



The Ultimate Guide to

Cybersecurity for Associations

A three-part guide with all you need to know (and more) about cybersecurity for associations.





The **Ultimate Guide** **to Cybersecurity** for Associations

For decades an imaginary line has separated cybersecurity from “the business.” But after years of unsatisfactory results, the time has come for both security and business leaders to start asking the right questions and formulating the right approach.

Cybersecurity is on the tip of everyone’s tongues these days.

And for good reason.

So we’ve created a three-part guide about the ins and outs of cybersecurity for associations.

Which means you have everything you need to ensure you’re keeping your organization and member data safe (with the least work and cost possible).

Let’s get started.



Part 1: Cybersecurity

What is cybersecurity?



The cybersecurity field is currently undergoing a massive shift to the mainstream. And as the volume and sophistication of cyber attacks grow, all organizations must take steps to protect sensitive information.

Over the course of doing business, organizations transmit information across networks. A significant portion of that data is sensitive in nature (i.e. intellectual property, financial data, personal information, etc.).

Cybersecurity, also known as information security (InfoSec), is dedicated to protecting that information and the systems used to process or store it.

Definition

cy • ber • se • cur • i • ty

the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.



Cybersecurity can be broken down into four main categories:

\$1.1 MILLION

The average cost of a data breach to a company in 2019, up 52% from the previous year.

1. Risk Management

Effective **risk management** allows an association to identify, assess, and control threats across the organization. Because a cyber presence exposes an association to constantly emerging new threats, risk management is particularly important for its information systems.

Threats can come from many sources, starting with blatant criminal activity such as data breaches or ransomware attacks. Threats, however, may also come to light after the initial attack is detected and may include financial and legal issues, management challenges, and accidents.

IT departments rely on a combination of strategies, technologies, and education to protect against cyberthreats. Cybersecurity risk management involves identifying your risks and vulnerabilities and applying administrative actions and comprehensive solutions to ensure your organization is protected.

However, risk management is not just an IT exercise.

Deciding which risks are acceptable and which are not is a collaboration that must involve senior leadership of the organization.



2. Policy Management

While many believe that responsibility for cybersecurity sits in the hands of the IT department, security should be a concern for each employee in an organization.

Policies are an effective way to educate employees on the importance of and responsibility for protecting confidentiality, integrity, and accessibility of systems and data. Cybersecurity policies can be used to set the standard of behavior for all employee activities (e.g. acceptable use policies and confidential data policies).

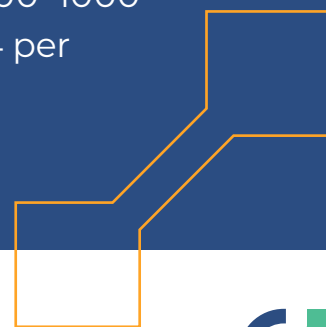
Grand Theft Data, a McAfee report on data exfiltration found that employees cause 43% of data loss, one-half of which was accidental.

Improved cybersecurity and the management of existing policies can help employees and partners better understand how to maintain the security of data and applications, ultimately lowering the chances of a breach.



\$35.33 per employee

is the average estimated cost of a cyberattack in organizations with 500–1000 employees, as compared with \$204 per employee for larger organizations.²



3. Vulnerability Management

Most organizations depend on a combination of commercial and custom-developed hardware and software to support their IT needs. These technology components inevitably include vulnerabilities in their design, setup, and code. In order to mitigate these risks, organizations must understand said risks and address vulnerability management in a well-defined and managed information security program.

Vulnerabilities are weaknesses that a threat actor (i.e. a hacker, nation-state, disgruntled employee, etc.) can exploit to adversely affect data security. These weaknesses typically focus on issues in the software, hardware, and/or systems an organization uses. For example, design, implementation, and other vendor oversights may create defects in commercial IT products.

A robust vulnerability management program can directly address these issues.

**Is your
association
vulnerable
to attack?**

Cimatri specializes in working with associations to assess vulnerabilities and develop a plan to manage them now and in the future.

Connect with one of our Certified Association Executives (CAE) and Certified Information Systems Security Professionals (CISSP) for a free consultation.

[Connect Now](#)



4. Cybersecurity Education

Many organizations still see cybersecurity as an 'IT thing.'

As such, they often forego investments in cybersecurity education. (Read: These organizations have little to no buffer in place to instill a culture of digital resiliency.)

Your employees need cybersecurity training to protect themselves and your organization against cyber attacks. By making employees aware of security risks and threats and what procedures to follow when a threat is identified, you're strengthening the most vulnerable links in the chain.

New hire training, as well as regularly scheduled refresher training, should be established in order to instill the data security culture of your organization. Cyber security training should include, but not be limited to:

1

Company policies and procedures

2

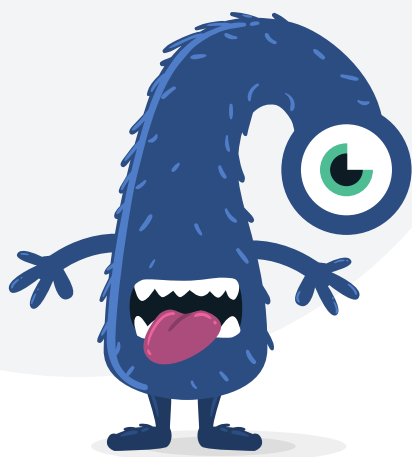
Handling sensitive data used in employee roles

3

Proper ways to store and transmit sensitive data



Why is cybersecurity important?



43%
of cyberattacks
in 2020 were
targeted at
Cloud-based
data, double
that of 2019.³

Cybersecurity encompasses everything pertaining to protecting sensitive data, personally identifiable information (PII), personal information, intellectual property, data, protected health information (PHI) and governmental and industry information systems. And therein lies its importance.

Driven by remote work, global connectivity, and cloud services, our society is almost entirely technologically reliant. As such, the widespread (and lacking) configuration of cloud services, as well as increasingly sophisticated cyber criminals, means your organization is more at risk today than ever before (and you may not even know).

And while you may be thinking that you're too small to have to worry about cybersecurity, you'd be wrong. GDPR and other laws now say that cybersecurity is no longer something anyone can ignore, regardless of staff size, profitability, or industry.



Why is cybersecurity increasing?



Largely driven by the increasing exposure of identity information to the web via cloud services, information theft is now the most expensive and fastest growing segment of cybercrime. But identity theft isn't the only goal.

Cyber attacks often aim to compromise data integrity by destroying or changing data to breed distrust in an organization or the government.

And it's only getting worse.

Cybercriminals are becoming more sophisticated, changing their targets, how they affect organizations, and their methods of attack depending on your security system.

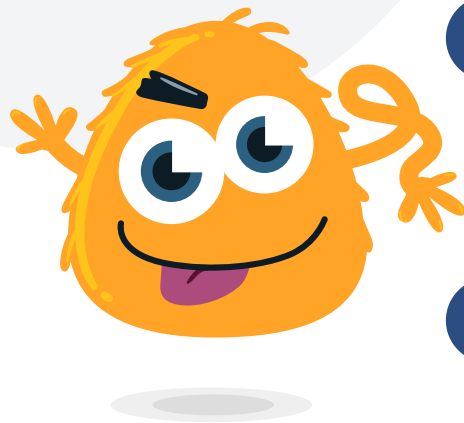
In fact, according to the Ninth Annual Cost of Cybercrime Study from Accenture, the average cost of cybercrime for an organization increased by \$1.4 million over the last year to \$13 million, with the average number of data breaches hitting 145.

As such, it's vital to take a deep dive into your third- and fourth-party vendors who process your data, as many have poor cybersecurity practices, which means the door is open for ransomware and phishing attacks.



What is the impact?

Without a specific focus on cybersecurity, your organization can be affected in numerous ways:



Economic Costs

After **theft** of intellectual property and corporate information, the corresponding disruption in trading and cost of system repair can bring even more damage to your organization than the original breach.



Reputational Costs

Breaches often lead to a loss of member trust and future and current customers, as well as poor media coverage. Meaning: Your company's reputation is going to take a serious hit, regardless of the data stolen or lost.



Regulatory Costs

GDPR and other data breach laws specify that your organization may suffer from regulatory fines or sanctions as a result of cybercrimes.

While it still may be difficult to detect and understand the direct and indirect costs of a security breach, the best first step for all organizations, regardless of size, is to ensure staff understand cybersecurity threats and how to mitigate them. This should include regular training and a framework that aims to reduce the risk of data breaches or leaks.



10 Tips to Improve Individual and Organizational Cybersecurity

1

Keep Your Software Up To Date

Installing regular updates for both enterprise and personal software is one of the most important defenses against ransomware attacks. Developers regularly identify vulnerabilities in their software and issue patches to deter malicious actors, making it harder for hackers to attack your system.

A best practice -- patching your system as soon as updates are available to keep all your devices secure.

We recommend:

- ✓ Updating your devices with security patches as soon as the patches become available. Most systems and apps include an automatic update feature. Be sure to turn it on.
- ✓ Allowing your web browser to install security updates automatically.
- ✓ Using the most recent versions of plugins like Flash, Java, and others.



2

Anti-Virus & Firewall Protection

Anti-virus (AV) software and firewalls are two effective tools to fight malicious attacks.

AV software keeps known viruses and other damaging code from infecting your devices by identifying the attacking code and preventing it from entering the device.

Firewalls control what enters your device by scanning the Internet for potential threats and denying access to your device. Windows and Mac OS X both have resident firewalls, but you should also install a firewall on your router.

Best practice: Use anti-virus software from trusted vendors and only run one AV tool on your device to increase your employee's personal cybersecurity and decrease your overall cyber risk.

3

Strong Passwords & Management Tools

Strong passwords are essential to keeping your personal devices secure, but they are also essential to keeping bad actors from accessing your data. What you know about creating strong passwords, however, may need updating.

The National Institute of Standards and Technology issued an update in 2017. According to NIST guidelines, you should:

- ✓ Use user-friendly passwords with at least eight characters instead of trying to combine random symbols, numbers, and uppercase letters.
- ✓ Create a new password for each site.
- ✓ Don't reuse passwords.
- ✓ Use one lowercase letter, one uppercase letter, one number, and four symbols in each password.



- ✓ Do not use “&”, “%”, “#”, or “@”.
- ✓ Make your passwords easy to remember.
- ✓ Don't make a list of passwords or hints, and don't make any password list available to the public where hackers may find it.
- ✓ Change your passwords at least once a year.
- ✓ Use a password tool or vault to manage your passwords.

Best practice: Make your passwords memorable, unique to you, and different for each platform. Using a password protection vault program is a great way to manage these passwords and who has access to them.

4

Two-Factor or Multi-Factor Authentication

To increase your personal cybersecurity, you can use a two-factor or multi-factor authentication service in addition to a standard password.

With two-factor security, you enter your password, but are then prompted to enter an extra authentication method. These methods could be a personal identification code, another password, or a fingerprint.

If you use a multi-factor security method, you will be asked for two or more authentication methods after you enter your password. The more levels you have, the greater your security.



5

What You Need to Know About Phishing Scams: Be Suspicious

Phishing attacks often look benign. They look like a legitimate email, attachment, or link. Because the “bait” looks real, the hacker tricks the user into divulging log-in credentials or other personal information. By clicking on malicious links or opening an attachment, the user can allow the hacker to infect the system with a variety of malware.

Best practices:

- ✓ Don't open emails from people you don't know. If you're not sure it's real, hover over the name of the person or company sending the email. The address will tell you whether or not you can trust it.
- ✓ Emails are always what they seem to be. Check for grammatical and spelling errors. Be sure of the sender before you click on any link.
- ✓ Friends aren't always infection free, so be careful that your “trusted sender” hasn't been infected, too.

6

Protect Your Personal Identifiable Information (PII)

Hackers can use information that identifies you, specifically, to identify or locate you. Known as Personal Identifiable Information (PII), it could include: name, address, phone number, date of birth, Social Security Number, IP address, location details, or any other physical or digital identity data. This type of data can be sold to bad actors for a variety of purposes— none of them positive for you.

Use of social media can increase your vulnerability online. Be careful about the details you share. Only share the very minimum.

Best practice: To increase your personal cybersecurity (both in and out of the office) review your privacy settings across all your social media accounts.



7

Secure Your Mobile Devices

McAfee Labs reported that your mobile phone was a target for more than 1.5 million new threats in the first quarter of 2017. Incidents have only risen since then.

Best practices include:

- ✓ Create a complex mobile passcode
- ✓ Install apps only from trusted sources
- ✓ Update your device regularly
- ✓ Avoid sending texts or emails containing personal identifiable information or other information like financial or health details
- ✓ Turn on Find my iPhone or the Android Device Manager
- ✓ Backup your mobile device regularly

39% of companies have suffered a mobile compromise in 2020, up 41% since 2018.⁴

8

Regular Backups Are Critical

Regularly backing up your data is an often overlooked step in personal online security.

Your goal is to ensure a clean backup in the event of a breach or data failure, so one backup is not enough. Top IT and security managers recommend at least three backups on both internal and external hard drives, in addition to one copy stored off-site (most often cloud storage).

With those backups in place, you can erase your system and restore a clean copy if your system is breached. You won't have to pay ransomware demands to restore your system.

Best practice: Set up a recurring task in your project management system to backup your systems, or invest in an automatic backup program to add to your website and data management process.

280 average number of days it takes to identify and contain a breach.⁵

4. Mobile Security Index (Feb 2020)

5. IBM's 2020 Cost of a Data Breach Report (July 2020)



9

Always Use a VPN

Using public Wi-Fi is convenient, but it's dangerous. So when you do, be sure to use a virtual private network (VPN), as well.

A VPN encrypts information as it travels between your device and the server. Encryption makes it harder for criminals to access your passwords or data.

Best practice: Use your mobile phone as a hotspot if a VPN is not available.

10

Review Your Online Accounts & Credit Reports Regularly

Consumers must take the time to safeguard their online accounts and monitor their credit reports. To protect your credit information, all three credit reporting companies allow customers to freeze their credit. This prohibits anyone from accessing a credit report or financial information unless they input a personal identification number.

The best action is pro-action. If you wait until a critical problem to address cybersecurity threats, it's too late.

With Cimatri's assessment options, you can find out right now what kinds of potential problems you need to address and begin solving them today.

[Learn More About Taking an Assessment](#)



How Secure is Secure?

Questions to Ask to Gauge Your Cybersecurity Risk

When considering the security of your data, systems, and online processes, it's important to know that there's no "one size fits all" solution. It's all about thinking about your organization holistically and investing in preparation, technology, and systems that will identify and mitigate risks.

While it's unlikely that your data is perfectly protected at this very second, here are some good questions to ask to ensure you're on the right track.

1

What Devices Are on Your Network and Have They Been Updated?

Sometimes you won't know what you don't know until it's **too late**. However, there are a few things to consider when you're trying to gauge your preparedness for a cyberattack. For example, when is the last time you did an audit of a) how many devices are using your network and b) whether they are up to date? The more devices you have and the less often you update them, the higher your risk.

Even more dangerous are unidentified devices—personal devices that team members may bring from home. If you are not actively scanning for and working to eliminate these technological wild cards, you have no idea the kinds of threats that are being brought to your association without your knowledge.



2

How Often Are You Attacked?

You might not know this information off the top of your head unless you are very involved in monitoring attacks with your IT leadership. Even then, it's nearly impossible to track every attempt bad actors have made against the integrity of your website or internal systems.

Still, it's not a good rule of practice to get involved in thwarting attacks after your "hull has been breached."

Asking the questions, "Have we been under attack?" "How many times?" and, "Has a bad actor ever stolen any data?" are keys to creating a strategy against further loss of data integrity.

3

How Long Does It Take You to Identify and Triage an Attack?

There are **three key metrics** that you should be using when you're answering this question:

✓ **Mean Time to Detect (MTTD)**

How long does it take to identify an attack?

✓ **Mean Time to Resolve (MTTR)**

How long does it take your team to respond to the attack?

✓ **Mean Time to Contain (MTTC)**

How long does it take to repair the weak places in your system integrity so that an attack doesn't recur?

If you are good at detecting attacks, but bad at containing them, there is a major issue. Consider running a simulated attack like you would a fire drill. Your team will learn how to respond faster, identify issues quicker, and proactively find weak places in the technology environment that they wouldn't have otherwise.



4

How is Your Security Objectively Viewed By Ratings & Compared to Competitors?

Once you have done as much internal analysis as possible, it is always a good idea to see how your security stacks up to third-party security ratings providers and as well as those in your area of association expertise. This is one of the areas that **Cimatri** excels at, and we are always happy to help you with a security assessment to define your cybersecurity weak and strong points.

5

How Safe Are Your Members and Vendors?

Although your members and vendors are huge parts of your association's core purpose, how you are interacting with them (and how they are interacting with you) is one of the likely places you will find a security breach. Not only do you have to know how safe your members and vendors are as they are interacting with you (threats on your networks that might pass through to them), but you must know how safe you are from their poor technology management.

In either case, the answer is usually better vendor/member technology management. Just be aware that the people you do business with are all potential threats. It is your job to protect everyone else in your sphere of influence from spreading that threat.

53% of organizations surveyed have experienced data breaches caused by a third-party vendor.⁶



6

What Are The Patching Cadences of Both You and Your Vendors?

Hackers and bad actors are always ready to take advantage of a **lazy update schedule**. When your team makes this a low priority (especially if they are too focused on reactive operations and not proactive preparation), it opens you, your vendors, and your members up to exploitation.

Develop a regular plan for updates and patching. And consult with your vendors to ensure they are doing the same. It doesn't matter what they're providing you with. If they are being lax in their updates, they are putting your association at risk.

7 Questions to Ask Regarding Vendor Risk Management

- 1 Do you have a governance framework in place to address vendor risk management?
- 2 Do you have policies, standards, and procedures in place for vendor selection, onboarding, offboarding and transition?
- 3 Are vendor contracts being managed appropriately based on risk, spend, and classification?
- 4 Is there a qualified vendor manager/team in place with oversight of process, security, and performance?
- 5 Is there a centralized point of contact for vendor management that departments can contact for information relating to vendors?
- 6 Is there periodic monitoring scheduled for vendors? What aspects are covered in your organization's periodic review of the vendor?
- 7 Is there a structured due diligence process to ensure critical vendors and risks are not missed?



7

Who Has Access to What and For How Long?

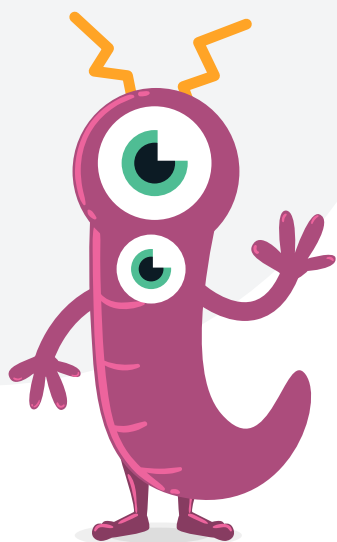
This isn't just about who has admin privileges. This is about who has **access** to anything in your organization. When you have high turnover, many volunteers, or guest speakers and writers managing your digital properties, the odds of overlooking passwords and access that shouldn't be retained are high.

Consider putting into place a key person or system that manages access quickly and automatically so that people who no longer should have access, don't. In addition, follow the rule of "least privilege," and never give someone more access than they need to do their job.



Part 2: Cyber Risk

What is cyber risk?



Evaluating your cyber risk answers the question, “What is the likelihood our association will suffer from damage to our reputation or have financial losses because of cyber attacks?”

Three key indicators help to calculate risk. **They are:**

- ✓ Nature of the threat
- ✓ System vulnerability
- ✓ Potential damage to reputation or finances if systems are breached.



What is cyber risk assessment?

Risk assessments identify potential threats to the cyber security of a company, but risk assessments also can be applied to individuals, other organizations, states and nations. In this case, a cyber risk assessment provides critical information to organization leaders about the vulnerability of its system, as well as proper responses to identified threats.

Your risk assessment will address areas, including:

- ✓ Ranking the most valuable technology assets. What should we protect first and best?
- ✓ Ranking the impact of various types of attacks. For example, could a ransomware attack be more damaging than a malware attack?
- ✓ Identifying potential threats and their sources. For example, does our payroll vendor pose a threat because of their lax security standards?
- ✓ Calculating areas of greatest risk both inside and outside the organization. Are our employees aware of security risks? Are our vendors?
- ✓ Forecasting the impact of various breaches.
- ✓ Determining the probability of successful attacks.
- ✓ Establishing an accepted level of risk.

If you can answer these questions, you can determine what to protect and how. Meaning: you can develop IT security controls and data security strategies to further mitigate your risk.



Why do you need one?

Here are four reasons why you may need a cyber risk assessment:

1

Reduction of Long-Term Cost

Malicious attacks can be expensive and detrimental to an association's reputation. Identifying threats early and developing plans to combat incursions ultimately can save your organization thousands, sometimes millions, of dollars.

2

Provides a Template for Future Assessment

Once your first risk assessment is completed and implemented, you have a **roadmap** for ongoing efforts to mitigate your risks. Of course, you'll revisit your plans regularly to ensure you've addressed new threats and accessed new defenses.

3

Better Organizational Knowledge

Developing your first risk assessment can give you an overview of vulnerabilities that affect your cyber security. It's not always just firewalls and anti-virus solutions. A **detailed risk assessment** can help you spot and correct hidden process problems.

4

Avoids Data Breaches, Issues, and Data Loss

Data breaches can put your financial stability and reputation at risk, as we've noted. If, however, the breach also highlights a failure to follow applicable regulations such as GDPR, HIPAA, or others you may have a much larger problem on your hands.



Part 3: Cyber Insurance

What is cyber insurance?

Cyber risk insurance provides certain protections for recovering from cyber related events. Data breaches and personal information theft are simply one segment of cyber risk. Cyber policies provide two main coverage components:

1

First-Party Coverage

First-party coverage protects an association from losses incurred due to a cyber attack. The coverage provides reimbursement for financial losses such as lost income, ransomware demands, required notification costs for those whose data was affected, and costs to restore networks or lost data.

Simply put, this is balance sheet protection.

2

Third-Party Coverage

Third-party coverage is a broader coverage than first-party coverage. It extends protection to expenses related to other parties, such as attorney's fees, damages, or lawsuit settlements. It can also cover an organization if it transmits a virus to another company or person, and can cover regulatory issues.



To research what policies may be available to you, contact your general liability coverage provider. A cyber policy can be added as a basic endorsement to an existing liability policy or can be written as a separate policy. A separate policy generally provides more coverage.

Types of claims covered:

- ✓ Extortion and ransomware attacks
- ✓ Virus infections of computer systems
- ✓ Distributed Denial Of Service (DDOS) attacks
- ✓ Data breaches and clerical errors
- ✓ Improper privacy policies
- ✓ Data collection practices
- ✓ Virus and malware transmissions



How can I assess my current policy?

Contrary to popular belief, cyber insurance isn't just a money pit.

The novelty of cyber insurance means that things are not yet standardized. This has led some insurers to hide behind vague policy language to avoid paying claims that would bankrupt them or set claim-paying precedents that might run them out of business in the future.

But, in many cases, the real problem is that association leaders don't know what the organization's policy covers and what it excludes.

So how can you get started assessing your current policy to ensure you're not falling into the typical insurance traps?



Assess The Threat Potential

You probably have a good sense of the current threats your organization is facing, but it's also important to consider the industry as a whole.

Ask yourself "What threats and risks are others in my industry dealing with?" This may align with your original concerns for your own organization, but there may be a few others you haven't truly identified.

Best practice: Run a Google search to confirm you have a full sense of the threat landscape. News articles, whitepapers, and industry trend reports are all good sources that may spark a new conversation around your association's cyber risk.

Once you have a decent list of common threats, assign each of those a risk score (1-10) based on your organization's exposure. Then, create a short list of the 3-5 threats that most concern you. This will help you determine exactly what you need most from your insurance policy.

Cybersecurity claims breakdown for 2020

41% Ransomware

27% Funds transfer loss

19% Business email compromise issues⁷



A large orange circle graphic on the left side of the page, containing text about the average cost of lost business for organizations.

\$1.4M

average cost of
lost business for
organizations.

Estimate The Possible Remediation Costs

To determine how much insurance coverage you need, it's important to have a reliable estimate of how much it may cost to remediate various incidents on your own.

The best way to do this is through a business impact analysis (BIA).

A BIA is an exercise used to help organizations understand their recovery and remediation costs. These assessments are often completed as part of a disaster recovery plan where IT security professionals set realistic recovery targets based on their current restoration capabilities and business requirements.

Because BIAs help project downtime losses and recovery costs, they can also ensure you understand just how much cyber insurance your organization needs.

Remember: Business input is important, but don't let a lack of it delay your BIA. Complete your draft based on your current knowledge of the organization. It's easier to edit estimates than start from scratch.

How much does it cost to withstand a cyberattack?

The costs of dealing with a cybersecurity attack can be incredibly high. If you need help assessing exactly how much, we would love to talk with you about your association..

[Talk to a Cyberattack Pro](#)



Overcome Typical Insurance Pitfalls

Cyber insurance comes in many forms. As such, policyholders must shop around and negotiate to find the coverage that best suits their needs.

Typical problems with cyber insurance are usually due to these 10 issues:

1

Unstandardized Products

Policies typically offer both first- and third-party coverage for the organization itself and its partners. But some don't. Ensure your policy covers both.

2

Data Loss Isn't The Same As Data Misuse

Some policies only cover cases of **data misuse** (i.e. by a bad actor) and as such, cannot be used if data is only discovered to be lost.

But be aware that data loss is often enough cause for customers to take legal action regardless.

3

Regulatory Fines Vs. Associated Cost

Costs other than the initial fine itself, such as legal costs, are not usually included in the coverage for regulatory infractions.

Make sure you understand your coverage limitations before a claim is made to avoid unnecessary headaches (and unbudgeted costs).

4

Know The Retroactive Date

Insurance coverage typically kicks in the date the policy is signed. But some policies will cover incidents that occur within the previous year (or longer).

Try to negotiate to have the retroactive date set as far back as possible.



5

Errors And Omissions

You will need to complete a **self-assessment** of your security posture. This needs the utmost accuracy, as any mistakes or forgotten information may be held against you during a claim.

Remember: in the future, it is up to you to update your insurer regarding any changes to the original security posture.

6

Third-Party Stipulations

Most policies cover **third-party support** for legal or technical recovery support, but sometimes there is an approved list of options you must choose from.

Familiarize yourself with this clause before you need it.

7

Mobile, Third-Parties And The Network

Policies generally agree to cover your organization's network, but the definition of "your network" is sometimes narrowly defined, potentially excluding remote work, mobile devices, or associated third parties.

8

Insider And Vendor Incidents

If an **incident** arises from a malicious insider or vendor (i.e. parties you've authorized to use your network), your policy may not cover you.

Review your risk tolerance for these types of incidents and decide what coverage you need in place.

9

Business Interruptions

In these **types of claims**, an adjuster will be appointed by the insurer to calculate losses. This may not cover third parties.

10

Coverage Caps

Many policies will **cap coverage** for a given area (e.g. total policy coverage is \$3M but only \$1M can be used for ransomware). In other cases, a noted exclusion may significantly reduce the policy's actual usefulness.

Before purchasing, confirm that these caps and exclusions will not interfere with your future claims and reimbursement.



Insurance Isn't a Get Out of Jail Free Card

Cyber insurance can be a great addition to an association's cybersecurity toolbox, but it is only one piece of the puzzle. Other important features of a sound strategy include a plan for continuity of operations, disaster recovery, and active patching.

When procuring cyber insurance, you will likely need to attest to the strength of your full security plan through a self-assessment. You may also be asked to provide yearly statements of security compliance. If they are not submitted on time (or are inaccurate), you may be denied coverage in the event of a cyberattack.

Some insurers may provide reduced premiums for clients demonstrating mature security programs, but this discount is often small. As such, it's usually not worth the risk to overstate your security protocols to receive said discount.



>1-20

breaches exploit vulnerabilities when patching is done regularly⁸



What type of policies are there?

Thanks to the increase in need, blanket claim exclusions via conditions-precedent language are fairly uncommon, but it's still something you should be mindful of before purchasing. Typical claim decisions are made case by case, so you should look ahead to see how your potential insurer handles various issues.

Let's take a look at a few typical coverages and what you need to know.

Cyber Warfare and Terrorism Coverage

War is typically excluded from many policies due to its widespread destruction, as this could potentially bankrupt insurers. Terrorism is sometimes covered, but it is not uncommon for it to be excluded if executed electronically.

And while you may not be worried about becoming a direct victim of either cyber warfare or terrorism, global cyber incidents (like 2017's NotPetya) show just how quickly such attacks can proliferate beyond their intended target.

Moreover, cyber attacks are impersonal and their origins aren't always clear. This creates a situation where one might argue that any widespread attack is an act of terrorism or war. Especially if there are indications that a government or government-sponsored group are involved.



Ransomware Coverage

Ransomware is one of the most popular reasons for acquiring cyber insurance. Which means your premium just went up by as much as 25%. But new privacy regulations are also affecting premiums, as ransomware infections mean data has been exposed and/or exfiltrated outright.

Your insurance policy may need to cover not only the ransom amount, but also the costs of recovery if the hackers fail to make good on unlocking the compromised systems.

Cyber Liability Insurance

Standard liability insurance covers cases where a third party sues an organization for some type of misfortune involving that organization (i.e. negligence).

Cyber liability insurance is used for the same reason (i.e. to cover third-party claims), but in cyber this usually applies to something regarding privacy or network security.

For example, an organization with a mature security program suffers a data breach and sensitive customer records are exfiltrated. The organization had appropriate controls in place, but the attack exploited an unknown security vulnerability.

The organization is liable, but it is not fair to say that negligence occurred. In this case, cyber liability insurance (rather than standard liability insurance). This also holds true in cases where malicious code was unintentionally sent to a third party.



What should I look for in a vendor?

Just like other types of insurance, it's more than worth it to review your policy and your vendor needs at least once a year to ensure you are still covered against your biggest threats and that your coverage matches your recovery cost estimates.



Forensic Expenses

Once you've determined that data has been compromised, you'll need to investigate what happened, how it happened, and what information was accessed, but this can take up a lot of your time and money. Luckily, some cyber risk policies will cover the expenses you may have when hiring an outside forensic team.

Be sure to ask if your policy covers forensic expenses, as the last thing you need when dealing with a breach is to realize you don't have the budget to mitigate it.



Legal Expenses

In order to determine the scope of the federal and state notification requirements, you'll need legal representation after a breach. You will also need legal counsel to defend you in the event a suit is brought against you.

Does your policy reimburse this? Some of it? None at all?





Notification Expenses

These expenses may include postage, paper, printing, call centers, etc., and while it may not seem like this would be worth a discussion, think again. They really do add up.



Regulatory Fines and Expenses

Out of compliance with even the smallest of applicable regulations? You better believe the government is coming for you, tooth and nail. Make sure both you and your vendor are aware of policies and regulations before you get started.



Credit Monitoring and Credit Repair

While not legally required, it's generally agreed that seeking both credit monitoring and ID theft repair with your vendor can reduce potential legal liabilities. (It's also best practice.)



Public Relationship Expenses

How your breach is reported to the media is crucial. Both to restore your reputation and maintain your members, customers, vendors, business associates, and partners.

Make sure you check with your vendor to see if they cover some of these expenses. If not, ensure your budget has wiggle room.



Liability and Defense Cost

These expenses may include postage, paper, printing, call centers, etc., and while it may not seem like this would be worth a discussion, think again. They really do add up.



Regulatory Fines and Expenses

Out of compliance with even the smallest of applicable regulations? You better believe the government is coming for you, tooth and nail. Make sure both you and your vendor are aware of policies and regulations before you get started.



The Wrap Up

Although the sheer number of attempted cyber attacks is growing every year, it is still possible to ensure your organization (and its data) stays safe and breach free.

Successful companies implement a range of strategies to protect themselves and their employees from criminal activity, and everyone gets involved. Responses are often complex, involving individual devices, networks, software, data, and employees. Security is no longer the sole purview of the IT department but requires a concerted effort.

And in today's hyper-connected, digital world, everyone benefits from advanced cyberdefense programs. That's why it's so important to take your first step towards cybersecurity today.





Your Association Deserves to Be Protected

**Certified IT professionals who understand
your association inside and out.**

Whether you have dealt with a recent cyberattack or are simply trying to keep your association as safe as possible, having professionals on your team who understand your unique issues is invaluable.

At Cimatri, we have been working alongside association leaders for over 25 years, helping them adopt and implement new technologies, find and train the right people to manage them, and develop the processes that will keep their associations safer and more financially secure.

When you are ready to stop hassling with your IT and start using it to achieve your strategic goals, we are only a click away.

[Get Your Free Consultation Now](#)



Part 4: Resources

1. Radware's 2018-2019 Global Application & Network Security Report (Jan. 2019)
2. IBM's 2020 Cost of a Data Breach Report (July 2020)
3. Verizon Business 2020 Data Breach Investigations Report (May 2020)
4. Mobile Security Index (Feb 2020)
5. IBM's 2020 Cost of a Data Breach Report (July 2020)
6. The Cost of Third-Party Cybersecurity Risk Management (March 2019)
7. H1 2020 Cyber Insurance Claims Report (September 2020)
8. Verizon Business 2020 Data Breach Investigations Report (May 2020)

