



Protecting against #cyberfail:

# SMALL BUSINESS AND CYBER INSURANCE

*November 2017*



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

Claire Wilkinson  
Consultant  
clairew@iii.org

[www.iii.org](http://www.iii.org)



# TABLE OF CONTENTS

	<i>Page</i>
Executive summary.....	3
I. The threat to small business.....	4
II. Growing appetite for insurance among SMBs .....	9
III. Cyber insurance solutions for SMBs .....	10
IV. Risk management/loss control services .....	12
V. Claims costs on the rise? .....	13
Conclusion .....	14
Resources.....	15
Sources and endnotes.....	16





# EXECUTIVE SUMMARY

While cyberattacks and data breaches at Fortune 500 companies tend to dominate the headlines, America's more than 28 million small businesses and their 56 million employees are increasingly vulnerable. Their exposure is much the same as that of larger companies, experts say, but many may overlook or underestimate the threat and may not fully understand the risks.

Small businesses (defined as firms with fewer than 250 employees) face a growing frequency of attacks and breaches which can result in potentially severe financial consequences. This paper will explore the cyberthreat landscape for small- and mid-sized businesses (SMBs), their growing appetite for insurance, how claims costs are unfolding, and how insurers are developing products and risk management solutions to help build resilience.

- Half of all SMBs in the U.S. experienced a data breach in the past year, and 55 percent experienced a cyberattack.
- Nearly 40 percent of businesses have experienced a ransomware attack in the last year, and of these, more than one-third lost revenue.
- Only 14 percent of small companies rated their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.
- Larger companies are more likely to purchase insurance coverage than smaller organizations, but appetite for coverage is increasing among SMBs as companies of all sizes become more aware of their exposures. In response insurers are developing dedicated, affordable cyber insurance products.
- Risk prevention and mitigation services are an increasingly important part of the offering made by cyber insurers to their policyholders as they look to build and encourage resilience.



# I. THE THREAT TO SMALL BUSINESS

From restaurants, to medical offices, to mom-and-pop shops, the reality is that no business is too small to evade a cyberattack or data breach. A 2014 attack on JPMorgan Chase compromised the accounts of seven million small businesses as well as 76 million households, for example.<sup>1</sup>

Such incidents can result from a wide range of causes, including hackers, malware/virus, malicious insiders, lost or stolen laptops and employee error.

Attacks and breaches have grown in frequency, and loss costs are on the rise. The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) reports that losses from cybercrimes totaled \$1.3 billion in 2016. The Center received close to 300,000 complaints during the year from hacking victims.<sup>2</sup>

The majority of the 1,093 data breaches tracked in 2016 affected the business sector, with 494 breaches or 45.2 percent of the total number of breaches impacting companies, according to the Identity Theft Resource Center.<sup>3</sup> These figures do not include the many attacks that go unreported or undetected.

Half of all SMBs in the U.S. experienced a data breach in 2016, and 55 percent experienced a cyberattack, according to the Ponemon Institute.<sup>4</sup> In the aftermath of an incident, SMBs spent an average of \$879,582 due to damage or theft of IT assets, based on extrapolated calculations. In addition, disruption to normal operations cost an average of \$955,429.

Negligent employees or contractors and third parties caused most data breaches experienced by SMBs. However, almost one-third of companies in the Ponemon survey could not determine the root cause (**Figure 1**).

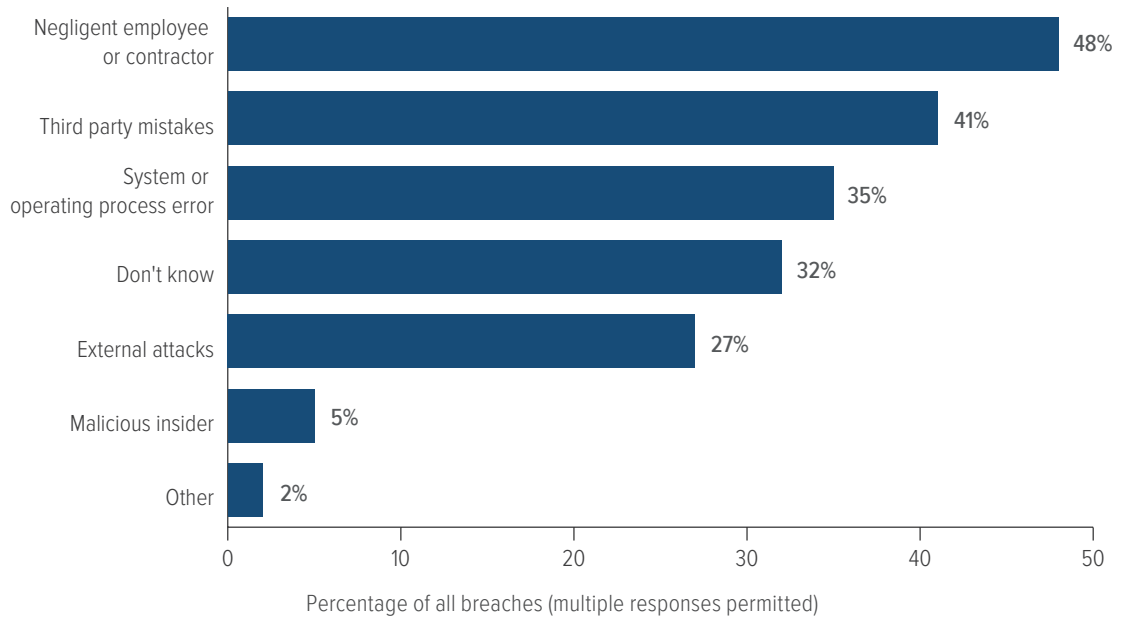
Both small and large businesses have a notification obligation in the event of a data breach, with 48 U.S. states enforcing laws that mandate breach notifications. State laws have various requirements, but in general, a business owner must investigate a breach of personal information and notify affected individuals promptly. Fines and penalties can be thousands of dollars per breach.

The bulk of reported losses involves breaches that expose personal identifiable information (PII), often because of these legal notification requirements, according to Deloitte.<sup>5</sup>



Fig. 1

### Data breaches of SMBs by root cause, 2016



Source: Ponemon.

## Types of cyberattacks

A special analysis of data performed for the Insurance Information Institute by Advisen Ltd. shows that for businesses with fewer than 250 employees, cyber-related incidents have been increasing since 2010. Of all the cyber incidents tracked by Advisen Ltd., attacks against SMBs represent approximately 40 percent<sup>6</sup> (Figure 2).

Malicious breaches<sup>7</sup> account for the greatest share of attacks tracked by Advisen Ltd., and represent the top type of cyber incident targeting SMBs over time. By event type, “Privacy violations: unauthorized contact or disclosure”<sup>8</sup> incidents have shown the largest long-term growth. Conversely, Advisen Ltd. has seen a reduction in events involving physical loss of data, in part because of the increasing amount of data stored online (Figure 3).

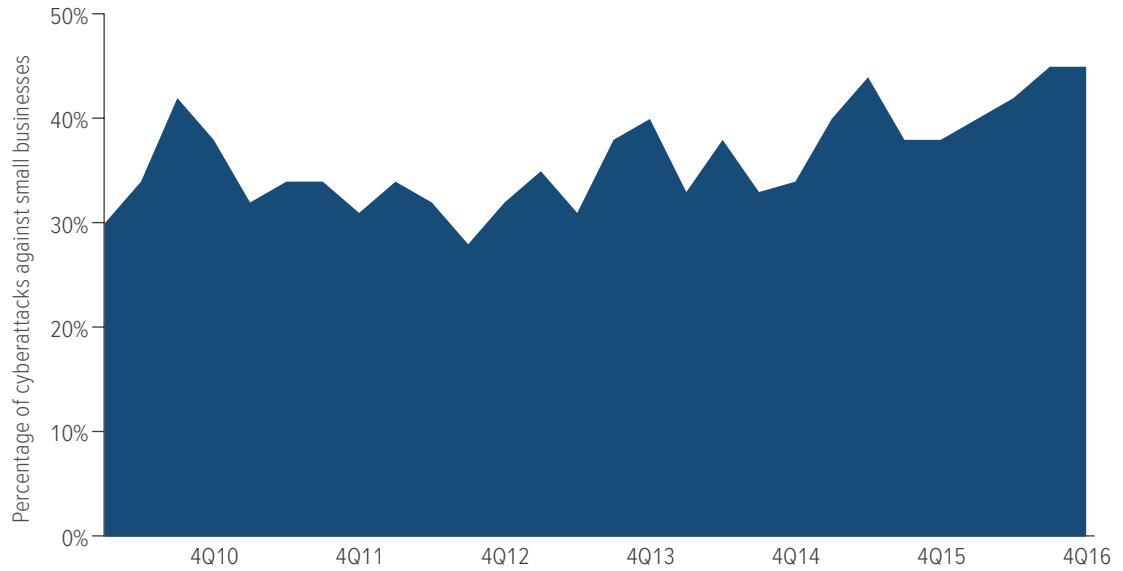
Historically by industry, financial institutions have been most frequently attacked (Figure 4).

## Social engineering attacks

Small businesses are especially vulnerable to social engineering attacks, which rely on human interaction and often manipulation to gain access to confidential information. Some 77 percent of social engineering attacks involve phishing, in which the attacker uses email to trick someone into giving them access to some type of account, login or financial information.<sup>9</sup>

Fig. 2

### Small businesses face a growing share of cyberattacks

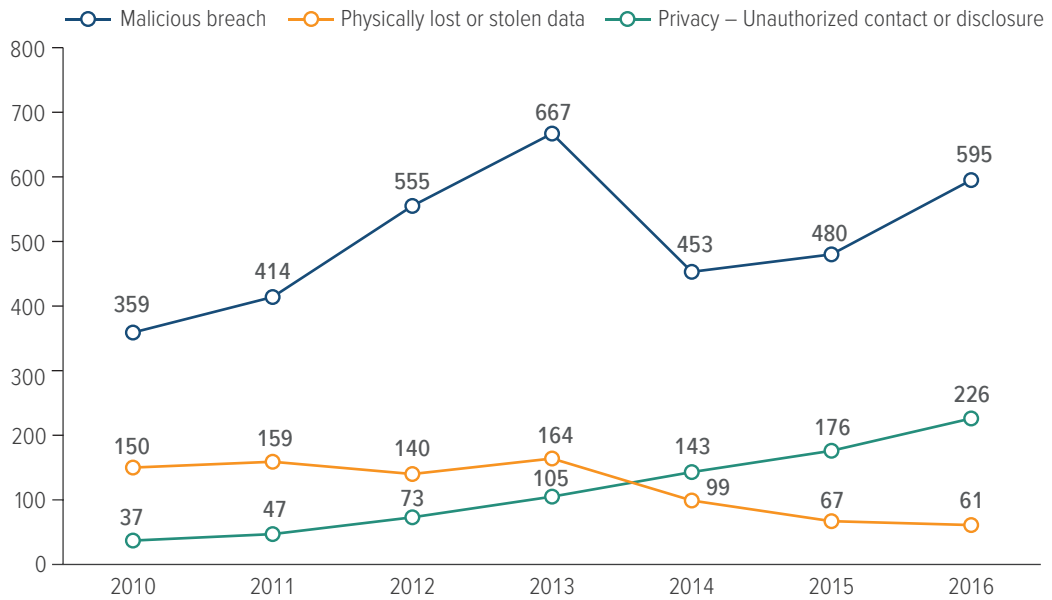


Data as of August 1, 2017.



Fig. 3

### Cyberattacks by type, 2010–2016



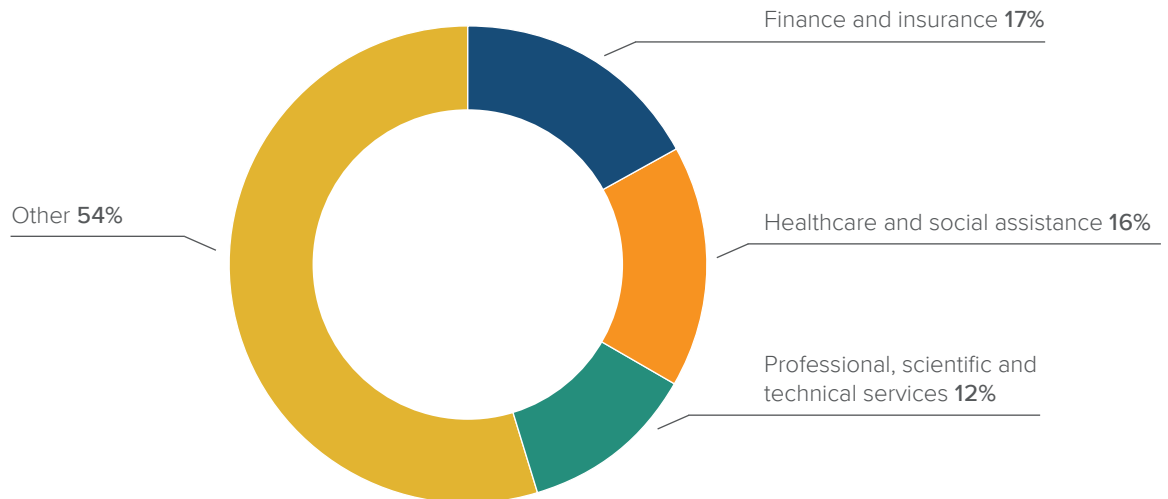
Data as of August 1, 2017.





Fig. 4

## Cyberattacks by industry, 2010–2016



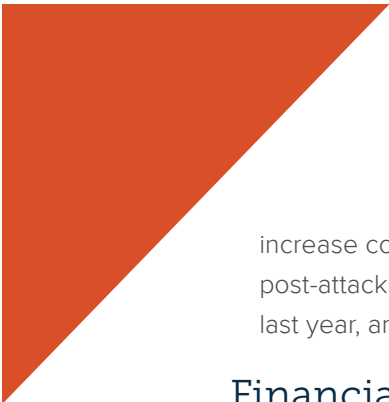
Data as of August 1, 2017.



Some of the top social engineering scams that businesses are vulnerable to include:

- **Business email compromise (BEC) and email account compromise (EAC) scams:** These sophisticated phishing attacks occur when cybercriminals send fake email messages from company CEOs, often when a CEO is known to be out of the office, asking company accountants to transfer funds to a supplier. Instead, the funds go to a criminal account.<sup>10</sup> Businesses lost more than \$360 million to cybercriminals in 2016, due to 12,005 BEC/EAC complaints, according to IC3. Tax-related email fraud schemes targeting businesses during tax-filing season have been described by the IRS as “one of the most dangerous email phishing schemes.”<sup>11</sup> These emails make it appear as if they are from an organization executive and target an employee in payroll or human resources in an attempt to obtain W-2 data on all employees. In the latest twist to the W-2 scam, cybercriminals follow up with an “executive” email to the payroll or comptroller and ask that a wire transfer also be made to a certain account. The IRS notes that some companies have lost both employees’ W-2s and thousands of dollars due to wire transfers.
- **Ransomware:** SMBs are actively targeted by ransomware attacks. In 2016, IC3 received 2,673 complaints from victims of ransomware, with losses totaling more than \$2.4 million. The WannaCry ransomware attack that affected more than 230,000 computers in more than 150 countries in May 2017 has been estimated to have cost businesses more than \$1 billion. The costs of handling a ransomware attack will typically eclipse the costs of the ransom demand, often by a large margin. The average ransom demand in 2016 jumped to \$1,077, up from \$294 the prior year, according to Symantec.<sup>12</sup> Additional factors that can





increase costs significantly include business interruption, and the need to restore lost data post-attack. Nearly 40 percent of businesses have experienced a ransomware attack in the last year, and of these, more than one-third reported lost revenue.<sup>13</sup>

## Financial impact of SMB cyberattacks

When compared to the largest companies, the financial impact of cyberattacks is disproportionately high for the very smallest companies (those with fewer than 100 employees), according to Hiscox.<sup>14</sup> For example in the U.S., the average cost of a cybersecurity incident for the very smallest organizations is \$35,967. That is more than one-third of the average for the very largest companies with more than 1,000 employees. In other words, the cost per incident for the smallest companies is far higher per-employee than for the largest companies.

Some 42 percent of small businesses surveyed by the National Small Business Association (NSBA) reported being a victim of a cyberattack, at an average cost of \$7,115 overall. For companies whose business banking accounts were hacked (10 percent of companies surveyed), the average cost rises to \$32,021. Given that small businesses often operate on very tight profit margins and seldom carry a lot of excess cash, these losses can be devastating.<sup>15</sup>

Despite the severe financial consequences, many SMBs do not have the budget and in-house expertise to protect their systems and networks against potential threats. Only 14 percent of small companies rated their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective, Ponemon said.<sup>16</sup>

A survey by Nationwide found that a majority of SMBs (57 percent) do not have a dedicated employee or vendor monitoring cyberattacks—37 percent cited cost as the reason for not monitoring attacks, and another 34 percent do not believe they will be the target of an attack.<sup>17</sup>

Without the necessary cybersecurity protections in place, small businesses across a variety of industries—many of which store customer information—are especially vulnerable to cybercrime and fraud.





## II. GROWING APPETITE FOR INSURANCE AMONG SMBs


Although the market is growing rapidly, the exact number of SMBs in the United States and elsewhere that have purchased a cyber insurance policy is difficult to determine.

While larger companies are more likely to purchase coverage than smaller organizations, appetite for coverage is increasing across the board, however, as companies of all sizes become more aware of their exposures and the potential financial impact of an event.

For example, Hiscox found that larger companies are more likely to be insured than smaller ones (48 percent versus 37 percent), but that more than half of both groups intend to buy or to enhance cover in the coming 12 months.


Lack of understanding about cyberrisks and insurance options, as well as lack of affordability all act as deterrents to prospective buyers of coverage, according to Deloitte.<sup>18</sup>

Estimates by Aon Benfield indicate that globally, more than 75 percent of certain large businesses but less than 5 percent of SMBs secured some cyber insurance in 2015.<sup>19</sup> In the U.S., around 19 percent of small businesses obtained coverage.

 Insurers foresee substantial growth coming from the SMB segment, as these companies become aware of the possibilities of liability, especially a breach and resulting response costs arising out of the possession of private data.

By industry sector, retail and wholesale, manufacturing, technology and financial institutions appear to be some of the biggest SMB buyers of standalone cyber insurance coverage in the U.S.

Based on the NAIC Cybersecurity and Identity Theft Coverage Supplement for insurer financial statements, a total of 140 U.S. insurers reported writing some type of cyber insurance premiums in 2016. Direct premiums written totaled \$1.35 billion in 2016, of which stand-alone policies



accounted for \$921 million, or 67.9 percent. Package policies, which include endorsements on a small commercial or Business Owners' Policy (BOP), accounted for \$432 million, or 32.1 percent.<sup>20</sup>

Insurers foresee substantial growth coming from the SMB segment, as these companies become aware of the possibilities of liability, especially a breach and resulting response costs arising out of the possession of private data. This is leading to a large increase in policy count, but far less in new premium volume, experts say.

Large companies have noticed the risks their smaller business partners and suppliers present. The massive 2013 Target data breach began when hackers gained access to the U.S. retailer's systems via its heating, ventilation and air conditioning (HVAC) vendor.

Some big companies have increased their due diligence. Many require their vendor networks to have cyber insurance and better security in place. As a result, many SMBs are now buying cyber insurance because they are required to do so if they want to conduct business with other partners.

## III. CYBER INSURANCE SOLUTIONS FOR SMBs

As SMBs have become more aware of the need for insurance, the market has responded by creating cyber insurance endorsements as well as products specifically addressing their needs.

Endorsements are added to packages and policies that these small businesses already buy, such as their Business Owners' Policy (BOP) or commercial property policy.<sup>21</sup> These endorsements add various coverages not already addressed in the existing policy.

Optional endorsements to the standard BOP, the package policy that is often purchased by SMBs, cover data breaches, data replacement and restoration, cyber extortion and business interruption.

These endorsements have offered the insured a streamlined and simplified product and application process, and a lower premium for a commensurate limit.

Cyber insurance forms now allow insurers to tailor coverage for SMBs.

In the United States, Insurance Services Office (ISO), a subsidiary of Verisk Analytics, is a key supplier of statistical, actuarial and underwriting claims information for property/casualty insurers. ISO also develops standard insurance policy forms, which are regarded as an industry standard. Many insurers elect to use ISO policy forms, or use them as a benchmark to develop their own forms.



ISO has developed a cyber product that is designed to address the specific needs of SMBs with up to \$250 million in annual revenue. The discovery-triggered policy form can help protect businesses if they uncover an incident, even if it began before the policy was in effect.

As of September 1, 2017, ISO has made filings in 48 states and five other jurisdictions and, subject to individual state approval, coverage will be available from January 1, 2018. Non-admitted insurers (those not subject to state approval) can offer the coverage today.

The ISO form provides a set of insuring agreements to address the cyber exposures smaller businesses often face. These agreements are available under a simplified limit and deductible structure with a base \$100,000 limit and flexibility to adjust from \$50,000 to up to \$1 million in coverage.

Creating an affordable product that SMBs will be willing to buy is a key component in the insurance offering. Since different industry sectors represent different levels of exposure, pricing will vary depending on the type of SMB. For example, a small convenience store is a relatively low hazard compared to a medical doctor's office.

In addition to a simplified limit and deductible structure, different credits may apply if an SMB has certain security procedures in place, such as employee training.

Typical cyber-related coverages can include:

**Data breach response and liability:** Covers the expenses and legal liability that arise from a data breach.

**Computer attack:** Covers damage to data and systems caused by a computer attack, such as a virus or other malware attack or denial-of-service attack.

**Network security liability:** Provides defense and liability coverage for third-party lawsuits alleging damage due to the insured inadequately securing its computer system.

**Media liability:** Covers defense costs and damages for claims asserting copyright infringement and negligent publication of media while publishing content online and via social media channels.

**Funds transfer fraud:** Covers losses from the transfer of funds as a result of fraudulent instructions from a person purporting to be a vendor, client or authorized employee.

**Cyber extortion:** Covers the "settlement" of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down and negotiate with blackmailers.



## IV. RISK MANAGEMENT/ LOSS CONTROL SERVICES

Risk prevention and mitigation services are an increasingly important part of the offering made by cyber insurers to their policyholders as they look to build and encourage resilience.

Insurers will often partner with vendors and consultants that specialize in awareness training, network security and data protection, and that have developed specialized technology and tools in threat intelligence and cybersecurity.

Cyber-related risk management services are a key product differentiator, and a very positive development for insureds, their intermediaries and for insurers themselves, experts have suggested.<sup>22</sup>

Insurers are also becoming more convinced of the value that these services can bring in controlling losses, though there is a long way to go before they reach their full potential.

 **Industry experts say that SMBs themselves need to be as proactive as their larger counterparts.**

In a survey of 31 cyber insurers, Betterley found that about half offer ‘active avoidance services’ that help the insured actively protect data from breach or other covered loss. Pre-breach planning services that help an insured prepare a contingency plan for use in the event of a breach are also offered by most of the insurers surveyed.<sup>23</sup>

In addition to up-to-date threat intelligence, insurers are seeing increased demand among insureds for risk assessments, employee training and preventive hardware or software services.<sup>24</sup>

Vulnerability assessments, next generation firewalls, IT security audits, and intrusion detection/penetration testing were ranked as the top five most helpful services related to cyber insurance in a 2016 survey of small businesses conducted by Hartford Steam Boiler.<sup>25</sup>

The provision of these types of services is considered a growth area in the cyber market for SMBs, where price may be a barrier to insurance coverage in the first place. For larger companies, cyber-related risk management services may be offered at a discount or for free.

For SMBs in particular, offering a risk management or training solution where they can learn more and keep themselves up-to-date on current threats is perhaps most valuable.



Industry experts say that SMBs themselves need to be as proactive as their larger counterparts, by conducting proper risk assessment and quantification; investing in a cyber-savvy culture; insuring cyberthreats they cannot mitigate; and allocating enough capital to cyber defenses.<sup>26</sup>

## V. CLAIMS COSTS ON THE RISE?

Claims costs associated with cyberattacks and data breaches appear to be rising, although a complete picture is hard to construct, and cyber losses vary widely among insurers.

Based on the NAIC Cybersecurity and Identity Theft Coverage Supplement for insurer financial statements, cyber insurance was profitable in 2016, despite higher loss ratios. The major cyber claims story of 2016 was ransomware, according to Aon Benfield, which some insurers saw quadruple compared with the prior year.<sup>27</sup> Yet ransom requests are typically (and intentionally) small, below most policy deductibles.

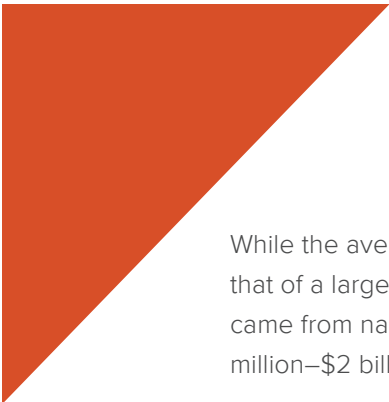
A potentially aggregating event in 2016 was the distributed denial of service (DDoS) attack on Dyn. However, the impact on insurers was expected to be minimal since the DDoS's duration was well below the standard 12-hour waiting time deductible for business interruption coverage.

With an average 47.6 percent direct incurred loss ratio in 2016, and an estimated industry expense ratio of 29.0 percent, Aon Benfield puts the 2016 industry combined ratio for cyber at 76.6 percent, up from 72.8 percent in 2015. It is also possible that the increase in loss ratio for 2016 is due to adverse development on earlier accident years or to price competition.

NetDiligence analysis suggests that smaller organizations experience most of the incidents.<sup>28</sup> This is because there are simply more small companies than there are large ones. Other contributing factors may be that smaller organizations are less aware of their exposure, or they have fewer resources to provide appropriate data protection and/or security awareness training for employees.

A 2016 review of 176 cyber insurance claims by NetDiligence found that approximately 75 percent were for organizations with under \$300 million in revenue. Some 50 percent of the claims were for organizations with less than \$50 million in revenue.

The vast majority of claims reviewed by NetDiligence involved the loss, exposure or misuse of some type of sensitive personal data. Perhaps surprisingly, smaller companies appeared to account for some of the largest data breach claims costs.<sup>29</sup>



While the average claim for a data breach for a small-revenue organization was one-tenth that of a large-revenue organization (\$599,907 vs. \$5.97 million), some of the largest claims came from nano- (<\$50 million), micro- (\$50 million–\$300 million) and small-revenue (\$300 million–\$2 billion) organizations, the study found.

The dataset for the 2016 report included 21 claims in excess of \$1 million (12 percent of all claims). Some 86 percent of these claims involved hackers or malware/virus, of which 81 percent involved nano-, micro-, and small-revenue organizations.

The largest legal costs (defense and settlements) in the NetDiligence study were from two micro-revenue organizations, one of which lost valuable trade secrets to a hacker, while the other exposed personal health information due to a lost laptop. The combined legal costs for these two organizations ranged from \$1.5 million to more than \$4.5 million.

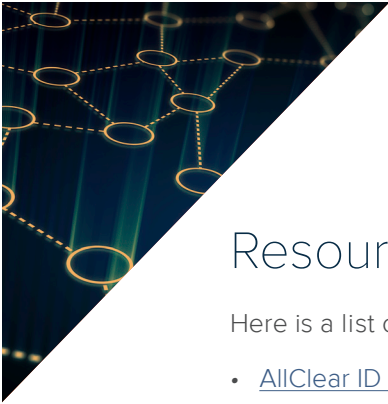
## CONCLUSION

SMBs are increasingly becoming targets of data breaches and attacks, and there is evidence that they suffer a disproportionate impact compared with larger companies in the event of an incident.

As this critical part of the economy becomes more aware of the risks and exposures they face, there is growing acceptance that insurance has an important role to play in mitigating some of the costs that arise from breaches and attacks. And insurance companies are evolving their cyber products to meet this new demand.

At the same time, SMBs need to embrace the many loss prevention tools and services now available as they look to build cyber resilience. Proper risk assessments, employee training and preventive hardware or software services, combined with a good insurance policy can help mitigate risk.

Connecting these two components with a cyber-savvy culture will best position them to protect their assets in the future.



## Resources

Here is a list of cybersecurity resources that SMBs might find useful:

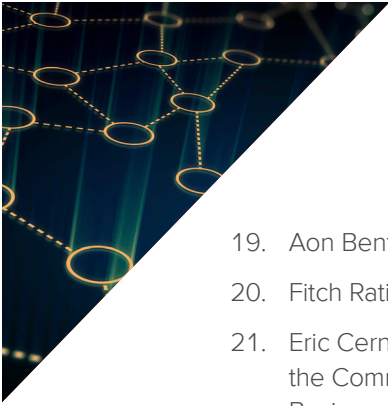
- [AllClear ID Incident Response Workbook](#)
- [FBI InfraGard Program](#)
- [Federal Trade Commission \(FTC\): Bureau of Consumer Protection Business Center](#)
- [FEMA: Business Emergency Plan](#)
- [Homeland Security U.S. Computer Emergency Readiness Team \(US-CERT\) Cyber Security Tips](#)
- [Microsoft Business Hub](#)
- [On Guard Online: Small Business Resources](#)
- [National Cybersecurity Alliance: StaySafeOnline](#)
- [National Institute of Standards and Technology \(NIST\): Computer Security Resource Center](#)
- [National Institute of Standards and Technology \(NIST\): Small Business Corner](#)
- [Small Business Administration: Cybersecurity for Small Businesses](#)
- [U.S. Chamber of Commerce: Internet Security Essentials for Small Business](#)



## Sources and Endnotes

1. Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perlroth, “[JPMorgan Chase Hacking Affects 76 Million Households](#),” DealBook, *The New York Times*, October 2, 2014.
2. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center, [2016 Internet Crime Report](#), June 2017.
3. Current statistics and prior year reports at [Identity Theft Resource Center](#).
4. Ponemon Institute, [2016 State of Cybersecurity in Small and Medium-Sized Businesses \(SMBs\)](#), June 2016.
5. Deloitte University Press, [Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising market](#), February 2017.
6. Advisen Ltd. Database highlights, comprised of data collected since 2010.
7. Advisen Ltd. defines a malicious breach as situations where personal confidential information or digital assets either has been or may have been exposed or stolen, by unauthorized internal or external actors whose intent appears to have been the acquisition of such information.
8. Advisen Ltd. defines privacy violations as unauthorized contact or disclosure as cases when personal information is used in an unauthorized manner to contact or publicize information regarding an individual or an organization without their explicit permission.
9. Laura Shin, “[Be Prepared: The Top ‘Social Engineering’ Scams of 2017](#),” Forbes.com, January 4, 2017.
10. The FBI defines Business Email Compromise (BEC) as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses who regularly perform wire transfer payments. The Email Account Compromise (EAC) component of BEC targets individuals who perform wire transfer payments.
11. IRS press release, [Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others](#), February 2, 2017.
12. Symantec, [Internet Security Threat Report](#), April 2017.
13. Malwarebytes, [Understanding the Depth of the Global Ransomware Problem](#), August 2016.
14. [The Hiscox Cyber Readiness Report 2017](#), February 2017.
15. Robert Luft, SureFire Innovations, testimony on behalf of the National Small Business Association, before the Committee on Small Business: House of Representatives, Hearing: [Protecting Small Businesses from Cyberattacks: The Cybersecurity Insurance Option](#), July 26, 2017.
16. Ponemon Institute, op. cit.
17. Julie Spitzer, “[45% of businesses unknowingly experience a cyber attack: 4 survey insights](#),” Beckers Health IT and CIO Review, August 23, 2017.
18. Deloitte, February 2017, op. cit.





19. Aon Benfield, [\*Global Cyber Market Overview\*](#), June 2017.
20. Fitch Ratings, [\*U.S. Cyber Insurance Market Share and Performance\*](#), June 22, 2017
21. Eric Cernak, vice president, cyber risk practice leader, Munich Re U.S., testimony before the Committee on Small Business: House of Representatives, Hearing: Protecting Small Businesses from Cyberattacks: The Cybersecurity Insurance Option, July 26, 2017.
22. Richard Betterley, [\*Cyber/Privacy Insurance Market Survey 2017\*](#), The Betterley Report, June 2017.
23. Ibid.
24. Advisen Ltd. database.
25. Eric Cernak, op. cit.
26. Willis Towers Watson Wire, [\*5 key cyber insurance considerations for small & middle market businesses\*](#), June 26, 2017.
27. Aon Benfield, [\*Cyber Update: 2016 Cyber Insurance Profits and Performance\*](#), May 2017.
28. NetDiligence, [\*2016 Cyber Claims Study\*](#), October 2016.
29. Daimon Geopfert, principal and national leader of security, privacy and risk at RSM US LLP, testimony before the Committee on Small Business: House of Representatives, Hearing: Protecting Small Businesses from Cyberattacks: The Cybersecurity Insurance Option, July 26, 2017.