Entech's 2024 Guide to Cyber Crime Risk Management

Steps to Take to Protect Your Business, Including Purchasing Cyber Insurance

Table of Contents

Our Entech experts teamed up with cyber insurance expert Alexandra Bretschneider to provide insights for this guide on cyber crime risk management. Alexandra is Vice President and Cyber Practice Leader at Johnson Kendall & Johnson, a privately owned independent insurance brokerage firm with 65 years of experience managing risk. The company recently won the 2023 Cyber Retail Broker of the Year at the Cyber Risk Awards.

Cyber Crime 101:
Security Posture Positioning in 2024

Cyber crime is a strong growth business globally, costing companies billions every year.

Our priority at Entech is to use technology to help with your secure-ability, accessibility and recoverability. We help our partners understand the risk they are confronted with, and provide them with options on how to best respond to that risk.

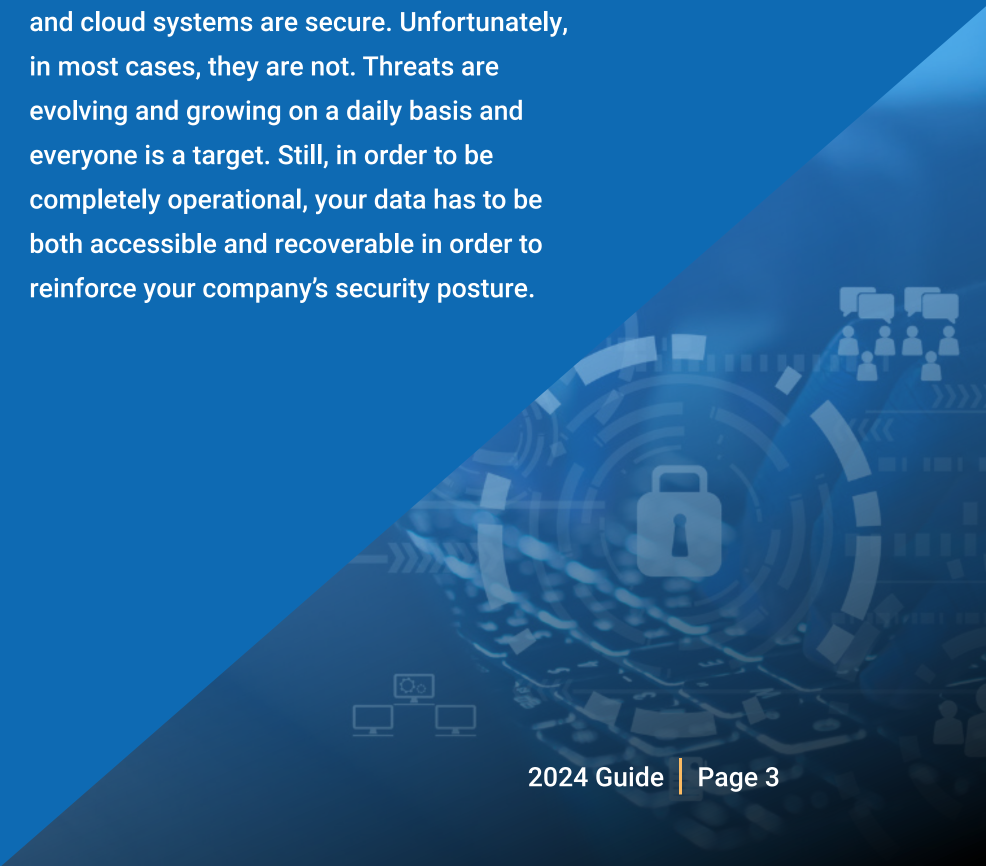
When it comes to risk, of any kind, be it personal or professional, there are only four choices.

We can:

- **Avoid it.**
- **Reduce/mitigate it.**
- **Transfer it.**
- **Accept it.**

The one thing we can't do is ignore it.

Most people hope and assume their network and cloud systems are secure. Unfortunately, in most cases, they are not. Threats are evolving and growing on a daily basis and everyone is a target. Still, in order to be completely operational, your data has to be both accessible and recoverable in order to reinforce your company's security posture.



This guide is designed to provide critical information on mitigating your risks. The more you know about cybersecurity and cyber crime risk management, the easier it will be for you to make sound decisions about your organization’s cybersecurity practices.

We’ll start with the basics of what qualifies as a cyber incident.

Incidents include:

- Ransomware.
- Theft of money.
- Phishing attack.
- Data breach.
- Denial of service attack (DoSA), which uses a vast array of compromised computers to bombard your website and overwhelm the servers with traffic.
- Lost or stolen device or files.
- Disclosure of private information.
- Hacking.
- Malware.
- Vendor error or negligence.
- Physical security breach.
- The unknown (new attack vectors).

Let's take a closer look at three of the most common incidents of cyber crime.

01 CyberData Breaches

The result of a breach is stolen data. The criminals will commandeer data and try to leverage it in return for money.

02 Social Engineering (aka Phishing)

With these types of incidents, criminals tap into personal information or rely on basic human behaviors to fool victims into sending the criminals money or valuable information. They may use fake invoices or email requests for your confidential information. Social engineering is the most common type of cyber crime, according to the FBI's Internet Crime Complaint Center.

03 Ransomware

Ransomware incidents result in stolen or encrypted data, that becomes inaccessible for the owner.
In the past, these attacks may have been carried out by rogue attackers. Today, these cybercriminals run sophisticated operations, complete with help desks, where victims wait in a queue to negotiate the release of their information. Typically, the helpdesk sets up the rules of engagement. For example, the helpdesk may make their demands, but reduce that price by 15 percent if the victim agrees to pay immediately.
Ransomware is particularly insidious because cyber criminals do not care about your data, but you do.
That's why everyone with data is a target.

By the Numbers

Tracking cyber crime statistics reveals important trends that should be on every organization leader's radar. Here, we look back on notable developments over the past several years.

in 2020

- The average extortion demand skyrockets from a few thousand dollars per incident to more than $100,000.
- The frequency of attacks increases exponentially.
- The number of "zero-day" exploits increases. (These incidents exploit software gaps or flaws to attack systems. They are called zero-day because developers have no time to fix them before they are exploited. Zero-day exploits can result in data loss, identity theft or malware infections. They are frequently discovered by hackers/programmers, then sold to the highest bidder on the dark web.)
- Ransomware is deployed across the manufacturing sector within the U.S., impacting supply chain for raw materials.

in 2021

- The average extortion demand continues to rise. By Q2 the average demand is more than $570,000.
- Businesses are attacked by ransomware every 11 seconds.
- Cybercriminals start to employ multiple layers of extortion, targeting employees, clients and vendors.
- Ransomware gangs know their victims would rather hide a ransomware attack than make it public, for fear the news can damage their reputation, stock price or both. The Egregor ransomware takes a novel approach, using all available printers in a company to issue the ransom note. This is now known as "print bombing."
- Federal and regulatory responses call for action nationally and internationally.

in 2022 *

- Phishing attacks increased by 48% in the first half of the year.
- 40% of cyber threats are now occurring directly through the manufacturing supply chain.
- The internet of things (IoT) continues to grow as a target for cybercriminals.
- Because larger corporations have more advanced security protocols, cybercriminals begin to target almost exclusively small to medium-sized enterprises (SMEs), because they often lack sound security protocols.
- 98% of cyber insurance claims impact SMEs.
- Average downtime of a ransomware event can stretch from one to five days, with full recovery stretching to weeks or months.
- The increase in financial pain and severity from ransomware attacks worsens.
- Increased regulatory response requires public companies to alert law enforcement to an attack within 72 hours.

* 2023 data is yet to be published

Typical Targets

While ransomware is widespread, we know that some industries are more heavily targeted. The following lists those industries in order of most targeted to least targeted:

1) **Manufacturing**
2) **Healthcare**
3) **Professional services (courts, attorneys, engineers, architects, etc.)**
4) Technology/telecom/hardware
5) Financial services
6) Education
7) Government/public sector
8) Retail/restaurant
9) Construction
10) Energy

How do cybercriminals get into the networks for these organizations? There are a variety of access methods. This list lays out the access approach by most common to least common:

1) **Phishing**
2) **Zero-day exploits**
3) **Remote desktop protocol**
4) Valid accounts
5) SQL infection
6) Social engineering
7) Card skimmers
8) Hardware additions
9) Construction
10) Misconfiguration

A Special Note About Phishing

Because it is so common, phishing should be brought to the awareness of every employee within an organization, from top to bottom. Security awareness training can be very effective and is critical, especially as phishing attempts and social engineering become more and more sophisticated, in part due to the use of AI to generate email content.

Insurance Coalition Reporting

Insurers are obviously tracking the trends in claims resulting from cyber crime.

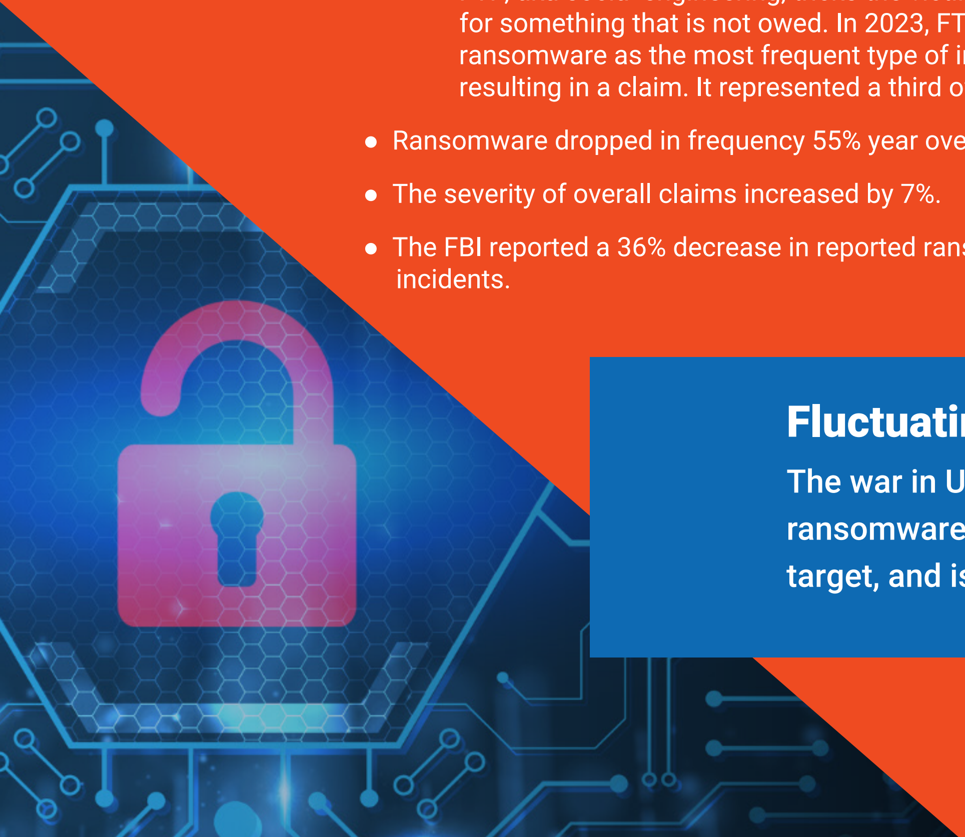
In 2023, the Insurance Coalition reported:

- A 22% decrease in frequency of claims year over year.
- Increased claims resulting from funds transfer fraud (FTF).

  FTF, aka social engineering, tricks the victim into paying for something that is not owed. In 2023, FTF overtook ransomware as the most frequent type of incident resulting in a claim. It represented a third of all claims.
- Ransomware dropped in frequency 55% year over year.
- The severity of overall claims increased by 7%.
- The FBI reported a 36% decrease in reported ransomware incidents.

Based on their data at the time, the insurance coalition in 2023 predicted:

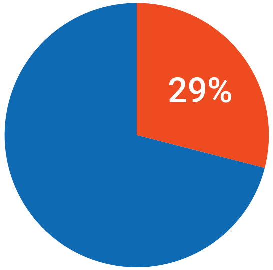
- The return of ransomware.
- FTF would remain an easy, frequent, cyber crime.
- Phishing attacks would become more personalized and persuasive, thanks to generative AI.
- Cybercriminals would specialize to target the most lucrative targets.
- Cyber insurers would play an important role in national and regulatory cybersecurity efforts.



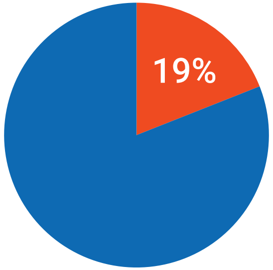
Fluctuating Ransomware Attacks

The war in Ukraine may play a role in the decrease of reported ransomware incidents. Frequency of these attacks is a moving target, and is expected to increase.

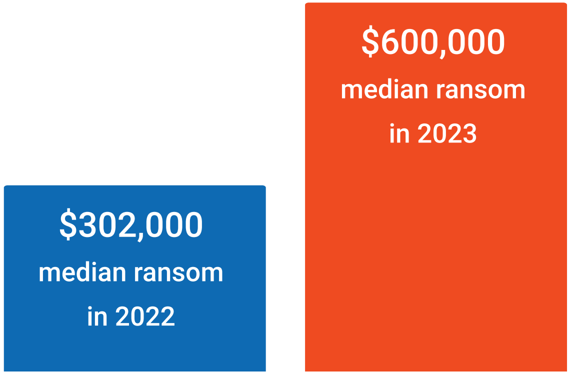
Ransom Demands and Payments



in the first half of 2022,
29% of companies that were
victims of ransomware
paid the ransom



in the first half of 2023,
only 19% of corporate victims
of ransomware
paid the ransom



How do targeted organizations deal with ransomware attacks?

The response appears to be shifting, as is the amount of ransom requested. According to the Arete 2023 Crimeware Report, in the first half of 2022, 29% of companies that were victims of ransomware paid the ransom. In the first half of 2023, only 19% of corporate victims of ransomware paid the ransom.

The median ransom demand rose from $302,000 in 2022 to $600,000 in 2023. The decrease in ransom payments stems from a variety of reasons, including companies having better backups of their information, and improved defenses of their networks that did not allow full access to their data.

Unfortunately, extortion tactics are getting more inventive and aggressive, changing the angles of attack. In some instances, cybercriminals will access a victimized company's cyber insurance policies and use the policy information to convince the company to pay. Likewise, if a company claims it does not have the money to pay the ransom, cybercriminals will extract profit and loss data from the company's files to prove there are enough funds to cover the ransom request.

Further, in the early days of ransomware, cybercriminals would just encrypt data on the company's own servers. Now they often exfiltrate the data to sell if the victim won't agree to pay the ransom.

Cyber Risk Management

Every organization is confronted with risk.

The way forward is to know how to best respond to that risk.

Avoiding or ignoring the risk is simply not a viable option in today's business climate. **Reducing, mitigating** or **transferring risk** are the approaches we typically recommend to our partners.

Consider this approach: Your organization can transfer risk to Entech as well as to a cyber insurance provider. By tapping into Entech's risk management services, you can reduce risk and also reduce insurance rates because the insurance company's risk is decreased.

Weighing Risks

In terms of damages, **not all cyber threats are created equal**. For example, a manufacturer may not be greatly impacted if a cybercriminal steals their data. But, if an attack stops the manufacturing operations, it directly impacts their bottom line.

Damage can also ripple out from the direct victim. Depending on the industry, this can mean more (or less) cyber risk on first-party damages versus third-party damages. For example, if a healthcare organization suffers an incident that affects their customers, then they have a duty to inform those third parties and cover legal costs they may incur.

Compliance and regulatory issues also come into play when assessing risk. There is **no federal law on privacy**. However, there are 50 states with a patchwork of privacy laws and requirements, plus, overarching laws for HIPAA, CMMC, FINRA and other organizations. Wherever your third party is located is where the applicable laws apply. European laws, such as GDPR, also cover compliance and must be considered.

Reporting requirements are the federal government's attempt to gather intel data on what is happening to businesses large and small. So that eventually, they can pass federal laws to address cyber crime.

Once there is a cyber incident or a breach, then a company must abide by the laws. The clock is ticking as soon as an intrusion is detected. As mentioned earlier, if a public company is a victim of a breach, it must notify law enforcement within **72 hours** of determining that there has been an infiltration.

Reputational damage is another variable. As an organization hit by cyber crime, when do you start to lose customers? When are you unable to deliver goods and services?

These questions all underline the importance of having expert guidance in terms of compliance. Transferring risk to these experts can put your organization in a better position when qualifying for cyber insurance coverage, as well.

Becoming Cyber Resilient

Cybersecurity is a misnomer. No security company can guarantee complete 100 percent security in all scenarios. Cyber risk management comes down to:

SECURITY AND PRIVACY. COST. CONVENIENCE.

+

PEOPLE. PROCESS. TECHNOLOGY.

+

CYBER INSURANCE.

The goal is to reach a state of cyber resilience, in which your organization can properly identify, respond and recover from a cyber incident. Be cognizant of the "reasonableness standard." Because cyber crime is evolving rapidly, businesses today must often operate in uncharted waters. The reasonableness standard is based on the question, **"What would I reasonably expect of a similar company?"**

Ransom Demands and Payments

Now that you have a clearer picture of the cyber crime landscape, let's turn our attention to cyber insurance. No doubt you're aware that having cyber insurance is no longer optional: Your vendors may require it. Your industry regulations may require it. Carrying cyber insurance is just a given if you're doing business in 2024.

So how does cyber insurance actually cover your business? Once an intrusion has been detected, insurance policies call for specific steps to be taken by a team of insurance brokers and other officials.

After the detection of an intrusion, the insurance broker will:

- Arrange for additional resources, including legal and forensics. (Insurance carriers typically have established forensic firms on call for this specific reason.)
- Approve and manage costs.
- Prepare notifications and credit monitoring services, if needed.
- Determine coverage.

The legal team will:

- Arrange for a breach coach.
- Establish privilege.
- Represent legal and compliance obligations.
- Declare if a breach actually occurred.
- Manage communications, including engaging professional public relations resources.

Forensic experts will:

- Determine the cause and scope of the incident.
- Provide reporting and evidence to legal.
- Advise IT on securing the environment and restoration.

When alerted, the FBI may:

- Assist in conducting a criminal investigation.
- Collect incident artifacts, which might include system images and malware samples.
- Determine they will not participate.

Cyber Insurance Details

Cyber insurance is designed to cover the costs of a cyber incident. This covers both services and financial risk transfer.

In terms of incident response, cyber insurers will help determine what happened, how to repair the damage, how to reduce downtime and how to meet privacy and regulatory requirements.

Insurance coverage typically includes IT forensics, legal expertise, public relations work, notification costs and restoration costs.

In lawsuits and privacy regulatory investigations, coverage may pay for legal fees, legal settlements and also regulatory fines where insurable, such as HIPAA, PCI, GDPR and CMMC violations.

Insurance coverage for cyber crime may pay for costs such as ransom, extortion payments and fraudulent transfer of funds caused by phishing or social engineering incidents.

Business losses may also be covered, such as impact on operations or the ability of the victimized business to generate revenue both during the incident and afterward, due to reputational damage.

First- and Third-Party Coverage

Most cyber insurance policies break down payments on claims into first-party and third-party coverages. First-party cyber liability insurance helps you respond to data breaches on your own network or systems. Third-party coverage is used to defray costs incurred by one of your clients or customers due to the breach on your system.

First-party coverage includes incident management costs, such as:

- Breach or incident response costs, including IT forensics, legal experts and breach coaching.
- Notification, credit monitoring and call center costs.
- Crisis management and public relations.

Crime Costs

- Extortion.
- Funds transfer fraud computer fraud/social engineering.
- Invoice manipulation fraud (reverse engineering).
- Service fraud/telecom fraud/cryptojacking.

Business Interruption & Extra Expense Coverages

- Direct versus dependent business interruption IT versus non IT partners.
- Extra expense.
- Reputational harm. (If you lose business and continue to lose that business, that would be covered.)
- System damages.

System Restoration Expenses

- Digital asset restoration.
- Computer hardware/bricking.
- Betterment (meaning, if hardware needs to be replaced, insurance will cover only what was previously in use, not the latest technology).

Insurance Costs Likely to Increase

By Q3 of 2024, insurance rates are likely to increase. Typically, rates are determined by your organization's annual revenue and industry, as well as its specific security posture. By way of example, for a law firm with $250 million in annual revenue and 500 attorneys, insurance rates would range from $80,000 to $215,000 annually, depending on the carrier and a host of variables and exclusions.

When shopping for insurance brokers and carriers, pay close attention to their qualifications and experience with cyber insurance. While you may be able to purchase cyber insurance through the same agent who provides your organization with more general insurance, **a cyber expert could be a wiser choice.**

Protecting Your Business

Clearly, managing cyber crime is critical.

At Entech, we approach cyber risk management by first identifying what data is the most sensitive, profitable and targeted by cybercriminals for each organization. Then we prioritize the defense of that data. It's difficult in today's cyber environment to protect everything, so protecting the most valuable assets first is a wise approach.

Reach out to Entech to adopt the latest technologies to protect your company. We can implement defensive software tools like AI-enhanced spam filtration that helps detect phishing emails. Generative AI is brilliant at detecting patterns, and that will make identifying even the most well-crafted phishing campaigns easier. You can trust the team at Entech to help segment and segregate your network so that access to one area of your data doesn't expose others.

We recognize you probably already have someone who takes care of your system. There are plenty of talented IT people, but they can't be experts at everything, nor can they have all the diagnostic tools. That's why Entech has individual specialists for each of the critical areas: **secureability, accessibility** and **recoverability**.

If you have questions about your company's security posture, reach out to the team at Entech. Our aim is to leverage technology most effectively in each area of an organization's business, such as sales, finance and administration. The goal is to improve protection and lower costs whenever possible. The outcome is reduced risk in your business and increased profitability.

We invite you to discover the three things that make Entech unique as a technology partner.

We are:

Passionate about our partnerships.

Fanatical about fast IT support.

Committed to predictable results.

Contact us today to take the weight of managing cyber risk off your shoulders.

entech

www.entechUS.com

(239)230-0282

Together, we can do what matters.

Bradenton | Sarasota | Fort Myers | Naples