NordPass®

Reduce Cyber Risk, Stay in Business:

The NordPass Guide to Cyber Insurance

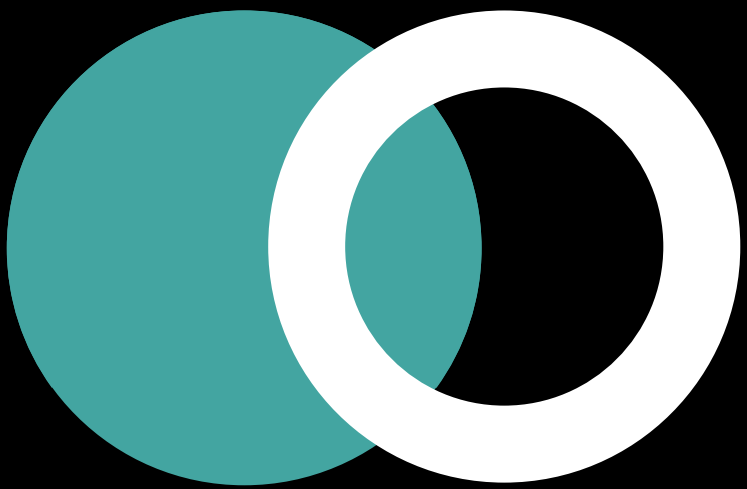


Table of Contents

1. Introduction

1.1 Foreword: why cyber insurance coverage is more important than ever

Like the rest of us, cybercriminals have been quick to adapt to the new normal: cybercrime is on the rise and the threat landscape grows ever more sophisticated by the day.

On one hand, a long line of high-profile data breaches have demonstrated that digital security is not a given even among industry titans. On the other, the booming cybercrime industry is benefitting economies of scale, making smaller and smaller businesses more affordable and attractive targets.

Unfortunately that means that, now more than ever, no one is immune from a potential attack. Which is daunting given that the impact of a single cyber event can be devastating, threatening insolvency.

If businesses are afraid, it's because they're paying attention.

But if fears are increasing awareness of the importance of cybersecurity and protection in a way that motivates action, that is a good thing. And the growing popularity of cyber insurance coverage is proof that that is exactly what is happening.

Jonas Karklys, CEO of NordPass and NordLocker, is a cybersecurity pioneer and co-founder of Nord Security—whose software products protect over 15 million people worldwide. Engaged in web-based projects since the age of 11, Jonas is steadfast in his commitment to help create a radically better internet for everyone.

When he is not driving innovation, you will find Jonas on the racetracks of the most famous European and global motorsport championships.

1.2 | State of the cyber insurance industry

If you have the impression that everyone's talking about cybersecurity insurance lately, you're not wrong.

In recent years, the industry has been growing rapidly. Data suggests that this is only the beginning, with the market size expected to grow by almost 150% by 2026.

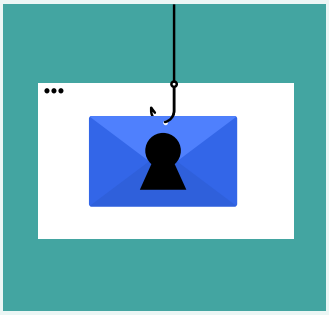
And, if you haven't yet, you're increasingly likely to see cyber insurance pop up as a requirement under contractual obligations.

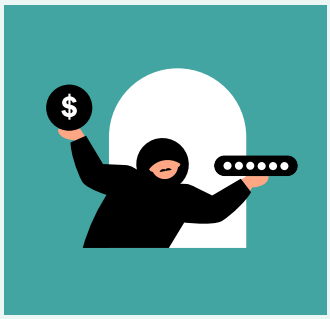
In the current climate, one thing is clear: what was once considered merely nice to have is quickly becoming a necessity. Accordingly, higher costs and stricter qualifications have followed, causing a shift in the burden — from agents and brokers to the prospective insureds — to do the convincing.

> **In 2022, businesses are more vulnerable while the cybercrime industry is strengthening. And on the question of whether cyber events are covered by other forms of insurance, the answer's often a resounding "no."**

Phishing (and smishing) are still going strong:

Social engineering is still the number-one cause of breaches, while **85%**[1] of breaches involve a human element, **36%** of which is phishing, (up from 25% last year)[1].





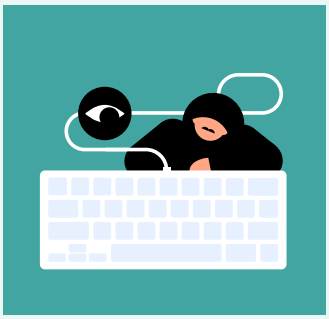
The rise of ransomware.

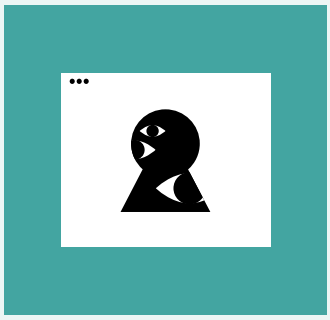
Ransomware attacks are increasing in number, and the ask is increasing too.

- ✓ The average ransom payment increased **82%** YoY between **2020** and **2021**[2].
- ✓ During the same period, the volume of recorded ransomware attacks has more than doubled — and has tripled since **2019**[3].

Increased vulnerability.

- ✓ The rise of work from home means cyber criminals have more chances to infiltrate, through unsecured networks, improper remote desktop protocol, the use of personal devices, and more.
- ✓ **25%** of all professional jobs in North America will be remote by the end of **2022**[4] and most (**56%**)[5] IT leaders believe their employees are using poor cyber hygiene at home.





The end of "silent cyber."

Property and liability insurers have stopped staying mum on whether cyber incidents are covered under their umbrella. In 2022, the answer is "no" more often than not.

[1]Source: Verizon's 2021 Data Breach Investigations Report

[2]Source: Paulo Alto Networks: Unit 42 Ransomware Threat Report, 1H 2021 Update

[3]Source 2022 SonicWall Cyber Threat Report

[4]Source: Ladders

[5]Source: Tessian

1.3 | Introducing our cyber insurance experts

NordPass invited seven cyber insurance industry leaders to participate in a two-part webinar series on cyber insurance:

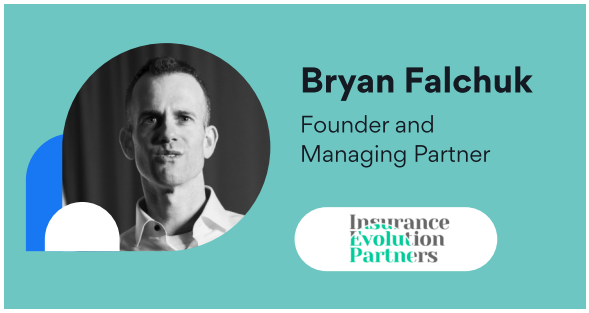
1. Cyber Insurance 101: Everything You Need To Know
2. Is Your Business a Good Candidate for Cyber Insurance?

Together, the seven specialists provided their best advice for businesses considering an investment in cyber insurance and answered attendees' questions. Their insights inspired this whitepaper.

Shiraz Saeed leads the cyber risk product for Arch Insurance Group. He is responsible for the strategic direction for the underwriting, distribution and marketing of the cyber risk products and services offered by Arch.

Alexander Cherry covers general insurance, London markets and life/pensions in the UK and Ireland, with responsibility for tracking key industry trends — including technology disruption, cybersecurity and sustainability.

Andrew Lipton is vice president, head of cyber claims at AmTrust Financial Services. He leads the cyber claim and incident response team and coordinates with the company's agents, brokers, and insureds nationwide to ensure superior cyber claim service.



Bryan Falchuk puts his 20 years of insurance industry experience to work as the founder and managing partner of Insurance Evolution Partners, which advises carriers and their partners on how to navigate an evolving industry facing disruption and change.

Theresa Le is head of claims and risk engineering at Cowbell Cyber and has over 20 years of experience working with insurers. Most recently, she served as vice president, cyber claims expert, at Swiss Re and prior to that, spent over a decade counseling international and domestic cyber insurers on cyber coverage and wording, data breach and crisis management, dispute resolution strategies, and the business impact of privacy and cyber liability.

Patricia L. Harman is the editor in chief of the PropertyCasualty360.com group, which includes Claims Magazine, National Underwriter Property & Casualty Magazine, and the PropertyCasualty360.com website, and chairs the annual America's Claims Executive Leadership Forum (ACE), which focuses on providing claims professionals with cutting-edge education and networking opportunities.

Dan Burke is a recognized industry leader and expert in cyber liability insurance. As national cyber practice leader, he drives the strategy to continue to grow Woodruff Sawyer's cyber business. Under his watch, the cyber practice has been nominated as Cyber Broking Team of the Year by Advisen two years in a row.

2 What is cyber insurance?

The commonsense understanding of cyber insurance is that it protects businesses from the financial fallout of a cyber attack. That's true.

The full scope of cyber insurance coverage is a bit more broad in two respects that will be covered in this section. But first, there are two types of cyber insurance: first party and third party.

> **First-party coverage is like commercial property insurance. It covers a company's own damages from covered cyber losses. Third-party coverage is like general liability insurance. It covers legal expenses that result from a firm being blamed for causing another firm's cyber losses.**
>
> **– Dan Burke**
> Senior Vice President and National Cyber Practice Leader
> Woodruff Sawyer

The second type, third party insurance, is sometimes called cyber liability insurance.

So cyber insurance covers damages following a cyber event that impact your own company and damages to others for which your business is accountable.

2.1 | The most common claim events

Cyber insurance coverage includes damages incurred from a variety of cyber events.

You will notice that in cyber insurance conversations, claim incidents are usually called cyber events, rather than "attacks." That's because not all events involve an attack, a breach, or even a malicious intent involving a bad actor.

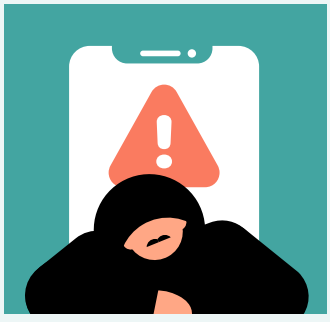
According to Saeed, the "big three" of cyber insurance claims involve:

1. **Ransomware:** the criminal practice of holding a business' digital assets for ransom, usually involving hacking.

2. **Business email compromise:** a subset of phishing, under the "social engineering" umbrella of cybercrime.

3. **Wrongful collection of private information:** an act that violates the law, usually unintentionally, by mistake due to human error or lack of proper security protocols.

And according to Saeed, "that collection and gathering of private information scares me more than losing it," suggesting that internal errors can be just as threatening as malicious attacks on businesses. Saeed added that as laws continue to regulate data collection, proper data hygiene will be paramount to comply with the law.



What about "hacking"?

Hacking involves finding and exploiting weaknesses in networks and systems — a legally and ethically neutral act. When hacking is used to commit cybercrime, it is considered "black hat."

Not all cybercrime involves hacking, and not all hacking is a cybercrime. Ransomware usually involves hacking and is a cybercrime. Social engineering, where information or money is given "voluntarily" under false pretenses, is a cybercrime but does not involve hacking.

2.2 | The scope of cyber insurance protection

Another aspect of cyber insurance coverage is that, unlike other forms of insurance, cyber insurers will work with insureds to mitigate the impact of a cyber event by implementing security measures beforehand and intervening to provide help while the event is happening.

Because insureds and insurers share the common goal of preventing incidents and mitigating the impact of a cyber event when they happen, cyber insurance is also a service.

Lipton illustrated this point by comparing cyber insurance coverage to property insurance, suggesting an analogous situation for a property insurer would be stepping in to help a homeowner protect their property during an active hurricane. Not only that, Le said:

> **We are also as a group collectively trying to anticipate a new type of hurricane so there are hurricanes in cyber that we just don't even know about and it's a partnership with the policyholders to anticipate, to help them mitigate new ... scary hurricanes that, you know, nobody's ever even seen.**
>
> **– Theresa Le**
> Head of Claims and Risk Engineering
> Cowbell Cyber

When asked, the experts agreed that the relationship between insurer and insured is a collaborative one. For this reason, qualifying for cyber insurance can be a complex process, one we'll tackle in more detail in the next section.

2.3 | What's (usually) covered

Per Lipton, "in my view cyber insurance ... covers the risk or it addresses the risk that your business will incur financial expense as a result of a cyber event."

That is indeed a "broad spectrum" of coverage according to Burke, given the variety of possible cyber events and the differing impacts that they may have. Burke adds that the focus is on recovering from a cyber event that happened and less about how that event happened — dispelling a common misconception.

Ransomware case study

> **Why the caveat of what's "usually" covered?**
>
> **Understanding exactly what's covered by your prospective insurance policy is important and depends on your class of business, among other things. When in doubt about cyber coverage, it is important to ask your insurer for details. The following is based on generalities provided by our experts.**

To get a more detailed understanding of what is covered by cyber insurance, let's dive into an all-too-common scenario: What is most likely to be covered by cyber insurance in the event of a ransomware attack?

For this miniature case study, we're borrowing from Lipton's imagination: It's seven o'clock in the morning in the United States. An administrator at a medical office has arrived to turn on the lights and open for the day. Instead of a usual start-up screen, he sees a confusing message stating that all electronic patient files have been encrypted. Not only is access to the files locked, but they're being held for ransom.

The first step for an insured business is to contact their insurer through the agreed-upon channel, like calling a hotline. This conversation will initiate the incidence response process, which is likely to involve:

1. **A scoping call:** the insurer will contact a cybersecurity vendor on the business' behalf to begin investigating the incident to find out what kind of assistance is needed.

2. **Legal compliance assistance:** including legal forensics services and counsel. In this case, this would include HIPAA adherence and reporting the crime to the FBI.

> **If it's a ransomware incident and there's been no exfiltration of the data but you're unable to demonstrate that somehow the patient's files were not accessed ... it's automatically a privacy breach under HIPAA regulations, so certain things need to be done and reported to the Department of Health and Human Services and various local regulatory authorities...**
>
> **– Andrew Lipton**
> Vice President, Head of Cyber Claims
> AmTrust Financial Services

3. **Negotiation and ransom payment:** through an appointed third-party cybersecurity vendor.

4. **Assistance in getting back to business:** including data recovery measures potentially involving either backups or decryption services.

5. **Loss compensation:** for down-time business interruption and any additional (direct) expenses.

6. **Public relations services:** to carry out mandatory communications with affected parties and reputation management.

And, that is a non-exhaustive list. Per Saeed:

> **Most policies addresses all of those things, and one ransom can trigger all these multiple parts. There's upwards of 12 different insuring agreements on a full cyber policy if you buy it from a reputable carrier, so a ransomware can trigger a large portion of them. So there is a tremendous amount of value in terms of also what Andrew [Lipton] said the financial economics of the risk transfer ... versus the potential loss that you might actually suffer if you were to be down for seven to ten business days from a ransomware event.**
>
> **– Shiraz Saeed**
> Vice President, Cyber Risk Product Leader
> Arch Insurance Group

Le describes the process as having “two parallel tracks that go on at the same time” which are, essentially, managing the event and getting the insured back in business as soon as possible.

What is data exfiltration?

Data exfiltration is a type of data theft that involves copying or exporting data without authorization — putting often sensitive information in the hands of opportunistic criminals. This activity on its own can be difficult to detect.

2.4 What's not covered

The holistic nature of cyber coverage means that most costs that can be directly attributed to the cyber event are covered by insurance, as you have seen above.

However, a single event can have ripple effects that can have costly outcomes. While coverage varies by insurer and agreement, a few items are generally outside of the scope of cyber insurance coverage, such as:

- a drop in future profits or an overall decreased business value.
- long-term reputational damage — and the costs associated with repairing it.
- security upgrades required to prevent similar attacks occuring in the future.

In some cases, acts that are considered under the umbrella of state-sponsored crime or as acts of cyberwarfare and (technically) non-digital social-engineering attacks may also be exempt from coverage.

2.5 | Cyber insurance myth-busting and FAQ

Though cyber insurance is becoming increasingly popular, it's not immune to misinformation. On the topic of common questions and cyber insurance myths, here is what the experts had to say.

1. Having encrypted backups banishes the need for cyber insurance

What's true of encrypted backups is they can help mitigate the damage of ransomware attacks — with a caveat:

> **I have experienced situations with insurance where encrypted backups did prevent a significant amount of damage and prevented even having to engage the attacker in the first place but only in situations where there's been no exfiltration of data. Actively managed encrypted backups that are segmented from the network is a phenomenal tool...**
>
> **– Andrew Lipton**
> Vice President, Head of Cyber Claims
> AmTrust Financial Services

Burke agrees that encrypted, segmented, actively managed backups are an essential tool for mitigating the risk of cyber attacks. But that doesn't mean they disqualify the need for cyber insurance coverage, which goes far beyond ransom payments.

2. I might already be covered for cyber events under general or property liability insurance

According to our experts, cyber coverage under general liability insurance is ancient history:

> **Back in 2017 the insurance community decided we are no longer going to tolerate silent cyber risk. We are going to be very explicit about [whether] cyber attacks [are] covered under this specific policy. So general liability policies now have an exclusion for cyber.**
>
> **– Dan Burke**
> Senior Vice President and National Cyber Practice Leader
> Woodruff Sawyer

3. Cyber insurance isn't worth the expense

This logic tracks if you don't expect to experience a cyber attack or liability event, but recent stats suggest that's wishful thinking. Assuming an event is at least possible, if not likely, cyber insurance might be the difference between staying in business or not.

In the event of an attack, it is highly unlikely that even substantial savings will save you from the multi-pronged impact. This is especially true as costs of events and attacks are on the rise.

4. My business has already suffered an incident or an attack, so it won't qualify for cyber insurance

Actually, a number of the insurance professionals asked agreed that having suffered a cyber event in the past might be an asset to your insurability:

> **The struggle has been to convince business owners that the risk is real, so the advantage of having an insured that comes up for renewal is that ... you don't have to convince them that it's real, they've experienced it. They know it's real.**
>
> **– Andrew Lipton**
> Vice President, Head of Cyber Claims
> AmTrust Financial Services

So understanding the possibility and gravity of a cyber event can be advantageous from an insurer's perspective.

> **Deciding whether or not it is a good risk really depends on having a conversation with the prospective applicant policyholder. If it's a renewal about exactly what happened and lessons learned...**
>
> **– Shiraz Saeed**
> Vice President, Cyber Risk Product Leader
> Arch Insurance Group

Le agrees. What's key is that the specific vulnerabilities that were exploited during the incident are addressed and repaired accordingly.

5. It’s too late to enter the cyber insurance market

Burke advises prospective insureds not to be discouraged by the ever stricter requirements brought on by the increase in demand. On how to find the right provider, he says:

> **That's the job of your insurance broker, to sort of help you through that process... I think currently in the insurance market there's probably 40 or 50 insurance carriers that are offering some form of cyber insurance — it only takes one really.**
>
> **– Dan Burke**
> Senior Vice President and National Cyber Practice Leader
> Woodruff Sawyer

Of course, it isn’t (only) a numbers game. Businesses can reduce their own risk and increase their insurability in plenty of ways, that topic is covered in part three.

6. Cyber insurance is for companies with poor digital hygiene

Quite the contrary. As cyber insurance is being considered more of a necessity for businesses of all sizes and industries, proper cyber hygiene is becoming the bare minimum to qualify.

So, good cyber hygiene and cyber insurance coverage go hand-in-hand, and each works best with the other. After all:

> **We've seen very good cybersecurity protocols in place ... there's no ironclad system so we acknowledge that things can still happen even if you have everything you needed, that we've recommended and there's always a human error potential element too.**
>
> **– Theresa Le**
> Head of Claims and Risk Engineering
> Cowbell Cyber

7. Cyber insurance coverage might put a target on my business' back

If cyber criminals learn that businesses have coverage, might they be more motivated to launch an attack, knowing a payment is assured? According to Falchuk, while that fear is understandable, it's simply not true. Because, for one, cyber criminals have no real way of knowing whether or not businesses have coverage. Unless, of course, they've already engaged in hacking:

> **There really is no basis for that in cyber ... there's no national registry of ... cyber insured entities ... If you have your cyber policy sitting in your server which gets hacked, well then they would see that you had it, but remember they had to hack you to see that, so you were already a target — they already came in whether you had coverage or not.**
>
> **– Bryan Falchuk**
> Founder and Managing Partner
> Insurance Evolution Partners

Lipton confirms that, in his experience, coverage has never encouraged an attack:

> **I don't know that in any instance where an attack has happened you can say that the attack was caused by the fact that the attackers knew insurance existed ... There's never been a cyber event I've been involved with on the carrier side or when I was an outside counsel before where the basis of the attack was the attacker's discovery that insurance existed.**
>
> **– Andrew Lipton**
> Vice President, Head of Cyber Claims
> AmTrust Financial Services

8. Because hackers are after a “big prize,” my small business is probably safe from a cyber attack

To be fair, this idea may have been true in the past. But, now? Not so much.

> **Up to a few years ago it tended to be viewed as the sort of thing that only happened to large companies and parts of that is just the economics of it ... hackers need a big prize to invest the money to actually set up the hack but now ... it's just become so cheap that they can basically go after anybody with a tailor-made ransom.**
>
> **– Alexander Cherry**
> UK Insurance Research Lead
> Accenture

Cherry goes on to explain that, from data breaches to double extortion, the cybercrime industry has innovated in recent years — making even small scale attacks profitable and unsuspecting small businesses a target.

3 How can businesses qualify for cyber insurance?

Because cyber insurance involves the transfer of risk, determining whether your business is a good candidate requires measuring and understanding that risk level.

Usually, that process involves some combination of risk scanning accompanied by a questionnaire. While there are generalities, the process is far from “one size fits all.” Different classes and sizes of business will be subject to different questions and measures.

What is risk scanning?

Risk scanning in this context refers to a process initiated by an insurance provider to assess the prospective client’s cyber risk and vulnerabilities This may be carried out by the insurer or a hired third party.

According to Le, insurers make decisions like these on an (almost) “policyholder by policyholder” basis, and notes that industry benchmarking is a factor. Saeed agrees that business size and class impacts the process, stating that:

> **You could get upwards of 125-plus unique questions being asked, depending on the size of your organization and the type of business that you’re doing.**
>
> **– Shiraz Saeed**
> Vice President, Cyber Risk Product Leader
> Arch Insurance Group

On what those one hundred plus questions will entail, Saeed provides a preview:

> **Do [you] have access management tools? ... Do you have a password management program or a service provider that helps you with that, that helps you implement multifactor authentication?**
>
> **– Shiraz Saeed**
> Vice President, Cyber Risk Product Leader
> Arch Insurance Group

In the evaluation of risk level, both conversations achieved a consensus: cyber hygiene factors strongly.

3.1 | The anatomy of risk

1. Risk

The following logical formula is sometimes used to “calculate” risk level and can be useful here:

> **Risk = (Cyber threats x Vulnerabilities) x Impact**

Risk is a summary of the danger level of suffering a negative consequence from a cyber threat, measured by the likelihood of an event and the impact that this event will have on your business.

Cyber threats including cybercrime — like phishing attempts and ransomware attacks — are calibrated by vulnerabilities: these are the open doors that could let threats in. Together, threat potential and exploitable vulnerabilities make up the likelihood of an event.

And this likelihood is calibrated by the impact that this will have on your business.

High likelihood and high impact is a high-risk scenario. Here’s what that looks like in practice

> **(Art thievery is at an all-time high x your art gallery is unguarded) x it contains the most precious artworks in the world**

Reducing either likelihood or impact significantly reduces the risk level.

Reducing the threat level means reducing the likelihood that art will be stolen by addressing the threat directly. Perhaps your art gallery is located in a community of artists where thievery is very uncommon. While your gallery remains unguarded, and the impact of a stolen painting is still great, it is less risky because it’s overall less likely to happen.

Reducing the vulnerability accepts that the high threat level and impact are immovable but addresses vulnerabilities directly — ones that might let threat actors inside. In this case, that means locking the doors, hiring security guards, and implementing an alarm system.

Reducing the impact alone while threat and vulnerability remain high would have to mean swapping out the works of art for children's drawings. While they may be precious in our hearts, the impact of those works being stolen amounts only to disappointment — instead of millions of dollars in losses.

Intuitively, businesses make these kinds of risk calculations all the time, if not in these explicit terms. Qualifying for cyber insurance is no different.

Saeed describes risk assessment more succinctly: "the major driving factor is the likelihood of an event happening and the severity of the downstream impact of that."

2. Cyber threats

Le describes cyber risk as "developing and dynamic" and warns that "tomorrow a new vulnerability might come up or a new threat actor and just blow everything up." That's why a list of cyber threats will never be an exhaustive one.

On the growth and evolution of cybercrime, Falchuk provides a helpful reminder that so-called cyber gangs are full-on enterprises in their own right:

> **The hackers and all the things we're talking about are absolutely being driven by the same sort of business innovations, tools, and business evolution that we're trying to use on the carrier side and the broker side.**
>
> **– Bryan Falchuk**
> Founder and Managing Partner
> Insurance Evolution Partners

Falchuk lists ransomware as a service (RaaS) as one such example of the ways criminals are taking advantage of "the democratization of data and ... tools."

However, while the list of crimes is long, it can be helpful to view them through the lens of the most common and often overlapping techniques that are used to carry them out. Most cybercrimes involve a combination of black hat hacking, malware, and social engineering.

Black hat hacking is when hacking techniques are used to commit cybercrimes. A reminder that hacking is a practice that involves finding and exploiting vulnerabilities. In such general terms, malware and social engineering might also be considered “hacking” in that they exploit vulnerabilities in code and human judgment, respectively.

In the context of cybercrime impacting businesses, black hat hacking usually involves unlawful access to private networks or software to steal data. One example is credential stuffing: the act of using leaked or stolen passwords to access other accounts. This technique relies on poor password hygiene.

Malware is the short form of malicious software. By definition, it is software designed to commit unlawful or at least outcomes unwanted by the recipient. For malware to infiltrate systems or software, it is usually used in combination with social engineering or hacking. A DDoS attack might involve all three.

Social engineering can be used either as a conduit or as a direct channel for cybercrime and involves using lies and manipulation to convince your team members to give away valuable information, access, or money.

The most common cybercrime involving social engineering is phishing.

Are all threats cybercrimes?

As noted elsewhere, internal "threats," such as errors or (unintentionally) illegal activities can be just as dangerous to your business. But because these vary significantly depending on your class of business, industry, and country, this section focuses on (external) cybercrime threats only.

3. Vulnerability

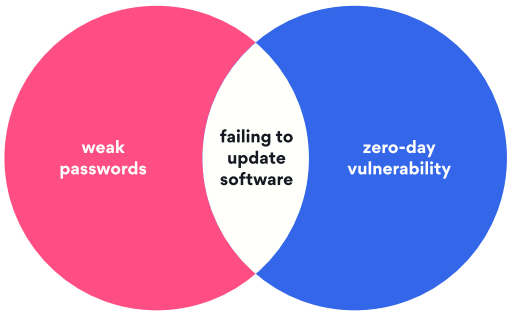
Vulnerabilities are just as dynamic as the crimes that threaten to exploit them.

For the sake of simplicity, here are two primary categories to consider: human vulnerabilities and technical vulnerabilities.

Human vulnerabilities

Vulnerable behavior and protocols:

- ✓ poor data management
- ✓ improper incident recovery measures
- ✓ unsafe browsing
- ✓ downloading malicious files



Technical vulnerabilities

Vulnerable systems:

- ✓ cloud vulnerabilities
- ✓ network vulnerabilities
- ✓ IoT vulnerability
- ✓ endpoint vulnerabilities
- ✓ injection vulnerabilities

Technical vulnerabilities do not require human intervention — they are simply highly hackable. A zero-day vulnerability, for example, is a flaw or vulnerability that has been identified by a hacker but is not known to the developer. The developer, then, has "zero time" to patch it before it can be exploited.

In the event that the developer found the flaw first, they would then release an update to patch it. But if due to either lack of protocols or education, this update isn't implemented by a member of your team, that would mean a human vulnerability creates a technical one: an unfortunately common combination.

A “pure” human vulnerability would be the use of weak and repeated passwords, for lack of proper protocols or software, and is one of the biggest entry points for attack.

Ultimately, the good and bad news is that most vulnerabilities have some degree of human involvement, suggesting that managing the “human factor” vulnerability is the “lowest hanging fruit” per Lipton.

Importantly, all vulnerabilities tend to scale to company size, depending on the number of team members, devices, and systems. And like impact, they will vary significantly depending on industry.

4. Impact

The impact of a cyber attack amounts to the legal and financial damage that a business will suffer as a result of the event.

Since most cybercrimes involve unlawful access to data, the impact is likely to depend on the “value” or nature of the data.

For example, direct-to-consumer businesses handling personal information will belong to a high-impact category. The legal and financial consequences will be substantial and will trigger a more robust response, as demonstrated in the mini-case study of a medical office.

On the other hand, B2B companies with no personal data storage are slightly lower risk because though they may have the same likelihood of an attack, the impact will not be as severe.

For that reason, the class of business is generally the greatest determinator of the severity of impact of a cyber event such as a data breach.

3.2 | Reducing risk and increasing insurability

You might have noticed there is much that businesses cannot control about their risk profile. Threat level is high and only likely to increase, while impact is largely dependent on the class of business and the "value" of your stored data.

Vulnerabilities, however, can be tempered — with excellent cyber hygiene, using a combination of proper protocols, and software.

After all, implementing strict protocols without empowering your team with software to support them is "a bit like telling people who made a spelling mistake not to make that mistake again ... They didn't mean to make the typo, you can't just say 'Hey don't do that' or 'Pay attention next time', so we need to bolster with tools to help with that," according to Falchuk.

This issue is especially relevant for password protocol, since our research suggests it is simply not possible to remember the variety and complexity of passwords that would count as secure.

By implementing the following measures, businesses will be closing the door to virtually all vulnerabilities that are within their control. And that alone will go a long way to reducing overall risk, thereby increasing insurability.

Cybersecurity Checklist

Determine your vulnerabilities

Consider networks, systems, and access. Use this information to develop a cybersecurity strategy, including protocols.

Train your team in cybersecurity

Reduce vulnerable behavior and human error as much as possible.

Secure access

A "human" problem with a software solution. Use a **password manager** to eliminate weak passwords, control access, and to implement multifactor authentication.

Keep software up to date

And make it automatic. Keeping software up to date should be a part of protocol and training but is such a common vulnerability that it's worth mentioning on its own.

Secure your network

Avoid network interception by encrypting your connection and data in transit by deploying a **virtual private network** (VPN).

Secure your database

Build a strong and secure defense against leaks and malware with a separate, secure, encrypted, and backed-up **cloud database**.

Use antivirus software

Be sure to enable default antivirus and antimalware tools that might already exist with your operating systems on all workstations, desktops, and laptops. Consider investing in an additional third-party antivirus software for more robust security controls.

Closing the loop on dangerous vulnerabilities is akin to having security guards at your gallery — simply a must. And a reminder that training and protocols need to be updated and followed up regularly. According to Harman, training, among other cybersecurity measures, is never "one-and-done."

Who are you going to call?

If you need help securing these services, Saeed has a recommendation: "If you're lacking password management, multifactor authentication, or in general, identity access management tools and we require that as one of the requirements, well what do [you] do, who should [you] call? Well you can call NordPass...

4 Conclusion:
insurability, cybersecurity, and acceptable risk

The threat from cybercrime is increasing at a time when some businesses are more vulnerable than ever.

For that reason, both the requirements and cost of cyber insurance are on the rise. But it's not too late to significantly reduce your risk and increase your eligibility.

Closing the loop on known vulnerabilities with excellent cyber hygiene is the first step in transforming your business from a juicy target to near impenetrable.

Next, know that even with best practices, the remaining risk level may still be significant. Consider transferring your remaining risk with a cyber insurance policy.

Finally, with the combination of the right cybersecurity protocols, software, and a robust policy, you can all but eliminate the chance of suffering a single cyber event that could drive you out of business, achieving acceptable risk.

Contact us

Ieva Labutytė, NordPass:
ieva.labutyte@nordsecbusiness.com
+370 674 75363

Simas Žvirblis, NordPass:
simas.zvirblis@nordsecbusiness.com
+370 681 27735