AXIS INSURANCE SERVICES, LLC

Your Guide to Cybersecurity Insurance in a Digitally Dependent World

Table of Contents

As the global workforce embraces digital technology more than ever, hackers are thriving.

151%

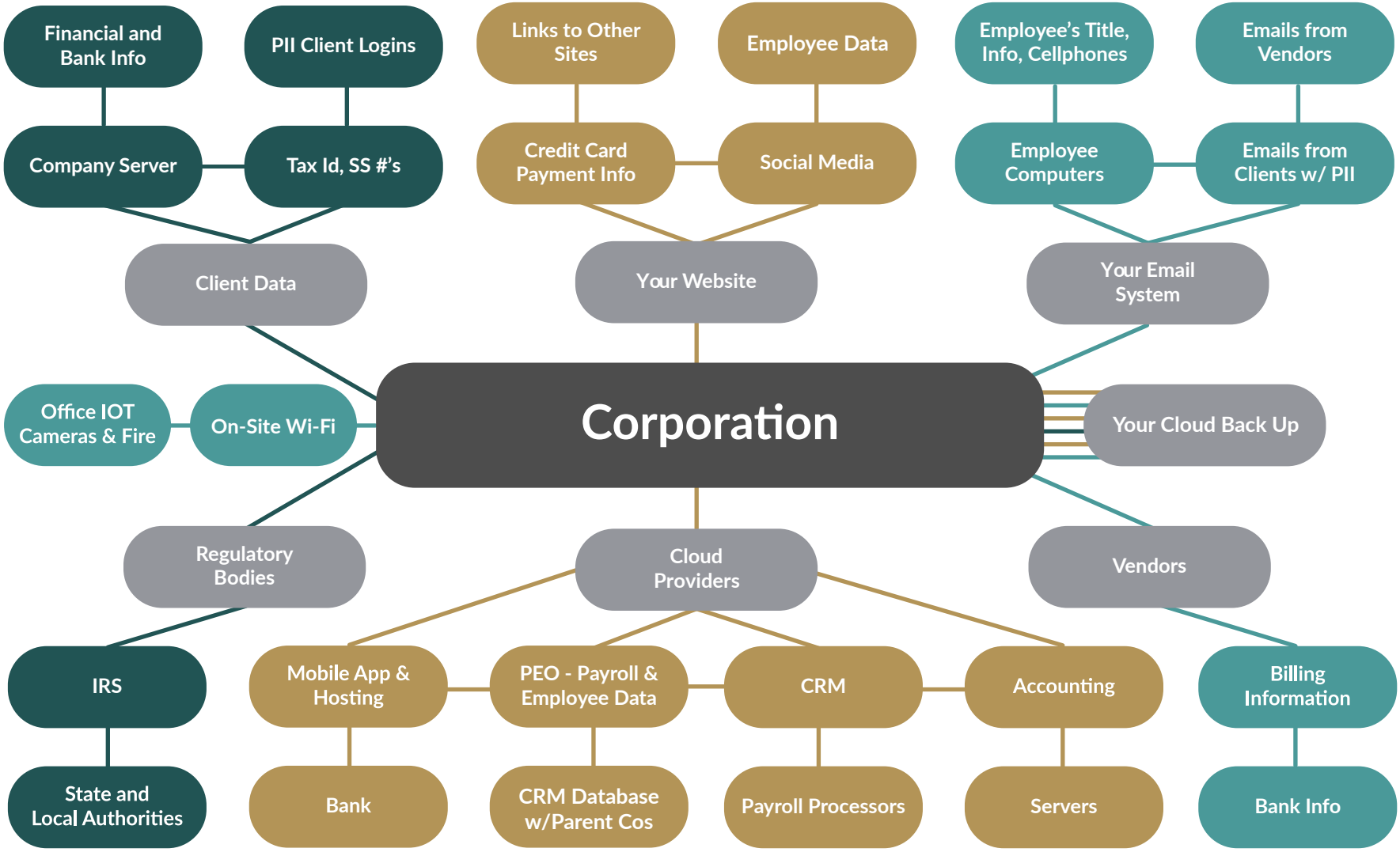
In just the last year, **ransomware attacks rose by 151%.** [1] Remote and hybrid work settings continue to make cloud-stored sensitive data vulnerable to security breaches.

To pile on the risks, 40% of global organizations have cut their cybersecurity budgets to recoup from revenue losses during 2020.[2]

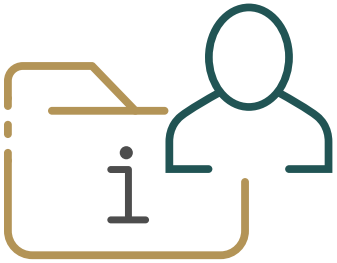
Due to digital vulnerabilities, businesses are likely to continue filing insurance claims related to manipulation, deletion, or extortion of sensitive data. Safeguarding your business from cyber threats and subsequent risk is essential.

[1] HIPPA Journal. (2021). Mid-Year Threat Report Shows Massive Increase in Ransomware Attacks (hipaajournal.com)
[2] Vizard, Mike. "Survey surfaces security stress stemming from pandemic" Barracuda, 2020.

Where Is Your Data at Risk?



What Type of Data Is at Risk?



Personally Identifiable Information (PII)

PII is any information that directly or indirectly indicates or infers the identity of an individual. Sensitive PII includes social security numbers, driver's license numbers, financial records, and more.

Protected Health Information (PHI)

PHI, also known as personal or protected health information, is a form of sensitive information relating to health status, provision, or payment. The Health Insurance Portability and Accountability Act (HIPPA) of 1996 requires businesses responsible for sensitive PHI to implement protections, such as cybersecurity measures. Under intense scrutiny, businesses responsible for this information face massive fines for compromised PHI.

Triggering A Claim: Types Of Cybersecurity Attacks

36b

Coined the “worst year on record,” 2020 experienced numerous data breaches, exposing over 36 billion records of sensitive information globally. [3]

These breaches take the form of phishing attacks, ransomware attacks, Denial of Service (DoS) attacks, password attacks, and more.

Phishing Attacks

Phishing is one of the most common social engineering, human-factor cyber attacks. Attackers send emails to individuals while posing as a credible brand, such as a bank, with the intent to either have the individual reveal their personal information or install malware.

Ransomware Attacks

Ransomware is a form of malware attack in which cyber criminals develop malicious software and threaten sensitive or PII to extort money.

[3] CisoMag. (2020). 36 Bn Records Exposed in Data Breaches in 2020.

Human-Factor Attacks

Actors using human-factor attack methods rely on employees to take an illogical and unsafe action based on the belief that they are communicating with a reliable human. Hackers deploy fake emails, posing as internal individuals of authority to lure employees with a false sense of trust and credibility. Unassuming employees will enable hackers to install malware and gain access to sensitive information.

Common Examples: Phishing, Pretexting

Malware Attacks

Malware attacks occur when cyber criminals deploy malicious software to threaten or seize sensitive PII.

Common Examples: Ransomware, Spyware, Trojans

DoS Attacks

The denial of access to network resources or services, such as emails or websites, by a bad actor is known as a Denial of Service (DoS) attack.

Common Examples: Smurf Attack, SYM Floods

Password Attacks

Actors will use sophisticated decryption tools to decode passwords and seize sensitive data, download PII, or threaten employees.

Common Examples: Dictionary Attack, Keyloggers, Brute-Force Attack

11-Step Checklist to Safeguard Your Business

Cyber attacks not only jeopardize personal information and sensitive data, but they also result in expensive insurance claims.

To protect your business, your staff, and your stakeholders from the damage of malicious cyber attacks, keep in mind these 11 preventative measures.

Set Up Multi-Factor Authentication (MFA)

When you sign into a site or program, have a second, remote way to confirm your identity.

Utilize Endpoint Detection Software

Install software that scans and monitors connections to servers, user stations, laptops, and other devices accessing your network.

Disable Remote Desktop Protocol (RDP) Access

Disabling the ability to remotely control a computer removes a potential point of access for hackers.

Maintain 3-2-1 Backups

Have three different sources of backing up your data that are separable, remote, and away from the office.

Utilize a Password Manager

Password managers allow you to easily use complicated passwords, keep them secure, and regularly update them.

Best Practices Continued...

Maintain Privileged Access Management Protocols

Company servers should be segregated by restrictions, only allowing certain people access to certain files.

Utilize Filtering Software

This software blocks high-risk websites and other sites that pose a risk to your network.

Develop an Incident Response Plan and Keep It Offline

Have a plan in place to deal with the fallout of compromised servers to expedite recovery and minimize damage.

Provide Employee Training Management Protocols

Train employees to spot malicious intent and demonstrate how to avoid potential breaches.

Regularly Test Backup Systems

Backup systems may fail when trying to restore files, so it is important to confirm their functionality.

Regularly Perform Penetration Testing

Deploy mock phishing for employees and attempt breaches to assess security.

Why Buy Cyber Insurance?

Despite proactive and protective measures, 64% of companies worldwide have been victimized by one or more cyber attacks.[4]

Recovering from cyber attacks is expensive and can compromise the sensitive PII of your business and its employees.

When a cyber criminal seized and extorted an engineering firm's data in a ransomware attack, the firm suffered $150 million in lost revenue, $600,000 in ransom payment, $1.2 million in business interruption, and $350,000 in breach response expenses.

Another manufacturer and distributor also suffered a ransomware attack, bearing the burden of more than $82 million in lost revenue, business income, ransom payments, and breach response expenses.

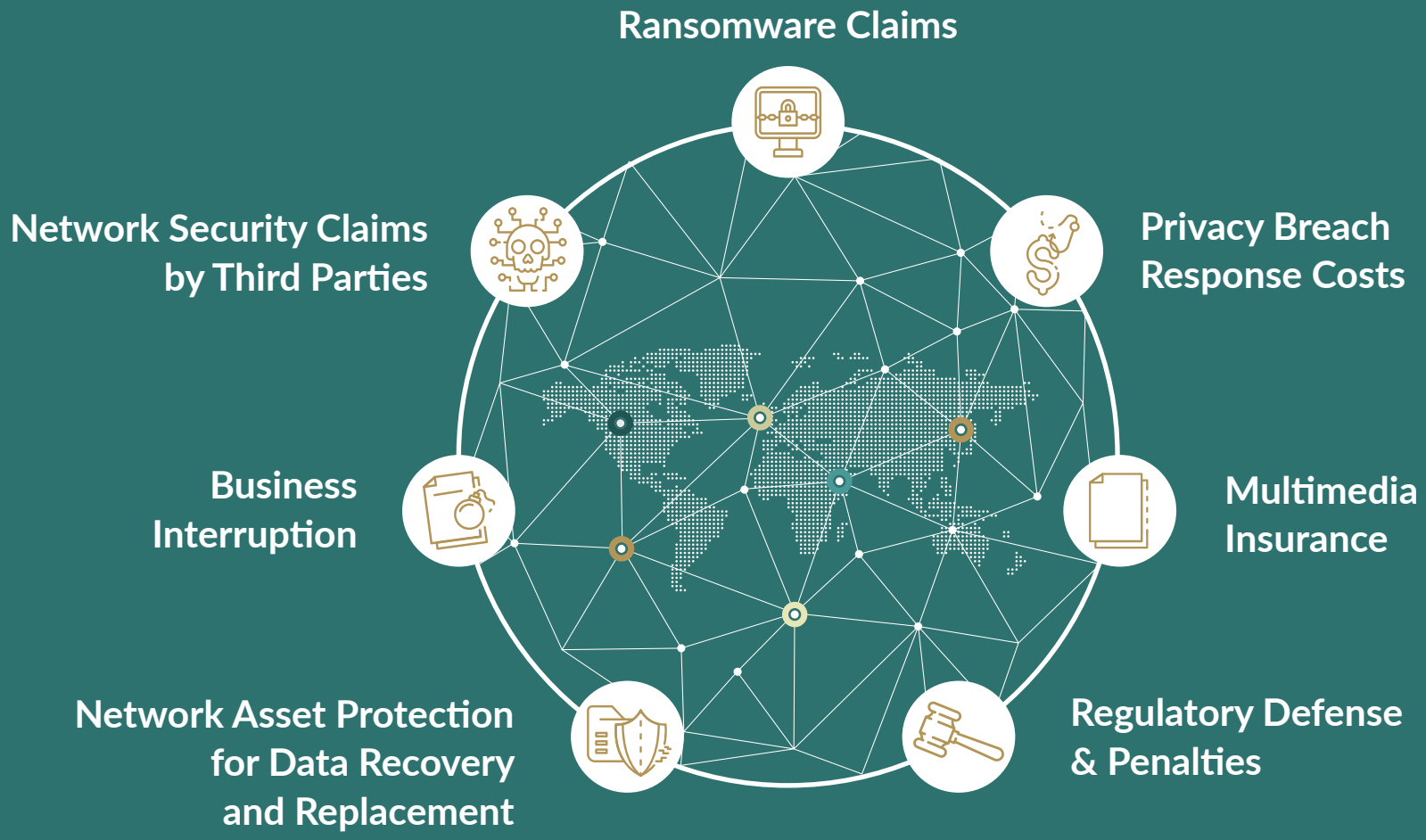
Businesses both large and small have continued to be targeted for cybercrime, with accounts of ransomware spiking by 151% since 2020.[6]

Hackers are cunning and employees get tricked, leaving companies perpetually at risk. Cybersecurity insurance covers the legal and financial fallout in the event that a breach occurs, ensuring your company is equipped to recover.

[4] Compatia.org. 25 Alarming Cyberattacks and Stats.
[6] HIPPA Journal. (2021). Mid-Year Threat Report Shows Massive Increase in Ransomware Attacks (hipaajournal.com)

The spike in strategic cybercrime has complicated a complex cybersecurity landscape where obtaining coverage is very difficult.

Insurance providers employ carefully worded policies to exclude cyber attacks under most policies. As a result, separate cybersecurity insurance policies exist to provide coverage. A Cyber/Privacy & Network Security Liability policy can be tailored to provide coverage for a number of expenses, including:



What's in a Cyber Policy?

A Cyber or Privacy & Network Security Liability policy will include first-party and third-party coverages for cyber incidents.

First-party insurance eases the financial burden on your business in the event that an insured breach or disaster occurs, such as a damaged server or cyber extortion. Financial assistance can be provided for recovery, such as breach response costs or a damage control campaign.

Third-party insurance eases the burden of legal expenses if a client or customer alleges that your business's cyber incident negatively affected them, such as releasing PII. A comprehensive cyber policy will assist in the financial legal fallout, such as paying lawyer fees. This is especially critical for businesses who handle high volumes of client information and are responsible for their online security.

Common First-Party Liability Coverages

- Breach Response Costs
- Breach Response Services
- Crisis Management and Public Relations
- Cyber Extortion
- Business Interruption and Extra Expenses
- Contingent Business Interruption
- Digital Asset Restoration
- Funds Transfer Fraud

Common Third-Party Liability Coverages

- Network and Information Security Liability
- Regulatory Defense and Penalties
- Multimedia Content Liability
- PCI Fines and Assessments

Contingent Business Interruption

Contingent business interruption (CBI), also referred to as dependent business interruption, provides coverage for lost business income due to a third-party vendor or provider service interruption. For example, if your business-essential, cloud-hosted system goes down due to your third-party hosting provider, a CBI policy would cover the lost business income.

About Axis

At Axis Insurance Services, LLC, we're proud of our mission to alleviate the struggles of obtaining insurance and help customers identify and prioritize their Cyber Liability Insurance needs.

Our team of nationally recognized brokerage specialists work to provide the most competitive coverage options available and offer superior customer service. We provide cost-effective Privacy, Cyber & Network Security Liability Insurance solutions which can be tailored to cover defense costs and other expenses.

Contact our team to build out your customized insurance package and secure the best cybersecurity premiums.

Get a Quote

Request a call by filling out the form on our website and we'll get back to you within the next business day.

Mike W. Smith

President and CEO of Axis Insurance Services, LLC with over 30 years of industry experience, Mike places his focus on risk analysis and coverages rather than pricing. Mike has become a valuable market resource and has been requested to be a frequent speaker, guest panelist, and writer on topics relating to professional and management liability risk and insurance.

Office: 201-847-9175 ext. 105

msmith@axisins.com

Mobile: 201-906-7802

LinkedIn

Get a Quote