Assurex™ GLOBAL

Exposed, Targeted and Breached:

The Risk of Cyber Crime

assurexglobal.com

OVERVIEW

REPORTS OF LARGE-SCALE CYBER ATTACKS ON COMPANIES often get top billing on media outlets. We listen in dismay—and sometimes disbelief—as newscasters describe audacious crimes:

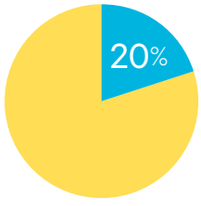
- The personal information of 80 million Anthem customers exposed in a database breach.
- 56 million credit cards compromised by hackers who infiltrated Home Depot's system.
- Employees at Hollywood Presbyterian Medical Center locked out of the hospital's system and forced to use pen and paper for record-keeping.

In 2015, a record-setting total of nine mega-breaches—those compromising more than 10 million records—were reported, according to Symantec's 2016 Internet Security Threat Report. But it would be a mistake to think cyber crime only affects large companies with millions of records at stake. Medium and small businesses incur cyber attacks, too, but you aren't as likely to hear about them on the news. Microsoft asserts that 20 percent of small to mid-sized businesses have been cyber crime targets.

So how can a company shield itself? Michael Richmond, JD, with The Horton Group, recommends a two-pronged approach: Set up a strong information technology security system to help prevent attacks, and invest in a cyber liability insurance policy to mitigate losses should an attack occur.

"As businesses become more concerned about cyber risks, they invest more in strengthening their cyber event protocols. However, there is still a lot more that businesses can do to protect themselves adequately," says Richmond. "Standalone cyber liability coverage remains an essential part of all risk management programs."

This white paper will explain what cyber crime is, why companies should be concerned about potential attacks, and how they can mitigate their risks through insurance.



Microsoft asserts that 20 percent of small to mid-sized businesses have been cyber crime targets.

Section 1:
A Look at Cyber Crime

Section 2:
Common Misconceptions About Cyber Attacks

Section 3:
Types of Cyber Liability Coverage

Section 4:
Reading the Fine Print in a Policy

ABOUT MICHAEL RICHMOND, JD

Michael Richmond, JD, is a sales executive for Risk Advisory Solutions at the Horton Group, a Chicago-based insurance, employee benefits and risk advisory firm. He analyzes every detail of a client's business to determine its exposure and provides risk management programs that contain the business's liability. As an attorney, Mike understands the legal exposures that companies face, in addition to the countless ways they can affect business.

In recent years, Mike has taken a particular interest in cyber crimes and the associated risks to companies. During the spring of 2016, he held several seminars throughout the Midwest on cyber crime, educating businesses on the growing pandemic and providing insight into insurance solutions.

Section 1:

A LOOK AT CYBER CRIME

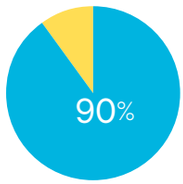
Cyber crime is any illegal activity conducted via the internet, a computer or computer network. The U.S. Department of Justice calls it "one of the greatest threats facing our country" with tremendous implications for our national security, economic prosperity, and public safety.

"Cyber crime is theft of important or protected information against an individual or business," says Richmond. "It could be personal information, bank account information, social security numbers—anything that could end up harming an individual or business one way or another." The breadth of cyber crimes ranges from social media scams to attacks on IT infrastructure systems. And the kinds of attacks grow and change daily, leaving companies increasingly vulnerable.

"Right now, phishing scams are the No. 1 cyber threat," says Richmond. "We see a lot of fake emails coming into businesses. Somebody poses as an important person in the organization and asks that money be sent to a certain location—like a CEO asking that payment is sent to a vendor. Believe it or not, some people are falling for it and sending payment."

Here's a brief explanation of four common cyber attacks aimed at businesses:

- **Phishing Scams** – Phishers pretend to be legitimate companies and use spam, fake websites, emails, and instant messages so they can fool people into handing over sensitive information or clicking on a malicious link. Spear-phishing, a new twist on phishing, is an email that appears to be from a person or company you know asking for information, such as bank account numbers, passwords, financial information, and so on. More than 1,250 brands were hijacked by phishers in the first quarter of 2016, according to the Phishing Activity Trends Report published by the Anti-Phishing Working Group.
- **Malware** – An abbreviated term for "malicious software," the intent of malware is to damage or disable computers or computer systems – often for the purpose of extracting a ransom. It's a comprehensive term for a variety of threats, including computer viruses, Trojan horses, adware, spyware, and worms. Malware is typically introduced to a company's computer system via email attachments, downloads, or operating system vulnerabilities. Symantec reports that the rate of malware sent to companies with less than 250 employees is one out of 184; that figure rises to one out of 82 for companies with 251 to 500 employees.
- **Password Hacking** – As the name suggests, this occurs when a con artist attempts to access your systems by figuring out your password. More than 90 percent of user-generated passwords are vulnerable, according to a 2013 report by global consulting firm Deloitte.
- **Distributed Denial-of-Service (DDoS) Attacks** – Hackers disrupt service to your company's network by sending high volumes of data or traffic through the network, thereby overloading it. For many companies, that means business comes to an abrupt halt, which can cause thousands of dollars in lost revenue depending upon the company and length of disruption. DDoS attacks are on the rise, increasing 23 percent in the first quarter of 2016, according to the Q1 2016 State of the Internet/Security Report by Akamai Technologies.

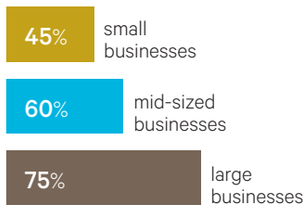


More than 90% of user-generated passwords are vulnerable, according to a 2013 report by global consulting firm Deloitte.

Section 2:

COMMON MISCONCEPTIONS ABOUT CYBER ATTACKS

A STUDY FROM MARKET ANALYST JUNIPER RESEARCH INDICATES that the cost of data breaches will reach $2.1 trillion globally by 2019. More companies are beginning to take note of the problems associated with cyber attacks and whether they could be vulnerable. The 2015 Travelers Business Risk Index notes that 75 percent of large businesses, 60 percent of mid-sized businesses and 45 percent of small businesses view cyber risk as a major threat.



VIEW CYBER RISK AS A MAJOR THREAT.

However, far too many businesses still cling to fallacies about cyber crime. Richmond cites four common misconceptions:

Misconception #1: **Cyber crime only happens to large companies.**

"Everyone hears about Target and Anthem getting breached because those stories make the papers," says Richmond. "You don't hear about the breaches at $50 million or $100 million manufacturers. But they are happening. Sometimes that's because the cyber protection at smaller companies isn't as sophisticated, so hackers see them as an easy target."

During a two-year period through February 2016, approximately 22 percent of small and mid-sized businesses surveyed by *CFO* magazine reported that they were victims of a cyber attack on their computer networks. If numbers alone aren't convincing, consider two real-life cases from small companies. In one week, PATCO Construction in Maine lost nearly $600,000 to a Trojan horse cyber attack. In the same state, Maine Indoor Karting, a go-cart racing business with about 20 employees, discovered its bank accounts were emptied in a phishing scam.

Misconception #2: **My type of business isn't a target.**

"Every business is a target," says Richmond. "Whether you operate a bank, retail establishment, hospital, or professional service firm, everyone is at risk." Cyber attacks aren't always the result of nation states seeking company secrets or hackers aiming for details on millions of credit card accounts. Thieves may target your company to access your bank account, gain trade secrets, steal intellectual property, gain a competitive advantage in your market, or simply ruin your reputation.

No industry is immune to the risks. Consider Symantec's wide-reaching list of the top five sectors breached by number of incidents in 2015:

1. Services
2. Finance, Insurance and Real Estate
3. Retail Trade
4. Public Administration
5. Wholesale Trade

Cyber Crime by the Numbers

Every 3 Seconds
Someone's personal identity is stolen

429 Million
Total reported exposed identities in 2015

1.3 Million
Average identities exposed per breach

430 Million
New unique pieces of malware discovered by Symantec in 2015

Source of Facts: Symantec

Misconception #3: **We can self-insure against a data breach.**

The steep cost of cyber attacks makes self-insuring a perilous option. The average total cost of a data breach for 350 companies who participated in the Poneman Institute's 2015 Cost of Data Breach Study was $3.79 million, up 23 percent from 2013. In addition, the report notes that the average cost of a malicious or criminal data breach incident in the United States is $230 per compromised record.

Why is the cost so high? Those figures include fees associated with data breach investigation, notification, public relations outreach, credit monitoring, regulatory fines, legal services, and settlements or judgments. Costs are likely to increase, too, based on the impact of a recent ruling by a federal appeals court related to P.F. Chang's 2014 data breach, in which hackers broke into the restaurant's computer system and stole consumer credit and debit card data.

The 7th U.S. Circuit Court of Appeals ruled that individuals can bring suit against the restaurant simply because they have an "increased risk" of fraudulent debit/credit card charges and identity theft. "If a data breach takes place, businesses will now be subject to defense costs even if customers have yet to suffer any immediate or identifiable loss that can be traced to the data breach in question," says Richmond. "Now the clock—and meter—starts ticking instantaneously."

Misconception #4: **We outsource our network security, data management, and payment transactions.**

"That's a great first step toward protecting your organization," says Richmond. "But to depend solely on a vendor is wrong for two reasons." The first is that as the original data owner, you will be named in third-party lawsuits and likely be held liable in most jurisdictions. Secondly, though your vendor agreement may contain indemnification provisions, there are several ways a vendor can get out of upholding those provisions.

Indemnification provisions often include limiting and exclusionary language, such as caps on indemnification amounts and exclusions for certain types of data breaches. In addition, you are not protected if the vendor becomes insolvent, goes into bankruptcy, or simply decides not to honor the agreement. "The best option is the front-end protection offered by a third-party provider in tandem with the back-end protection of a cyber liability insurance policy," says Richmond.

> "Every business is a target. Whether you operate a bank, retail establishment, hospital or professional service firm, everyone is at risk."
>
> *Michael Richmond, JD, The Horton Group*

Section 3:

TYPES OF CYBER LIABILITY COVERAGE

DESPITE THE POTENTIAL DEVASTATION THAT CYBER CRIME CAN CAUSE, 29 percent of businesses list cyber threats as one of the risks they are least prepared to face, according to the 2015 Travelers Business Risk Index. There are many steps to protect your company, including the deployment of frequently updated firewalls, regular assessment of your website for vulnerabilities and malware, restrictions on the use of unauthorized removable media devices, regular system backups, password policies, and employee education. It's equally important to have a cyber insurance policy.

"We're working with customers now to continuously improve their front-end protection, then adding insurance into the equation to make sure that if something slips through the cracks, then the company has insurance in place to pay for it," says Richmond. That can have significant consequences. The NetDiligence® 2015 Cyber Claims Study, which summarizes findings from 160 data breach insurance claims, estimates that data breach costs for an uninsured organization could be up to 30 percent higher than costs for an insured organization.

29 percent of businesses list cyber threats as one of the risks they are least prepared to face

Richmond recommends companies consider two primary types of coverage for cyber crimes: a cyber liability/data breach policy and a commercial crime policy.

Cyber Liability/Data Breach Policy

These policies can include third-party coverage, first-party coverage, and media liability. Third-party liability coverage offers protection against claims from vendors, clients, and others outside your company. The coverage often includes network and information security, as well as regulatory defense expenses and fines.

First-party liability coverage may pay for network business interruption, notification costs, crisis management, data restoration, and cyber extortion. "If you have a breach and can't operate your business, this would cover your loss of income," says Richmond. "It works in the same fashion as a property policy: If a fire burnt down your operation, it would cover the loss of income you sustain until you rebuild."

Media liability coverage protects your company against defamation, libel, slander, infringement of copyright, and invasion of privacy.

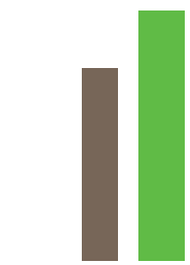
Cyber Liability Policy Example: Imagine if an employee inadvertently leaves a company laptop at the airport. The laptop contains protected health information for 300 employees and personal identifiable information for 5,000 customers. Customer information is used against them, leading to a class action lawsuit. Network security liability could pay the settlement or judgment fees, plus attorney expenses. In addition, the company would be required to notify all the individuals affected, and the cyber liability policy could pay related notification expenses.

Commercial Crime Policy

Some cyber attack exposure—particularly related to bank fraud—is not covered under a cyber liability policy, says Richmond. It requires a commercial crime policy. “Personal bank accounts are all protected. If someone gets into your personal account and steals funds, the bank has to reimburse you,” says Richmond. “But under the Uniform Commercial Code, the bank doesn’t have to pay back businesses for any losses if it was ‘commercially reasonable’ in protecting your account.”

Crime policies, in general, may cover fidelity, forgery or alteration, money orders and counterfeit money, computer crime, and funds transfer fraud. Within the area of computer crime and funds transfer fraud, the policy can be written to include the kind of phishing scams and corporate account takeover often assumed to be covered under a cyber liability policy.

Commercial Crime Policy Example: An advertising agency’s computer system is hacked by an employee of one of its customers, who changed the ad agency’s bank routing code in the system to her personal bank routing code. When the company paid the advertising agency for services rendered, the money went directly into the employee’s account instead. A commercial crime policy could cover this funds transfer fraud.



Data breach costs for an uninsured organization could be up to 30 percent higher than costs for an insured organization.

Source: NetDiligence 2015 Cyber Claims Study

General Liability Has You Covered . . . Maybe

In April 2016, a federal appeals court in Virginia upheld a district court ruling that a commercial general liability (CGL) may cover a data breach. The case centered around the publication of private medical records on the Internet. The United States Court of Appeals for the 4th Circuit ruled that Travelers Insurance was obligated to defend its customer, medical records safekeeping firm Portal Healthcare Solutions, who was the victim of the data breach. The court found that coverage was provided under the Personal & Advertising Injury section of the company's CGL policy.

"But the devil is in the details," says Richmond. "This case emphasizes the need for businesses to obtain standalone cyber coverage." First, the issue in this particular case is narrowly focused on the wording of Travelers' CGL policies in place during the breach. "It does not address cyber liability and its global applicability to general liability policies," says Richmond.

Many CGL policies only cover bodily injury and property damage—things caused by "tangible" means. Viruses, hacking, and other data breaches are electronic in nature and therefore deemed intangible. Plus, says Richmond, though the ruling sets a precedent for federal cases in the five states represented by the 4th Circuit, there's no guarantee that other federal courts will find the ruling persuasive.

"While this case provides an interesting perspective on how courts can view policies, the insurance carriers that provide those policies have already taken measures to prevent similar results, such as adding exclusions to policies limiting their liability for cyber-related losses," says Richmond. "Therefore, standalone cyber liability coverage remains an essential part of all risk management programs."

Section 4:

READING THE FINE PRINT IN A POLICY

THERE ARE TWO MAIN OPTIONS FOR COVERAGE: It can be endorsed to a package policy or be a standalone policy. Richmond says cyber policies that are endorsed to a package policy typically have limits (up to $500,000 or $1 million), contain more exclusions, and are "one-size-fits-all" policies. Standalone policies usually have higher limits, feature less exclusions, and are more comprehensive.

No matter what policy you choose, pay attention to the details and work with your insurance agent to customize boilerplate language in your favor. "The policy will only be as good as the work you put into it," says Richmond. He notes four things to look for:

- **Encryption exclusions** – Insurers will ask about your encryption protocols. "No matter what you state on the insurance application, a lot of times the insurer will still include an encryption exclusion," says Richmond. He recommends asking the insurance company to remove the exclusion, adding that most will do so if you are following protocol for encrypting devices.
- **Vendor exclusions** – "A lot of policies include vendor exclusions," says Richmond. "So if you sustain a breach, and it's from one of your vendors, there won't be coverage." The Target data breach in 2013, in which hackers stole millions of credit and debit card records of the store's customers, began with a malware containing email received by Target's HVAC contractor. The malware stole credentials to an online vendor portal Target provided to the HVAC contractor. This allowed hackers to access Target's network via the vendor portal. Try to remove vendor exclusions, says Richmond.
- **Exclusions for failure to update/maintain software** – "If companies aren't properly updating their malware protection, anti-virus software, or firewalls, then insurance carriers don't want to protect them," says Richmond. This is a tough exclusion to remove, he says. But you must use the most current protection software.
- **Record count restrictions** – Rather than set a monetary limit for coverage, some policies provide coverage for a certain number of records – up to 5,000 or 10,000. "For most businesses, your record threshold can go up and down," says Richmond. For instance, if you merge with another company, your records may double. Be sure to have adequate coverage for all your records.

Three Tips to Start Your Insurance Search

Michael Richmond, JD, offers three pointers for companies as they consider cyber liability insurance.

1. **Work closely with your insurance agent**. "Have a dialogue about your true risk, then go through the process of filling out an application," says Richmond. The applications can be lengthy, asking for details on your risk management protocols and practices. When completing the application, lots of companies realize they aren't doing enough to protect themselves. It provides a good reminder to step up your security measures.
2. **Get support from C-level executives.** "This decision and process needs to be taken out of the IT department and brought into the boardroom," says Richmond. "Cyber crime presents such a colossal exposure to the bottom line that CEOs, CFOs, COOs, and company boards need to be a part of the process, at least in the initial stages."
3. **Identify your exposure.** "What's the operation and critical piece of information that you need to protect?" asks Richmond. For example, a restaurant needs to protect the customer credit card numbers it has on file. If the restaurant has 100,000 records, multiply that by $230 – the average cost per record after a breach. The restaurant could face approximately $23 million in costs if a breach occurs.

In Summary

"IF A DATA BREACH HAPPENS, HOW WOULD YOUR COMPANY PAY for the damages?" asks Richmond. It's this question that should impel businesses to investigate and purchase cyber liability insurance. One final finding from the NetDiligence 2015 Cyber Claims Study may sway your decision: The average claim reported was more than $673,000, with the top one hitting $15 million.

"It's my job to convince companies that they have exposure and need to invest in a cyber liability policy," says Richmond. "Hopefully one or two years from now it will be commonplace. Companies will just buy it like they do property and general liability insurance."

The average claim reported was more than $673,000

Assurex™ GLOBAL

assurexglobal.com

Founded in 1954, Assurex Global is an exclusive Partnership of the most prominent independent agents and brokers in the world. With $28 billion in annual premium volume and more than 600 Partner offices, Assurex Global is the world's largest privately held commercial insurance, risk management and employee benefits brokerage group. An international insurance powerhouse, the Partnership combines the local expertise and global reach of international brokers on six continents.