Top 3 Myths of Cyber Risk

For Small & Medium-Size Businesses

Relation™

We've changed our name.
Ascension Insurance is now Relation Insurance Services / relationinsurance.com

Ascension™

We live in a world in which our global economy increasingly relies on data and information stored & carried through cyberspace. Almost daily, hackers target major retailers, large financial institutions, healthcare organizations, and hospitality & government entities specifically for the wealth of personal information they use to run their operations.

To weather the risks of security breaches, large firms typically rely on a combination of financial strength, extensive IT security operations, and cyber-risk insurance. For small and medium-size businesses, the risks are no less prevalent. Without the protection backstops available to larger organizations, however, the consequences for smaller firms who lack coverage are potentially catastrophic—if not existential. Though cyber-risk insurance is an invaluable tool for companies of all sizes, small-to-medium-size groups are often deterred from including it in their business insurance portfolios due to 3 common myths.

High-Profile Cyber Hackings

TARGET

EA 2013 data breach theft of credit card and other personal information of 40m customers resulted in a loss of more than $200m. Reputational damage was severe and impacted their share price. In addition, a shareholder derivative suit was filed.

EQUIFAX

In September 2017, the credit bureau disclosed that the names, social security numbers, birth dates, addresses, and, in some cases, driver license and credit card numbers of 145.5m individuals had been hacked.

JPMorgan Chase & Co.

A 2014 data breach affected 76m households and 7m small businesses.

SONY

In 2014 Sony's network was breached by North Korean hackers who disabled the network and released numerous embarrassing emails.

WannaCry

In early 2017, hundreds of thousands of computers in 100+ countries were hit with a malware that encrypted victims' files. Had a "kill switch" not been discovered, the potential impact of "wiped" files for numerous individual firms could have been catastrophic.

Anthem BlueCross BlueShield

In 2015 hackers gained access to the social security numbers and personal health infomation of more than 80m Anthem customers, resulting in a loss expected to be in excess of $100m.

In this white paper, we dispel these three myths and offer a roadmap to guide you through the landscape of cyber-insurance solutions. Turn the page to learn how you can help prevent yourself from becoming a victim of cyber hacking.

1 We're too small to be a target

According to Jeff Bardin, Chief Intelligence Officer of cyber-risk consulting firm Treadstone71, **"Forty percent of cyberattacks are aimed at companies with 500 employees or less."** Common sources of big claims for smaller businesses include the following:

- Poor control and lack of encryption tools on laptops and mobile devices
- Rogue employees or simple human error
- Fraudulent email invoices
- Spyware intrusion targeting unsecured customer records
- Ransomware attacks, which affect thousands of firms of all sizes and are increasing at an ominous rate

The impact of cyber attacks on small and medium-size businesses includes lost customers, distracted staff, reputational harm, fines and damages, and expenses for forensics, remediation, notification, credit monitoring, and legal defense and/or settlements. As the following claims scenarios show, there is no such thing as a firm being too small to suffer a cyber loss.

Small-Business Claims Scenarios[2]

Stolen Laptops

Two laptops were stolen from an IT service provider containing the data of more than 80k customers of one of its clients, a regional retailer. Notification laws required the retailer—not the IT service provider—to notify victims. Price tag? Nearly $5m.

Rogue Employees

After learning she was due to be fired, a disgruntled employee stole customers' personally identifiable information (PII) and used it to fraudulently obtain credit cards. The company—not the former ex-employee—was sued.

Funds Transfer Fraud

A small manufacturer transferred more than $300k to an account in China based on a fake email invoice for raw materials.

Spyware Virus

A man sent an email with spyware to a former girlfriend. She opened it from her work computer, and he was able to access the confidential data of 150+ customers. The employer was held liable.

Dumpster Diving

An employee of a medical office disposed of confidential information in a garbage bin. A "diver" (a woman hunting for coupons) found the information. The incident constituted a HIPAA violation, and the medical office was fined.

"Ransomware, along with social engineering, is the fastest growing area of incidents,"

Richard Bortnick, senior counsel, Traub Lieberman Straus & Shrewsberry, Red Bank, New Jersey, said—adding that about $1b was paid to ransomware attacks in 2016.

From the 2017 Global Cost of Data Breach Study by Ponemon Institute & IBM Security[3]

The biggest financial consequence for firms that experienced a data breach is lost business.

Hackers and criminal insiders caused the most data breaches.

DATA-BREACH CAUSES

criminal and malicious attacks | *system glitches* | *human error*

The longer it takes to detect and contain a data breach, the costlier the claim.

$225 *The average cost per lost or stolen record in the U.S.*

$1.56 *Post data breach response costs per record.*

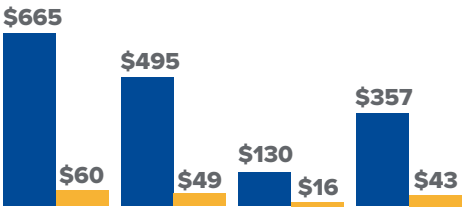
E.g., forensic investigation, notification, remediation, credit monitoring, identity protection & legal guidance.

Mitigation strategies, such as an incident response team, extensive encryption, and employee training had a demonstrably positive impact.

From the 2016 Cyber Claims Study by NetDiligence Analyzing 176 Individual U.S. Cyber Claims[4]

Records exposed ranged from 1 to 78m with an average of 2m and a median of 1,339.

in thousands of dollars **AVERAGE** **MEDIAN**



total breach cost | *claim payout* | *legal defense costs* | *post claim crisis service cost*

30% *Submitted claims with insider involvement.*

$1.5–2m *Amount settled for the claim with a single lost record.*

Some firms are recognizing the value of cyber-risk insurance. The April 2017 Council of Insurance Agents & Brokers' *Cyber Insurance Market Watch Survey* noted that **32% of surveyed companies purchased some form of cyber coverage, up from 24% the prior year**. That's a significant year-over-year jump, but the fact remains that *two-thirds of companies* are still not buying in.

In addition to targeting firms of *all* sizes, cyber criminals are exploring new hacking methods and techniques. Many firms believe their business operations are uncomplicated or low tech and they don't recognize the scope of their vulnerabilities. Cue myth number two.

2 Our exposure isn't that great

Believing their IT operations are low-tech and therefore unappealing to cyber attackers, many small and medium-size firms are unaware of their many cyber threats. Meanwhile, hackers see an opportunity for valuable, easily accessible data. Any business using technology to conduct its operations and store or transfer data is at risk. Cyber-risk exposures can be financial, physical, or reputational and can fall broadly into two categories:

Third-Party Liability Exposures

Information Security Liability results from a breach, including unlawful access to a network, transmission of malicious code (a virus), or denial of service (preventing others from gaining access to a network).

Privacy Liability occurs when a hacker breaches a network & accesses or releases personally identifiable information (PII), private health information (PHI), and/or other confidential material.

Content Liability includes intellectual property liability (e.g., copyrights, trademarks, patents), advertising liability (e.g., false advertising, disparagement), and employee liability (e.g., privacy violation, defamation).

First-Party Liability Exposures

Business Interruption results from a network breach that causes an equipment malfunction that leads to a loss of income.

Contingent Business Interruption refers to lost profits resulting from an interruption of business at the premises of a customer or supplier.

Extra Expenses are costs to minimize the duration of a loss event.

Data Asset Loss occurs when data assets are destroyed.

Cyber Extortion results from a hacker locking a business out of its files until a desired ransom is paid.

Computer Fraud occurs when a hacker gains access to valuable data or information.

Funds Transfer Fraud occurs when a hacker transfers company funds to another account.

Miscellaneous Crime Losses includes hackers' defacing web pages, intercepting proprietary emails, posting source code, and/or spamming.

To further intensify matters, the cyber-risk environment is dynamic and evolving. Emerging risk exposures creating uncertainty and concern for businesses, IT-security specialists, and cyber-risk underwriters now include the following:

- Social Media
- Cloud Computing Systems / Outsourced Data Management
- Internet of Things (IoT)
- Artificial intelligence (AI)
- Autonomous vehicles
- Wearable Medical Devices

Whether launched by run-of-the-mill hackers, criminals, insiders, or even nation-states, cyber attacks are likely to occur and can cause moderate to severe losses for organizations large and small.

Even for firms that recognize the expanding scope of their cyber-risk exposures, many are lulled into a false sense of confidence that they already have protection, which leads to myth number three.

3 Our existing coverage protects us

This third myth is perhaps the easiest to debunk, as the following conventional business insurance policies may afford only some degree of protection:

- Commercial General Liability
- Property
- Blanket Crime
- Executive Protection (e.g., EPLI, D&O)
- Professional Liability

There are two crucial caveats to consider:

1 **These policies were not designed to respond to cyber attacks, and coverage is limited—beware of policy exclusions.**

2 **Underwriters are increasingly carving cyber coverage out of conventional polices in favor of cyber-specific policies—the modest coverage you have today may be gone at your next renewal.**

The takeaways?

Understand

the unique cyber risk exposures of your business

Determine

what is and isn't covered by your existing insurance portfolio

Evaluate

whether you need cyber-risk insurance

Dovetail

your traditional policies and your cyber-risk insurance policies

The cyber-risk insurance market is crowded, complex & dynamic:

There are 60+ insurers—with varying degrees of underwriting expertise—who write cyber-risk insurance.

Policies are "non-standard" meaning there is wide variation in policy terms and conditions from carrier to carrier.

Policies can be structured on an a-la-carte basis to offer a wide range of coverages.

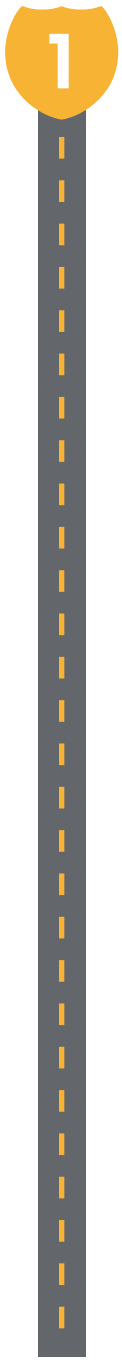
Carrier pricing methodologies vary widely, leading to premiums that are "all over the map."

Many firms are considering purchase of cyber insurance for the first time, and it is important for buyers to invest the necessary time to understand their individual risks and the available coverages. A systematic approach is needed to guide business owners through this complex terrain.

So, Do You Need Cyber Insurance?

A Roadmap

Although the *subject matter* may be new to you, the process of evaluating whether or not to buy cyber-risk insurance is no different than purchasing any other line of insurance coverage.



Assessment

Identify your unique risks.

The first and most critical step is to understand the nature and extent of the risks facing your company:

- Get input from various stakeholders within the organization (e.g., finance, IT, sales, legal).
- Look at hypothetical claims scenarios.
- An insurer-coverage application can serve as an informative, systematic checklist.

Understand your existing coverage.

This will make it less likely that you end up with either duplicate coverage or, worse, coverage gaps.

2

Understand Which Cyber Coverages are Available in the Marketplace[6 7 8]

Third-Party Liability Coverages

Privacy Liability coverage for breaches of private information of third parties (e.g. employees, customers, business partners).

Breach Notification Costs expenses to notify customers, employees, and other victims.

Credit Monitoring ongoing costs to monitor victims' credit.

Transmission of Viruses or Malicious Code protects against claims alleging damages from the transmission
by the insured of viruses and other malicious code or data to a third party.

Media Liability coverage for intellectual property infringement claims resulting from publication by the insured.

First-Party Liability Coverages

Network Interruption / Business Interruption covers lost income and related expenses when an insured is unable to conduct business due to a cyber event either on their premises or at a supplier or customer.

Cyber Extortion / Ransom pays ransom costs when hackers deny an insured access to their own network and threaten to obtain or disclose sensitive information unless a ransom is paid.

Data Loss and Restoration covers physical damage to or loss of use of computer-related assets including cost of retrieving or restoring data, hardware or software due to a cyber attack.

Reputational / Crisis Management costs of engaging a crisis-management team
to help mitigate reputational harm due to a cyber event.

Theft / Fraud covers destruction or loss of insured's data as the result of a criminal or fraudulent cyber attack, including theft and transfer of funds.

Forensic-Investigation Costs covers costs for legal, technical, and forensic experts to determine the cause and impact of an attack.

Regulatory Fines assists the insured in responding to governmental inquiries related to a cyber attack and provides coverage for fines, penalties, investigations, or other regulatory actions.

3 Program Design and Marketing Strategy

Determine what cyber coverages you need

The range of first- and third-party liability coverage parts should give you the flexibility to tailor a program that best treats your risks.

Select targeted markets

Determine which carrier(s) offer the coverage, limits, and support service capabilities that align with your objectives.

4 Evaluation

Review carrier proposals

Your broker should analyze the following key provisions:

- Coverage parts offered
- Coverage triggers
- Who is an insured
- Defense coverage (choice of counsel)
- Policy term (need for retroactive coverage)
- Policy territory
- Exclusions
- Limits and sub-limits
- Premiums and deductibles

5 Placement

Once you've determined the best path forward, the broker will bind the program.

6 Ongoing Monitoring

Many carriers offer risk-management services to assist their insureds reduce their susceptibility to claims, including cost-favorable access to third-party security experts and lawyers, as well as employee educational materials.

Above all, keep current on cyber-risk exposures and trends—hackers are constantly seeking new victims and new ways to target them. It is important to stay vigilant!

Cyber-risk insurance is a new option for many businesses. Talk to an insurance consultant well versed in this type of policy to determine the appropriate amount of coverage for your business. All types and sizes of organizations are at risk, not only the high-profile firms making headlines.

ARTICLES AND SOURCE DOCUMENTS REFERENCED IN THIS DOCUMENT

1 "Reflecting on WannaCry and What it Means for Insurers" http://www.insurancebusinessmag.com/us/news/breaking-news/reflecting-on-wannacry-and-what-it-means-for-insurers-69720.aspxCyber
2 Liability Claims Examples and Why Your Business Needs Coverage", Hill & Hamilton (2015)
3 2017 Cost of Data Breach Study: Global Analysis—Ponemon Institute, LLC
4 NetDiligence 2016 Cyber Claim Study
5 International Risk Management Institute (IRMI) "Cyber and Privacy Exposures and Insurance Coverage (2013)
6 "Cyber Insurance: Considerations for Businesses", Terri Cotton Santos, RIMS Professional Report (2016)
7 Legal Alert "A Buyer's Guide to Cyber Insurance", McGuire Woods (2013)
8 "Cyber Risk Insurance Policies: What You Need to Know", Manatt Phelps & Phillips, LLP (2015)

ABOUT RELATION INSURANCE SERVICES

Relation Insurance Services offers superior risk-management and benefits-consulting services across the U.S. It is ranked within the top 45 largest agencies in the country by revenue, with approximately 500 employees in more than 34 locations nationwide. Relation is a privately held corporation; alongside its private-equity partners, Parthenon Capital and Century Capital Management, the company expects to continue its strong growth trajectory through additional acquisitions and organic growth.

CORPORATE HEADQUARTERS / WALNUT CREEK OFFICE

1277 Treat Boulevard, Suite 400
Walnut Creek, California 94597
(800) 404-4969