DATA PRIVACY
+
DATA SECURITY
IN THE INSURANCE INDUSTRY

US SIGNAL®

TABLE OF CONTENTS

THE RISKY BUSINESS OF INSURANCE

When it comes to risk, what business sector knows it better than the insurance industry? After all, insurance companies are in the business of assuming and diversifying risk, and insurance policies are used to hedge against the risk of financial losses.

Unfortunately, the insurance industry hasn't shown that it's been able to use that knowledge to avoid the risks of cyberattacks and noncompliance with various regulatory requirements. Just ask State Farm, Marsh & McLennan Cos. Inc., Ryan Specialty Group Holdings Inc., Chubb Corporation and Pacific Specialty Insurance Company, all which fell victim to cyberattacks in the last few years.

Don't forget about ***Anthem Blue Cross and Blue Shield*** either. It still holds the record for the largest healthcare data breach, which resulted in a record-breaking $115 million class-action settlement with breach victims and the largest Office for Civil Rights settlement in the agency's history ($16 million).

In this eBook, we look at the risks insurance companies face and what's make them so challenging, and offer tips for overcoming them.

IT'S THE DATA

Insurers collect, process and store a wide variety of information on individuals. Depending on the type of insurance services provided, that information could include anything from Social Security numbers and credit reports to prescription histories and driving records. Most of it could be used to identify specific individuals, hence the reason it's often referred to as personally identifiable information (PII).

On any given day, insurance data scientists may also gather data from satellite data, smart phones, social media, telematics devices, website analytics, wearables, and more. By itself, that information may seem innocuous. When linked with other information, it can become data that identifies specific individuals – in other words, PII.

This wealth of personal data makes insurance companies popular targets for cybercriminals, and frequent victims of data breaches. That same data also makes them subject to numerous laws, regulations, industry standards and contractual requirements related to data privacy and security.

IMPACT OF DATA BREACHES

- + Non-compliance fines
- + Legal Fees
- + Lawsuits
- + Fraud Monitoring Costs
- + Damage Reimbursement
- + Business of Disruption
- + Loss of Consumer Trust
- + Negative Impact Market Value
- + Brand Damage

THE GROWING COMPLIANCE LANDSCAPE

Companies in the insurance industry have long been heavily regulated, and subject to regulations at the federal, state, and local levels. With the increasing use of digital technologies and data analytics, along with increases in cyberattacks, the list of requirements specific to data security and privacy are expected to grow. Failure to comply with them can subject insurance companies to significant penalties, among other negative effects.

Among the requirements insurance companies may be subject to are:

+ The ***General Data Protection Regulation*** (GDPR)
+ The ***California Consumer Privacy Act*** (CCPA)
+ The ***Health Insurance Portability and Accountability Act*** (HIPAA)
+ The ***Gramm–Leach–Bliley Act*** (GLBA)
+ The ***Sarbanes–Oxley Act*** (SOX)
+ The ***Payment Card Industry Data Security Standard*** (PCI DSS)
+ ***Federal Information Security Modernization Act*** (FISMA)

An increasing number of states are also adopting the ***NAIC Insurance Data Security Model Law***. It requires insurance companies and other entities (those licensed under the Department of Insurance) to implement and maintain an information security program to better protect consumer data.

PCI

HIPAA COMPLIANT

AICPA SERVICE ORGANIZATIONS SOC aicpa.org/soc — AICPA Service Organization Control Reports — Formerly SAS 70 Reports

AICPA SOC 2 — AICPA Service Organization Control Reports — Formerly SAS 70 Reports

THE PRICE OF NONCOMPLIANCE

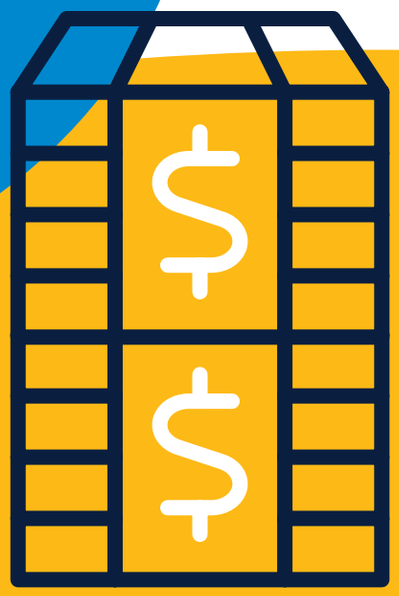
Failing to comply with requirements for data privacy and security doesn't come cheap. These are just a few examples of what noncompliance costs can run:

+ HIPAA - The fine is calculated based on the number of medical records exposed, with fines ranging from $50-$50,000 per record. Violators may face 1-10 years prison time.
+ GLBA - Organizations are fined up to $100,000 for each violation; officers and directors may be fined up to $10,000 personally. Individuals may also face up to 5 years in prison.
+ PCI DSS - Being in breach of PCI DDS exposes organizations to minimum fines of $5,000 per month and maximum fines of $100,000 per month.

If you think these kinds of laws aren't enforced, think again. Two notable examples:

In 2020, the Office for Civil Rights fined Premera Blue Cross $6.85 million. The HIPAA violations stemmed from a phishing email that enabled hackers to install malware on the company's systems, giving them access to members' data.

In 2021, the New York Department of Financial Services imposed a $1.8 million penalty on First Unum Life Insurance Company of America and Paul Revere Life Insurance Company after investigating two phishing incidents. The NYDFS found the companies violated its Cybersecurity Regulation by failing to implement multi-factor authentication or equivalent or more secure access controls.



CYBERCRIME PAYS

No one gets rich on noncompliance penalties, but they do on cybercrime. The 2022 cybercrime economy is worth at least $1.2 trillion, according to economists. That makes it the 15th largest economy in the world, by International Monetary Fund estimates. It generates more profits than the combined global trade in all illegal drugs.

The insurance industry is fast becoming one of the most appealing targets for cybercriminals. That includes state-sponsored actors, as demonstrated by the previously referenced Anthem breach, which was attributed to Chinese hackers.

The opportunity to steal or hijack personal data is the big motivator, as well as the potential for insurance fraud. Not surprisingly, ***nine out of ten insurance industry data breaches*** are financially motivated. According to ***Accenture***, the insurance industry was the most frequent target of ransomware attacks in the first half of 2021.

However, cybercrime isn't just a matter of exploiting system vulnerabilities. According to Verizon's 2020 ***Data Breach Investigations Report***, the most common outsider attacks on the insurance and financial industry were scams, phishing attacks, and pretexting attacks. Mistakes made by employees play a role too.

WHAT DO HACKERS DO WITH PII?

- **Sell it on the dark web**
- **Use it to commit identity theft**
- **Use login details to take over accounts with payment deals**
- **Use it to target victims with phishing attacks**
- **Use it to extort victims**
- **Use it to harm companies**

WHERE THE RISKS ARE

There's no shortage of cyberthreats facing insurance companies. Here are some of the most common – and costly.

Cloud Exploits
Despite its built-in security advantages, the cloud is still susceptible to threats such as DDoS, injection attacks, misconfiguration and account hijacking

Patch Management
Failing to update software patches makes an organization vulnerable to numerous data breaches.

Social Engineering
Social engineering takes advantage of human psychology to compromise victims' information. Common attack types are phishing, pretexting, baiting, quid pro quo, and tailgating.

Ransomware
Ransomware is malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. They don't always follow through with decryption, and once a ransom is paid, victims set themselves up for future attacks.

Third-party Exploits
Hackers can use malware to access sensitive data through a company's third-party providers. It's imperative to understand each of vendors' cybersecurity posture and ensure they employ best practices for data protection.

Through 2025, 99% of cloud security failures will be the customer's fault.

- Gartner

DATA PROTECTION TACTICS

Unfortunately, there's no single solution that can protect insurance companies against every kind of cyberattack — or ensure compliance with data privacy and security regulations and requirements. However, layering on various defense mechanisms can help. It's an approach known as defense in depth (DiD).

The idea is to use multiple cybersecurity solutions to provide protection at the perimeter, application, endpoint, and physical security layer. If one mechanism fails, another is available to thwart an attack. And if an attack is successful, you can at least contain the threat and mitigate potential damage.

The use of several layers of security technologies, along with numerous security protocols, can also help meet many of the technical and process requirements associated with various data privacy and data security laws and standards.

13 TIPS TO ENHANCE DATA SECURITY + PRIVACY

To help create a DiD strategy, considering employing these tools and technologies:

1. Implement a ***vulnerability management program*** that includes vulnerability scans and ***analysis of the scan results*** with recommended, prioritized actions.

2. Strengthen endpoint protection with a proactive ***Endpoint Detection and Response*** solution. It should incorporate continuous monitoring and advanced technologies to protect against, detect and quickly respond to ever-changing threats.

3. Create a comprehensive ***patch management*** program that ensures you have the latest patches available, prioritizes them by importance, and applies them – manually or automatically -- in a timely manner.

4. ***Develop, continuously review and refine your IT security policies and procedures***, including those specific to cybersecurity, to ensure they meet your organization's business objectives, fit within its culture and address current and emerging threats.

5. Install ***next-generation, managed firewalls***. They go beyond stateful inspection of incoming and outgoing network traffic, with additional features like integrated intrusion prevention and cloud-delivered threat intelligence.

6. Perform regular risk assessments. Identify what data and systems need to be protected and determine the threat of exposure. Develop and implement an action plan, prioritizing what needs to be done, when and by whom.

7. Establish a culture of security. Regularly impress upon employees their roles and responsibilities in ensuring data protection. Secure support and participation from your organization's leadership.

8 Continuously monitor and test website security, including online portals. Implement solutions that protect against a wide range of internet-based threats, including volumetric, distributed and multi-vector DDoS attacks, SQL Injection attacks, and content scraping.

9 Appoint a data protection officer. In addition to meeting GDPR and PCI DSS obligations, this will increase your organization's ability to pass security audits and respond to security incidents.

10 Limit data access. Implement a policy of zero trust or least privilege. Access to your IT infrastructure can be strengthened with multi-factor authentication and strong password policies.

11 Reduce third-party risks. Verify all third-party vendors have implemented strong third-party risk cybersecurity monitoring and plans and use security best practices.

12 Encrypt data at rest and in transit. Data encryption is required or recommended by the GDPR, LGBA, PCI DSS, and other regulations, laws, and standards.

13 Use managed security services, so you can take advantage of the leading-edge security technologies and specialized security expertise that outside firms can offer—and without any upfront capital investment.

THE US SIGNAL APPROACH ADVANTAGE

There are many great tools, technologies, processes and practices to help ensure data security and privacy. There are also companies that can partner with you to determine the right ones for building effective, well-rounded data protection and data security plans, as well as meeting a wide variety of compliance requirements.

US Signal stands out among them. US Signal has extensive experience in working with companies across a wide range of industries, insurance included. We understand the regulatory environment insurance companies must work in, as well as the many other challenges they face.

While we favor cloud-based options because of the many benefits they deliver, we know that insurance companies often must strike a balance between technologies that drive innovation and transformation and their legacy IT systems and applications. By taking the time to understand your unique systems, challenges, and plans, we can devise solutions and options that best meet your needs.

Learn what we can do for you.

Call 866.2.SIGNAL, email info@ussignal.com, or visit ussignal.com