

While small companies recognize the growing cyber threat, many remain reluctant to insure against it

October 2019



J.D. POWER

Sean Kevelighan Chief Executive Officer Insurance Information Institute seank@iii.org

James Lynch, FCAS, MAAA Chief Actuary Insurance Information Institute jamesl@iii.org

David Pieffer
Property & Casualty Insurance Practice Lead
J.D. Power
david.pieffer@jdpa.com

TABLE OF CONTENTS

| | Page |
|--|------|
| Executive summary | 3 |
| Increased focus on smaller targets | 4 |
| Resistance to cyber insurance remains | 5 |
| Business interruption still most common type of loss | 8 |
| Regulatory impact | 9 |
| Compliance changes and IT improvements | 9 |
| Coverage called "adequate" | 10 |
| Conclusion | 11 |
| Sources and endnotes | 12 |

EXECUTIVE SUMMARY

While cyberattacks against large enterprises, compromising massive amounts of personal customer data, continue to consume media attention, small-business leaders would be well advised to focus on the evolving risks targeting their companies.

According to the Insurance Information Institute (I.I.I.) and J.D. Power 2019 Small-Business Cyber Insurance and Security Spotlight SurveySM, 12 percent of businesses that responded had experienced at least one cyber incident in the past year, up from 10 percent in 2018. Nearly 71 percent said they are "very concerned" about cyber incidents, up from 59 percent in 2018, and 75 percent said they believe the risk of being victimized by a cyberattack is growing at an alarming rate – up from 70 percent in 2018.

Nevertheless, getting small companies to purchase coverage remains a challenge.

Based on a survey of more than 500 small business leaders, insurers, and insurance service providers across the United States, this paper discusses the rising awareness among small business owners that they, too, are vulnerable to evolving cyberattacks. It addresses some of the reasons for their continued reluctance to buy cyber insurance and discusses cyber-related loss trends and what small firms and their insurers are doing to address these perils.

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 cyberthreats. The survey reached 531 respondents, consisting of small businesses from across various industries and sectors (63 percent), and insurance brokers, agencies, carriers, and third-party suppliers (37 percent). Of firms measured, 75 percent had 50 or fewer employees. Forty-five percent had an annual operating revenue/budget of less than \$1 million; 16 percent had \$1 million to \$2.49 million; 28 percent had \$2.5 million or higher; and 11 percent did not report it.

Increased focus on smaller targets

Smaller companies are uniquely vulnerable, and cybercriminals know it. Larger enterprises can devote more attention and resources to security and employee training. This makes smaller firms and high-net-worth individuals lower-risk targets for criminals. Less-sophisticated enterprises may become even easier marks as the Internet of Things (IoT) evolves, creating more – often less well protected – access points for hackers.

With 25.8 billion IoT devices <u>predicted</u> to be connected to the internet by 2022¹, the risks and potential costs will only increase. In one case, for example, hackers acquired information from a casino's database by way of an internet-connected <u>fish tank</u>. <u>Smart light bulbs</u> also have been identified as potentially providing points of access for those who mean to do harm.



Less-sophisticated enterprises may become even easier marks as the Internet of Things evolves.

Cyberrisks constantly evolve.
Threats from past years fade while new ones emerge, and the rate of technological change makes it hard for busy small business leaders to keep up. The latest threat? Ransomware. Extortionists take advantage of Bitcoin and other crypto-currencies that allow ransom demands to be made and paid anonymously.

For example, a small Battle Creek, Michigan, medical practice recently <u>fell victim</u> to a ransom-ware attack. The two-doctor practice lost access to medical records, billing, scheduling, and other critical documents after attackers encrypted the data. Rather than pay a \$6,500 ransom for a decryption key or try to restore the data themselves, the doctors decided to retire early and close the practice for good.²

Seven percent of respondents to this year's I.I.I./J.D. Power survey reported losses related to cyber extortion.

Cryptocurrency has spawned its own form of cybercrime. Cryptojacking is a process by which criminals hijack personal or work computers to "mine" for cryptocurrency – basically outsourcing computing power and energy demands to unwitting third parties. Cryptojacked systems can cause serious performance issues and result in costly downtime as an IT team works to identify and resolve the issue. Technological and procedural approaches can mitigate these risks, and cyber insurance can help companies reduce the impact of losses.³

Emerging threats like "deepfake" technology, in which manipulated video and audio can impersonate an individual, further complicate the perils of cybercrime.⁴ In a chilling recent example, criminals used artificial intelligence (Al)-based software to impersonate a chief

executive officer's voice to request a fraudulent €220,000 (US \$243,000) transfer from a vendor.⁵ Another danger that recently received attention is the use of innocent-looking USB cables to transmit malware.⁶

"To remain relevant in an increasingly interconnected and cyber-vulnerable world, we are seeing more insurers work with commercial customers to mitigate risks – in particular, with small and mid-size businesses," said Sean Kevelighan, president and CEO of the Insurance Information Institute. "We know many of the large cyber incidents can be sourced back to a smaller business or vendor, and, thus, it's increasingly critical to assist in loss prevention measures that can make the customer more resilient, while also reducing claims and damages overall."

Among the small company owners responding who said they had cyber coverage, 70 percent said their insurer helps with some form of cyberrisk mitigation (up from 65 percent in 2018). Fifty-one percent said their insurer offers contingency planning for data breaches, up from 40 percent in 2018, and 53 percent said their insurer offers a risk assessment of their business's vulnerability to data breaches, up from 51 percent in 2018.

Resistance to cyber insurance remains

Despite increasing awareness and concern among small companies, getting them to buy coverage remains an uphill battle.



Of the small business leaders surveyed, 42% said their company is not fully equipped to handle cybersecurity threats.

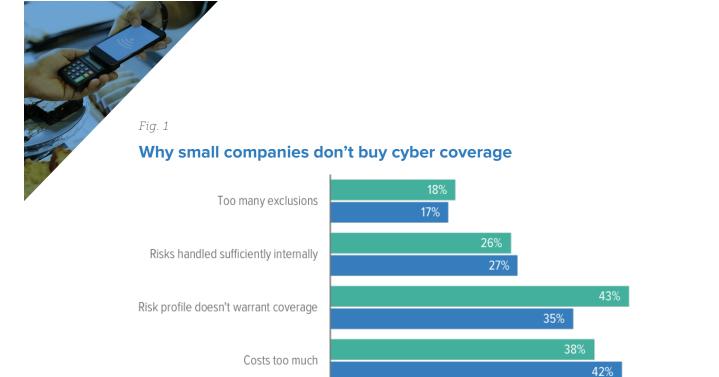
About 35 percent of all firms surveyed said they have cyber insurance, up from 31 percent in 2018. Of those without cyber coverage, 36 percent indicated they were "probably" or "definitely" likely to purchase a cyber insurance policy in the next 12 months, up from 30 percent in 2018.

But among the 44 percent of respondents who said they do not currently have cyber insurance and the 21 percent who said they do not know whether they do, 64 percent said they do not plan to purchase a cyber insurance policy in the next 12 months.

While this is down from 70 percent in 2018, it remains a concerning number.

Why do many small companies seem reluctant to buy cyber coverage, despite the widespread recognition of cyberrisk? (Figure 1)

Of the small business leaders surveyed, 42 percent said their company is not fully equipped to handle cybersecurity threats, down from 46 percent in 2018. Looking at it another way, small businesses' confidence about their ability to handle cyberrisks was higher in 2019 than in 2018, despite the growing concerns and increased number of attacks.



Source: 2019 Small-Business Cyber Insurance and Security Spotlight SurveySM, August 2019.

0%

This confidence is reflected in the fact that 38 percent of respondents said they believe their business is "very familiar" with the cyber insurance coverage options available – up from 28 percent in 2018. It also correlates with the one percent increase, from 26 percent to 27 percent, in companies responding that cyberrisks are "handled sufficiently internally."

10%

2018

20%

2019

30%

40%

50%

Is that confidence justified? Perhaps not, according to a recent survey of underwriters and brokers.

In the <u>Advisen/Partner Re survey</u>, 75 percent of underwriters and brokers said the primary obstacle to sales continues to be a lack of understanding about the exposure. The second-highest response (56 percent) was clients "not understanding the coverage."⁷

The report went on to say that in some cases, "respondents felt that the issue was one of overconfidence and belief by insureds that they don't have the type of data cybercriminals would be interested in stealing. Many organizations forget...that cyberrisk increasingly involves more than just [a] data breach and is not just a problem for larger companies."

This confidence (or overconfidence, depending on your perspective) does not seem to be confined to U.S. businesses. A recent Chubb <u>survey of Australian companies</u> found that 60 percent of small to medium-sized companies have experienced a cyberattack in the past 12 months – the same percentage that responded that they believe they are better prepared for an attack than their larger competitors.⁸ A Chubb <u>survey of firms in Singapore</u> reported similar findings.⁹

Whether you believe the small business owners or the underwriters and brokers, one thing is clear from the I.I.I./J.D. Power results: two of the top four reasons – pricing and exclusions – small companies give for passing on cyber coverage lay squarely in the hands of insurers.

"Given small companies' growing awareness and concerns about cyberrisk, insurers and agents and brokers might be able to increase their overall support of this market by addressing the issues of affordability and coverage limitations that seem to be an obstacle to purchasing," said J.D. Power Vice President, Head of the Property & Casualty Insurance Practice David Pieffer. "Changing company owners' perception that they don't need coverage may require a longer-term education strategy and coordination between agents and broker and the insurers."

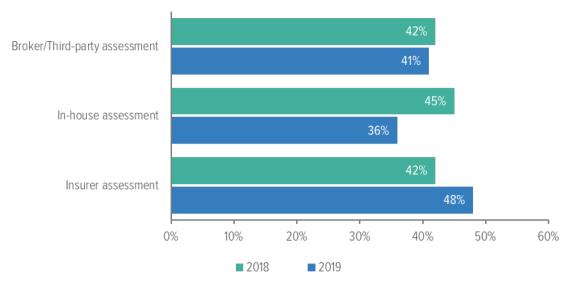
Part of that education might include the size of the financial and reputational risks cyber incursions present. For example, a <u>recent study</u> by Bank of America Merchant Services found that 41 percent of small businesses surveyed that had suffered a data breach paid more than \$50,000 to recover. This was up from 31 percent of small businesses two years ago.

Not only could such a loss be devastating to many small businesses, the Bank of America study further found that 29 percent of small-business customers surveyed said they would never go back to a firm that has had a data breach. This was an increase from 20 percent two years ago.¹⁰

In 2019, 48 percent of small businesses responding to the I.I.I./J.D. Power survey said they determined their cyber insurance needs based on their insurers' assessments, up from 42 percent in 2018. The number of firms basing their decisions on in-house or third-party assessments declined from 2018 to 2019. (Figure 2)

Fig. 2

How small businesses determine their insurance needs



Source: 2019 Small-Business Cyber Insurance and Security Spotlight SurveySM, August 2019.

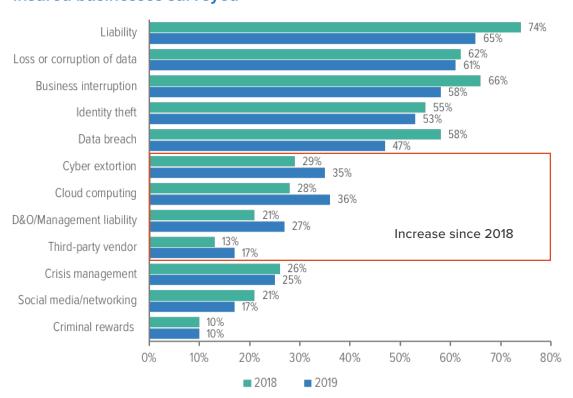
Business interruption still most common type of loss

Of the respondents that had experienced a cyber incident in the past year, 41 percent reported losses from business interruption (down from 44 percent in 2018). About 35 percent said they suffered losses from data loss or corruption (up slightly from 33 percent in 2018), and 24 percent said they suffered losses from data breaches (up from 23 percent in 2018).

The most common coverages in cyber policies held by insured businesses surveyed were for: liability (65 percent), loss or corruption of data (61 percent), and business interruption (58 percent). (Figure 3)

Fig. 3

Coverages common to cyber policies held by insured businesses surveyed



Source: 2019 Small-Business Cyber Insurance and Security Spotlight SurveySM, August 2019.

Potential impacts to a business as a result of a cyber incident in rank order are:

- Financial loss (43 percent)
- Information breach/theft (38 percent)
- Reputation/brand image issues (13 percent)
- Regulatory/governance and legal issues (5 percent).

Looking specifically at financial losses, businesses were most concerned with direct financial losses (70 percent) and, to a lesser extent, indirect financial losses (30 percent) in 2019 – roughly the same breakdown as in 2018.

Regulatory impact

Of the businesses surveyed, 11 percent said they are affected by regulations governing reporting of data breaches of personally identifiable information (up slightly from 10 percent in 2018), and another 16 percent were unsure whether they were affected (compared to 13 percent in 2018). Respondents address these regulatory requirements in a variety of ways, as indicated below. (Figure 4)

Fig. 4

How respondents are addressing regulations on breaches involving personally identifiable information



Source: 2019 Small-Business Cyber Insurance and Security Spotlight Survey[™], August 2019.

Compliance changes and IT improvements

Forty-eight percent of respondents to the I.I.I./J.D. Power survey said they are implementing compliance changes to address cyberrisks (up from 42 percent in 2018). Thirty-eight percent have recently improved IT security measures (up from 31 percent in 2018). Thirty-six percent have instituted an employee cyberrisk training program, up from 25 percent in 2018, and 24 percent of respondents had an incident response plan, up from 19 percent in 2018.

Even so, a recent <u>Ponemon Institute study</u> found that "human error and system glitches" remain the root cause of 49 percent of cyber breaches.

"Human error as a root cause of a breach includes 'inadvertent insiders' who may be compromised by phishing attacks or have their devices infected or lost/stolen," the Ponemon report says. "These were responsible for about one-quarter of breaches. System glitches, or inadvertent failures that could not be tied to a human action, accounted for another quarter of breaches."¹¹

Coverage called "adequate"

Nearly all respondents surveyed by I.I.I./J.D. Power called their cyberrisk mitigation "adequate."

Most firms that experienced a cyberattack and had cyber coverage indicated that their insurance adequately covered their losses (90 percent, down from 97 percent in 2018). Among those that had an incident and did not have cyber insurance, 89 percent said their



businesses surveyed that experienced a cyberattack and had cyber coverage indicated that their insurance adequately covered their losses

internal mitigation efforts were adequate to address the cyber loss (up from 79 percent in 2018). This leaves 11 percent of those surveyed exposed to losses without insurance or adequate mitigation.

Most resondents 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 policy coverages and costs, customer service, and claims processing experiences (if

applicable). The "average satisfaction" rating for cyber insurance programs was 7.67, up slightly from 7.19 in 2018. The policy retention rate is relatively strong: 84 percent have not switched their cyber insurer in the past five years, down from 83 percent in 2018.

Of the survey respondents that offer insurance services, 46 percent said they currently provide cyber insurance or cyber-related services, unchanged since 2018. Of these, the top coverages provided address:

- Loss/corruption of data (35 percent, up from 26 percent in 2018)
- Business interruption (35 percent, down from 41 percent in 2018)
- Liability coverage (31 percent, down from 33 percent in 2018)

Among these respondents, 39 percent said their clients ask about cyber insurance (down from 46 percent in 2018) and 25 percent said they plan to offer some form of cyber insurance next year (down from 36 percent).

CONCLUSION

Threats from cyberattacks and system failures are not diminishing. As IoT, Al-driven engagement, and cashless transactions become more commonplace, the risks small business owners face, along with larger businesses and individuals, from digitally empowered bad actors are likely to increase in number and cost; evolve in complexity and diversity; and become less distinct from risks traditionally associated with property and business interruption.

Large enterprises have the resources to address and perhaps even head off some of these evolving risks. Small companies, however, often are less well equipped to defend themselves effectively against cyber-related perils. Given the potentially life-threatening costs of cyber events, insurance coverage may be even more important to these companies than to their larger, better funded counterparts. Improving small businesses' understanding of coverages and protections is an important step toward closing the gap.

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 has offices serving North America, South America, Asia Pacific and Europe.

Sources and Endnotes

- 1. Natalie Gagliordi, *ZDNet*, "<u>IoT to Drive Growth in Connected Devices Through 2022:</u> Cisco," November 27, 2018.
- 2. Marianne Kolbasuk McGee, *Bank Info Security*, "Medical Practice to Close in Wake of Ransomware Attack," April 2, 2019.
- 3. Dan Twersky, Willis Towers Watson, "<u>Cryptojacking: Ransomware's Sneaky Cousin is the New Kid on the Cyber Block</u>," January 18, 2019.
- 4. Tonya Mosely, *Here & Now*, "Perfect Deepfake Tech Could Arrive Sooner Than Expected," October 2, 2019.
- 5. Tim Sloane, *Payments Journal*, "<u>It Happened! Al Deep Fake Mimicked a CEO's Voice and Stole €220,000,"</u> October 4, 2019.
- 6. Charanjeet Singh, *Fossbytes*, "<u>USBHarpoon: How 'Innocent' USB Cables Can Be</u> Manipulated To Inject Malware," August 21, 2018.
- 7. PartnerRe/Advisen, "2018 Survey of Cyber Insurance Market Trends," October 2018.
- 8. Chubb, "Too Small to Fail? Australia SME Cyber Preparedness Report," February 2019.
- 9. Chubb, "Too Small to Fail?" Singapore SME Cyber Preparedness Report," January 2019.
- 10. Bank of America Merchant Services, "Small Business Payments Spotlight," Fall 2019.
- 11. Larry Ponemon, Security Intelligence, "2019 Cost of a Data Breach Report," July 23, 2019.