LEARNING MADE EASY

Cowbell Cyber Special Edition

Cyber Insurance

for dummies®
A Wiley Brand

Discover why you need cyber coverage

Review how coverage and claims work

Find out how to apply for coverage

Brought to you by

COWBELL® CYBER

Steve Kaelble

About Cowbell Cyber

Cowbell Cyber makes cyber insurance easy and delivers customized, standalone cyber policies to small and mid-size enterprises. Its robust coverages deliver financial protection against all flavors of cyber incidents, including data breaches, ransomware attacks, and other kinds of cybercrime. All policies are bundled with free-of-charge risk assessments, risk insights, cybersecurity awareness training, and risk management services to help businesses reduce their cyber risk exposures.

Cyber Insurance

Cowbell Cyber Special Edition

by Steve Kaelble

for dummies®
A Wiley Brand

Cyber Insurance For Dummies®, Cowbell Cyber Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-83924-8 (pbk); ISBN: 978-1-119-83925-5 (ebk). Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Carrie Burchfield-Leighton

Acquisitions Editor: Ashley Coffey

Sr. Managing Editor: Rev Mengle

Business Development Representative: Cynthia Tweed

Table of Contents

Introduction

Few businesses today could function without their computer-based operational tools and their internet connections to the world, their customers, their partners, and their suppliers. The irony is, the digital technologies that make it all happen are also opening the door to threats that can be downright existential.

For most threats to your business, you implement safety measures for prevention and buy insurance to transfer whatever risk remains. You buy a fire sprinkler system and also fire insurance. You have company cars with collision prevention technology, along with collision insurance. You try to hire honest employees, but you also have property insurance in case someone turns out to be a thief.

The same holds true for today's cyber threats. Smart, forward-thinking businesses carefully build cyber defenses to protect against data breaches, ransomware, and other cybercrimes. And increasingly, these businesses are buying cyber insurance.

Cyber insurance is coverage designed specifically for the ever-growing cyber threats your organization faces. Traditional coverage has big holes through which bad actors can easily drive a cybercrime, but cyber insurance is designed to fill in the coverage gaps. It also evolves as the threats evolve. And it helps you understand where your risks and vulnerabilities are so you can mitigate them.

About This Book

Cyber Insurance For Dummies, Cowbell Cyber Special Edition, is your guide to this vitally important insurance specialty. It's designed to help your organization understand the cyber risks you face and why your business can't afford to let those risks go uncovered. Your traditional business insurance policy isn't up to this increasingly vital task. Explore how cyber coverage is written and how your carrier can come to the rescue in times of crisis. And find out how much you can learn from the process of obtaining cyber insurance — knowledge that helps protect your organization.

Icons Used in This Book

In the margins of this book, you may notice some eye-catching icons. They're there for more than just good looks.

REMEMBER

This book is concise, but if you don't have time for every word, be sure to catch what's in the Remember paragraph.

TIP

My aim is to equip you with actionable advice and ideas, and some of that advice is right next to the Tip icon.

WARNING

This book includes cyber risks and awful things that can happen to your organization. Pay attention to the Warning icons to avoid these pitfalls.

Beyond the Book

This book isn't lengthy, and you're likely to read through it fairly quickly. There's a good chance you'll come away hungry for more insights about cyber insurance. If that's the case, check out these ideas:

- **Cowbell Cyber:** Visit `cowbell.insure` for more information about Cowbell Prime insurance, Cowbell Factors, and Cowbell Insights.
- **Cowbell Factors:** Get risk ratings and understand how your organization's risk profile compares to your peers. Visit `cowbell.insure/for-businesses`.
- **Examples:** Understand the types of cyber threats and cyber incidents. Check it out at `cowbell.insure/examples_of_cyberincidents`.
- **Costs:** Manage the bottom-line impact of a cyber incident at `cowbell.insure/cost_of_cyberincidents`.
- **Glossary:** Familiarize yourself with the terms commonly used in cyber insurance. Head to `cowbell.insure/cyberinsurance_glossary`.

IN THIS CHAPTER

- Understanding the purpose of cyber insurance
- Avoiding costly gaps in coverage
- Exploring the benefits of standalone cyber policies

Chapter 1
Introducing Cyber Insurance

The news is filled with shocking stories of cyberattacks that shut down medical records systems, expose credit card or identity data, and even grind business to a halt at some enterprises. It's a growing problem, incredibly disruptive, and extremely costly.

This chapter explores the concept of cyber insurance policies that cover the kinds of losses that arise from a cyber incident. It explores how cyber coverage developed and why standard business policies often leave dangerous cyber coverage gaps that need to be filled. This chapter also explains why your best approach may be to obtain a standalone cyber policy rather than to hope that you can work it out through your existing business policies.

Understanding the Concept

The concept of cyber insurance emerged from third-party liability. The early incarnations grew out of errors-and-omissions insurance, when it became clear that companies have a duty to protect their clients' or customers' data as well as that of their employees.

REMEMBER

Cyber insurance has evolved along with the understanding of cyber threats. The costs of cybercrime are far more than third-party considerations. You have plenty of first-party losses and expenses to think about, too.

Take a ransomware attack as an example. From the very start, during and after an incident you need the assistance of forensic investigators to help figure out what exactly has happened. That's an immediate expense and not an insignificant one.

Then come the first-party losses. There may be a business income loss or interruption. A company may lose a potential client or a contract as a customer becomes nervous about doing business with the cyberattack victim.

REMEMBER

Cyber insurance protects businesses from these various and evolving risks related to security and privacy. The risk exposures continue to grow as digitization accelerates, and like other types of insurance, cyber insurance offers financial protection.

Closing Gaps

One thing that's true about virtually all kinds of insurance is that what you don't know can really hurt you. When it comes to cyber risks, a lot of small and mid-size enterprises aren't adequately covered, and it often boils down to basic misunderstandings about their standard coverage.

WARNING

They may, for example, carry a business owner's policy (BOP) or other property policy and just make the assumption that they're covered for this increasingly common business risk through a data breach endorsement. In reality, there may be significant insurability gaps.

Such misunderstandings are, well, understandable. Policies can be complex, and the definitions of coverage may not exactly be clear to the layperson. What's more, obtaining the right kind and amount of coverage can be cumbersome. Many questions need to be answered because insurers have to understand your situation and the controls you have in place.

Ultimately, trying to insure your cyber risks with a BOP policy may leave you with a lot of question marks or outright "no" answers.

For example, your coverage for first- and third-party exposure is going to vary from one policy to the next. It may be adequate; it may not.

WARNING

When a BOP *does* cover something that needs to be covered, you may not have much choice regarding limits and deductibles. Indeed, the issue of limits may be a major concern because many BOPs will set limits too low to be fully helpful when a cyber situation unfolds.

And as for what a BOP often won't cover, you may be surprised. Business interruption from a cyber incident? Not necessarily. The wide-ranging expenses, losses, and headaches that come from ransomware attacks? Don't count on it. Cybercrime in general? It quite possibly isn't the BOP's concern.

REMEMBER

Certainly, plenty of good reasons exist to have a BOP because it can simplify a lot of insurance matters for small and mid-size businesses. You just have to be well aware of what it *doesn't* cover. Just as your BOP is generally not intended to deal with such things as professional liability, medical coverage, and worker's compensation, it also is unlikely to handle all the various risks related to cyber incidents.

Choosing Standalone Cyber

TIP

One way to sort through the complexity and cumbersome nature of covering your cyber risks is to seek a standalone cyber insurance policy. This can be advantageous for a number of reasons.

To begin with, a good standalone cyber insurance policy fills in all the coverage gaps. It takes care of the first- and third-party exposures that are linked to cybercrime. It accounts for the kinds of situations inherent in a ransomware attack. It'll be there for the business interruption losses that are often inevitable. And it's likely to offer a wide range of limits and deductible options.

At the same time, it focuses on only the coverages that are relevant for your situation. Your enterprise's exposure is unique to your situation and certainly different from that of your business neighbor next door. There's no point in buying coverage that your enterprise doesn't need. And then there's the advantage of dealing with a provider that specializes in this kind of coverage.

You're likely to gain a better understanding of what the coverage looks like and much greater clarity with regard to how a claim scenario will play out.

It's not all that different from other kinds of purchases. You could, for example, get your next mattress at your nearby wholesale club — it's in the aisle next to the giant jugs of laundry detergent and across from mega-TVs. But you'll learn more about your purchase if you go to a mattress specialist.

The ease of doing business is a big consideration, too. A cyber insurance provider should be able to get you a proposal faster, getting your coverage up and running more easily and promptly.

To use Cowbell Cyber as an example, you can get a cyber insurance quote in just a few minutes simply by inputting an organization's name and the state where it's located. Because Cowbell specializes in cyber, it can use its data-driven risk assessment factors to quickly determine your individual cyber risk ratings and compare your organization's risk profile to that of industry peers.

TIP

Risk ratings, of course, help determine insurance rates, but they're just a start. They can also provide a window into where your organization is vulnerable and what you can do proactively to reduce your risk. In that way, a standalone cyber insurance policy can serve your needs beyond the actual coverage it provides. Certainly, you want to be sure you're well covered in the event that something bad happens. But at the end of the day, you and your cyber insurance carrier are both better off if you can prevent cyber incidents in the first place.

IN THIS CHAPTER

- Exploring the need for cyber insurance
- Understanding your specific cyber risks

Chapter 2
Understanding Why You Need Cyber Insurance

Cyber insurance is all about addressing the many ways a cyber incident can adversely impact your business. This chapter examines the reasons why cyber insurance is essential, from covering financial losses, to paying for the resources you need to investigate and recover quickly, to shining the spotlight on vulnerabilities you may have missed earlier. And it spells out how cyber risks vary from one company to another and from one industry to another.

Listing the Reasons

Why do you purchase insurance? Generally speaking, it's how you ensure you can withstand the impact of various kinds of losses and incidents. If a company vehicle is involved in an accident, you need that vehicle repaired or replaced. If someone breaks into your warehouse, you want compensation for what was stolen or damaged.

Cyber incidents are quite a bit more complicated than your average truck crash or physical break-in. There are certainly going to be financial losses, but that's just the start of your concerns.

REMEMBER

A cyber incident quite possibly could shut down whole segments of your operation. It can leave you on the hook for losses that impact your customers, employees, or business partners. The havoc it can wreak is potentially widespread and devastating, so obtaining coverage that's cyber-specific is good for many reasons:

- **Mitigating financial loss from cyber incidents:** A cyber incident can cost you money — directly and indirectly. There are legal costs and plenty that may be less obvious, such as the cost of forensics to investigate the incident and the cost of providing notifications to all who are impacted.
- **Recovering from an incident quickly:** A big cost, of course, is disruption to your business. Cyber insurance can help you minimize disruptions by bringing in the expert services you need to get back to business as soon as possible.
- **Being one step ahead of the game:** If it hasn't happened already, your organization may face a contractual obligation to get cyber coverage. Better to start down that path and obtain coverage while there's time to evaluate what you need instead of waiting until you're under pressure of a contractual deadline.
- **Understanding your risk exposure:** What you don't know about your cyber risks is dangerous. The process of obtaining cyber coverage can be instructive in helping you assess your risks, and the right insurer can help you continually monitor your coverage and steer clear of coverage gaps.
- **Benchmarking your security:** Your cyber insurance policy should bring with it the ability to compare your business with that of your peers to ensure you aren't behind in your cybersecurity measures compared to your industry standard.
- **Covering your specific situation:** A good cyber insurance policy aligns with the unique needs of your business and the ways you use technology. You must ensure your coverage fully matches your risk exposure and is tailored to your needs.

REMEMBER

It sounds complicated, but it doesn't have to be. As I discuss in Chapter 1, by choosing an experienced provider, it's possible to obtain a cyber insurance quote quite quickly with only a minimal amount of information required.

Protecting Your Specific Situation

No one is safe from cyber threats. It doesn't matter what industry you're in; your organization is at risk. Some industries are especially hot targets because of the nature of the data in their care. And the types of risk may vary from one sector to another. In this section, I give you the details about how a variety of business types are impacted by cyber risk.

Keeping healthcare healthy

WARNING

If your organization operates in the medical field, you're among the top targets for cybercriminals. That's because the healthcare sector handles some of the most valuable and sensitive data possible: electronic medical records. It also is involved in significant monetary transactions, and in many cases, it operates a complicated variety of medical software systems that are internet-connected.

Consider these common but frightening risks experienced by medical and dental practices:

- **Breaches of patient data:** A cyber incident could compromise the patient medical records stored in your electronic health record system. If that happens, you could end up with Health Insurance Portability and Accountability Act (HIPAA) violations, which can carry hefty fines of well over a million dollars.
- **Lost or stolen devices:** Medical staff typically can access a lot of patient data, and if there's a theft involving their phones, computers, or tablets, that could compromise patients' data privacy. The resulting lawsuits could be downright unhealthy to your business.
- **Business interruption:** Depending on the nature of the cyber incident, your office may be forced to shut down for some period of time, which could mean a loss of income.

And if malware interferes with your data backup, you could have a tough time restoring medical records and getting your operation up and running quickly.

- **Compromised payment information:** As with any industry, a successful phishing attack could allow a cybercriminal to initiate fraudulent transfers of funds.

TIP

What can cyber insurance do to mitigate these risks? To begin with, it can cover expenses related to recovering from an incident, notifying patients, and it may cover related regulatory penalties. It can cover the costs of breach investigation and mitigate reputational damage costs. It can address the costs of business interruption and also help cover financial losses and expenses related to fraudulent activities.

Addressing risks in the legal business

Law firms are susceptible to some of the same general kinds of risks that impact healthcare organizations and others. Specific risks and impacts are unique to the law field, though.

WARNING

Law firms may have e-discovery tools that connect to clients' network systems — helpful technology that unfortunately adds some vulnerability. And they may have cybersecurity practices or operate cyber labs to aid clients, which can, ironically, put them at extra risk, too. Here are some thoughts on cyber risk for lawyers and law firms:

- **Compromised client data:** Lawyers maintain highly confidential and privileged data on their clients, but a cyber incident can put that data at risk of exposure, which can cause significant damage to the firm's reputation and the level of trust it has earned through the years. What's more, cyberattacks can block access to client files, and that can be a serious blow to providing exceptional legal services.
- **Stalled business operations:** A cyber incident can shut down much of a firm's ability to operate. Lose those billable hours and your income will decline precipitously. And if your data backup is impacted, the ability to restore client files will be jeopardized.
- **Lost or stolen equipment:** Lawyers often access client data on-the-go, at the courthouse or in a client's office. But that puts laptops and tablets at risk for theft, and theft of equipment can lead to a breach of sensitive data.

TIP

Cyber insurance has answers to all these risks and many others, such as ransomware, social engineering attacks, and bricking. It can cover financial losses from fraudulent activities, investigation and recovery expenses, business interruption, reputational damage, and many other impacts.

Making manufacturing safer from cybercrime

Manufacturers face the usual array of cyber risks, too, like any business. But they have their own set of vulnerabilities as well.

WARNING

For example, they may operate the factory floor with a connected supervisory control and data acquisition system (SCADA). This hardware and software system makes modern manufacturing and industrial processes more efficient and even safer, but they provide cybercriminals with windows of opportunity. And you need your factory floor operational to keep making money — business interruptions linked to ransomware average 23 days.

Manufacturers are also likely to make electronic payments to suppliers or accept them from customers, which creates another risk. And if you're a smaller organization contracting with a bigger firm, you may be targeted as a way to infiltrate your customer.

Cyber insurance policies tackle all these manufacturing-specific risks and a lot more. They're there to cover losses, recoup expenses, and bring in experts to get your business operational again after an incident.

Building a defense for contractors

Say your organization is a construction contractor, or some other type of contractor, serving a large commercial organization. You have all the usual cyber threats that are common for all businesses, plus some of your very own.

Here's one incredibly important consideration. Cyber criminals are interested in the big fish, but those big fish often have the strongest defenses. If you're a smaller fish doing contract work for the bigger entity, you've got an "in."

WARNING

With that "in," you may have access to client information, with sensitive client files stored on your digital devices. Perhaps you even have a digital connection into the client's internal systems. That makes you a point-of-entry target. And you can bet that if a cyberattack finds its way into your systems and impacts your big customer, you may be held responsible.

TIP

Cyber insurance provides a good safety net for these kinds of risks that come from being a smaller fish swimming in the big pond. You can expect coverage for incident losses and expenses as well as recovery, business interruption, breach investigations, notification costs, and fraudulent transactions. With first-party liability coverage, you'll have help dealing with compromised client information.

Exploring other industry-specific situations

Countless other industries have their own individual situations and idiosyncrasies that cyberattackers are itching to exploit. Here are some examples:

- **Insurance agencies:** These businesses maintain a wealth of private information about customers and the things that they own. They process payments and transfer claims information electronically. And they'd be almost completely shut down if ransomware locked up their data.
- **Auto dealerships:** A car dealer also has electronic connections to customers' financial information for processing loans and payments, and perhaps connections to the bureau of motor vehicles, too. Exposing any of that could cause a world of trouble and significant damage to a dealer's reputation, and reputation is incredibly valuable in this line of work.
- **Tax preparers and accountants:** These professionals obviously have full access to some of the most sensitive information any client will ever share. They may also have professional tools that connect directly with clients' network systems. Government regulators have an interest in their data security plans. And their good reputations are worth their weight in gold and must be protected fiercely.

- **Realtors:** In recent years, the real estate industry has been the second-hottest target for email fraud attacks, particularly *whaling,* which is essentially phishing that fakes the email address of a high-ranking individual. Agents may have online databases of clients and partners, store clients' financial files in the cloud, and process fees and payments electronically. All kinds of risks knock at real estate's door.
- **Freight brokers and truckers:** Computer connections are essential and complex in the world of logistics. There may be connections to supply chain customer relationship management (CRM) systems, electronic payments zipping back and forth around the world, fleets managed by sophisticated technologies, connected devices on vehicles that are traveling virtually everywhere. The volume of payment data processed through supply chain CRMs is huge and attractive.
- **Agriculture:** Just because you're down on the farm doesn't mean you're safe from cybercrime. Smart agriculture brings information technology literally into the field, livestock may be tagged with radio frequency ID devices, and online services store financial files and other sensitive data. Every new connection is a new opportunity for a breach.
- **Retail:** Shops large and small couldn't operate without computers and connections to data. The customer database might be stored locally or online. There's a good chance there's an online store, there could be a customer loyalty program with self-service options, there may be social media interactions with customers. And, of course, payments are made electronically to suppliers and from customers. Any transaction is susceptible to fraudulent activity.
- **Hospitality:** Hotels and conference centers are full of enticing opportunities for cybercrime. Dedicated Wi-Fi network for guests? That can be a problem. Sensitive and confidential meetings on-site? You don't want inadvertently to be responsible for breaches of their info. Rewards programs will store customer data, guests' payment information is stored on the network, and reservations may be made online. If hackers shut things down, there may be no rooms available.

- **Nonprofit organizations:** A nonprofit usually relies heavily on the support of generous benefactors, and it's essential to protect their information. That said, the organization is vulnerable if it accepts donations online and processes them electronically, or uses a donor management system for compliance reporting. The keyword here is "donor." There may be donor-related software tied into the network that's vulnerable. And volunteer staffers are dedicated to the cause but may or may not be great at spotting a phishing expedition.

IN THIS CHAPTER

- Understanding multifactor authentication
- Helping your employees become cyber warriors
- Planning ahead for the worst
- Establishing a solid backup

Chapter 3
Beefing Up Your Cybersecurity

This book is all about obtaining cyber insurance so that you're covered in the event of a cyberattack. But no matter how well you're covered, wouldn't you rather avoid experiencing an attack altogether? You still fasten your seatbelt and obey traffic signals, even though you have car insurance, right? Of course you do because the best outcome is one that steers clear of mishaps.

This chapter covers concepts your organization should consider to reduce your exposure to cyber events and speed up the recovery should something happen. These ideas — such as adopting multifactor authentication (MFA), training your employees, planning ahead, and maintaining a good backup — are undeniably beneficial to you. But they also help ease your insurance application process because an insurer wants to ensure that you're doing everything possible to stay safe.

Understanding and Adopting MFA

As many as four out of five web application breaches happen when a hacker obtains account credentials. If cybercriminals can get hold of basic account credentials — usernames and

passwords — it's essentially game over. The attacker can log right in and gain access to whatever sensitive information is locked inside, right? Well, not necessarily. Not if the account is protected by MFA. Those four out of five breaches could have likely been prevented by MFA.

With MFA enabled, the basic account credentials alone won't provide access to the account. Whoever is trying to log in must also get through one or more additional factors, sometimes known as *secrets.* These factors may be generated dynamically, and the idea is that only the account owner will be able to get through the extra layer of protection.

What may these extra factors be? There are three main possibilities:

- **Special knowledge:** This bit of information is known by the account owner but presumably not the hacker. It may be another password or some kind of security question.
- **Physical possession:** This kind of factor is something the account owner possesses that a hacker can't get. It may be an SMS code texted to the account owner's mobile device or even a physical key. Authentication apps can take care of this, too.
- **Biometric identification:** This factor taps into something that's inherently part of the account owner themselves, such as fingerprints or face IDs.

TIP

Be sure all users on email and cloud applications use MFA. Same for those people gaining remote access. And if possible, use authentication apps such as Google Authenticator instead of sending a text code because phones can be compromised through such tactics as SIM swapping or fake SIM recovery messages.

MFA is hard for hackers to defeat but relatively easy for your organization to deploy. You can obtain it out of the box for free with various systems you acquire. One more bit of advice? While you're rolling out MFA to your teams, suggest that they also activate it on all personal accounts that offer it. Online banking most likely does, along with email apps and other commonly used technologies. It's a good idea all around, at work and elsewhere.

Preparing Your People

Good employers recognize that their employees are among their most important assets. Unfortunately, it's shockingly easy for a good employee to inadvertently open the door to a cyberattack.

REMEMBER

Phishing emails are a common culprit. These are those emails that trick the recipient into clicking on a malicious link that ends up installing malware on systems or enticing the recipient to provide sensitive information. Many ransomware attacks happen in this way.

A phishing email looks legitimate. It may appear to come from a person of authority. The recipient may think it's the real deal, click on the link, and — BAM! The malware gets installed, the attack begins, and your organization is hit with weeks of business interruption and a hefty demand for ransom.

TIP

Your valuable employees happen to be your best line of defense against this kind of attack, but you need to train your defenders. All employees should learn to instinctively check the "from" email to ensure it's a valid sender and not a clever fake.

If you sign up for cyber insurance, your carrier may provide you with a training program for your workforce. In fact, you may even be required to implement training in order to obtain or renew a cyber policy.

Planning and Collaborating on a Response

Think back to your days as a student in school. Remember fire drills? They may have been scary, but they certainly were a good idea. When the building's on fire, it's a terrible time to be thinking for the first time ever about how all the kids will get to safety.

Same is true with cyber incidents. They put a business in hyper-crisis mode, they're stressful, and you need to take the right actions right away. That's why you need to plan your response in advance.


TIP

What you need is an incident response plan that documents what to do in case of a cyberattack, whom to contact, and who needs to be involved in the response. It needs to be written up, circulated, tested, and updated regularly as the organization evolves and grows. As you get new systems or encounter new risks for any other reason, your incident response plan must be updated.

Again, your cyber insurance provider will likely be glad to help with this. There may be outlines already created that you can use as starting points.

Along the lines of advanced preparation, your organization may choose (or be asked by your cyber insurance provider) to conduct annual penetration testing. It's basically another kind of fire drill. You may even explore deployment of a variety of systems, such as a managed detection and response system, an endpoint detection and response system, or an intrusion detection system.

Backing it Up

No one wants to experience a cyber event such as a ransomware attack. But if you do, you'll be in a much better situation if you've maintained an isolated, offline backup. Note that I said *isolated* backups. They must be separate from your main systems, and isolated from the internet, so they're less vulnerable to being hit in the same attack. They should be fully encrypted, and any account with access to the backups must have multifactor authentication enabled. If a backup is in your back pocket, you're in a stronger position for negotiating with the criminals and potentially even recovering your data and systems without paying a ransom.


TIP

These backups should cover all critical data and systems you deploy and manage in-house. If you have third-party systems running certain operations, they likely have backup procedures, but you need to check with them on the details. Whatever options they offer, it's wise to opt in.

IN THIS CHAPTER

- Monitoring risk exposures and threats
- Responding to a cyber incident
- Getting started with cyber insurance

Chapter 4
Making Cyber Insurance Happen

If you're concerned that your standard business policy may not fully cover your cyber needs (spoiler alert: it usually doesn't), now's the time to figure out how to make cyber insurance happen. This chapter tells you how cyber underwriting works and how it differs from other kinds of underwriting. It explores what transpires when a cyber incident takes place, how a cyber insurance carrier helps with the response, and how to get the ball rolling.

Understanding How Cyber Underwriting Works

Everything about the digital world constantly evolves. For the most part, that's a good thing for your organization and your customers. Unfortunately, cybercriminals are always innovating and evolving, too. The cyber risks your organization faces are always on the move. A quick look back at how cyber insurance emerged sheds light on how it helps you navigate the ever-changing risks.

Cyber insurance grew out of professional liability insurance, with policies covering errors and omissions that can occur in the course of providing services. In the 1990s, technology evolved and regulations changed around the protection of data, creating a gap in insurance coverage. There was a need for insurance coverage that paid when companies weren't able to fully protect their customers' or employees' data.

Out of this void, the cyber insurance world emerged. It started as a liability (third-party) policy and then eventually extended to cover first-party costs as well. As cyber threats have grown, coverage has continuously evolved to transfer new risks.

Cyber-related coverages labeled "business interruption" or "cyber crime" were born out of necessity and real-life experiences. Actual losses happened, and when the insureds and their brokers looked for coverage on various policies, they couldn't find it.

Insurance providers decided to build such coverages into their policy contracts, pricing the contracts in accordance with the risk transferred. A cyber underwriter evaluates and analyzes the risks involved in covering cyber incidents and then establishes pricing for accepted insurable risks. Your business gets a tailored policy addressing your true exposures.


WARNING

As technology changes so should the tools used to protect your company's assets and assess cyber risk. That's one reason your cyber needs can't be fully met by a standard cyber insurance policy. Traditionally, you go through underwriting and obtain a policy and then you're set for some period of time, perhaps a year. The problem is, well before that policy is up for renewal, threats have changed and your risk exposures have changed with them. The policy ultimately becomes disconnected from the risks that need to be covered, which is a dangerous situation.


TIP

What you need is *continuous risk assessment*. The aim is to always be aware of what the newest developing exposures and risks are and then evaluate whether your cyber coverage needs to be changed. Continuous risk assessment is vital because if you're going to the trouble of insuring your risks, you really want to be certain all risks are covered, including whatever new threats emerge.

Not only do you want to cover your risks, but also you want to actually prevent incidents whenever you can. Continuous risk assessment provides valuable insights for preventing incidents, avoiding losses, or at least reducing them, planning for incident response, and strengthening resiliency.

If you can find out in real time about a new kind of threat and further determine that your organization is exposed, you can evaluate what type of protective measures should be deployed. That discovery opens the door for activities such as preventive security measures, which may include upgrading software to the most recent version (patching) and other risk mitigation activities.

REMEMBER

In the world of cyber insurance, continuous risk assessment takes a lot of specialized expertise and requires thoughtful data science approaches. Cyber insurers apply machine learning to better understand and predict threats, run models, and better understand connections between technology stacks, supply chains, and the rest of your organization's operations.

Cowbell Cyber offers an example of how this can work through continuous risk assessment and continuous underwriting. The company is constantly reviewing the threat landscape, adding new risk signals, pondering new threats, and exploring new industry-unique exposures. Organizations covered by the company's insurance benefit from an evaluation known as *Cowbell Factors* that provide a relative rating of your organization's risk profile compared with a larger risk pool. In simple terms, it estimates whether your organization is more or less secure than industry peers. Some 1,000 data points and risk signals are used to determine Cowbell Factors.

Sources of information include public databases, third-party vendors, dark web intelligence, proprietary external scanners, and repositories of exploits and software vulnerabilities. It's all run through artificial intelligence and machine learning algorithms to quantify and model risks.

On top of that, Cowbell Factors bring in inside-out data when connectors to security vendors and cloud applications are activated. For example, if you authorize your insurer to have direct insight into your Microsoft Office 365 as to whether all users have activated multifactor authentication (MFA), your insurability will be immediately improved and access to specific coverages, limits, and prices will be provided.

The end result is a series of specific Cowbell Factors that are continuously compiled and updated. Areas covered include

- Network security
- Cloud security
- Endpoint security
- Dark intelligence
- Funds transfer
- Cyber extortion
- Compliance
- Supply chain


TIP

Cowbell Cyber also compiles two aggregate factors. One gives a picture of the organization as a whole; the other focuses on its industry. With that kind of information, companies can assess what their greatest risk exposures are and how they compare to industry peers.

Check out `cowbell.insure/for-businesses` for more information.

Dealing with a Cyber Incident

You may wonder what a cyber incident looks like and how your company may respond. That all depends on how well prepared you are. Your cyber insurer will help at every step.

Being prepared to respond

Cowbell Cyber provides its clients with a detailed incident response guide to help prepare and plan in advance what should happen if that dark day arrives. That planning includes establishing an incident response team, determining how systems are monitored and by whom, specifying who decides when a security incident has taken place, and most importantly, who to contact when a potential cyber incident has been discovered.

Involving your cyber insurance provider

You don't have to deal with a cyber incident all by yourself. As soon as a potential cyber event is discovered, keep the following in mind:

- **Don't try to resolve the problem yourself.** Contact your cyber insurance provider as soon as you experience or suspect a cyber incident and prior to engaging in any remediation efforts or contacting third-party vendors.
- **Provide the proper information.** Your insurer collects preliminary information and assesses the need for an incident response team and appoints a breach counsel.
- **Prepare a brief summary of the incident.** This report includes a timeline of events leading to the incident and the discovery of the incident along with the current status of operations or impact.

TIP

Notifying your insurance provider rapidly unleashes a flurry of recovery activities. Your insurer immediately sets up a response team made of cyber experts. This team includes breach counsel, ransom negotiators, and data recovery specialists — all of whom are working to get your organization back to normal operations as quickly as possible.

Your role in the response varies depending on the incident. For example, for a wire fraud event, gather all communications you believe may have led to the event, along with pertinent banking information or transaction confirmations, plus any related contracts.

For an email breach event, you need to create an outline of customer information and data that may have been sent to your email system, stored, or attached. That may include contracts, invoices, and personal information related to employees, partners, or customers.

REMEMBER

If your organization has experienced a ransomware event, consider these specific pointers:

- **Don't engage with the bad actor.** Let experienced ransom negotiators appointed by your insurer handle that.

- **Don't attempt to restore data from backups just yet.** You need experts to ensure the system is safe and secure first; otherwise, your backup could be at risk, too.
- **Collect information to help accelerate recovery.** Create an outline of sensitive data or information that might have been in your system and impacted.
- **Don't leave unchecked blind spots.** Check whether any legacy or specialty equipment or software has been affected.

Getting Started on Coverage


TIP

If you've decided it's time to look into a standalone cyber insurance approach for your organization, how do you proceed? Cowbell Cyber uses the following approach:

1. **Assess your cyber risks.**

   This real-time, automated exercise quantifies your company's security threats, determines their probability, and assesses the severity of your risk exposure. Start optimizing your insurance immediately by addressing identified security weaknesses.

2. **Select coverage.**

   Coverage options are based on your company profile and identified risk exposures. Discuss and confirm limits and types of coverage with your insurance agent based on your risk appetite.

3. **Use the remediation guidance provided.**

   Expert guidance helps improve your insurability and, perhaps even more important, reduces the risk of a devastating attack.

4. **Review your risk profile regularly.**

   Be sure your premiums cover your insurance needs. Accessing real-time risk exposure visibility helps make that happen. Your broker can offer advice, best practices, and risk management resources to keep your business safe. Take advantage of all resources offered.

IN THIS CHAPTER

- Recognizing the target on your back
- Understanding your coverage
- Clarifying whether your claim will be paid
- Avoiding getting a tad too overconfident
- Spotting your cloud vulnerabilities

Chapter 5
Debunking Five Myths about Cyber Insurance

Organizations have been able to obtain some form of cyber coverage since the 1990s, but only recently has cyber insurance emerged as a vital standalone business. The need is finally getting attention because cyber incidents are becoming much more common and the effects more devastating. But it's also likely that, in the past, the need has been underestimated because of certain myths and misunderstandings. This chapter aims to debunk five of the most common myths.

Recognizing Your Vulnerability

Of course, cybercriminals go after the biggest players in healthcare, financial services, or some other lucrative industry. That's where the real spoils are, right?

WARNING

Well, if you think your organization is relatively safe because it's small or medium-sized, think again. You need exceptional cyber protection, too, because companies of all sizes are susceptible to an attack. Your small organization may even be targeted as a means of gaining access to a bigger organization with which you

do business or partner. All it takes is one wrong click in a phishing email or a misconfigured cloud service, and you've got a problem.

Indeed, one study found that a third of all breaches involve small or mid-size enterprises, and breaches at small organizations were up more than 400 percent in 2020. Two out of every five small businesses don't have a cybersecurity defense plan, and one survey found that only 14 percent believe they have an effective defense plan in place. Yet another study found that the chance of any particular small business falling victim to cybercrime is roughly 50-50. The odds really aren't in your favor.

Relying on Data Breach Coverage

You've already got property and casualty insurance, and it may even have a data breach endorsement. So, you're in good shape, right? Wrong.

WARNING

The reason it's called a *data breach endorsement* is because it covers data breaches — and nothing else. What about ransomware? It's probably not covered by a data breach endorsement. Nor fraudulent funds transfers and other kinds of cybercrime. It's like having auto insurance that only kicks in when your car hits a deer but not another vehicle.

Because its focus is narrow, a data breach endorsement isn't likely to keep up with the evolving threat landscape. Ransomware, for example, isn't exactly new, but attacks grew by nearly 500 percent between 2019 and 2020. What will be the up-and-coming kind of attack two or three years from now? Who knows? But your cyber coverage needs to evolve as new threats emerge or existing threats get worse.

Another issue with a typical data breach endorsement is the coverage limit. Some endorsements on a business owner's policy (BOP) may limit data breach coverage to $50,000 or $100,000, which is really just a drop in the bucket when you're tallying up the total costs of a cyber incident.

Getting Claims Paid

You may have heard that it's nearly impossible to get a cyber incident insurance claim paid. That may be true if you're not carrying the right kind of coverage (see the preceding section "Relying on Data Breach Coverage") — you're probably not going to receive reimbursement for a loss that's not covered.

REMEMBER

But that perception isn't true about standalone cyber insurance coverage. What you can expect with a cyber policy is clarity about what's covered. You can expect it to cover — and pay claims for — the kinds of real cyber threats that are out there today. And you can expect clarity on anything that may be excluded.

Again, it's no different from any other insurance situation — you need to be covered for the risks you face, and your insurance isn't going to pay a claim for something that's not covered. Though some organizations with standard business policies have had a hard time getting cyber claims covered, the Insurance Information Institute stated that 97 percent of those with cyber-specific insurance have found that their insurance has adequately covered the costs of cyber incidents.

Overcoming Overconfidence

Speaking of myths, you know the story of Achilles, the greatest of the mythological Greek warriors. His mother dipped him in the river Styx when he was a baby, holding him by his heel. His whole body was said to be invincible except for that vulnerable heel. The arrow that killed him may or may not have hit him in the heel, but the point is, he was overconfident in his protection.

WARNING

The same holds true for a lot of companies that sign up for good cyber insurance coverage. They feel pretty confident that they're in good shape. And when it comes to coverage, that's true — but it doesn't mean they're not vulnerable to a cyberattack.

Obtaining cyber insurance coverage definitely doesn't mean you can let down your cybersecurity guard. You need to maintain all of the solid cybersecurity practices that I outline in Chapter 3, from multifactor authentication (MFA) to employee training to disaster planning to isolated backups.

TIP

As a matter of fact, you may be required to demonstrate that kind of good cyber hygiene to qualify for the best coverage. Coverage or not, you really do want to avoid cyber incidents, and the carrier that covers you wants you to avoid incidents, too. A good insurance provider will even work with you to understand your risks and help mitigate them.

Doing Business in the Cloud

There are a lot of great reasons to move various digital functions to cloud resources. It can be cost-effective and make life a lot simpler for your IT department and other employees. And in fact, quality cloud resources maintain their own security infrastructure, which should help you rest a little easier.

That said, it *doesn't* mean you no longer have to worry about cyber incidents. To begin with, you need to have a full understanding of the protections your cloud resources do and don't provide. And then, you must be certain your cloud services are properly configured.

WARNING

In fact, cybercriminals commonly scan the web looking for safety gaps and misconfigured cloud services. They're always on the lookout for your weaknesses, so you need to be, too.

And of course, you need to maintain frequent backups that are isolated from the internet. If your data and systems reside solely in the cloud and then become compromised, your situation could be dire.

COWBELL® CYBER

Cowbell Cyber will be there for you every step of the way:

ASSESS. INSURE. IMPROVE

- $0 Assess Your Cyber Risks Prior to Purchasing a Policy
- Is Your Business as Secure as Your Peers'?
- Customize Coverage Based on Your Unique Profile
- Benefit from Our Risk Advice Every Day of Your Policy

ABOUT US

Cowbell Cyber delivers standalone cyber insurance policies to small and mid-sized enterprises nationwide. Policyholders gain access to partners and resources that enable a closed-loop approach to risk management: assess, insure, improve.

Learn more at www.cowbell.insure.

Explore the concept of cyber insurance

Cyber insurance can be overwhelming. What are the various coverage options? How do claims work? Do you really need a policy? (Spoiler alert: Every business, no matter its size, should have a standalone cyber insurance policy). This book not only answers common questions but also explains how cybersecurity and insurance work together to protect your business.

Inside...

- Get an introduction to cyber insurance
- Learn about coverage types
- Recognize your industry's exposures
- Understand the role of cybersecurity
- Debunk common insurance myths
- Get prepared to start your application

Steve Kaelble is the author of many books in the *For Dummies* series, and his writing has also been published in magazines, newspapers, and corporate annual reports. When not immersed in the *For Dummies* world or writing articles, he engages in healthcare communications.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-83924-8
Not For Resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.