Apptega

WHITEPAPER

How to Secure and Ensure Cyber Insurance Coverage in Case of a Cyberattack

Apptega

Contents

Apptega

In an unprecedented 2022 federal ruling, a U.S. District Court found in favor of a request from Travelers Property Casualty Company of America (Travelers) to rescind the cyber insurance policy of one of its customers.

Following a $1 million claim filed by International Control Services Inc. (ICS) in response to a ransomware attack, Travelers asked the court to absolve them of any responsibility to cover the loss.

The reason? Travelers alleged that ICS misrepresented their multifactor authentication (MFA) status when filling out the insurance application, nullifying the policy. While they did use MFA to protect their firewall, ICS wasn't using it to protect their servers or other digital assets as they had stated in the application. Travelers claimed they would not have issued the policy had they known about the misrepresentations, and ICS agreed to have the court rescind the policy, forfeiting all coverage.

The ruling is a harsh reminder to be detailed and accurate when filling out a cyber insurance application. Easier said than done with applications increasing in length and complexity. Underwriting questions are more specific than ever, as are the requirements for coverage.

With cyberattacks on the rise, insurance carriers are starting to protect themselves against massive payouts, ensuring businesses have the right controls in place to minimize the likelihood of incidents. A false statement on your insurance application is just one of the many reasons you may be ineligible for coverage. Policies are filled with loopholes and hidden "gotchas" that can result in a rejected claim.

Policies are filled with loopholes and hidden "gotchas" that can result in a rejected claim.

Taking the proper steps to secure and ensure coverage could spell the difference between a seven-figure claim payout and a business-ending event.

What is cyber liability insurance?

Cyber liability insurance helps protect organizations from financial risk after an incident. When aligned with a thorough risk assessment and compliance program, cyber insurance can help mitigate the damage caused by threats to security, privacy, service, and operations.

Apptega

Key Takeaways

- Cyber insurance has become much more difficult to acquire over the last five years, and coverage isn't guaranteed — even if you have a policy.
- As cyber security risk climbed, so did costs. Insurer loss ratios started high but have since improved due to higher premium rates and more rigorous underwriting.
- Federal and state compliance laws are driving strict insurance requirements. The laws not only regulate data security but also provide a list of considerations for organizations to follow — with penalties for those who don't.
- While compliance is often self-attested, whistleblowers and watchdogs are helping keep organizations honest.
- Organizations should follow best practices when filling out a cyber insurance application to show they have the right controls in place.
- When selecting an insurance carrier and policy, make sure they complement your cybersecurity program and enhance your security posture.
- Beware of hidden gotchas hiding within your cyber insurance policy. They may mean you're ineligible for coverage.
- Be proactive after a breach or incident, and make sure you can prove you're meeting compliance requirements.
- A continuous compliance program can create a more sustainable security posture over time.
- A compliance platform can make it easier to manage frameworks and compliance.

27%

of data breach claims had exclusions that resulted in non-coverage (*Willis Towers Watson*).

<20%

of organizations have more than $600K in coverage *(Blackberry & Corvus)*.

↑ 62%

Direct written premiums *(premiums received before reinsurance)* were up 62% from 2021 to 2022 *(Fitch Ratings)*.

Apptega

The Evolving Cyber Insurance Landscape

How Did We Get Here?

Relative to today, cyber insurance was once very easy to acquire. It was low-cost with little underwriting involved. But adoption was minimal, as were the potential threats of a cyberattack, making it a low-risk investment.

That's no longer the case. Today cyber insurance is one of the fastest-growing segments in property and casualty (P&C) insurance. It's much more difficult to acquire, and coverage is not guaranteed.

So, how did we get here?

Risk and Demand Skyrocketed

In the last five years, there's been a steep rise in cyber insurance claims driven in part by the proliferation of ransomware attacks. According to Statista, nearly 73% of businesses were impacted by ransomware attacks in 2023, a 32% (17.6 percentage points) increase from 2018. Overall, more than half of businesses have been victimized by ransomware each year since 2018.

Pandemic-induced remote work has exacerbated the growing problem. Organizations had to quickly enable remote access for their teams, creating new vulnerabilities across a decentralized security infrastructure.

As the risks went up during the pandemic, so did costs. From May 2020 to March 2021, the average cost of a data breach for organizations with at least 81% of their employees working remotely was almost $1 million more than the global average, according to IBM Security's 2021 Cost of a Data Breach Report. It also took majority-remote organizations longer to identify and contain those breaches. And when remote work was a factor in causing the breach, the average cost was $1.07 million higher.

Overall, more than half of businesses have been victimized by ransomware each year since 2018.

$4.62M

Average global cost of a ransomware breach from 2020 to 2021.

$5.54M

Average cost of a breach at organizations with at least 81% of employees working remotely.

Source: IBM Security Cost of a Data Breach Report 2021

Growing risk led to greater demand. Global insurance broker and risk advisor Marsh reported that client cyber insurance purchases climbed 33% from 2018 to 2022 (9 percentage points). And by 2023, 55% of U.S. organizations had a standalone cyber insurance policy, according to Sophos.

Smaller Organizations Became Targets

Attackers were not only targeting large corporations but also smaller companies with low awareness and defenses. Nobody was immune. Small managed service providers were a particularly popular target, and not just for their low defenses. They also had access to client systems through remote monitoring and management, providing additional victims for attackers.

The average cost of a data breach for small businesses (i.e., less than 500 employees) increased 26.8% in 2021. And while there were increases across the board for all company sizes, small businesses saw the largest percentage growth.

This concerning trend continued after the pandemic, as seen in the 2023 IBM Security Report. While organizations with more than 5,000 employees saw a decrease in average data breach cost, small businesses experienced a 12% increase from 2021 to 2023. That's a 41% increase in only three years.

Why the disparity? Large organizations have the resources to invest in improving their security postures, but smaller businesses are much more vulnerable to attacks. Only half of U.S. small businesses had a cybersecurity plan in place at the start of 2022, according to an UpCity survey.

Cybercriminals are realizing their nets are better cast toward smaller fish. The individual payout may be lower, but they're easier targets, allowing for higher overall volume.

Smaller businesses also have lower cyber insurance adoption, which means they're more likely to be responsible for any losses. In 2023, only 34% of organizations with less than $10 million in revenue had a standalone cyber insurance policy, according to Sophos. Adoption increased with revenue, jumping to 40% for companies with less than $50 million in revenue and as high as 58% for organizations making more than $5 billion.

Insurance Carriers Raised Premiums

As incidents and claims continued to rise, insurers were unprepared for the costs. They didn't anticipate the increasing risk and demand, and they were ill-equipped to properly underwrite cyber insurance policies.

The increase in claims paid and low cost of premiums meant high loss ratios for insurance carriers — the relationship between premiums earned and losses paid out in claims. In 2020, for example, when attacks were increasing and insurers had not yet adjusted, the loss ratio peaked at over 70% according to Fitch Ratings, an 111% increase from 2018.

Eventually, insurance carriers corrected for losses by raising premiums. Cyber insurance renewal premium rates grew steadily from 2020 to 2021, increasing by 34% in Q421 compared to 11% the previous year. Total direct written premiums (premiums received before reinsurance) for standalone cyber coverage also increased considerably during this time, climbing 90%.

Industry Trends: What We're Seeing

It's becoming common practice to extend coverage across multiple insurers for higher limits in the $5 million to $10 million range. Insurers don't want to be left holding the bag for major incidents, so you'll end up with multiple carriers to spread out the risk.

Underwriting Became More Rigorous

The problem for insurers extended beyond their low premium rates. They also realized businesses weren't doing enough to stand up to the growing cybersecurity threat. Insurance was being used as a crutch, providing payout with little work or accountability on the customer side.

To minimize their risk, insurers increased requirements for coverage. The applications became longer and more detailed. And they enacted minimum requirements like backups and MFA, as mentioned in the Travelers insurance example earlier in this whitepaper.

As a result of more rigorous underwriting and premium increases, insurers saw an immediate improvement in loss ratios, falling 6% from 2020 to 2021. These trends continued in 2022, with loss ratios dropping an additional 37%. Premium increases continued but decelerated, with DWP climbing 62% and renewal premium rates increasing by 15%.

This data shows that things are starting to stabilize. Policies weren't priced correctly before, but with better data and control, insurers are becoming more comfortable with cyber risk.

Underwriting Impact by the Numbers

In a 2022 Sophos survey, 94% of organizations with cyber insurance said the process for securing coverage had changed compared to the previous year:

- 54% said the level of cybersecurity needed to qualify was higher.
- 47% said policies were more complex.
- 40% said fewer companies offered cyber insurance.
- 37% said the process took longer.

Apptega

Cyber Security Compliance and Enforcement

Compliance Laws Driving Strict Insurance Requirements

Maintaining a robust cybersecurity compliance program is essential for protecting your data and complying with various regulatory standards. Federal and state compliance laws not only regulate data security but also provide a list of considerations for organizations to follow — with penalties for those who don't.

The fines and sanctions in this section are not always covered under your cyber insurance policy, making compliance even more critical. The best way to avoid a penalty is to ensure you're meeting the requirements of any regulations that apply to your business. Doing so can also make it easier to secure cyber insurance coverage with a favorable rate.

Personally Identifiable Information (PII)

PII is any representation of information from which an individual's identity can be reasonably inferred by either direct or indirect means. In simpler terms, it's data collected about a person's identity, such as their name, email address, phone number, or social security number.

This could apply to staff, students, patients, donors, or other individuals who have trusted your organization with their information. A common example is data collected for marketing purposes. When you fill out a website form or sign up for a product, the company is collecting potentially sensitive data about you. This information is PII, and organizations have a responsibility to safeguard it.

Customer PII was the most breached record type the last three years, with 52% of all breaches involving this type of information in 2023. It was also the costliest record type to have compromised at $183 per record, surpassing employee PII, other corporate data, intellectual property, and anonymized customer data.

Enforcement of PII privacy and protection falls under the jurisdiction of the FTC. They can not only audit any organization at any time but also levy fines for those who have not employed "reasonable protections" to secure their data — even if a breach hasn't occurred.

From the Field:

In 2019, Equifax Inc. agreed to a $575 million (potentially up to $700 million) global settlement with the FTC, Consumer Financial Protection Bureau, and 50 U.S. states and territories. The FTC complaint alleged that Equifax failed to take reasonable steps to secure the massive amount of PII stored on its network, leading to a breach that affected around 147 million people.

State Privacy Laws

Data privacy requirements can vary by state, and some are more prescriptive than others. For example, California requirements are very prescriptive, providing individuals with greater control over their data through the California Consumer Privacy Act (CCPA), which narrowly resembles the strict governance of GDPR.

CCPA is a comprehensive consumer protection law that broadened the definition of PII as well as the rights of Californians to know how their information is collected, used, and to request that it be deleted.

CCPA has far-reaching implications and has influenced requirements in other states, such as Connecticut, that are looking to model their requirements after the strictest state guidelines. Others take the opposite approach, opting for vague, non-prescriptive guidelines that allude back to those "reasonable protections." These guidelines aren't very clear, which can make it difficult for organizations to know what they should be doing to meet requirements.

FTC Safeguards Rule

Financial institutions under the jurisdiction of the FTC have their own data privacy requirements. The Safeguards Rule requires these organizations to take certain measures to keep customer information secure. They're also responsible for making sure their affiliates and service providers are doing the same.

In 2023, the FTC amended the rule to extend their reach, requiring non-banking financial institutions to report on data security breaches. This includes auto dealers, mortgage lenders, payday lenders, collection agencies, tax prep firms, and other organizations that process financial applications but don't fall under the banking or credit union umbrella.

For these organizations, compliance with the FTC Safeguards Rule is an even bigger challenge. They're likely unfamiliar with the requirements and how to put the right protections in place. They'll need to:

- Assign a qualified individual to execute and oversee an information security plan.
- Conduct regular testing of the safeguards.
- Update their program on a regular basis.
- Educate their staff on how to stay compliant.
- Document an incident response plan.
- Report annually to their C-suite and board.

These tasks can be a major undertaking for organizations that have never done them before. Especially for those without internal IT or security and compliance teams.

SEC Guidelines

In July 2023, the SEC adopted new rules around the disclosure of material cybersecurity incidents. The rules include public disclosure of board and management oversight of cybersecurity risks as well as the steps being taken to protect sensitive information. The purpose of these guidelines is to equip investors with enough information to make informed decisions.

Incidents must be reported within four days of a material incident, which has raised some valid concerns. If an organization is in the middle of a forensic investigation or still negotiating with an attacker, they may not want to prematurely disclose information to the public. What if they don't want the attacker to know they've detected them and are taking steps to remediate the situation? There's still a lot of gray area to sort through.

SEC Definition of Material Inside Information

"Information which, if known, could reasonably be expected to affect the value of the Company's stock, or which would affect the investment judgment of a person making a decision to buy or sell the stock. Information is considered "material" if there is a substantial likelihood that it would be considered important by a reasonable investor in deciding whether to purchase or sell stock, or other securities, or if the information would be viewed by the reasonable investor as having significantly altered the total mix of information available to the investor before making the purchase or sale. The information need not be the determining factor but must assume actual significance in the investor's deliberations."

How Compliance Is Enforced

While we touched on how the FTC can audit organizations and levy fines, we haven't discussed how these regulations are enforced. Who is reporting on compliance? And if an organization isn't complying, how does anyone know without an audit?

Compliance Reporting

Regulations alone should not be the only driver of compliance. You should also consider the societal, consumer, and business impacts. For one, organizations often have a fiduciary duty of oversight. As mentioned in the SEC Guidelines section, there are rules in place to ensure proper, timely disclosure of cybersecurity risks to the public. And it's up to the organizations to make sure they're abiding by those rules.

Organizations are also responsible for reporting on their own compliance with regulatory standards. For example, non-federal organizations that handle controlled unclassified information (CUI) on behalf of the U.S. government are tasked with protecting it.

The standard for protecting CUI is the NIST 800-171 framework, which establishes requirements for compliance. As is often the case with cybersecurity reporting, NIST 800-171 compliance is self-attested. The Department of Justice relies on the False Claims Act to encourage accurate reporting, imposing liability on organizations that knowingly submit false claims to the government. And like with the laws in the previous section, the penalties for noncompliance can be severe.

So, while reporting responsibility often lies with the organization, it's in their best interest to be upfront and honest.

Exposing Noncompliance

While compliance is often self-attested, regulatory agencies don't completely trust organizations to disclose cybersecurity risk. As such, they've created certain incentives for whistleblowers to expose noncompliance.

In a 2022 settlement, Aerojet Rocketdyne Inc. agreed to pay $9 million to resolve allegations it violated the False Claims Act. In this example, Aerojet's former director of cybersecurity became a whistleblower, exposing the company's noncompliance with cybersecurity requirements in certain federal government contracts. In return, he received a $2.61 million share of the recovery — an enticing incentive for anyone to expose a company misrepresenting their protections.

The Justice Department also has a new watchdog division called the Civil Cyber Fraud Initiative that is tasked with rooting out cybersecurity failures and misrepresentations. They recently announced their first settlement, a $300,000 fine against a one-person web hosting company, serving as a warning to others. Companies of all sizes are subject to these rules and regulations — and the fines that come with noncompliance.

Apptega

Meeting Cyber Insurance Coverage Requirements

5 Tips for Obtaining Cyber Insurance and Ensuring Coverage

There's a good chance that at some point your organization will become the victim of a cyberattack — if it hasn't already.

According to Delinea's 2023 State of Cyber Insurance Report, 79% of organizations had to file a claim with their insurer in 2023, and 47% used their cyber insurance more than once. Most experts agree it's no longer a matter of "if" but "when" an attack will happen.

And when it does, will you be covered?

You may have a cyber insurance policy (if you were even able to obtain one), but that doesn't mean you're covered when an incident occurs. **In fact, a report from Willis Towers Watson shows that 27% of data breach claims from 2013-2019 had exclusions that resulted in non-coverage, with more recent industry estimates indicating similar findings.**

Common Reasons for Rejected Claims

- Lack of security protocols in place
- An internal bad actor
- Human error
- Bodily injury
- Acts of war, terrorism, or geopolitical unrest
- Failure to follow compliance procedures
- Damage caused by criminal activities such as theft or fraud
- Property damage
- Not reporting the incident to the insurer first

There are no guarantees when it comes to obtaining a cyber insurance policy or securing coverage. But there are certain steps you can take to improve your chances.

1 Prepare for the Application Process

The first step in protecting yourself against a cyberattack is securing a cyber insurance policy. As mentioned earlier in this whitepaper, the process can be intensive. How you answer questions during the application will not only determine whether you get a policy but also if you'll be covered when an incident occurs.

This isn't an application you can fill out in a day. It takes a lot of preparation to do it right. According to Delinea, 45% of organizations took 1-3 months to obtain or renew cyber insurance, 30% took 4-6 months, and 7% took more than 6 months.

Why does it take so long? Insurance carriers want to know what controls you have in place to protect your organization, and the information can take some time to collect and verify. Are your systems encrypted? Do you have MFA? How are you protecting workstations? Cyber insurance applications have a growing list of requirements for coverage. And while these can vary for different policies and providers, there are some general best practices to consider:

- **Access Management** – How do you manage access to critical systems, applications, privileged accounts, and data? Insurers want to ensure you're reducing the risk of unauthorized access to avoid security breaches and insider threats. MFA is a staple for many cyber insurance applications, requiring multiple levels of identity verification. But questions about identity and access management as well as privileged access management are also becoming more common.
- **Backups and Downtime** – What happens if your data and systems are impacted? Do you have backups in place to ensure they can be quickly restored (both on-site and off-site)? And how long might your systems be down? Longer downtime can result in larger insurance claims.
- **System Encryption** – Encryption ensures that even if unauthorized users access your systems, they won't be able to read it.

- **Staff Training** – Human error is one of the top reasons for rejected claims. You can implement every possible protection, but they won't be effective if your employees aren't trained to use them. Business email compromise should be a major focus area, as phishing attempts are the initial attack vector in 16% of breaches, according to IBM Security.
- **Workstation Protections** – Make sure your workstations aren't vulnerable. That means, among other things, password protections and firewalls. You should also remove admin rights from workstations, so if one gets infected, it won't spread through the organization like wildfire.
- **Threat Monitoring** – How are you identifying cyberattacks? You should have the right procedures and technologies in place to identify incidents, breaches, unusual behavior, and other threats.

If you say you have a protection in place, you better mean it. Don't stretch the truth or overstate your status (as we learned from the Travelers example). An in-depth risk assessment and analysis of your security posture can help identify areas of strength and weakness. Unfortunately, many organizations struggle with these assessments, overlooking critical risks that can lead to protection gaps if a breach or other incident occurs.

Additional investments are almost always needed. Before being approved for a policy, 96% of organizations purchased at least one new cybersecurity solution. There are sure to be gaps, and you'll need to fill them if you want to meet insurance requirements.

To make sure you're taking proper stock of your cybersecurity posture, consider having a third party validate the information for you. It may even be required by the insurance provider. In fact, 55% of organizations needed an external risk assessment to obtain their cyber insurance policy, according to Delinea.

2 Select the Right Carrier and Coverage

There are hundreds of cyber insurance providers to choose from, and you don't want to choose the wrong one. It's best to stick with the top 20 when possible. These carriers tend to have the best policies and breach response teams, so they're better situated to cover all major and minor events. But sometimes a top-20 carrier isn't an option for municipalities or organizations that need to stack layers of coverage between multiple insurers, for example.

Making sure you have the right coverage isn't just about selecting the right carrier. You must also consider whether your policy provides an adequate financial safety net to cover a major incident. According to a study by Blackberry and Corvus, only 19% of organizations have more than $600,000 in coverage.

Here are some things to keep in mind when seeking a cyber insurance policy:

- **Look for a standalone policy** – Avoid endorsements, which are changes or add-ons to your existing package policy. To obtain comprehensive coverage, a standalone policy is much better, as endorsements usually have additional exclusions and lower coverage ($50,000 probably won't get you very far after a major breach). To make sure you can cover the business interruption, forensics, ransom, downtime, data replacement, and other costs, you should look for a standalone policy with the highest possible coverage based on your organization's size, risk, and budget.
- **Consider both first- and third-party coverage** – Look for first-party cyber coverage to protect your organization's data. It will be difficult to find an insurer that will cover all your risks, but first-party coverage can offer reprieve for areas such as forensic services, recovery and replacement of lost or stolen data, or cyber extortion and fraud. Third-party coverage protects your organization from liability for third-party claims. Coverage may include payments to consumers, claim and settlement expenses, or other losses.

- **Find a complementary policy** – Risks can be different for each organization. When exploring your cyber insurance options, you should seek out a policy that complements your security program and improves your security posture. This is where those risk assessments come in handy. Knowing your risk can help you identify the right cyber liability coverage for your organization.

Key Risk Assessment Considerations When Choosing Your Policy

- → **Security** – Errors and omissions, contractual liabilities, and aggregation of cyber risk
- → **Privacy** – Network vulnerabilities such as ransomware, data breaches exposing PII or other sensitive information, and confidential data such as CUI
- → **Service** – Regulatory considerations (CCPA, GDPR, etc.) and consumer-related issues such as collection, storage, and usage
- → **Operational** – Technology reliance, cloud adoption, and enterprise systems

3 Watch Out for Hidden (and Not-So-Hidden) “Gotchas”

Once you have a cyber insurance policy, don’t assume you’re covered. Even if you carefully fill out the application and accurately attest to your security posture, there may be restrictions in place to keep you from a full or even partial payout.

These gotchas aren’t to be mistaken with the common reasons for rejected claims listed at the top of this section. The following aren’t exclusions but rather common loopholes/blind spots in your policy:

- **Endorsements** – This was discussed in the section above, but it’s worth repeating. Make sure you have stand-alone coverage and not an endorsement attached to another line of coverage. Have you spoken with an agent and filled out an application? If not, you don’t have a stand-alone policy and may be surprised by your limits if you experience an incident.
- **Sub-Limits** – These are the maximum payments an insurance carrier will provide for a specific type of incident. If the cost of an incident exceeds the sub-limit, you won’t receive payment for those overages.
- **Deductibles** – If you have other types of insurance, you’re likely familiar with this term. Your deductible is the amount you must pay before insurance kicks in for a covered loss. If the cost of an incident exceeds your deductible, you’ll have to cover a chunk of the costs. And if your deductible exceeds the cost of an incident, you won’t receive any payment.

4 Respond Immediately Following a Breach

This one is straightforward. Once you discover a breach or incident, you should move quickly to minimize impact. Here are immediate steps you should take:

- Call the breach response team. The insurance carrier will have a phone number and can provide next steps. They'll organize a response team to handle the situation: IT, legal, forensics, PR, and so forth.
- Reaching the carrier and creating a response plan can take time. You should already have your own plan in place (i.e., detect, respond, recover).
- Localize the breach. But be careful not to jeopardize forensics.
- Call an MSSP or IT Consultant. Don't handle the situation alone. A trained professional can help ensure the process goes smoothly.

5 Provide the Right Evidence to Ensure Payout

If you submit a claim, you should be able to defend it. Did you align your protections to a framework? Continuously test and monitor compliance over time? It's not enough to say you have controls in place. With increased insurer scrutiny in the underwriting and claims payout processes, you need to show your work and prove you're meeting compliance requirements.

In general, P&C insurers are moving toward a continuous validation model, employing real-time monitoring to track policyholder behavior. Auto insurers are already using telematics data to track certain driving behaviors, adjusting policies for drivers who exhibit safe driving. And now cyber insurance is heading the same way with a focus on continuous compliance.

For example, the U.S. Department of Health and Human Services (HHS) recently instituted a 12-month lookback period when conducting audits and administering penalties for HIPAA noncompliance. HHS must now consider whether a covered entity and their business associates have adequately demonstrated that recognized security practices were in place for at least the previous year.

We'll dive more into continuous compliance in the next section.

Apptega

The ROI of Compliance

Continuous Compliance Is Driving Better Cybersecurity Postures

Cyber insurance is a last line of defense against attacks. You can't just sit back and let a breach happen because you think you'll be covered. Cybersecurity requires a much more proactive approach. A well-structured compliance program not only ensures continuous compliance but also makes it scalable, creating a more sustainable security posture over time.

Don't wait until you're filling out an insurance application or going through an audit to think about improvements. Organizations that implement continuous checks and evaluations along with best practices will be better positioned from a compliance standpoint — and more appealing to insurance carriers.

When you start to factor in the potential costs of an incident with more tangible considerations like reduced premiums, increased investor confidence, and the ability to win more competitive deals, the full value of compliance becomes clear.

Everyone Needs a Cybersecurity Framework

The easiest way to meet insurance coverage requirements is by aligning to a recognized cybersecurity best practice or compliance framework.

Frameworks are your organization's roadmap to compliance. They're prescribed methodologies and security baselines that take the guesswork out of the process, showing the specific standards your organization must meet. By reevaluating your position and alignment to a given framework, it becomes easier to ensure ongoing, continuous compliance. It's your best protection against potential lawsuits, regulators, and insurance coverage issues.

Some states have even instituted "safe harbor" as an incentive to take proper cybersecurity precautions. If you live in a safe harbor state and can show proactive alignment to a recognized framework, you'll be protected from regulatory fines or even legal judgment when an incident occurs.

Choosing a Framework

There are many frameworks to choose from depending on your industry or other requirements. But if you're looking for a good starter framework, NIST CSF provides standards, guidelines, and best practices to manage your cyber-related risk.

With a little more than 100 controls, NIST CSF is ore condensed and prescriptive than some of the sector-specific frameworks with hundreds of controls. The framework also provides a sliding 0-5 maturity scale for addressing risk rather than a strict yes/no format. Finally, NIST CSF is the foundation for other U.S. frameworks. You can start with a CSF assessment and later map controls to sector compliance frameworks if you work with health data, CUI, credit cards, or other sensitive information.

The Role of Technology in Continuous Compliance

A risk assessment is one of the first steps toward compliance and achieving cybersecurity coverage. But once you know where you're vulnerable, you still need to manage, maintain, track, and report on your security controls. If you're doing that through spreadsheets and files in multiple folders, you're going to have trouble pulling it all together on demand.

Automating the compliance process can reduce human error and increase efficiency. It also simplifies reporting and documentation for audits and when demonstrating compliance to regulatory bodies.

As mentioned earlier, you need to be able to prove you have the right protections in place. Insurers want to see program maturity in real-time, which can be difficult to demonstrate in a spreadsheet.

A cybersecurity compliance platform such as Apptega can make it easy to manage frameworks and bring all your compliance data together in one place. You can see where you stand in your framework implementation and gain insight into individual controls and sub-controls, which you can export and submit with your cyber insurance application.

Conclusion

Cyber insurance requirements are more intensive than ever. Applications are longer and more in depth, requiring organizations to employ strict controls to minimize risk of a breach or other incident.

When looking for coverage for your organization or having initial conversations with clients, consider how to align the actions your policy requires with a broader compliance program:

- Start with an in-depth assessment of your security posture to identify areas of strength and weakness.
- Understand the specific cybersecurity regulations and frameworks that apply to your business and industry.
- Perform a thorough risk analysis to identify vulnerabilities and threats to your information security.
- Develop clear, comprehensive cybersecurity policies to cover data protection, access control, incident response, employee conduct, and more.
- Implement your policies and provide regular training to employees.

Following these guidelines can make it easier to secure a cyber insurance policy and ensure coverage in case of an incident.

Apptega

About Apptega

A perennial G2 leader across various risk management categories, Apptega is the end-to-end cybersecurity compliance platform that security-focused IT providers and in-house teams use to build and manage cybersecurity compliance programs simply, quickly and affordably. It's trusted by hundreds of MSSPs, MDR companies and security-focused MSPs, who are growing lucrative compliance practices, creating stickier customer relationships, and winning more business from competitors.

To learn more visit apptega.com