Apptega

Whitepaper

The Evolving Cyber Insurance Landscape: How to Get (and Keep) Coverage for Your SMB



Apptega

Last year was nearly a record-breaking year with nearly 1,900 publicly-reported breaches affecting more than 422 million people, according to the Identity Theft Resource Center. Among impacted companies were household names like Twitter and AT&T. Which leads to the question, if global companies like these — with a lot of money, resources and skilled professionals — can become victims of cyber breaches, what does that say for small- and mid-sized businesses (SMBs)?

That, even with strong cybersecurity measures, anyone can be hit by a cyber-attack.

The reality for SMBs today is the attack surface is expanding. The threat landscape is evolving and quickly shifting away from what may happen *if* your organization experiences a breach to *when*. That's why it's more important than ever to add an extra layer of protection to your business with cyber insurance coverage.

What is cyber insurance?

Cyber insurance helps organizations manage and mitigate financial losses related to cyber incidents; yet, many organizations still don't understand why they need it, why it's an important piece of the operational resilience puzzle, or why they must stay on top of rapidly changing requirements and expectations.

This white paper addresses what cyber insurance is, how the industry is changing, what's driving those changes, and what you can do to secure coverage and feel confident your plans will pay out in the event of a breach.



Apptega

Changing Trends, Changing Requirements

Over the past five years, the cyber insurance industry has rapidly changed. Premiums cost more. Coverage is harder to get. Insurers have greater expectations — and require more proof — that covered organizations have industry-recognized cybersecurity standards implemented across their attack surfaces.

Increased breaches and record exposures are driving much of this change, particularly an increase in ransomware attacks and social engineering scams like phishing attacks. The National Association of Insurance Commissioners (NAIC) says data breaches in 2021, for example, increased by 68% compared to 2020.

While ransomware (236.1 million attacks in 2022) frequently makes headlines, in 2022, phishing gained notoriety of being one of the most common attack vectors for threat actors. There were more than 255 million phishing attacks launched last year. That's an increase of more than 60% compared to 2021, and more than half of SMBs today say that phishing is the primary threat to their business. NAIC says that social engineering "has become a top cyber security threat."

Between 2019 and 2020, for example, the FBI's Internet Crime Complaint Center reported an almost 200% increase in phishing attacks year over year. A report from AdvisorSmith correlates the increase in ransomware attacks and data breaches with a 25% increase in premiums from 2021 to 2022, and in some cases, policyholders saw an increase of almost 80% year over year. Over time, if these trends continue, it's likely the cyber insurance industry will continue to evolve and become more complex along with the changing threat landscape.

Apptega

Securing Cyber Insurance Coverage

A decade ago, most organizations could get a cyber insurance policy by answering a few questions. For example:

- Business name, address, and size
- Industry type
- Asset inventory (devices, hardware, software, networks)
- Security controls and frameworks followed
- Previous claims history

But the increase in cyber breaches and related response and recovery costs have driven the industry to make underwriting requirements much more stringent.

The 2017 WannaCry malware attack, for example, affected more than 300,000 computers around the globe and directly impacted how cyber insurers think about risk assessments for coverage. Previously, the industry focused more on single risk, but as WannaCry affected thousands of computers, that shifted attention to aggregated risk (what happens when a cyber event impacts thousands of potential claims). The attack also played a large role in the increase in demand for cyber insurance.

To acquire coverage today, in addition to the previous requirements, an underwriter might ask about:

- **Risk assessments:** It's no longer enough to tell the underwriter which assets you have, you must also demonstrate you understand risks and risk impact to essential operations. Not just for your organization, but your vendors as well, even those further down the line, like second- and third-tier suppliers. Insurers may also want to do their own risk assessments. The types of risk your organization faces and how you're mitigating them can directly impact the type of coverage you'll get, as well as premiums.

- **Implement and demonstrate security controls:** It's no longer enough to tell an insurer you have security controls in place. To get — and maintain coverage — you'll need to document the controls and frameworks you're using (sometimes down to the individual sub-control level). Many insurers also want you to demonstrate those controls work as intended and may even require you to submit to third-party penetration testing to validate your attestations. They may also conduct third-party vulnerability assessments to validate your claims.

- **Data:** The volume, types, and sensitivity of the data you create, access, transmit, store, or process may affect coverage. The more sensitive and confidential the data (like personally identifiable information) and the more you have, the more likely it is a carrier will determine your business faces higher risk, which in turn, could impact the type of coverage you get.

- **Breach history:** Insurers want to know if you've experienced any breaches in the past, the frequency with which they occur, what happened, who was behind them, breach impact, how you stopped the attacks, and the effectiveness of your recovery processes.

- **Financial information:** You may also be asked to provide detailed financial information such as your annual revenue and your organization's net worth.

- **Compliance:** Depending on your industry or location, the insurer may also require you to demonstrate you're meeting all of your regulatory and compliance standards (for example, PCI DSS, HIPAA, GDPR, state privacy laws, etc.)

- **Employee awareness:** As incidents like social engineering impact cyber insurance payouts, insurers may also want to know about the policies and processes you have to train and educate staff about basic cyber hygiene and cyber risk.

Apptega

It's a Whole Lot More Expensive

As application requirements become more complex, premiums are also increasing. In 2021, for example, NAIC reported cyber insurance premiums, driven by increased cyber threats, increased more than 60% from the previous year. In 2021, insurers reported $4.5 billion in direct-written premiums (the amount of money an insurer gets from customers excluding the amount it pays to other insurance companies to help cover losses) and another $2 billion in premiums written as part of a broader package policy. Direct-written premiums increased by 92% from the previous year.

The report from BravoPolicy.com also indicates more than half of small businesses choose policies with a $1 million per-occurrence limit (others go up as high as $5 million) and a $1,000 deductible.

Today, on average, an SMB can expect to pay about $1,824 per year in cyber insurance premiums, according to BravoPolicy.com. Five years ago, according to a report from Advisor Smith, that rate was about $1,500. Other reports estimate annual small business cyber premiums ranging from as little as $250 to $2,287 annually.

The top three industries with the most expensive premiums are:

- Payment processing
- Financial services
- Investment services

The top three with the lowest premiums are:

- Transportation and logistics
- Administrative services
- Manufacturing and industrial

Reports vary for large organizations based on a range of factors, but on average, a cyber insurance premium for a large business could range from between $30,000 a year to more than $150,000. According to the report from Advisor Smith, in addition to risk factors and coverage amounts, many insurers also consider annual business revenue when setting premiums. The higher the annual revenue, the higher the premium. Other insurers base this on the number of employees.

While the increase in cyber breaches and record exposures play a large role, there are other factors influencing increases:

- Increased cyber extortion where attackers make threats against organizations for money so they won't disclose sensitive information publicly
- Attacks causing higher impact, longer-lasting business interruptions
- Data loss, corruption and manipulation impacts
- Larger claims

Apptega

What Does Cyber Insurance Cover?

What cyber insurance covers for businesses varies based on many factors and which types of coverage your organization gets. For example, you may choose coverage for a specific type of attack like ransomware or opt for a broader umbrella that offers more cyber protections.

However, in general, here are some of the things cyber insurance policies generally cover for businesses:

- **Network security:** Costs related to recovering or replacing impacted data, as well as forensics, and response and recovery costs
- **Breach response:** Costs related to notifying those impacted by the breach, credit monitoring fees for individuals with data exposures, and legal fees related to response
- **Liabilities:** Costs associated with legal claims filed by third-parties or other compliance or regulatory fees or fines
- **Errors and omissions:** Some policies offer coverage for costs related to professional negligence from within your organization that led to the breach
- **Lost income:** Costs associated with business interruptions



Apptega

The List of Exclusions is Growing

While there are many cyber insurance policies that may meet your organization's needs, there is also a growing list of exclusions. In the past five to 10 years, as insurers have issued more cyber-related claims, they've increased exclusions to decrease their exposures. The exclusions may also work to get organizations more focused on implementing proper policies and procedures to decrease the likelihood of a cyber-attack.

Be sure to carefully review your policies to understand all exclusions and limitations. Consider working with a consultant, like an MSP, who can help you complete your application and select coverage that's best for your organization.

Here are some examples of incidents or events your policy might not cover:

- War
- Terrorism
- Geopolitical unrest
- Damage caused by criminal activities like theft, embezzlement or fraud
- Property damage
- Bodily injuries
- Intellectual property infringement
- Incidents that happened before the effective policy date
- Intentional employee acts
- Data exclusions for certain types of data

Claims and Payouts

Cyber insurers don't want to pay claims, if they don't have to. That's why they're increasing application requirements and attestations, and requiring continuous monitoring of your environment and the changing threat landscape. When they do pay, your claim must meet standards in your policy, and even then, there's list of reasons they might reject it, for example:

- You didn't meet specific requirements. For example, you said you had controls in place you didn't or you claimed controls functioned as required, but they did not.
- You knew there was a breach before you applied for coverage and you didn't include it in your application.
- It's a black-and-white issue outlined in your exclusions.
- You didn't report the breach within the policy-required timeline or didn't follow breach reporting requirements in your policy.
- You didn't properly document breach impact so you can't provide evidence a breach impacted your business the way you claim.
- Someone who works for you intentionally caused the breach.

Exactly how much an insurer pays out depends on the specifics in your policy. For example, an insurer may base a claim payout on breach severity and impact (if it's less than your policy limits), or the payout could be the maximum amount covered by your policy. According to IBM, the average cost of a data breach today is about $4.35 million. That's an all-time high and nearly 3% higher than 2021. If your limits are too low and breach-related expenses exceed that, your policy may not cover the full cost of response and recovery.

Your insurer might also not pay out if you've exceeded the number of breach claims your policy allows. That's important to note when seeking coverage because at least 83% of organizations say they've had more than one breach.

One report evaluated cyber claims from 2016-2020 and found that 99% of claims were from SMBs.The average amount an insurer pays out for an SMB claim is about $345,000.

And, sometimes when cyber insurers won't pay out, policy holders won't take no for an answer. In 2022 for example, Mondelez International, a food and beverage company, settled a lawsuit against Zurich American Insurance Company after Mondelez sued Zurich for not covering $100 million in expenses when Mondelez was hit by a NotPetya ransomware attack in 2017. Zurich denied the claim based on a war exclusion saying that NotPetya was a Russian state-sponsored attack. The case was settled but exact details of the settlement have not been released.

A new court ruling on another NotPetya lawsuit, this one filed by Merck, a pharmaceutical company, has rejected insurers' appeals they didn't have to cover the claim because of a war exclusion. Merck sued insurers after the initial claim denial and in January 2022 a judge awarded Merck $1.4 billion. The insurers appealed saying the attack was excluded because Russian nation-state actors were behind it. Just this month, a judge upheld the previous court decision saying the insurers could not use the war exclusion on a non-military organization, even if it was caused by a government entity.

The original lawsuit included 30 insurers. Over time, many resolved the claim, but eight remained, fighting against paying out on Merck's "all risk" policy that had a $1.75 billion limit and $150 million deductible.

The impact of the attack and related lawsuits have had a direct impact on the global cyber insurance industry. For example, in late 2022, Lloyd's, the world's largest insurance marketplace, issued a market bulletin saying all of its insurers must add exclusions about sovereign state attacks for all policies and renewals that cover cyber attacks, effective March 31, 2023.

The bulletin doesn't apply to U.S.-based insurers, however, it is a reflection of how the industry evolves after cyber events and is something U.S. insurers may soon mimic.

Getting — and Keeping — Cyber Insurance Coverage

So, what can you do to ace your cyber insurance application and ensure you have coverage when you need it?

First, understand applications are complex and ever-changing. Instead of tackling it yourself, consider working with a consultant like an MSP who can help you. While each insurer may have different coverage requirements, in general, your organization should be prepared to demonstrate:

- You've conducted a risk assessment and identified cyber risks across your networks, systems, and other assets. You've discovered all vulnerabilities, misconfigurations, and other security issues and made plans to mitigate them. Be prepared to show proof of testing and potentially undergo a third-party assessment, like a vulnerability assessment or penetration testing.
- You've created and implemented a continuous risk management strategy to reduce your exposure to cyber risk, for example, framework implementation and other security controls such as encryption, employee education, firewalls, anti-malware, and more.
- You're in compliance with all of your regulatory and legal requirements. Have proof of self-attestations, audits, or certifications.
- You've got an incident response plan and you've tested it to ensure it works as planned. If you discover fail points within that plan, be sure to document how you've addressed them or have a timeline that outlines the steps you'll take to rectify the issues.
- Document. Document. Document. Remember, insurers have too great of a liability to just take your word for it anymore. Be sure to document all of your security and compliance policies, processes, and controls. Bonus points if you can demonstrate executive or key-stakeholder support, understanding, and accountability for your program.

Once you've gotten coverage, you can't just sit back and rest. Your insurer is well aware of how quickly the threat landscape, attack vectors, and the modern attack surface are changing. It may periodically require a security assessment to make sure everything is still functioning as it should be. If not, you may have a decrease in coverage or could potentially lose your coverage entirely.

Maintaining (and Possibly Decreasing) Premiums

While industry changes are likely to dictate your premiums, there are a few best practices you can employ to keep your premiums in check and possibly even reduce what you're paying now. Here are a few recommendations:

- Know your environment, risks, and threshold and continuously monitor for changes. Make adjustments to your security program as needed.
- Know your vendors and their risks, and establish security and compliance requirements early in your service level agreement (SLA). Routinely assess your vendors to ensure they're meeting all of your compliance requirements and security standards. Conduct a risk assessment to determine third-party risk and be prepared to switch to a new vendor if one exceeds your risk threshold.
- Implement industry recognized controls and frameworks.
- Use a solution that automates and monitors security functions for you, as well as manage important controls such as encryption or other security-focused technologies.
- Pass security and compliance audits and get certifications where you can.
- Conduct routine security testing to ensure controls work as intended and close gaps when discovered.
- Partner with a consultancy to implement, improve, or manage your security and compliance program.
- Work with an insurance broker or MSP that knows the specifics of the cyber insurance market, will help you find the best policy, understands your specific requirements and exclusions, will help you complete the application process, and will stay abreast of any changes in your policy or the market.

Another less-time consuming, but potentially riskier way to decrease your cyber insurance premium is to choose a plan with a higher deductible. Higher deductible plans usually cost less than those with lower deductibles.

Apptega

Use a Cybersecurity Compliance Platform to Simplify Cyber Insurance

While the list of cyber insurance requirements is long and constantly evolving, it doesn't have to be as challenging to get and maintain coverage as it once was.

First, put away those spreadsheets and word processing documents. Throw your dusty old binders in the trash. Instead, implement a cybersecurity and compliance management solution that can help you automate tasks, give you insight into your real-time security and compliance status, identify weaknesses, make mitigation recommendations, continuously monitor your frameworks and controls, and help you document and report every step of your journey.

Here are some examples of how a platform like Apptega can help you simplify cyber insurance:

- **Conduct your risk assessments with Apptega's Assessment Manager**. Assessment Manager comes with pre-defined templates to help you quickly choose and implement the right risk management, security, or compliance (or all three) framework(s) for your organization. Something not the right fit? You can easily customize any templates, including reports, to meet your needs. There's also a built-in questionnaire to help conduct readiness assessments for all of your frameworks. You can even divide and conquer the questionnaire by assigning different sections to different experts within your organization. With Apptega's Assessment Manager, you'll have more comprehensive visibility into your cyber risk and you can even align it with your organization's goals to demonstrate to your insurer your cyber program is a key part of operational resilience.

- **Assess and manage your risk and your vendor risk with Risk Manager and Vendor Risk Manager**. With Vendor Risk Manager, you can track all of your vendors and send them security questionnaires designed specifically to your security and compliance requirements. The platform can help you identify and manage vendor risk from the start of your vendor relationship all the way through the vendor lifecycle. You can even compare vendor security and compliance data against other business-critical security information in your dashboard and then use that information to create reports to communicate vendor risk to the appropriate teams and key stakeholders.

Apptega

- **Use the full power of the Apptega platform to implement and manage all of your frameworks and controls.** You can identify and remediate risks simply within the solution and even do an assessment to determine how prepared you are for your next audit. The platform can automate many of your compliance and security functions, freeing up your team to focus on other tasks and ultimately save you time and money. The Apptega Harmony feature can also simplify framework management by enabling framework crosswalking from one framework to another or from one framework to many. Want to know how your frameworks and controls are functioning? The Apptega dashboard puts real-time compliance scoring right at your fingertips.

- **Ace your audits with Audit Manager**. With Audit Manager, you'll know exactly how prepared you are to pass your next audit (or how well you're doing with those cyber insurance requirements), without chasing down team members or scrolling through thousands of cells in a spreadsheet. No more running around trying to find the documents your auditor wants. You can manage all of your evidence within a single repository right in the platform. You can also track your audit progress with a Kanban-style board, assign tasks with notifications and alerts, and quickly provide updates to your stakeholders, complete with customizable reports.

- **Apply for cyber insurance coverage through Apptega Edge**, which will automatically connect you with providers that offer coverage based on your current security and compliance posture.

To learn more, visit apptega.com

Visit apptega.com

