ACRISURE®

CYBER

Cyber insurance guide

acrisure.com

As we become increasingly reliant on technology, the potential impact of cyber-related incidents continues to grow. Yet the cyber insurance market is relatively new in comparison with other lines of cover.

This straightforward guide explains how cyber risk and insurance has evolved and how a good cyber policy addresses these modern exposures.

Contents

What “cyber” means

“Cyber” is one of the most talked about topics in business, insurance and media but also seems to be one of the most misunderstood. And with good reason – it is an area associated with jargon, buzz words and what feels like a whole lot of complexity.

This is largely down to the fact that the development of cyber insurance has historically focused primarily on third party privacy exposures. At the same time, traditional insurance policies have tried, but rarely succeeded, at addressing cyber risks; this has left clients believing many exposures are covered when they actually aren’t.

So what should we mean when we talk about cyber risk? What do clients need to protect themselves against? The real answer is crime.

Technology has revolutionized the world for businesses and individuals alike and the past twenty years in particular have seen monumental shifts in human behaviour directly linked to technological advancements. From the way we shop to the way we access bank accounts and book vacations, everyday life has changed fundamentally.

Cyberattacks are the modern crime and cyber insurance is the way to protect against them.

How cyber risk has evolved

The technology revolution has irreversibly changed the way that businesses operate: the ability to send electronic mail rather than physical mail; the ability to store information electronically rather than physically; and the ability to move money remotely rather than in person has brought speed and efficiency, allowing businesses to reach levels of productivity that were never before imaginable.

But technology has also fundamentally changed the nature of assets. The shift from the physical (post, paper records and bank cheques) to the digital (email, data and electronic funds) means that some of our most valuable business assets are now accessible by anyone in the world from anywhere in the world.

This fact also changes the nature of the risk of them being lost, stolen or destroyed. And that's what cyber insurance is there to protect against – the loss, theft or destruction of a company's digital assets.

Rise of crime

The internet Crime Complaint Center (IC3) has been recording the complaints of cyber-enabled crimes for several years. Here's a snapshot of incidents that they've seen globally since 2014, which shows not only a steady incline in frequency but a steep rise in severity.

	2014	2015	2016	2017	2018	2019
Financial losses	$800m	$1.1bn	$1.5bn	$14bn	$2.7bn	$3.5bn
Number of complaints	269,422	288,015	298,728	301,850	351,937	467,361

*Figures available from the FBI's IC3 Annual Report. Here's the latest: https://pdf.ic3.gov/2019_IC3Report.pdf

The need for a new type of insurance policy

Cyber insurance is necessary because traditional insurance policies were not designed to handle 21st century threats. Many standard first party insurance policies such as property and traditional crime were designed to deal with threats to a company's physical assets – their buildings, machinery, office equipment and tangible money only.

There has historically been little to no protection offered under these policies for loss of, theft of or damage to data, systems and electronic funds.

However, most businesses these days now have a much greater reliance on their digital assets than they do on their physical ones, which makes a new kind of policy essential.

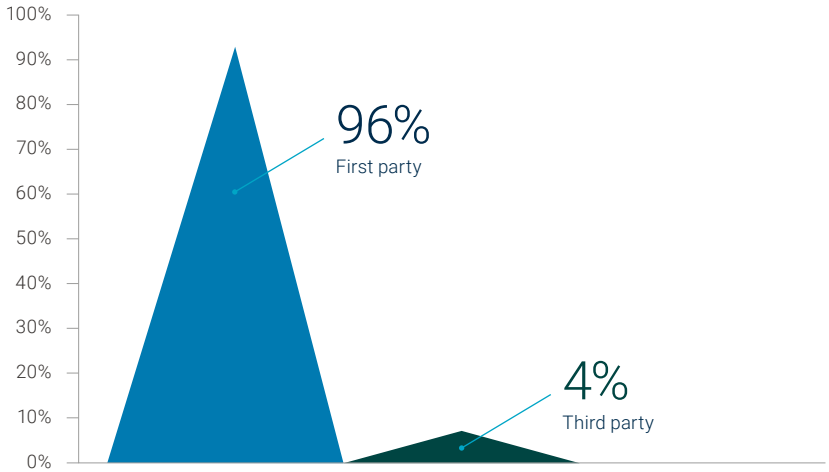
First party risk and the history of cyber "liability"

Cyber insurance for a long time was (and still is) referred to as cyber "liability" which is really a by-product of where it came from. The first cyber insurance products were developed by professional liability underwriters, which naturally meant they were focused on third party exposures, such as passing on a computer virus to a third party and being sued for it.

However, today it's clear that the vast majority of cyber events tend to cause financial loss to the insured themselves as opposed to third parties that they deal with. In fact, cyber claims figures show that less than 5% of cyber claims by volume involve third party legal action.

Given that cyber is predominately a first party exposure, cyber policies are actually much more akin to traditional property and crime policies than they are to liability policies, making cyber "liability" a misnomer.

First party v third party claims



CFC Underwriting cyber claims statistics, 2019

Did you know?

Nearly every business today moves its money around electronically. Cybercriminals have caught on and businesses are now being defrauded out of thousands every day.

Funds transfer fraud is now a leading source of cyber claims. Two easy ways to help protect yourself are by implementing multifactor authentication and following up any transfer requests by phone.

Please see the 'More about cybercrime' section on page 16 to learn more about this growing risk.

Data breach notification

While cyber is predominantly a first party exposure for the majority of businesses, the US has been particularly active historically in its approach to privacy regulation. In 2002, the state of California passed the first data breach notification legislation for organizations that collect personally identifiable information on individuals.

Under this act, if this information is stolen, lost, or accessed by someone without permission then that organization is legally responsible for notifying each individual that their information had been compromised. Sixteen years later, in 2018, South Dakota and Alabama finally became the 49th and 50th states, respectively, to enact data breach notification statutes.

The United States has subsequently become a patchwork of privacy regulation, with the rules around what constitutes a data breach, what is defined as personally identifiable information (PII) and what action must be taken and by when, varying from state to state.

The common theme is that there is typically a significant cost incurred by any organization which suffers a data breach, regardless of the state(s) in which they are operating. Those costs range from legal advice in relation to the breached organization's obligations under the relevant privacy law(s) to the cost of actually carrying out the notification to affected individuals. Additionally, the state Attorney General can usually issue financial penalties to breached organizations and there is also the potential for class actions to be brought by affected individuals.

In addition to data breach notification statutes enacted by individual states, there is also privacy legislation at a federal level that organizations need to be aware of, the best known being the **Health Insurance Portability and Accountability Act (HIPAA)**. Enforced by the Office for Civil Rights (OCR), HIPAA sets out to protect the privacy of health information of US citizens. It contains some of strictest privacy regulation in the country with regards to notification obligations and the OCR has also issued some of the largest ever penalties to healthcare entities, and their associates, who have been found guilty of violating HIPAA rules and regulations.

New breed of privacy regulation

In recent years, the privacy landscape has developed further and the environment in the US has been affected by changes occurring globally. In May 2018, the European Union (EU) introduced its General Data Protection Regulation (GDPR) which aims to give more control to EU citizens in relation to their personal data. In addition to setting out how organizations should respond in the event of a data breach, it also legislates that organizations must clearly disclose to individuals which data they are collecting, why they are collecting it, how long they are retaining it for and if it is being shared with third parties, among a range of other stipulations.

The GDPR also empowers regulators to enforce some of the largest penalties in the history of privacy regulation, the maximum amount being up to €20 million (≈ $22m) or up to 4% of the organization's global revenue, whichever is the largest. Any US organization that collects, stores or transmits data on EU citizens is subject to the GDPR.

The GDPR has provided a new model for privacy regulation around the world and some US states have already responded. The California Consumer Privacy Act (CCPA), adopted in June 2018, has a lot of similarities with GDPR and even goes further by providing California residents with a private right of action in the event that their personal information is subject to a data breach, in addition to a new swathe of potential penalties. New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act was passed into law in July 2019 and also expands the range of obligations that it expects organizations to meet, with penalties to back them up too.

Types of cyber claims

More than 95% of cyber claims are for first party losses only and they fall into three broad categories:

1

Theft of funds

This is straight forward theft of money from a company's bank account. The fact that nearly every business can now move its money around electronically and remotely means that it is much easier to steal. Instead of stealing physical funds, criminals are increasingly stealing electronic funds through social engineering scams. And if a business has somehow been negligent in allowing this to happen, the bank will not reimburse them.

2

Theft of data

Data is valuable, and if something has value, it is worth stealing. Identity theft has reached record levels around the world and in order to commit identity theft, criminals need data. Seemingly innocuous information such as names and addresses stored on a computer network can be worth more money than you think.

3

Damage to digital assets

In order to operate, businesses now have an incredibly high dependency on their systems, and criminals know that. By either damaging or threatening to damage a firm's digital assets, attackers know that they can extort money from their victims who might prefer to pay a ransom rather than see their business grind to a halt. And even after paying up, the victim is often left with systems that are unusable and costly to fix.

In some cases, there may be no financial incentive for the attacker at all. In the same way that criminal damage to property doesn't always have a financial incentive, damage to digital assets doesn't need to either.

Claims for theft of funds are actually very easy and quick to quantify, but for theft of data claims, the financial impact can vary depending on the nature of the data compromised and how much of it was stolen.

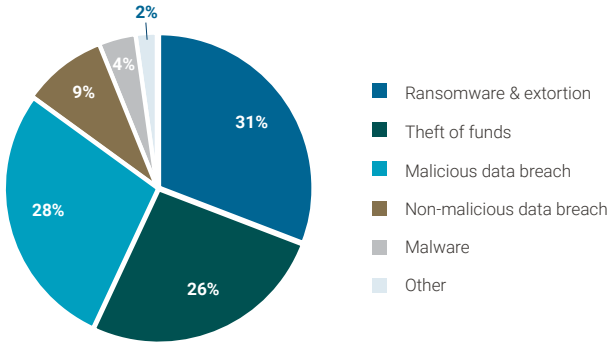
The costliest part of a cyber event is often responding to the incident. For example, if an attack has managed to compromise a company's computer network, then IT specialists are going to be needed to stop the attack, protect against further immediate threats, and work out what has been stolen.

There is then a financial cost associated with limiting reputational damage, notifying clients or customers whose data has been stolen, and offering them identity theft protection solutions if necessary.

Damage to digital assets claims can be easy to determine especially if there is an extortion demand which the victim has paid (the amount of the claim is the cost of the ransom) but more difficult if we're talking about the cost of using IT specialists to rebuild systems or data – which might only be calculated after the work is completed.

The key point underpinning each of these types of claim is that there is a direct financial loss to the victim business which can be transferred with a cyber insurance policy.

Cyber claims notified in 2019



How a cyber policy works

Cyber insurance policies tend to be modular in nature, meaning that they consist of a variety of different coverage areas and, for many, that has led to confusion around what exactly they cover and how they work.

Broadly speaking, most cyber policies can be divided into two areas – first party covers and third party covers.

The first party sections cover the insured's own financial loss arising from a cyber event, which is defined as any actual or suspected unauthorized system access, electronic attack or privacy breach. The third party sections cover the insured for liability actions against them arising out of a cyber event.

Typical "first party" cyber policy covers include:

Incident response

This section of cover will generally pick up all of the costs involved in responding to a cyber incident in real time, including IT security and forensic specialist support, gaining legal advice in relation to breaches of data security, and the cost associated with having to notify any individuals that have had their data stolen. One of the most important aspects of a cyber policy is that it provides access to the right specialists as well as paying for their services.

Cyber extortion

As the name suggests, this section covers costs incurred in responding to fraudsters attempting to extort money out of an insured by either threatening to carry out a cyberattack or by threatening to expose or destroy data after having already compromised the victim's network. Ransomware, where the victim's data is encrypted (converted into an unreadable format) and only made accessible again by the payment of a ransom demand to the attacker, is one of the fastest growing forms of cybercrime.

System damage

This section covers the costs for an insured's data and applications to be repaired and restored in the event that their computer systems are damaged as a result of a cyber event. This is often critical in getting a company back up and running.

System business interruption

This cover aims to reimburse loss of profits and increased costs of working as a result of interruption to a business' operations caused by a cyber event. It works in a very similar way to traditional business interruption insurance except the trigger is a non-physical peril as opposed to a physical one.

While third party liability claims tend to be less common in cyber insurance, it is still important to have cover for them.

Typical third party (liability) cyber policy covers include:

Network security and privacy liability

This covers third party claims arising out of a cyber event, be it transmission of harmful malware to a third party's systems or failing to prevent an individual's data from being breached.

Regulatory fines

If permitted to be included under a policy, this will cover the cost of certain fines and penalties that a regulatory body might enforce on an organization as a result of them having suffered a data breach.

Media liability

This covers any third party claims arising out of defamation or infringement of intellectual property rights. Media cover started out in cyber policies to offer protection in respect of online content only, but as policies have broadened over the years, it's not uncommon for full media cover to be provided.

Make sure your policy is fit and healthy

It is very common for any one claim to trigger multiple sections of cover, so ensure your policy adequately addresses the most critical areas of coverage – namely the first party sections like incident response, cybercrime and system damage and business interruption – and that these are available on an unlimited reinstatement basis. First party losses accounted for a staggering 9% of cyber claims last year*, and the nuances of coverage within these sections can mean the difference between a weak policy that doesn't perform when put to the test, and a fit and healthy policy that can endure multiple blows but stays on its feet.

* CFC Underwriting cyber claims statistics, 2019

More about cybercrime

Most cyberattacks are criminal acts and so technically can be labeled "cybercrime". Within the context of a cyber insurance policy, however, cybercrime usually refers to attacks that involve theft of funds from the victim as opposed to theft of data or other digital assets. Theft of funds generally occurs in one of three ways:

1. **Extortion**
   As mentioned earlier in this guide, the attackers use the threat of a cyberattack or the threat to expose or destroy data that they have already compromised, to extort money out of the victim;

2. **Electronic compromise**
   The attackers manage to hack into the insured's network, gain access to their online accounting or banking platforms and start wiring money out of the victim's account;

3. **Social engineering**
   The attackers imitate a third party (e.g. a vendor or supplier of the victim business) and trick the victim into wiring money to the wrong bank account. The victim believes they are wiring funds to a third party they know but in actual fact it is going to the fraudsters.

While extortion, in the form of ransomware, has been one of the fastest growing forms of cybercrime in recent years, social engineering scams have also increased dramatically. So called "CEO fraud", where fraudsters impersonate the CEO of a company (or other senior executives) and email instructions to staff in the accounts department to transfer funds to criminals' bank accounts, has been incredibly successful and a huge source of claims by businesses.

It is critical to note that not all cyber insurance policies include cover for the above types of loss. Many will include extortion as the bare minimum but no theft of funds from a victim's bank account. Some will extend to cover for theft arising from electronic compromise but not from social engineering. Some will cover all of them. It is also worth noting that some of these covers can be found in a traditional crime policy too but the cover varies widely.

Policies in action: claims examples

Social engineering

A financial controller in a law firm received a call from someone purporting to be from the firm's bank, explaining that some suspicious wire transfers had been flagged on the business account. The caller insisted that, in all likelihood, funds had been stolen and the business was in immediate danger of the remaining funds being drained unless they put a freeze on the account; a password and pin code would be required to do so.

Not wanting to cause any further loss, the financial controller confirmed the pin code and password to the caller, and the caller confirmed that the freeze had been successfully applied and that they would be in contact once the situation was resolved. Upon calling the bank the next day, however, the financial controller was told that the bank had not in fact been in contact and that $118,830 had been wired to three overseas accounts in nine separate transactions, all of which were too late to recall. Because the transactions had seemingly been authorized, no reimbursement was offered by the bank.

Fortunately, the law firm had purchased a cyber insurance policy containing cybercrime cover with social engineering and was able to recover the full amount from insurers less their policy deductible.

Data breach

An online retailer of medical products discovered that its primary website was attacked. Spotting a vulnerability, hackers had inserted malware onto the site and managed to gain access to a database containing the credit card details of over 90,000 customers.

Due to local breach notification laws in place, the retailer had to notify all 90,000 individuals affected by the incident and provide them with identity theft restoration services. This wasn't the end of the incident, however. Immediately after the notification, the business noticed a significant drop-off in sales.

Following an investigation by forensic accountants, it was established that the insured had lost a total of 5,196 orders as a direct result of notification over a 12-month period, resulting in a business interruption loss of $475,646. The cost of this reputational damage came on top of the $230,000 incurred to remove the malware from the business's website, provide legal advice, and carry out the notification process. The entire loss, including the business interruption caused by reputational damage, was covered under the retailer's cyber insurance policy.

Business interruption

A food trucking company suffered a ransomware attack where cybercriminals encrypted all of their data files and requested a ransom of $9,920 in exchange for the decryption key. Like many modern companies, their entire business was run via their systems and hackers had encrypted every single piece of data that they required to run their operations – their routes, logistical information, key contacts, and how much stock they had and needed to order – as well as shutting down their payment card processing capabilities.

Even though business had come to a halt, the CEO refused to give in and pay the demand. Instead, the company immediately set about reconstituting data from a collection of paper records and their employees' knowledge of day-to-day operations, resulting in a large amount of overtime costs right away. What was worse, however, was the loss of business income that resulted from the extended outage of their systems and the consequential impact on operations.

For the month of November, the insured had forecast that they would complete 220,000 sales transactions but, due to the system outage, they were only able to process around 140,000. With an average transaction value of more than $12, that was a loss in revenue of nearly $1 million. After adjustment by their cyber insurance provider, the insured was able to recover nearly all of the financial loss suffered under their policy.

Selling cyber insurance

Objections to a new insurance product that a business has never before invested money in is natural. But it's important to overcome these objections to ensure that clients have relevant cover in place. Here are some of the most common objections we've seen raised and the reason why it's important that they are countered:

Cyberattacks only affect big companies. I'm not a target…

This is wrong. While blockbuster data breaches against household names tend to make the news, attacks against smaller organizations are now so frequent that they are no longer newsworthy. In the most recent Verizon Data Breach Investigations Report, for example, 58% of victims were categorized as small businesses.

We are a "traditional" business that doesn't collect sensitive data so we have no exposure…

Cyber risk is not just about data breaches. Any business that makes wire transfers from a bank account is at risk of funds transfer fraud, and social engineering scams have made victims of businesses ranging from building contractors to beauticians. First party business interruption losses do not require a business to collect sensitive data to be exposed – merely being unable to access their systems puts businesses at risk of financial loss, particularly where technology is increasingly utilized in day-to-day operations.

We already spend money to secure our networks so we don't need cyber insurance…

It's important that businesses are conscious of IT security and take steps to protect themselves from threats, but no one can ever be 100% secure. Cyber threats are rapidly evolving and there are a plethora of ways in which attackers can access networks. Additionally, strong IT security controls don't always protect against events which don't necessarily involve a third party accessing the network such as social engineering attacks or the actions of a rogue employee. Refusing to purchase cyber insurance because you have IT security controls is akin to refusing to buy property insurance because you have physical security controls – the two should not be mutually exclusive.

We use a third party cloud provider to host all of our data and networks so the risk is with them, not us…

Incorrect. If the cloud service provider suffers an attack and goes down, meaning you cannot operate, it is your business that will potentially suffer first party business interruption and the additional costs incurred in attempting to continue trading. It can prove extremely difficult, potentially impossible, to recoup these losses from your IT provider. Additionally, if a breach of data that you are responsible for occurs at a third party provider, it is still you that is responsible and your reputation that will suffer.

Don't the bank have a duty to reimburse theft of funds from my account?...

Not if you were negligent in allowing access to a fraudster and not if you or an employee of yours were duped into wiring the funds themselves. If the bank is not at fault, they will not reimburse.

This guide was produced by cyber insurance specialist, CFC, the insurer behind Acrisure Cyber. All information enclosed is correct as of May 2020.
For more information about CFC, visit www.cfcunderwriting.com or speak to your Acrisure insurance broker.