feet and ensure that you don't have a total loss if your home is destroyed by a fire or natural event. Cyber insurance does the same in the event of a cybersecurity incident. These policies cover the immediate costs of incident recovery such as forensic efforts, data restoration, consumer outreach, and legal expenses related to the attack. In the case of ransomware, insurance companies will not only cover at least a portion of a ransom, they have negotiating teams that know how to bargain with ransomware gangs to reduce the payout. Many policies also cover losses sustained during the duration of a business disruption that originated from an attack as well as any liability claimed by your customers because of that disruption.

The Current Insurance Climate

While insurance companies were more than willing to issue these types of policies a few years ago, that is not the case today. In the same way that a string of excessive natural disasters in a calendar year can force insurance companies to readjust their premiums and stipulate requirements to absorb unpredicted losses on policies, cyber insurance providers are having to raise premiums and qualification standards to continue offering such policies.

Insurance companies began bleeding money as the payouts for ransomware attacks grew existentially overnight, creating massive direct-loss ratios for those policies. Case in point, in 2021, the CNA Insurance Company was forced to payout $40 million for their client to regain control of their systems, the highest disclosed ransom to date. It's those kinds of payouts that now lead the industry to believe that the cybercrime costs will reach $10.5 trillion by 2025. The losses have become so great that Lloyds of London began discouraging its syndicate from taking on new policies in 2022. This shouldn't be surprising as the U.S. cyber insurance market in 2020 alone experienced a combined loss ratio of 103%. With losses like these, something must give, and it is.

As CYREBRO Co-founder & CEO, Nadav Arbel explains:

> *What is common to all cyber insurers today is an increased demand for validation of sufficient cybersecurity precautions as part of the underwriting process. The age of innocence for cyber insurance has passed. Today's cyber insurers adhere to the age-old Russian proverb: trust but verify.*

The result is that it is much tougher to even qualify for affordable cyber insurance today. Unfortunately, cyber insurance is no longer considered as "optional coverage" anymore. That's why we created a cybersecurity insurance checklist to help businesses of all sizes attain the cyber insurance they so urgently need to protect themselves in a world that is increasingly under siege by threat actors the world over.

Key Changes in the Cyber Insurance Industry

The cyber insurance industry is just like any business. Companies flock into the market when profits are clearly prevalent and retreat when the model appears no longer profitable. Multiple insurance companies have left the market since 2021 as the ability to properly evaluate the changing dynamics of future risk environments has made it challenging to price policies accordingly. Those companies that have chosen to remain for the time being are demonstrating greater caution in policy issuance. Some refer to it as cherry-picking businesses according to their perceived risk factor. Those companies deemed high-risk are simply denied coverage. Insurance companies have also begun enforcing a practice called "line deduction" that caps the maximum payout for a policy. In many instances, coverage has been slashed by fifty percent.

Ever Increasing Premiums

Cyber insurance premiums have been rising each quarter since 2019. According to Fitch Ratings, premiums rose by 74% in 2021. Premiums seem to have peaked in December of 2021, having risen by as much as 133% in North America. While cyber insurance rates appear to have moderated after a two-year surge, the reduced-price acceleration is not necessarily good news as the price deceleration is mostly due to a tightening of underwriting terms designed to eliminate "higher risk" organizations. Insurers are now requiring policyholders to maintain a list of prescribed security controls and strategic measures that can ensure a desired security posture. Most renewal applications ask for proof of their required tools as part of the approval policy.

Get Started With a Cyber Insurance Checklist

Of course, you need security controls for more reasons than simply qualifying for cyber insurance coverage. Cyber resiliency is a given today. While there was certainly a time when companies could allot standard users blanket local admin rights and prioritize convenience over security, those days are long gone. Cybersecurity incidents are no longer isolated incidents. Eight of ten companies that pay the required extortion for a ransomware attack experience a second attack. In the mentioned Ponemon Study, 86% of companies experienced at least two data breaches. A history of cybersecurity incidents not only affects a company's ability to obtain cyber insurance, but it also has a negative impact on a company's bottom line, merger and acquisition interest, employee retention, and stock performance. It is clear today that companies must quickly transition to a state of cyber resiliency to succeed in today's threat environment.

Below is a consolidated list of the most popular requests made by cyber insurance providers today. This is by no means an exhaustive list as different companies may have different requirements. Because cybersecurity is a moving target, this list will most likely be appended or modified as time goes on due to the dynamic nature of cybersecurity. Regardless, attention to these basic requirements will go a long way in securing your company's IT estate and digital resources.

The Cyber Insurance Checklist

1. MULTIFACTOR AUTHENTICATION

Let's just say it, a password is no longer enough. The idea that a single password is all that is preventing the credentials of a key executive or privileged user from being compromised is almost absurd; the world experienced 193 billion credential stuffing attacks in 2020 alone. Yet, 300 billion passwords were used by humans and machines worldwide in 2021. Multifactor authentication (MFA) provides an added layer to ensure that access is given to the right identity. Every login attempt using a designated user account triggers an MFA notification request to the actual user which they can accept or deny. For most insurers, some type of MFA solution is near the top of their required lists.

2. DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

The purpose of insurance is to protect a policyholder from risk, so it only makes sense that insurance companies want assurance that you know what those risks are. A Business Continuity Plan (BCP) requires organizations to go through a process that identifies the most likely risks that could cause significant disruption to their business. An applicable BCP should comply with the ISO 22301 framework that specifies the structure and requirements that should be followed. The BCP should include a Disaster Recovery Plan (DRP) that outlines how a business can resume operations and function in the event of a disruptive event.

3. EMAIL AND WEB SECURITY FILTERING

According to a January 2020 report by Deloitte, 91% of cyber attacks begin with a phishing email. While that number has decreased slightly since then, phishing attacks are still used as a primary delivery system for malware, ransomware, and other types of attacks. Most phishing attacks induce an unsuspecting user to click on an embedded link which then downloads some type of payload from a site controlled by the attackers. Therefore, email and web security filtering serve as a one-two punch to thwart these attacks. Modern email security solutions today strip out embedded links that appear suspicious while web filtering prevents users from accessing malicious sites at all.

4. SECURED AND ENCRYPTED BACKUPS

A backup is your ace in the hole in the event of a ransomware or data destruction attack. That's why the perpetrators of these attacks target backup systems as part of a preliminary attack to eliminate them. Backups must be protected using a well thought out strategy that isolates them from the production environment. This is done through network segmentation using next-generation firewall protection. Backups must be encrypted at rest in the event they are exfiltrated by an attacker.

5. PAM – PRIVILEGED ACCESS MANAGEMENT

Privileged access management (PAM) is a cybersecurity strategy that is founded on the principle of least privilege. A PAM system is used to control, monitor, and audit all human and non-human privileged identities to ensure that standard users are limited to the exact access they need to do their jobs and that elevated privileges are restricted to select designated accounts only. This prevents malware or attackers from inheriting admin rights or elevated privileges from a compromised user account and using them to conduct their attacks.

6. ENDPOINT DETECTION AND RESPONSE (EDR)

Endpoint security has been an integral part of the equation for decades, but don't confuse EDR with signature-based endpoint protection. EDR is an advanced security solution that utilizes data analytics to detect suspicious system behavior in quick order so that automated rules can be engaged on the endpoint to block or remediate malicious activity and alert the appropriate security personnel. EDR gives you visibility into all your computer devices to know what potential threats are lurking, while providing you with automated ruleset remediation.

7. PATCH AND VULNERABILITY MANAGEMENT

Perhaps the most important measure your IT staff can take is to ensure that all operating systems, application software, and firmware are patched and updated in a timely manner. Vulnerabilities are constantly discovered, and hackers exploit them to gain access into your systems. While it doesn't require additional tool sets to patch and update your existing systems, it does pay to have an update management system that allows IT to readily identify machines that are vulnerable and out of compliance.

8. INCIDENT PLANNING AND TESTING

According to a 2022 Ponemon Study, organizations that experienced a cyberattack and had a tested Incident Response Plan (IRP) realized a 58% cost savings over those organizations that did not. An IR plan lays out the blueprint of how your organization will proactively react to a cybersecurity incident using a stated list of remediation and recovery steps. It's imperative that IR plans be tested on a regular basis so that each player knows their role and what is expected of them during a highly stressful time. Insurance companies want to know that you have a team in place that is ready to respond to an inevitable attack.

9. CYBER AWARENESS TRAINING

The users behind the keyboards are your weakest security links. Users are tempted every day with compelling reasons to click an embedded link or malware infested attachment, prompting them to make daily decisions that could prove devastating to their organizations. An educated workforce is one of the best deterrents your organization can have to combat cyberattacks. An effective cyber awareness training program can pay big dividends down the road.

10. HARDENING TECHNIQUES (RDP MITIGATION)

Hardening your IT estate is an ongoing process that must be undertaken by your IT team or MSP. Hardening requires that all unused ports, services, processes, applications, and server components be disabled or uninstalled. A prime example is the remote desktop protocol. Hackers specifically target RDP and use it as a means of connecting to key servers in your environment. You should disable all outside RDP connections whenever possible.

11. EOL (END-OF-LIFE) SYSTEMS PROTECTION OR REPLACEMENT

EOL doesn't mean that your hardware or software stops working. It means that it is no longer supported by the vendor, so patches and security updates are no longer released for it. Unfortunately, exploitable vulnerabilities are still discovered by the hacking community long after the EOL date, which means that these deprecated systems are exposed to attacks. No organization today should have any equipment or software that has exceeded its EOL.

12. SOC (SECURITY OPERATIONS CENTER) – LOGGING AND MONITORING

If your organization is connected to the internet, then it's perpetually under attack. The threat environment is so prevalent today that every company could use a security operations center (SOC). A SOC includes a dedicated team of highly experienced cybersecurity specialists that oversee the cybersecurity of their customers on a 24/7 basis. Their team is supported by automated threat monitoring technology that integrates with a customer's system environment to provide log management and monitoring, threat intelligence analyses, and incident mitigation.

Unfortunately, few SMBs can afford this combination of analytical technology and experienced personnel. Fortunately, SMBs have access to third-party SOCs that fill an important void. CYREBRO provides a world leading SOC and the first SOC Platform. With CYREBRO, SMBs have access to the same security protection that large corporations employ from their own internal SOCs.

13. VENDOR/ SUPPLY CHAIN RISK MANAGEMENT

Businesses no longer operate as islands today. Your company is a mesh of network connections that link your IT estate to your service providers, vendors, business partners, and contract workers. All these connections represent a point of entry into your network. That's why supply chain attacks are so prevalent today as hackers simply target the weakest link within the mesh. It's no longer just your own security you must worry about.

Maintaining a strong cybersecurity posture today requires a lot of work. That doesn't mean you need to rush out and purchase a bunch of best-of-breed security tools, however. Every organization regardless of size only has a finite budget for cybersecurity, which is why it's important to understand which security controls produce the maximum ROI. Cyber insurance companies are well informed about the available security controls today and what works. By following their guidance, you not only have a much better chance of attaining affordable coverage, but you also end up keeping your network secure so that your organization can focus on its core business and achieve its objectives.

Meet the SOC Requirement With CYREBRO's SOC Platform

Where a SOC Comes In

The reason why cyber insurance providers are requiring security controls now is for assurance. They need to know that their policyholders have the tools and strategies in place to properly secure their digital assets. Of course, you can have the right tools and strategies in place, but if you don't have experienced professionals with the right skill sets in place, you will never get the full benefit of those implementations. That's where a SOC comes in.

CYREBRO SOC Platform

CYREBRO is a first-of-its-kind SOC Platform; meaning that organizations leverage CYREBRO's SOC Platform and capabilities to have the equivalent of an in-house SOC, without the need to build and maintain it themselves. Users receive an online, interactive SOC Platform, which is powered by CYREEBRO's expert cyber teams and advanced technology. The Platform allows users to see their organization's real-time security posture, review ongoing investigations, communicate directly with a SOC analyst, and more. Gain peace of mind with 24/7/365 monitoring and detection, incident response, threat hunting, SIEM optimization, and more.

Any Tool, Any Stack

CYREBRO works by connecting to all your security tools and systems, centralizing all the incoming alerts and information, and shows you precisely what you need to know, and what to do about it. CYREBRO is technology agnostic, meaning it will connect with any tool you are using, so there's no need to change your tech stack.

Want to find out more about how to protect your business with CYREBRO's SOC Platform?

Learn more here