

# Small business, big risk: Lack of cyber insurance is a serious threat

October 2018



**INSURANCE  
INFORMATION  
INSTITUTE**

**J.D. POWER**

Sean Kevelighan  
Chief Executive Officer  
Insurance Information Institute  
[seank@iii.org](mailto:seank@iii.org)

James Lynch, FCAS, MAAA  
Chief Actuary  
Insurance Information Institute  
[jamesl@iii.org](mailto:jamesl@iii.org)

Jessica McGregor  
Strategy and Growth Director, Global Insurance Practice  
J.D. Power  
[jessica.mcgregor@jdpa.com](mailto:jessica.mcgregor@jdpa.com)

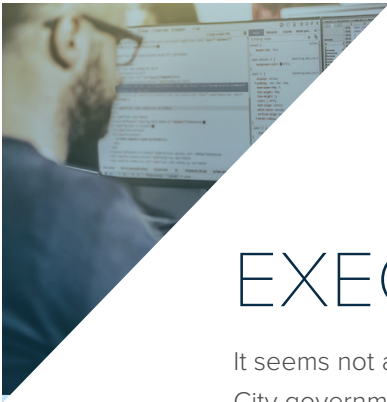
David Pieffer  
Property & Casualty Insurance Practice Lead  
J.D. Power  
[david.pieffer@jdpa.com](mailto:david.pieffer@jdpa.com)



# TABLE OF CONTENTS

	<i>Page</i>
Executive Summary.....	3
Cyberrisk: Business Perceptions and Reactions .....	4
Data Breaches and How Insurance Helps.....	5
The Current State of Cyber Insurance Among Commercial Insureds .....	6
The Cyber Insurance Market Has Growth Potential .....	7
Current Insurance Offerings for Cyber Coverage .....	8
Conclusion.....	8
Sources and Endnotes.....	10





# EXECUTIVE SUMMARY

It seems not a day goes by without another disclosure of a major cybersecurity incident. City governments getting shut down.<sup>1</sup> Millions of people's personally identifiable information compromised.<sup>2</sup> Entire energy grids at risk of hacking.<sup>3</sup> The cost of these incidents is staggering. One estimate pegs cyberattack losses in the United States at between \$57 billion and \$109 billion in 2016.<sup>4</sup>

While most small business leaders are aware of the risks, they don't think the threat will reach them, according to an Insurance Information Institute (I.I.I.) and J.D. Power *2018 Small Business Cyber Insurance and Security Spotlight Survey*<sup>SM</sup> conducted in July 2018. According to the survey, 10 percent of firms surveyed suffered one or more cyber incidents in the prior year, and the average cost of cyber-related losses over the past year was \$188,400, an increase of \$73,000 from the J.D. Power 2016 Cyber Insurance Pulse Study<sup>SM</sup>.

About one-third of firms surveyed had cyber insurance, a relatively new type of coverage, the terms of which vary widely from insurer to insurer. Of those without cyber coverage, one quarter indicated they were probably or definitely likely to purchase a cyber insurance policy in the next 12 months.

This spotlight survey is part of the alliance between J.D. Power and the I.I.I. to measure how small businesses in the U.S. are reacting to growing cyber threats. The survey reached 536 respondents, comprised of small businesses from across various industries and sectors (85 percent), and insurance brokers, agencies, carriers and third-party suppliers (15 percent). Of firms measured in this survey, 91 percent had 50 or fewer employees. In terms of operating size, 59 percent of firms had an annual operating revenue/budget of less than \$1 million, 18 percent had \$1 million to \$2.49 million, 21 percent had \$2.5 million or higher and 2 percent did not report it.

# CYBERRISK: BUSINESS PERCEPTIONS AND REACTIONS

According to the Spotlight Survey:

**Most businesses are concerned about the cyberrisks facing their organization.** Nearly 60 percent of respondents said that their company is very concerned about cyber incidents – and 70 percent think that the risk of being victimized by a cyberattack is growing at an alarming rate. Moreover, nearly half of respondents said their company is not fully equipped to handle cybersecurity threats.

**Business risk profile and premium costs are the top reasons why business don't hold cyber coverage.** 59 percent of businesses do not have cyber coverage, with the top three reasons being: their business risk profile does not warrant coverage (42 percent); the premiums are too expensive (36 percent); or they felt that the risk is sufficiently handled internally (27 percent).

**Potential impacts to a business as a result of a cyber incident in rank order are financial loss (47 percent), information breach/theft (35 percent), reputation/brand image issues (14 percent), and regulatory/governance and legal issues (4 percent).** Looking specifically at financial losses, businesses were most concerned with direct financial losses (71 percent) and, to a lesser extent, indirect financial losses (29 percent).

**Recent data protection regulations are impacting some operations.** In May 2018 the new General Data Protection Regulation (GDPR) came into force in the European Union. The GDPR governs the processing of personal data by professional or commercial organizations.<sup>5</sup> California recently

## A Quick Primer on Commercial Cyber Insurance

Commercial general liability insurance policies usually exclude damages arising out of losses of electronic data because electronic data often isn't considered "tangible" property.

Companies can best protect themselves from cyber-related financial losses with a specific cyber insurance policy. These typically offer liability coverage (and sometimes partial property coverage) for losses related to data breaches. Most of these policies cover a commercial insured's losses related to the loss of personally identifiable information and expenses from a data breach. These expenses can include legal expenses, investigating a breach, notifying people affected by the breach, managing the insured's reputation and other crisis-management expenses, and recovering lost or corrupted data.



Some policies also offer coverage for business interruption losses – losses related to expenses and lost revenue resulting from a breached system. Others may also offer "cyberextortion" coverage, which covers costs resulting from an extortion event such as ransomware. It's important to note that this is a relatively new market, so policies may differ widely on the specific policy terms and conditions.



passed legislation that some have argued is similar to the GDPR, in that it also regulates the use of personal data for commercial purposes.<sup>6</sup> Other states have legislation addressing data breach notifications.<sup>7</sup> Ten percent of the businesses surveyed said that they are affected by regulations governing reporting of data breaches of personally identifiable information, and another 13 percent were unsure whether they were impacted. To help comply with these regulations, impacted businesses indicated they were taking internal action, including: purchasing encryption programs (53 percent); hiring a data protection consultant or firm (45 percent); having a chief data protection officer in place (33 percent); and developing a reporting process to meet regulatory reporting requirements (33 percent).

**Compliance changes and IT improvements are being implemented.** Forty-two percent of the respondents said they are implementing compliance changes to address cyberrisks. Thirty-one percent have recently improved IT security measures. Only 25 percent have instituted an employee cyberrisk training program, and even fewer respondents (19 percent) had an incident response plan. However, research from the Ponemon Institute found that cyberrisk training may yield significant results: a recent survey found that 54 percent of small businesses identified negligent employees as the root cause of data breaches.<sup>8</sup>

## DATA BREACHES AND HOW INSURANCE HELPS

**Cyber incidents hit small businesses roughly as often as drivers suffer auto accidents.** The survey found that 10 percent of respondents said they have experienced at least one cyber incident in the prior year. A similar percent of auto insurance customers filed a collision claim last year.<sup>9</sup> Cyber-related losses over the past year were about \$188,400 on average per company according to the survey, an increase of \$73,000 from the J.D. Power 2016 Cyber Insurance Pulse Study<sup>SM</sup>.

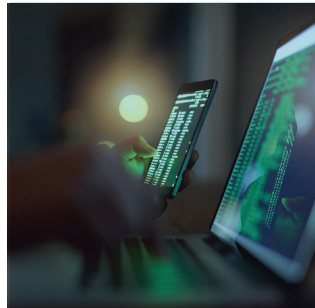
**Of businesses that were hacked and had cyber insurance, 97 percent said their insurance was adequate to cover their losses.**

**Business interruption is the most common type of loss from a cyber incident.** Of the 10 percent of companies that had experienced a cyber incident in the past year, 44 percent reported losses from business interruption. Another 33 percent said that they suffered losses from data loss or corruption. Twenty-three percent said they suffered losses from data breaches.

**Nearly everyone affected said their cyber insurance was adequate.** The majority of small businesses that experienced a cyberattack and had cyber coverage indicated that their insurance adequately covered their losses (97 percent). 76 percent of businesses with an incident – but without cyber coverage – said that their internal mitigation efforts were adequate to address the cyber loss, leaving 24 percent exposed to losses without insurance or adequate mitigation.

## THE CURRENT STATE OF CYBER INSURANCE AMONG COMMERCIAL INSURED

**Businesses with cyber insurance often have similar coverages.** About two-thirds of respondents who say they have cyber insurance have some sort of coverage for: loss or corruption of data, business interruption and liability. More than half have data breach and identity theft coverage, while another third have cyber extortion and cloud computing coverage. Twenty-five percent



68% percent of respondents who had cyber insurance said their insurer helps with some form of cyberrisk mitigation.

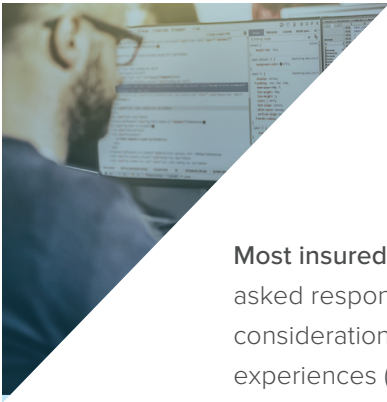
have crisis management and directors and officers/management liability coverage.

**Insurers typically offer additional services.** Sixty-eight percent of respondents who had cyber insurance said their insurer helps with some form of cyberrisk mitigation. Forty

percent said their insurer offers contingency planning for data breaches, and 51 percent said their insurer offers a risk assessment of their business's vulnerability to data breaches.\* As Sean Kevelighan, president and CEO of the I.I.I. recently noted, "We are seeing many carriers partner with technology companies in order to assess the actual vulnerabilities within the customers' [profiles]. This presents more stability for underwriting. Customer value may evolve in the future toward risk mitigation and resilience building."<sup>10</sup>

**Cyber coverage is usually combined with other coverages.** Sixty-five percent of insured businesses said their coverage is combined with other, non-cyber coverages. Thirty-three percent have stand-alone coverage. How insured businesses determined their coverage needs was evenly split among in-house risk assessments (45 percent), insurer assessments (42 percent), and broker or third-party assessments (42 percent).\*


\*Note: survey participants were permitted to choose more than one answer.



**Most insureds have average satisfaction with their cyber insurance policies.** The survey asked respondents to rate their cyber coverage experience on a scale of 1 to 10, taking into consideration the policy coverages and costs, and customer service and claims processing experiences (if applicable). The average satisfaction rating for cyber insurance programs was 7.19. The policy retention rate is relatively strong: 80 percent have not switched their cyber insurer in the past five years.

## THE CYBER INSURANCE MARKET HAS GROWTH POTENTIAL

**Cyber insurance uptake is still a work in progress.** Only 31 percent of respondents said they have cyber insurance – and 70 percent of respondents said they don't plan to purchase a cyber insurance policy in the next 12 months. "Insurers have the opportunity to add incredible value for their small business customers through proper education, training and risk assess-



About one-third of firms surveyed had cyber insurance. 70% do not plan to purchase coverage in the next year.

ment services regarding cybersecurity. This survey found it is still a poorly understood and underpenetrated coverage with valuable future growth opportunities for the insurance industry," noted Jessica McGregor, Director of Insurance at J.D. Power.

**Many businesses say they don't need coverage.** As noted, forty-two percent of all respondents said their current risk profile doesn't warrant cyber insurance.

Others aren't sold on the value proposition: 36 percent said the coverages currently available in the marketplace are too expensive, and 19 percent said there are too many exclusions. Twenty-seven percent believe that cyberrisks are sufficiently handled internally.

**But many don't think they can handle threats.** Forty-six percent of respondents do not think that their business is fully equipped to handle cyberthreats, but not for lack of trying: The same amount stated that their business is actively pursuing ways to combat these threats.

**Cyber insurance is still poorly understood.** Only 32 percent of respondents said that they believe their business is very familiar with the cyber insurance coverage options available.



# CURRENT INSURANCE OFFERINGS FOR CYBER COVERAGE

Fifteen percent of the respondents are involved in insurance activities, including insurance brokers, agencies, carriers and third-party suppliers.

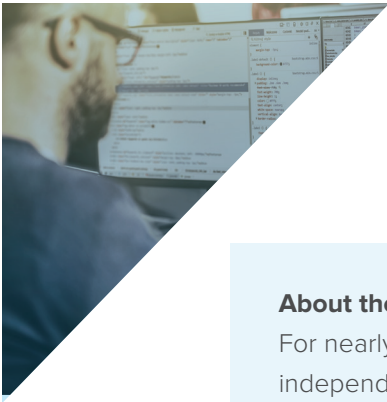
**Many offer cyber insurance or services.** Forty-six percent of insurance respondents said that they currently provide cyber insurance or cyber-related services. Of these, the top coverages provided address identity theft (43 percent), business interruption (41 percent), data breach protection (36 percent) and liability coverage (33 percent).

**And many of their clients ask about cyber insurance products.** Forty-six percent of insurance respondents also said that their clients ask about cyber insurance. Thirty-six percent plan to offer some form of cyber insurance in the next year.

## CONCLUSION

Small businesses are not immune from cyberrisks and these businesses are increasingly aware of this threat. As these risks facing their business increase, so will their need for cyber insurance increase, offering a potential growth area for insurers as more small commercial clients begin seeking cyber coverages for their businesses. Education of current and future clients is critical to help them understand both the value and need for cyber coverage, even if they initially think they do not need it. Nearly one-quarter of respondents that had a cyber breach without insurance coverage did not have sufficient internal mitigation plans in place to protect themselves. Insurers have an opportunity to bring both value and security to their small business customers as long as they can help clients understand how cyber coverages work.





### **About the Insurance Information Institute**

For nearly 60 years, the Insurance Information Institute (I.I.I.) has been the leading independent source of objective information, insight, analysis and referral on insurance for a wide range of audiences, including: Consumers, insurance professionals, the media, government and regulatory organizations, educational institutions and students. The I.I.I.'s mission is to improve public understanding of insurance—what it does and how it works. The I.I.I. is an industry supported organization, but does not lobby for insurance businesses; instead, our central function is to provide accurate and timely information on insurance subjects.

### **About J.D. Power**

J.D. Power is a global leader in consumer insights, advisory services and data and analytics. These capabilities enable J.D. Power to help its clients drive customer satisfaction, growth and profitability. Established in 1968, J.D. Power is headquartered in Costa Mesa, Calif., and has offices serving North/South America, Asia Pacific and Europe. J.D. Power is a portfolio company of XIO Group, a global alternative investments and private equity firm headquartered in London, and is led by its four founders: Athene Li, Joseph Pacini, Murphy Qiao and Carsten Geyer.





## Sources and Endnotes

1. Kimberly Hutcherson, *CNN*, “Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand,” March 27, 2018.
2. U.S. Federal Trade Commission, Consumer Information, “The Equifax Data Breach: What to Do,” September 8, 2017.
3. Dustin Volz and Timothy Gardner, “In a first, U.S. blames Russia for cyber attacks on energy grid,” March 15, 2018.
4. U.S. Council of Economic Advisors, “The Cost of Malicious Cyber Activity to the U.S. Economy,” February 2018.
5. European Commission, “What does the General Data Protection Regulation (GDPR) govern?”
6. Daisuke Wakabayashi, *New York Times*, “California Passes Sweeping Law to Protect Online Privacy,” June 28, 2018.
7. National Conference of State Legislatures, “Security Breach Notification Laws,” March 29, 2018.
8. Ponemon Institute, “2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB),” September 2017.
9. ISO, Fast Track, “Private Passenger Automobile Fast Track Data: First Quarter 2018,” July 3, 2018.
10. *Insurance Journal*, “The E-merging Risk that Keeps on E-volving: Cyber,” September 3, 2018.