Nationwide®

Cyber coverage | Cyber solutions

Cyberthreat protection for business owners

Contents

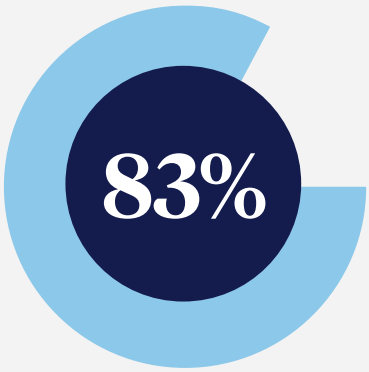
Ask any commercial business customer about their exposure to data breaches, computer attacks, and identity theft and most will reply that cybersecurity is a growing concern. Many believe that digital risk will continue to grow as we become more reliant on technology. As larger businesses find themselves vulnerable to data breaches, small and medium businesses still remain the easiest targets for hackers because of their lack of resources and security expertise.

Cyberthreats are real. Please refer to the information below to help your clients understand the importance of incorporating cyber protection into their Nationwide commercial insurance program.

Top 4 reasons small to midsize businesses (SMBs) need cyber coverage

1 SMBs are easy targets due to weak security.

SMBs may think they don't have information that cybercriminals want. Yet, SMBs accept credit card payments, collect and maintain personal information on their employees and customers, have websites and do online banking. These activities create opportunities for cybercriminals to obtain the type of information they are looking for. Cybercriminals understand that SMBs have fewer resources to invest in proper data protection and security controls, making them an attractive target. A survey commissioned by Nationwide in 2020[1] revealed that only 37% of small-business owners believe they are at risk to fall victim to a cyber attack though nearly half of cyber attacks are aimed at small businesses. And 53% say they do not offer cybersecurity training to their employees.

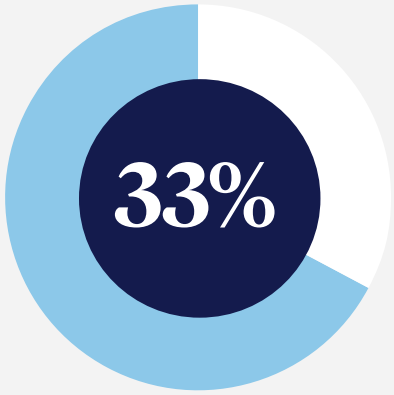


of small business say they do not have cyber liability insurance.[1]

[1] Nationwide's October 2020 Agency Forward Survey.

2 Value-added services are essential for SMBs.

Once a breach of personally identifiable information (PII) occurs, it is unlikely that the SMB will have an available team of resources to comply with various state legal requirements. Our members who purchase cyber insurance will have Data Compromise coverage which provides access to a helpline staffed by experts to assist in responding to a data breach. States can require notification to affected individuals within a required time frame and by a specified method, plus credit monitoring offered at no charge for a specified duration. A call center may need to be set up to answer questions from the affected individuals and to assist in providing credit monitoring services. To further complicate matters, state breach notification laws are governed by where the affected individual lives, not where the SMB is located. So for any one breach of PII, several state laws may determine the appropriate response. Fines can ensue if a business fails to comply with these laws. Further, many businesses suffer a loss in productivity following a data breach because employees spend time dealing with the aftermath of the data breach instead of focusing on their job duties.



of business owners say they are not confident they could recover if their small business was attacked.

3 Breach notification laws can be triggered in other ways.

It's not just about cybercriminals hacking in to an SMB's computer system. A lost or stolen laptop containing unencrypted sensitive information may trigger breach notification laws. Even sensitive information contained in paper files poses a risk. Thieves go through garbage in search of financial statements, receipts and documents with personal information, or an office that is burglarized may find paper files missing that contain tax records, bank accounts or Social Security numbers. The thief could even be a disgruntled employee. Data Compromise coverage will respond to expenses associated with the loss of third-party information as well as that of employees and owners. Identity Recovery coverage will apply to key individuals/owners and employees and their resident family members to give them further assistance should their identity be stolen.

4 Weak security and lack of controls can result in first-party and third-party claims.

In addition to stealing information directly from an SMB, the SMB can be a gateway for hackers to access the systems of its large suppliers, customers or banks. Such was the case with the Target Corporation breach, whereby hackers targeted a midsize HVAC contractor whose networks were directly connected to Target's. Upon obtaining an employee's credentials via a phishing email, the hackers used that to gain entry to Target's systems completely undetected. Cyber insurance is intended to provide defense and settlement costs for similar situations.

A small-to-midsize business could also unintentionally forward a virus or malware to a supplier or customer, causing that third party's website to go down. This could result in loss of income, for which they could bring suit against the SMB. With the purchase of cyber coverage from Nationwide, the business would be covered not only for a third party's loss of income, but also for its own loss of income, as well as for any costs incurred to restore computer systems or data.

▲Return to Contents

Nationwide's cyber coverage

Nationwide partners with Hartford Steam Boiler to offer cyber coverage that addresses several key data security exposures. This coverage—outlined below—is automatically quoted on new businessowners and general liability policies in Nationwide's rating systems. Contact your Nationwide representative for details.

- **Data Compromise**—This endorsement includes both first-party coverage (Response Expense) and third-party coverage (Defense and Liability). Response Expense covers the cost of notifying clients, employees and others affected by a breach of personally identifiable information. Also included is coverage for expenses associated with credit monitoring and identity restoration to help businesses retain their clients' and employees' trust and goodwill following a breach. Defense and Liability coverage responds to third-party actions brought against the insured by individuals affected by the breach. (Defense and Liability coverage is not available in N.Y.)
- **Identity Recovery**—Identity Recovery insurance combines case management services and expense reimbursement coverage for key individuals/owners and employees and their resident family members who become victims of identity theft. This coverage helps to restore their credit history and identity records to pretheft status, regardless of how the theft occurred.
- **Computer Attack**—Computer Attack coverage protects businesses against damage to electronic data and computer systems from a virus or other computer attack. It also protects a business's liability to third parties that may have suffered damage due to security weaknesses in the business's computer system.

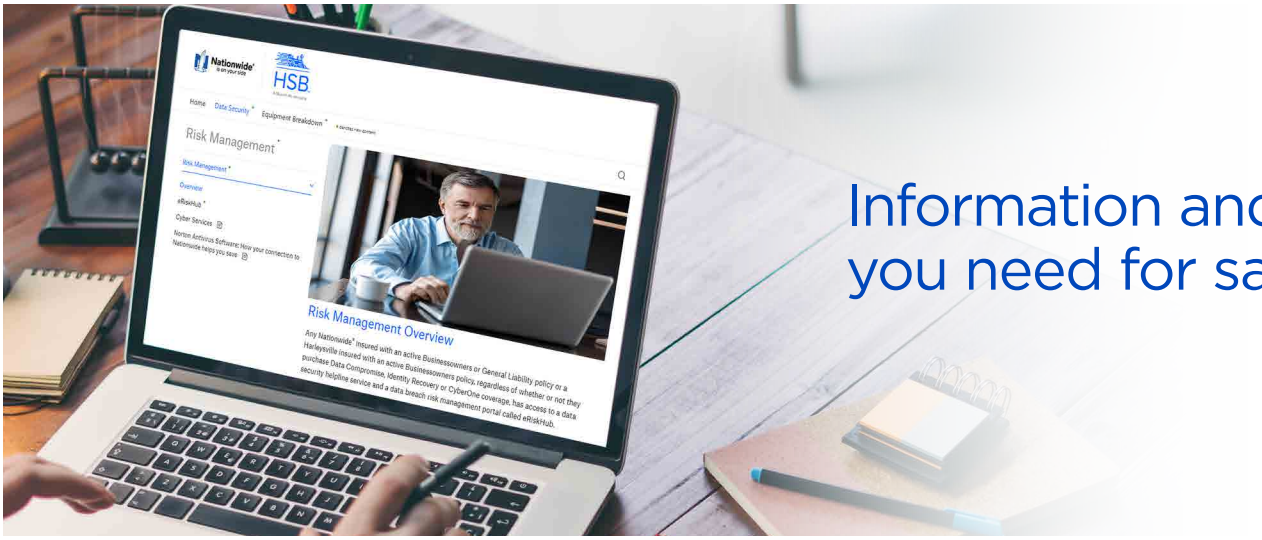
Claim examples that show the importance of cyber coverage.[2]

Claim Description	Coverage
A box of rental applications with the name, names, addresses and Social Security numbers of 500 individuals was stolen from the office of an apartment complex.	**Data Compromise**
COST: $17,500 for notification, call center and credit monitoring expenses	
Identity thieves used credit card skimmers at a gas station to steal credit card numbers from 550 customers. Breach notification laws of 5 states were triggered.	**Data Compromise**
COST: $19,250 for notification, call center and credit monitoring expenses	
An employee's Social Security number was stolen and the thief opened credit cards in his name, charging over $20,000. Having the services and protection from his employer's Identity Recovery coverage, the employee was able to minimize time away from work and had experts to assist in restoring his credit history and records to pretheft status.	**Identity Recovery**
COST: $5,875 for attorney fees and lost wages	
Our insured manufacturer unknowingly sent an email containing a virus to one of their distributors. The distributor's computer system became infected, causing their website to be down for 2 days. The distributor incurred expenses in having the virus removed and computer system restored, plus loss of income due to their website being down. They sued the manufacturing company when their IT vendor determined that they were the source of the virus. The manufacturer also incurred expenses from hiring an IT firm to remove the virus and restore their system.	**Computer Attack**
COST: $40,000 in third-party expenses incurred by the distributor to have the virus removed and their system restored, plus loss of income. $7,500 in first-party expenses for the manufacturer to hire an IT firm to remove the virus from their system.	

A virus could be unintentionally forwarded to a customer or vendor, causing their website to go down.

[2] Each claim is handled on the basis of its individual facts and circumstances and in accordance with policy language, including applicable exclusions, conditions and limitations. Insurance overview is for informational purposes only and does not replace or modify the definitions and information contained in individual insurance policies or declaration pages, which are controlling. Terms and availability vary by state and exclusions apply.

▲Return to Contents



Information and tools you need for sales

- **Internal Cybersecurity Products Website**

  Following is a link to the internal Cybersecurity Products website containing educational cyber resources and marketing materials for agents. This site includes coverage information, loss examples, FAQs, sales and marketing resources, including a coverage/limits needs-analysis tool, selling techniques, a PowerPoint presentation for agency communication purposes and promotional materials. The risk management section of this website identifies the value-added services provided to Nationwide customers with an active businessowners or general liability policy.

  - hsbfrontdoor.com/content/munichre/hsbgrp/nationwide/en/home/data-security/coverages/overview.html

- **eRiskHub®**

  Below is a link to the eRiskHub® cyber/data breach risk management portal. The information and tools contained within this portal will help your Nationwide customers understand their data information exposures and plan and prepare for a cyberattack or data breach. There, they can also learn how to establish a response plan to manage the costs and minimize the effects of a data breach. All Nationwide customers with an active businessowners or general liability policy will receive notice of this website.

  - eriskhub.com/nationwide **access code:** 12116-73

- **Other Resources**

  - nationwide.com/business/insurance/cyber-liability
  - dhs.gov/stopthinkconnect
  - privacyrights.org/

Questions?

Contact your sales manager or underwriter with questions or for additional information.

Nationwide®

nationwide.com

▲Return to Contents