2018 Cybersecurity Survey of Connecticut Businesses

AT&T

BlumShapiro
Accounting | Tax | Business Consulting

Cooperative Systems

EVERSOURCE ENERGY

KeyBank

cbia

INTRODUCTION

CBIA's first-ever cybersecurity survey of Connecticut companies was designed to both raise awareness of the issues and challenges and better understand the level of preparedness within the state's business community.

We wanted to know what companies were doing to:

- Prevent and detect cyberattacks
- Minimize damage from an attack
- Raise the level of threat awareness within their organizations
- Engage and educate employees
- Strengthen and evaluate response efforts during and after an attack

Given the increasing number of attacks on businesses of all types and sizes, CBIA believes it is critical to gauge the levels of preparedness and risk mitigation among Connecticut firms.

Nonetheless, cybersecurity is a sensitive subject, which presents challenges with surveying organizations.

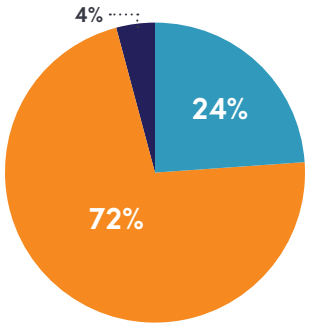
While this survey saw lower response rates than our typical surveys on economic and public policy issues, there is clear evidence that businesses must evolve much faster in understanding and managing cybersecurity threats.

KEY FINDINGS

- Almost a quarter of Connecticut businesses suffered data breaches or cyberattacks in the last two years, with 26% unsure of the sources behind those incidents.
- While 38% say risks have increased, 23% of companies are unsure.
- There is a broad lack of awareness for not only identifying threats, but understanding how to prepare, manage, and respond.

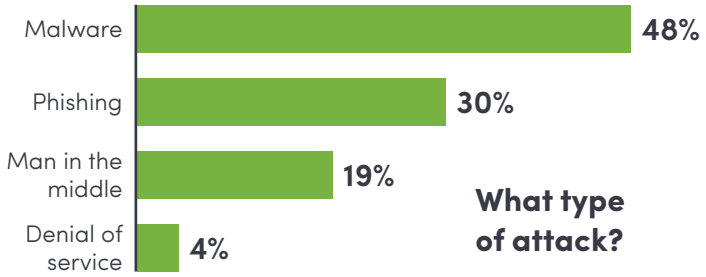
CONTENTS

- Financial resources and lack of expertise hinder companies' cybersecurity management efforts.
- Only 18% of surveyed companies have an annual budget dedicated to cybersecurity.
- Almost half of surveyed companies provide cybersecurity training to employees; of those, only 58% make training mandatory.
- While 73% of companies have a disaster recovery or business continuity plan, just 22% have an incident response plan in place for vendors, customers, and subsidiary operations.



Did your company suffer a cyberattack in the last two years?

Yes
No
Unsure



What type of attack?

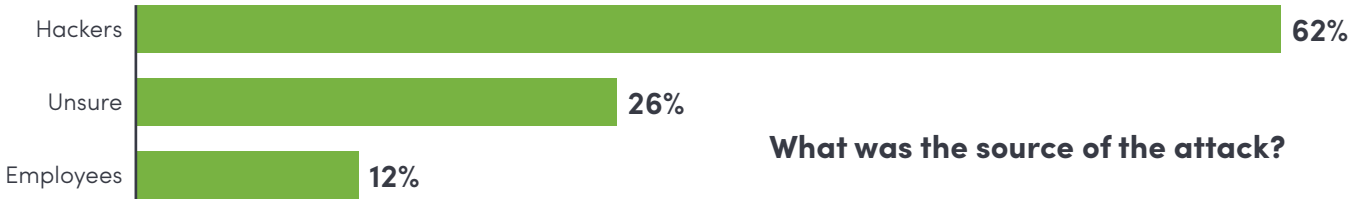
THREATS & RISKS

In the last two years, 24% of Connecticut companies suffered data breaches or cyberattacks. While 72% reported no attacks, 4% of surveyed businesses say they are unsure whether their firms were compromised.

Malware, including viruses, spyware, and other unwanted software, drove almost half (48%) of those reported attacks, while phishing—using fraudulent emails or texts to obtain confidential company or personal information—accounted for 30%.

Man-in-the-middle attacks—where hackers intercept and compromise communication between two systems—were responsible for 19% of cyberattacks on Connecticut companies.

Four percent were generated by denial of service attacks, where hackers target networks with a flood



What was the source of the attack?

of requests designed to slow down or crash servers, disrupting business operations.

What are the sources of these attacks?

Sixty-two percent of companies report hackers were responsible and 12% blame employees. What's most telling is that 26% of companies are unsure who is behind the attacks.

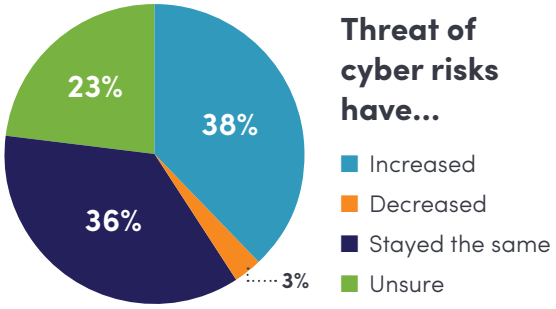
Over a third of companies (38%) believe cyber risks are increasing, 36% say the threat levels remain the same, 23% were unsure, and just 3% see a decline in overall threats.

Lack of knowledge and/or awareness is a constant theme throughout this survey.

For instance, when asked to identify the greatest known cybersecurity threat to their company, 30% said they were unsure and 18% cited a lack of general knowledge.

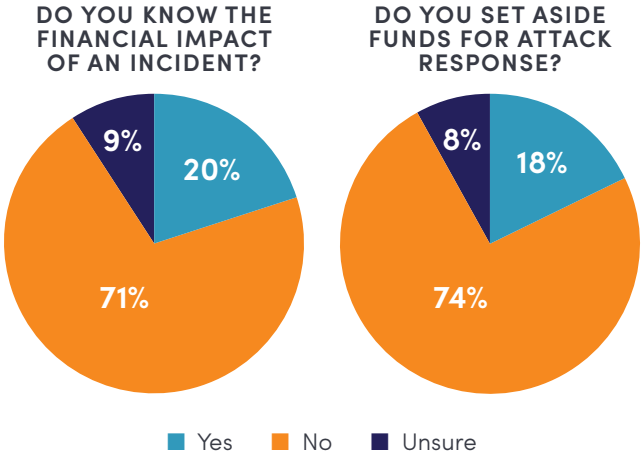
Twenty-four percent identified an inability to recognize phishing or malware attacks, 8% nominated poor mobile device security awareness, 5% have difficulty identifying suspicious network traffic, and another 5% pointed to insufficient third-party risk management resources.

> **I commend CBIA for the part they are playing in starting a constructive dialogue about cybersecurity and providing businesses with the tools they need to confront the challenges they face.**
>
> **John Emra** | President | AT&T Connecticut



Who is compromised when a company comes under attack?

Multiple constituencies, say surveyed companies, with 65% citing clients and customers, 65% employees, 11% vendors, and 6% subsidiaries. Nineteen percent said they were unsure.

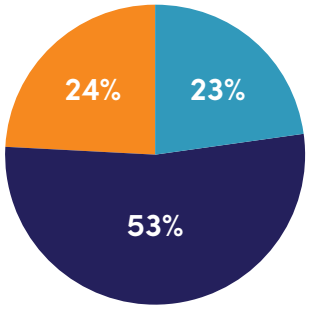


Significantly, just 20% of surveyed companies have estimated the fiscal impact of a cyberattack. Seventy-one percent have not and 9% are unsure.

RESOURCES

A minority—18%—of surveyed companies have an annual budget dedicated to their cybersecurity efforts.

Twenty-three percent plan on implementing a budget line for cybersecurity management in the near future, 53% have no plans, and 24% are uncertain.



Are you adding a budget line for cybersecurity?

- Yes
- No
- Unsure

However, more than half (58%) report that spending on cybersecurity personnel and/or resources increased over the last 12 months, while 42% said it stayed the same. No companies said they decreased their spending in this area.

Just 14% of surveyed companies manage their information technology functions solely through dedicated internal staff, while 32% use the services of managed service providers or consultants. Over half (52%) rely on a mix of internal and external resources.

Of those with internal IT staff, 25% have employees dedicated to managing their cybersecurity efforts, with the number of employees ranging from one to 10 workers.

Three-quarters of all surveyed companies have contracts with external IT vendors, 22% do not, while 2% are unsure.

Most businesses—88%—that contract with external IT vendors report those vendors are involved in their company's cybersecurity management efforts.

Only 44% of all surveyed companies say they actively manage their IT security functions, 29% do not, and 27% are unsure.

Less than half of all companies (47%) maintain a physical operations center that houses their websites, data centers, and network servers to allow for monitoring and breach protection.

> **"This report shows a lack of understanding of the scope and impacts of a data breach event, indicated by the apparent inability of businesses to obtain sufficient resources to address these very real and constant threats.**
>
> **Chris Leigh** | Director & Chief Information Security Officer | Eversource

RISK MANAGEMENT

Few companies report high degrees of confidence with their risk management operations.

Just a quarter (26%) say they are very confident

about their network security operations, while 68% are somewhat confident. Four percent are not confident and 3% are unsure.

Only 22% believe their company's networks are highly secure, with 68% describing their networks as moderately secure. Six percent say their networks are insecure and 4% are unsure.

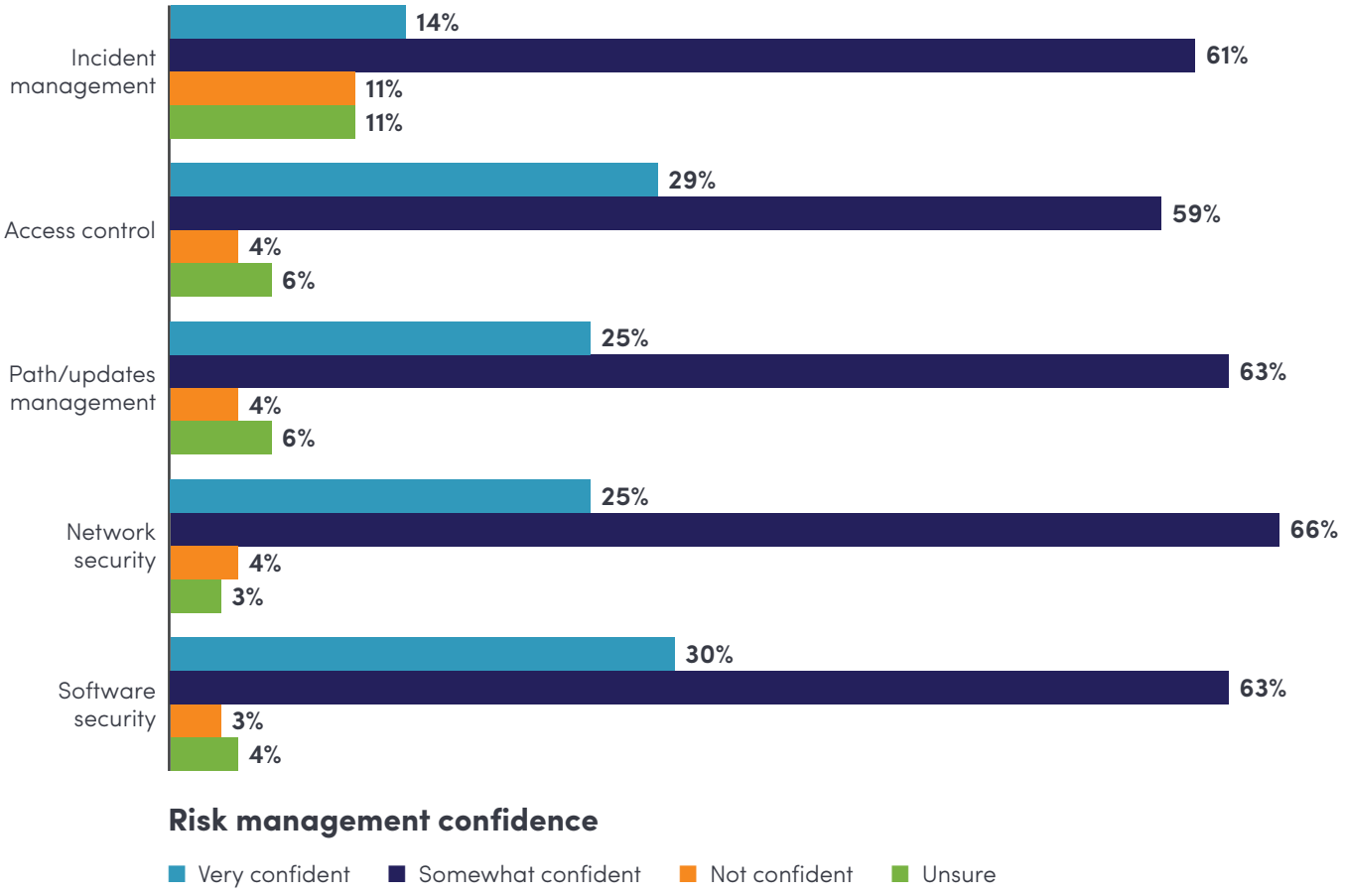
The patterns are similar across incident management, access controls, and software security.

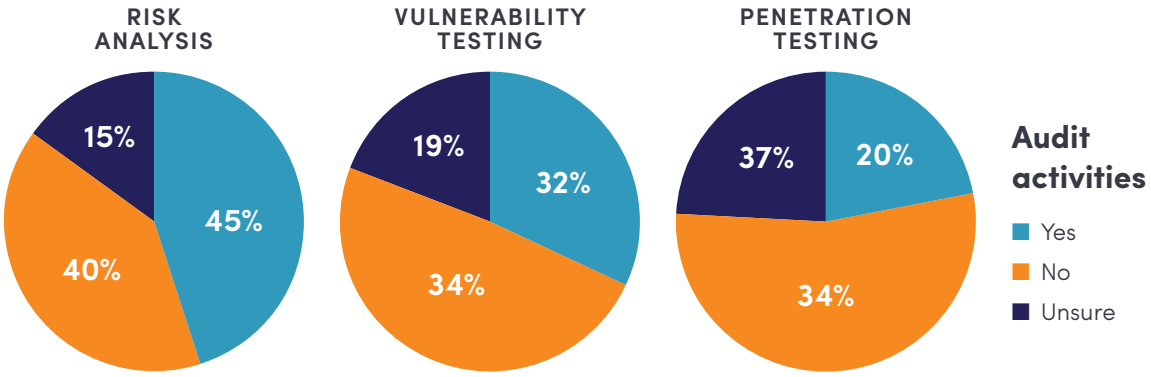
For instance, 14% of surveyed companies are very confident about their incident management plans and activities, 63% are somewhat confident, 12% have no confidence, and 12% are uncertain.

Half the companies we surveyed are somewhat confident in their management of software security patching and updates.

Based on their industry sector, Connecticut companies must comply with a range of state, federal, or industry laws, regulations, and standards governing privacy, data security, and breach notification.

Twenty-seven percent of companies represented in this survey say they are required to comply with state and federal data privacy and breach notification requirements.





Almost a third (32%) must comply with the 1996 federal Health Insurance Portability and Accountability Act, which governs companies operating in the healthcare sector. HIPAA's administrative safeguards provisions require covered entities to perform risk analysis as part of their security management processes.

Thirteen percent of businesses report falling under the 2006 Payment Card Industry Data Security Standard, which requires all companies that accept, process, store, or transmit credit card information to maintain a secure environment.

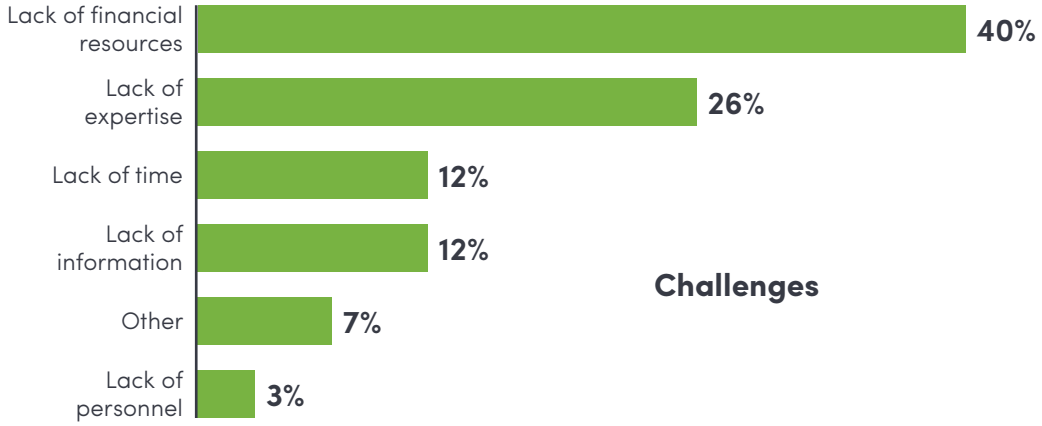
PCC DSS is administered by the Payment Card Industry Security Standards Council, an independent organization created by the major payment card brands. PCI SSC can fine banks $5,000 to $100,000 per month for violations, with banks often likely to pass those penalties to non-compliant merchants.

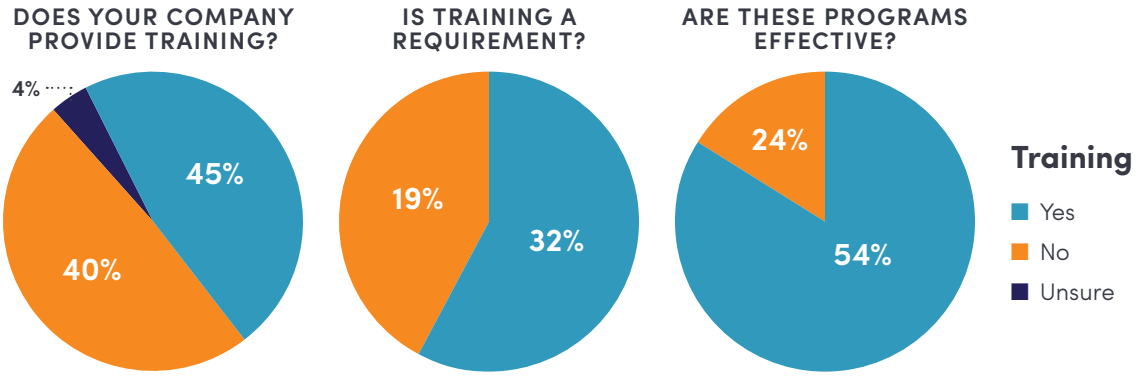
What challenges do companies face in managing cyber risks?

For 40%, it's a lack of financial resources, while 26% cite a lack of expertise. Time constraints challenge 12% of companies, as does a lack of information, while 3% cite personnel shortages.

TESTING & TRAINING

Less than half of surveyed companies (45%) conduct risk analysis audits or tests, 40% do not, and 15% are unsure.





Of those that conduct risk testing, 18% are uncertain about the frequency of those tests. Only 3% run weekly tests, 15% monthly, 21% twice a year, 18% annually, and 12% say they run tests when needed or after an incident.

Almost half (49%) of companies do not conduct vulnerability testing, while 32% run those tests and 19% are unsure.

> **Nearly 80% of survey respondents do not know or are unsure of the financial impact a cyberattack can have on their businesses, and the majority are not setting funds aside or putting cybersecurity insurance in place. The fact is the majority of cyberattack victims are businesses with fewer than 1,000 employees.**
>
> **Jeff Hubbard** | Market President
> KeyBank

In terms of frequency, 8% run weekly vulnerability tests, 21% do so monthly, 21% twice a year, 8% annually, and 17% as needed or following an incident. Eight percent are unsure.

Connecticut companies are less likely to run penetration tests, with 54% reporting they do not use this tool to assess the strengths and weakness of their computer systems and networks.

Twenty-two percent utilize penetration testing and 24% are unsure.

Companies that run penetration tests are most likely to do it semi-annually or annually (56%).

Less than half (47%) of all companies provide cybersecurity training for employees, with 49% reporting they offer no training programs, and 4% are unsure. Of those that provide employee training, only 58% say it is mandatory.

Thirty-four percent conduct annual training, 21% when needed or following an incident, 16% hold sessions based on an outside provider's availability, 13% run quarterly programs, 13% semi-annually, and 3% monthly.

> **It's clear that companies need to take a more proactive position on vulnerability and penetration testing and monitoring to better identify and remediate significant technology gaps.**
>
> **Jeffrey Ziplow** | Risk Management Partner
> BlumShapiro

Group sessions are the preferred format for 52% of those who offer training, while 17% provide individual sessions and 27% rely on webinars.

Is that training effective? Eighty-four percent say yes, while 16% are unsure.

RESPONSE & RECOVERY

We asked business leaders if their firms have a disaster recovery or business continuity plan. Encouragingly, 73% do have such a plan, while 18% do not and 9% are uncertain.

Most of those firms (52%) update their plan annually, with 14% reviewing and revising it when needed or after an incident. Thirteen percent update their plan twice a year, 2% monthly, and 2% weekly.

Eighteen percent are unsure how often their disaster recovery or business continuity plan is updated.

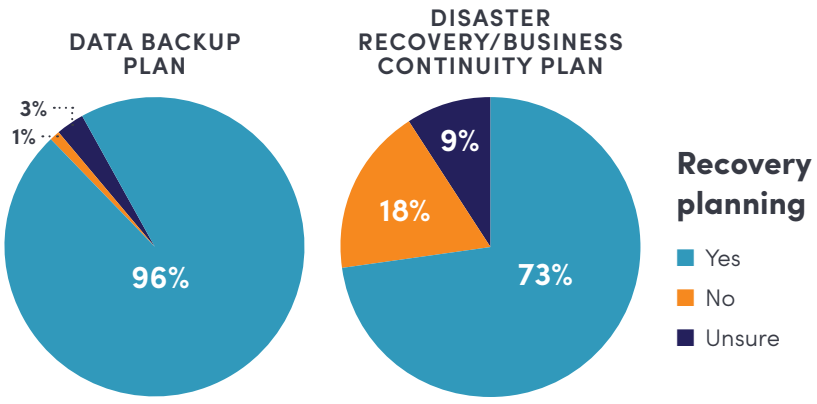
Those plans are tested annually by 29% of firms, with 21% testing when needed or following an incident, 14% semi-annually, 7% weekly, and 4% monthly. Twenty percent are unsure of the frequency of their testing.

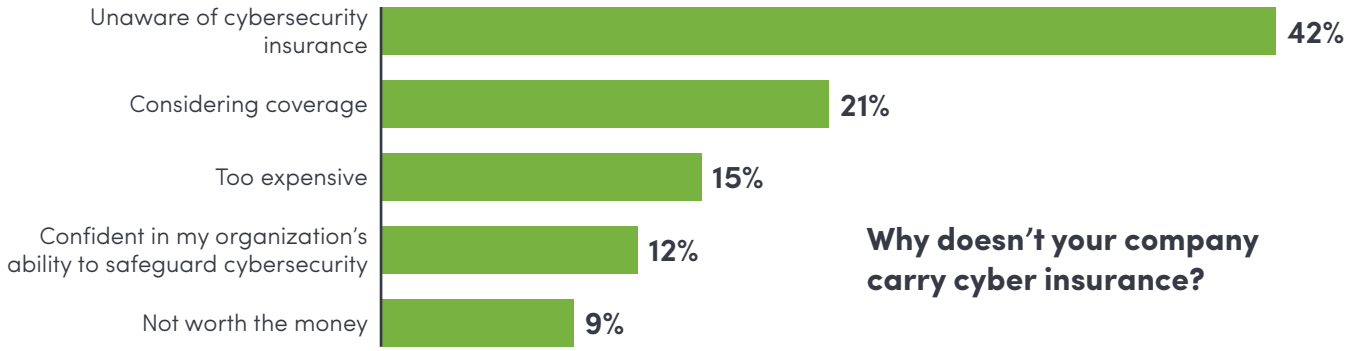
Almost all surveyed companies (96%) have a data backup plan.

Only a third of companies (33%) say they are required to notify vendors, customers, and/or subsidiaries following a cyberattack or data breach. Forty-seven percent have no requirement and 20% are unsure of their notification responsibilities.

Just 22% have an incident response plan in place for vendors, customers, and subsidiary operations, with 55% having no plan, and 22% unsure. For those with such a plan, 47% have tested it, 47% have not, and 6% are uncertain.

We also asked companies if they set aside funds to respond to attacks. For example, paying hackers to resolve ransomware attacks—where malware is used to lock user computer files—or engaging outside legal help.





Why doesn't your company carry cyber insurance?

While almost three-quarters (74%) do not set aside emergency funds, 18% of companies do and 8% are unsure.

Just over half (51%) of surveyed companies also have insurance policies to cover damages caused by cyberattacks. Forty-four percent do not carry cyber insurance and 5% are uncertain.

Of those who not carry a specific policy, 42% are unaware of cyber insurance and how it works, 21% are considering coverage, 15% say policies are too expensive, 12% are confident in their company's safeguards, and 9% say policies are not worth the cost.

Most of the companies (54%) carrying cyber insurance increased their policy coverage in the last two years.

CONCLUSION

This was CBIA's first survey on the topic of cybersecurity. As we noted earlier, this is a sensitive issue, and that impacted the overall response rate—3.4%, well below what we usually see with other surveys on economic and public policy issues.

Obviously, cybersecurity is a topic that worries, even scares, many business leaders.

Based on the results of this survey, while many companies are tackling the issues and are implementing appropriate measures, it is clear there is a great deal of uncertainty, particularly among small businesses, which are most vulnerable to threats.

There's an obvious lack of knowledge about the issues and a lack of clarity among many business leaders about their own efforts to prepare, manage, and respond to this growing threat.

> **Cyber resilience is not just an IT function. It absolutely must come from the top down, and the approach needs to become part of the overall business strategy.**
>
> **Bob DeLisa** | President | Cooperative Systems

> **The sooner businesses step up and take control of their cybersecurity, the lower the chances of government stepping in with heavy-handed regulations.**
>
> **Pete Gioia** | Vice President & Economist
> CBIA

Whether it's fear of the unknown, information gaps, inadequate fiscal or personnel resources, or a too-casual attitude, businesses small and large must acknowledge and understand the risks.

Any company is just one click away from an attack and the potential for significant financial, reputational, and legal exposure if they do not adapt, plan, and prepare.

As Art House, the state's Chief Cybersecurity Risk Officer says: "To think it's not going to happen to you is dangerous thinking. You have to assume that what's happening to everyone else, someday will happen to you."

Every company must have a thorough understanding of their current risk exposure. If you do not have enough in-house personnel resources, we encourage you to engage outside help.

While it may be difficult to assign appropriate financial resources, the risks of not taking appropriate action could potentially be far costlier—to your bottom line and your brand.

Implement layered security protections, building up appropriate defenses for servers, networks, workstations, and mobile devices.

Make sure you have a data back-up solution in place. Develop a disaster response or business continuity plan. Have a clear path to recovery should the worst happen.

Follow that with regular training and testing programs.

And remember, your employees are your frontline defense against hackers.

The sooner businesses step up and evaluate their cyber defenses—hardening them as needed—and implementing regular employee training, the lower the chances of government stepping in with heavy-handed regulations.

CBIA CYBERSECURITY RESOURCES

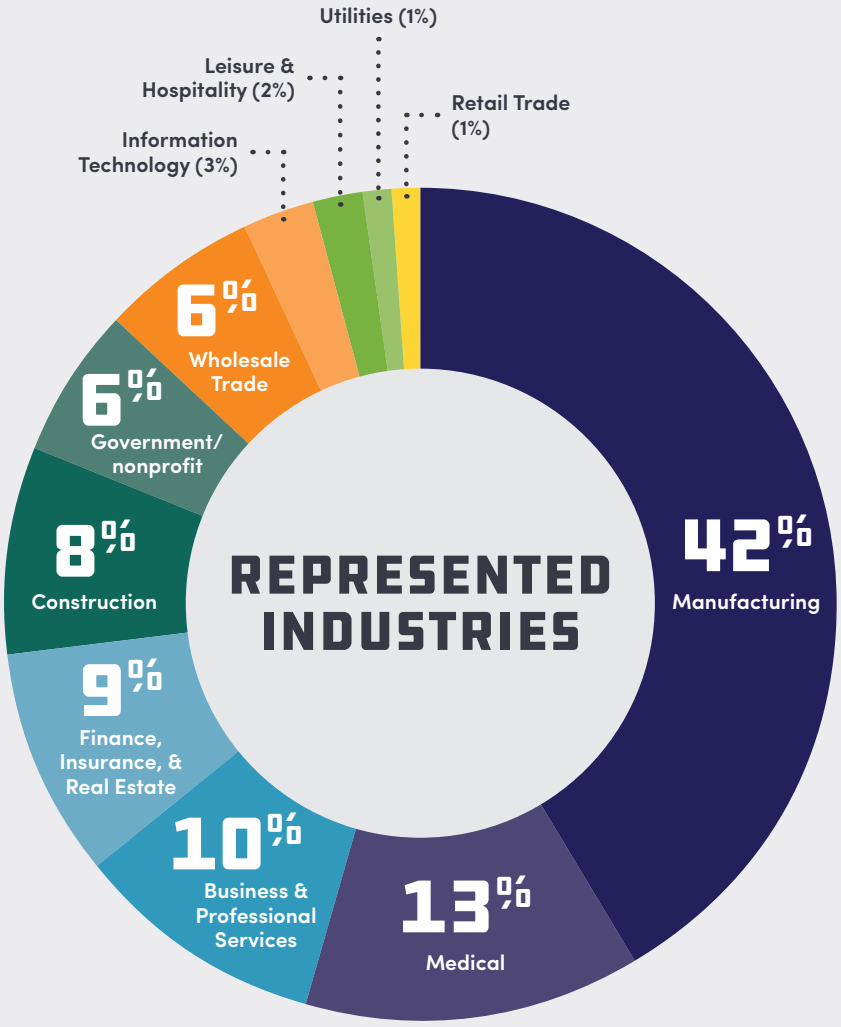
bit.ly/cbia-cybersecurity

ABOUT
THE SURVEY

METHODOLOGY & DEMOGRAPHICS

In late 2017, CBIA mailed and emailed the Cybersecurity Survey of Connecticut Businesses to approximately 3,400 executives throughout the state.

We received 117 responses, for a response rate of 3.4% and a margin of error of +/-9.1%. All figures are rounded to the nearest whole number and may not total exactly 100%.



ABOUT
THE SPONSORS

AT&T

AT&T Inc. (NYSE:T) helps millions around the globe connect with leading entertainment, business, mobile and high speed internet services.

AT&T has the nation's largest and most reliable network and the best global coverage of any U.S. wireless provider. The company is one of the world's largest providers of pay TV, with customers in the U.S. and 11 Latin American countries.

Nearly 3.5 million companies, from small to large businesses around the globe, turn to AT&T for our highly secure smart solutions.

For more information, visit att.com.

BLUMSHAPIRO

Blum, Shapiro & Company, P.C. (BlumShapiro) is the largest regional business advisory firm based in New England with over 500 accounting, tax, consulting and administrative professionals in Massachusetts, Rhode Island and Connecticut, making us the 54th largest public accounting firm in the country.

BlumShapiro was also named one of the fastest growing private U.S. companies by Inc. magazine in the publication's 2015 Inc. 5000, and have been selected as the #1 firm in the New England Region for the second consecutive year by Accounting Today.

BlumShapiro serves as your business advisors, helping you solve challenges and maximize opportunities. Drawing upon its breadth and depth of experience, BlumShapiro strategically tailors and consistently delivers tested solutions for unlocking the full potential of your organization.

BlumShapiro's highly valued team members bring their diverse backgrounds and strengths to the engagement, resulting in you receiving a true blend of national firm experience and local firm delivery. Our team shares a common passion: a personal commitment to each client's success as well as to the communities in which we live and work.

For more information, visit blumshapiro.com.

ABOUT
THE SPONSORS

COOPERATIVE SYSTEMS

For 25 years and counting, Cooperative Systems has been a strategic IT partner to small and medium businesses across New England. They assist clients in achieving their business goals through exceptional customer service and support, tailored and cost-effective solutions, and a consultative approach to each business' unique needs.

The Cooperative Systems team works with you to create a custom IT strategy roadmap for your business with your goals and needs in mind.

Cooperative Systems' NOAH managed IT services make doing business easier and more efficient than ever. NOAH services encompass proactive monitoring and maintenance of your environment and assets, backup and disaster recovery solutions, high-quality communication solutions with superior reliability, hosted cloud solutions, a comprehensive multi-layered array of cybersecurity and compliance solutions, and advisory services as a CIO-level business partner with extensive experience and unparalleled expertise.

With best-in-class strategies and tools, NOAH services will minimize down-time, tighten your security, and give you peace of mind.

For more information, visit coopsys.com.

EVERSOURCE

Eversource (NYSE: ES) transmits and delivers electricity and natural gas and supplies water to approximately four million customers in Connecticut, Massachusetts, and New Hampshire.

Recognized as the top U.S. utility for its energy efficiency programs by the sustainability advocacy organization Ceres, Eversource harnesses the commitment of about 8,000 employees across three states to build a single, united company around the mission of safely delivering reliable energy and water with superior customer service.

For more information, visit eversource.com.

ABOUT
THE SPONSORS

KEYBANK

KeyCorp's roots trace back 190 years to Albany, New York. Headquartered in Cleveland, Ohio, Key is one of the nation's largest bank-based financial services companies, with assets of approximately $137.7 billion at December 31, 2017.

Key provides deposit, lending, cash management, insurance, and investment services to individuals and businesses in 15 states under the name KeyBank National Association through a network of approximately 1,200 branches and more than 1,500 ATMs.

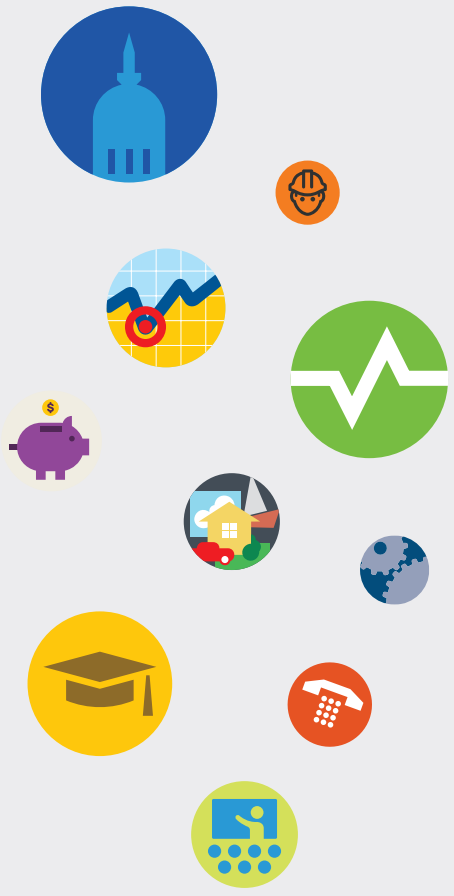
Key also provides a broad range of sophisticated corporate and investment banking products, such as merger and acquisition advice, public and private debt and equity, syndications, and derivatives to middle market companies in selected industries throughout the United States under the KeyBanc Capital Markets trade name.

For more information, visit key.com.

ABOUT CBIA

The Connecticut Business & Industry Association is the leading voice of business in the state, representing thousands of member companies, small and large, across a diverse range of industries.

We fight to make Connecticut a top state for business, jobs, and economic growth: driving change, shaping legislative and regulatory policy, and promoting collaboration between the private and public sectors.



DRIVING GROWTH, PROMOTING BUSINESS

Powerful, dynamic leadership and advocacy at the State Capitol, driving policies that promote a globally competitive business climate.

Valuable resources, information, and professional assistance, sharing expertise and best practices across a broad range of issues to help companies compete, grow, and succeed.

Innovative, high-value products and member services, including insurance and employee benefits, business and HR resources, energy purchasing solutions, and more.

Learn more at cbia.com

Connecticut Business & Industry Association | 350 Church St., Hartford, CT 06103-1126 | 860.244.1900 | cbia.com | @CBIANews