



Cyberthreats and solutions for small and midsize businesses

A framework for mitigating risk and defending your company against a cyberattack

VISTAGE



A framework for mitigating risk and defending your company against a cyberattack



62% of SMBs don't have an up-to-date or active cybersecurity strategy in place.



24% of SMBs are aware of having had a cyberattack in the past 12 months.



67% of SMBs work with an external partner to manage their cybersecurity.

Picture this: It's tax season, and your HR director receives an email from someone who's pretending to be you — the CEO. The HR director thinks that the email is legitimate and complies with the request to send over copies of all of your employees' W2s. Days later, the email sender — who's actually a skilled hacker — uses those W2s to file a batch of fake tax returns.

Cyberattacks like this happen every day. The cost to the global economy is staggering, currently exceeding \$350 billion worldwide, according to the National Center for the Middle Market (NCMM) at The Ohio State University Fisher College of Business.

Cyberattacks are increasing against businesses and individuals, translating into enormous costs in terms of system downtime, resources and money. If a business hasn't yet been hacked, it's only a matter of time before it will be. Hackers are becoming increasingly skilled and professional, and their tactics are becoming more sophisticated and successful. Hacking is an effort backed by big money, demographic data and refined analytics.

'Soft targets' for hackers

Small and midsize businesses (SMBs) are not immune to the threat of cyberattacks. In fact, the majority of all cyberattacks happen to SMBs. Many cybersecurity experts call these companies "soft targets" because SMBs tend to lack sufficient security measures and trained personnel to thwart a cyberattack. They're also attractive to hackers because they hold valuable data and can be leveraged to break into larger companies. In fact, in 2013, hackers were able to breach Target via one of the partners in their supply chain: a small HVAC company based in Sharpsburg, Pennsylvania.

SMBs are also prime targets for ransomware, which encrypts company data until a ransom is paid. Why? Unlike many large companies, SMBs often neglect to use an offsite source or third-party service to back up their files or data. In the event of an attack, they almost always have to pay the ransom to decrypt their files.

4 myths about cyberattacks

1 Myth: Hackers only go after large companies.
Fact: Most cyberattacks happen to small and midsize companies.

2 Myth: Small businesses don't offer anything of value to hackers.
Fact: Small businesses have credit card numbers, protected health information, personally identifiable information and other data that hackers can use to take out loans, steal identities, make wire transfers and complete other scams.

3 Myth: Most hackers aren't dangerous; they're just teenagers.
Fact: Hackers are sophisticated computer criminals who are constantly refining and adapting their tactics. They are organized and ruthless.

4 Myth: Law enforcement will protect me from a cyberattack.
Fact: Law enforcement doesn't have the time, resources or staff to protect most companies from cyberattacks.

Most SMBs are not prepared for cyberattacks.

In Q4 2017, Vistage — in partnership with Cisco and the NCMM — conducted a survey to gauge the preparedness of SMBs for cyberattacks and determine the business impact of these kinds of attacks. According to Anne Petrik, director of research for Vistage, of the 1,377 CEOs who participated in the survey:

- 27% said their company did not have a defined cybersecurity strategy.
- 18% said their company did not have a cybersecurity strategy but were working on it.
- 17% said their company had a strategy but it wasn't current.

Only 38% of SMB CEOs said that their company had a cybersecurity strategy in place that was both current and reviewed on a regular basis. In other words, 62% of SMBs don't have an up-to-date or active strategy — or any strategy at all. This “gap of ignorance,” coupled with the absence of a cybersecurity strategy, is a major threat and financial risk to every business.

The cost of cyberattacks

In the Vistage survey, 24% of respondents indicated they have experienced a cyberattack in the last 12 months. It's likely that this percentage is under-reported for two reasons: One, some companies don't know they've been hacked; a recent study from Ponemon Institute found that it takes U.S. companies 206 days to detect a data breach. Two, some companies don't want to admit that they've been hacked because it can cause a loss of credibility with customers and compromise their brand and reputation.

For SMBs, the cost of a cyberattack ranges. On the low end, a company can lose a couple hours of productivity and a couple thousand dollars. On the high end, a company can experience a complete loss of data, extended periods of system downtime and financial losses that exceed \$500,000.

Michael Markulec, Vistage Chair, partner and co-founder of Harbor Technology Group, says that according to Symantec, the average cost of a cyberattack is \$188,242 for SMBs. But that figure doesn't account for productivity losses, trust losses, or brand and reputation costs, nor does it reflect the potential cost of losing our business entirely.

Protecting and defending against cyberattacks

This research report was created to help bridge the gap of ignorance preventing most SMB CEOs from building an effective cybersecurity strategy. We've broken down the report into four parts:

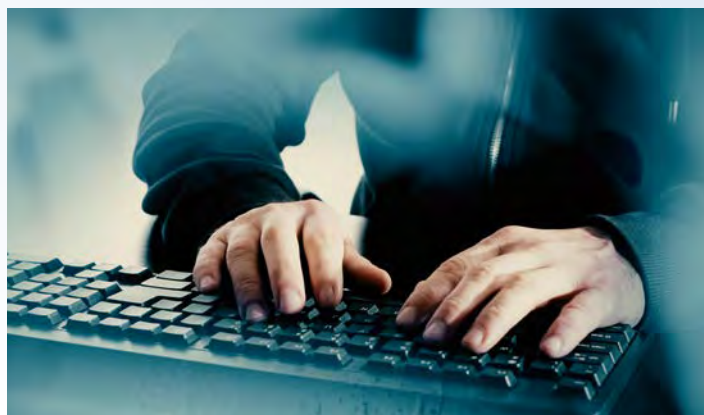
Part I: Threats you should know: Common cyberattack threats and their implications for SMBs

Part II: Getting started: Tactics for assessing the cybersecurity of a business

Part III: A framework for cybersecurity: How to establish a strong cybersecurity program

Part IV: Best practices: Required and recommended approaches to cybersecurity

Our goal is to help SMB CEOs make a conscious decision about the level of risk they're willing to take with their cybersecurity and then chart a course forward based on that decision.



“Attackers come through the soft underbelly of the supply chain — through the Fortune 5000.”

Ken Barnhart

Founder and President, Highground Cyber

206


Number of days to detect a data breach
Ponemon Institute

\$188,242

Average cost of a cyberattack
Symantec

60%

Percentage of hacked small and
midsize businesses that go out
of business after six months
National Cyber Security Alliance



“Attackers are always at least one step ahead — and sometimes 10 steps ahead.”

Mike Foster

Founder and CEO, The Foster Institute

Part I: Threats you should know

At its most basic level, the goal of a cyberattack is to steal and exploit sensitive customer, employee and financial data. SMBs are at risk for the following threats.

Malware:

Code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other “bad” or illegitimate action on data, hosts or networks.

Ransomware:

Ransomware is a form of malware that locks up computers and demands money in exchange for the key. Innovations such as cryptocurrency — which prevents payment tracking — have spiked the use of ransomware in the past few years.

Business email compromise (BEC):

An attacker creates an email that appears to come from the head of the company. Many times, this email instructs someone in the company to wire funds.

Supply chain hacking:

An attacker hacks a service provider and then uses that company to enter a larger company in their supply chain.

Remote access Trojan (RAT):

Hackers control a computer through remote means. The RAT often gains access when an employee opens a fraudulent link or attachment in an email, which allows the malicious software to bypass firewalls.

Drive-by downloads:

Attackers embed malware within an ad that’s posted on a reputable site and entice users to click on it.

Spyware infections:

Spyware can steal user and company information, weaken the security of devices and increase malware infections. Spyware downloads itself onto your computer via an email you opened or a website you visited, and scans your hard drive for personal information. It differs from a virus in that a virus is a piece of code that causes damage to your computer either by deleting or corrupting files.

Security breaches via IoT:

The internet of things (IoT) is making it harder for companies to determine which devices are connected to their network, and hackers are moving faster to exploit security weaknesses in these devices.

“No CEO wants to send a message to their customers letting them know their data has been exposed or have that communicated in the market. Few SMBs can afford or are prepared to take the cash hit a cyberattack can inflict.”

Joe Galvin

Chief Research Officer, Vistage

Real stories of cyberattacks

Wire transfer fraud in the C-suite

A hacker used social engineering to impersonate a CEO — over both email and phone — and convinced a CFO to wire funds to their account over the holidays. The company lost \$400,000 in fraudulent wire transfers.

Ransomware disguised as an invoice

At a local government office, a finance administrator clicked on what she thought was an invoice. It ended up being ransomware that infected all of the servers within the municipality. Leadership paid the ransom to decrypt the files, but the key didn't work. They had to hire an external security expert to fix it.

Former employee steals data

A top salesperson stole customer relationship management (CRM) data when they left the company. The company tried to sue, but the case never went to trial because the company couldn't demonstrate that they had any security measures in place to protect their data (e.g., policy documents, governance controls, technical controls).

Malware at a coffee shop

A CFO was working remotely at a coffee shop. He clicked on an email attachment, which turned out to be ransomware. It locked up his computer until his company paid the ransom. But once the computer was unlocked, the company had to decrypt it — a process that cost several weeks of productivity and caused reputation damage.

Part II: Getting started

If your company doesn't have a cybersecurity strategy in place, where should you begin? Thomas Stewart, executive director of NCMM, recommends that CEOs take these four steps, which should include different leaders from your company as well as your accountant/auditor and lawyer/legal counsel.

	Goal	Recommendations	Questions to ask
Step 1	Determine your company's current cybersecurity status.	Bring together members of your senior leadership team, board of directors and investors to conduct an informal audit of the business. Get a sense for the level of security you have today.	<ul style="list-style-type: none"> Is anyone in charge of our cybersecurity? If so, are they the right person to oversee our security? What defenses, if any, do we already have in place? Is our strategy comprehensive and coordinated? If not, can we pinpoint our weak spots?
Step 2	Determine who will oversee and be accountable for your cybersecurity strategy.	Engage leaders from across the organization — not just those within IT. Include different functional areas, such as human relations, marketing, operations and finance. Other players essential to this conversation are your lawyer and your accountant/auditor.	<ul style="list-style-type: none"> Who should be responsible for our cybersecurity? What process can we implement to ensure accountability? How can we communicate and increase awareness about cybersecurity in our different departments and teams?
Step 3	Take an inventory of your assets, determine their value, and prioritize your most critical assets.	Identify the "crown jewels" in your company, whether they're employee records, intellectual property or customer data. Recognize that you will never be 100% safe from an attack, so prioritizing areas of defense is important.	<ul style="list-style-type: none"> What are the most important assets we need to protect? Customer data? Intellectual property? Employee records? Can we measure the degree of confidentiality, integrity, availability and safety of our most critical assets?
Step 4	Decide what business capabilities and cybersecurity measures you want to manage yourself versus outsourcing.	Consider whether it makes sense to outsource certain aspects of your business to a cloud-based system to increase your security. At the same time, consider whether it makes sense to engage a cybersecurity expert or provider. Decide whether you want to work with a consultant to figure out your cybersecurity plan, or if you want to outsource your cybersecurity entirely.	<ul style="list-style-type: none"> What aspects of our business — such as order fulfillment — should we handle internally versus outsourcing to a third party, such as Amazon, Cisco or Google? Should we outsource our cybersecurity to a third-party service? Should we use a fractional CIO model and seek out cybersecurity consulting? Or should we handle the entire process ourselves?

Part III: A framework for cybersecurity

Many assessments are available to determine your state of cybersecurity readiness. The NCMM has developed a cybersecurity framework and self-assessment tool for establishing a comprehensive security plan that includes three core components: people, process and technology.







"This is about having a layer defense," says Joey Muniz, security architect for Cisco. "You could have the best technology in the world, but in the end there also have to be people behind this. And process is extremely important. You have to have all three."

The following recommendations can help you align your cybersecurity strategy with this best-practice model.

PEOPLE

Bring awareness and training to employees.

There are many ways to approach training — and many economical solutions that cost less than \$100 per employee. Here's what the experts recommend:

-  **Train employees to abide by basic security principles.** Establish basic security practices, such as using strong passwords, maintaining appropriate internet use, and handling customer information and data with care.
-  **Build a security consciousness.** Consider using internal phishing simulations to teach people how to spot common signs of an attack.
-  **Invest in a stock test package.** Similar to the simulation tool, this training will teach employees how to spot email scams and to evaluate whether a link is suspicious.
-  **Cross-train employees.** Give employees the opportunity to shadow IT personnel so you can build a team of unofficial deputy IT managers. This also creates more redundancy in your security by spreading out responsibility.
-  **Communicate why security matters.** Help your employees understand why this training is important and what's at stake for the company. Get past legal language and make it personal.
-  **Hire a fractional CIO.** If you're on a budget, use a fractional (contract or third-party service provider) model to get IT experts when you need them.

Q: How do I help my employees understand that cybersecurity is important?

A: Make it personal, so that employees realize that this isn't just a rule, it's something that's impacting them and impacting the business. You might say something like "We're getting hit with these attacks, and it's costing the company X amount, which means that we might not be able to give out raises in the next few months."

Joey Muniz
Security Architect, Cisco





Ken Barnhart

President and Founder,
Highground Cyber

Cybersecurity is a CEO problem

Far too many CEOs mistakenly believe cyber is an IT problem. IT lacks the organizational authority to run a cybersecurity program effectively. IT professionals have operational and technical responsibilities, but they cannot run a competent cybersecurity program from the first-amongst-peers position.








CEOs have to take back the authority they have abdicated to IT. Only the CEO has the decision rights necessary to make the trade-off calls that have to be made. A CEO is the only corporate officer with sufficient authority to say, "HR, we are going to rewrite a policy. I am going to get corporate counsel involved. We are going to make sure this is done in concert with operations." They are the air traffic control tower for the organization.

If the CEO doesn't do this, the consequences are real. The courts have been extremely clear on this issue. They're holding the CEO and the board of directors personally accountable for the cybersecurity of their firms. If you don't demonstrate that you have a credible, competent cyber program, and you have a cyberattack, you will be found to be grossly negligent.

PROCESS

Implement robust policies, processes and procedures.

Policies, processes and procedures help a company stay in control of their cybersecurity. Here's what the experts recommend:

-  **Have an acceptable use policy.** Tell your employees how they are allowed to use the company assets — whether that's Office 365, a laptop or a mobile phone. Provide guidelines for social media use.
-  **Create a playbook for different scenarios.** Four times a year, get your team together and work through a cyberattack scenario as if it were a fire drill. Work out your game plan and figure out whom you'd call in an emergency.
-  **Limit employee access to sensitive data and information.** Your employees don't need full access — or equal access — to your sensitive data and information. Make sure each employee's access is tailored to their individual role and responsibilities.
-  **Meet with a cybersecurity expert on a biannual basis.** Routine meetings with your cybersecurity advisor are as essential as regular meetings with your financial advisor.
-  **Put someone in charge of checking logs.** Assign a member of your IT staff to look at firewall logs, antivirus logs and anti-malware logs on a routine basis. They can document this on a simple spreadsheet.
-  **Conduct an external review of IT.** Regularly review what IT is doing as a function to ensure the data and network of your organization are secure and that everything that is in place is current.
-  **Stay current on security issues.** Set up an RSS feed so you're tuned in to the latest cybersecurity news.

"In the end, it's all about protecting the confidentiality of your data, making sure your data is accessible and making sure your data maintains its integrity," says Muniz. To meet those goals, he advises companies to use the following matrix to set expectations and hold people accountable:

Type of expectation	Who is accountable	Why they matter
Policies	C-level leaders	Fulfill the goals of the business, as established by senior leadership (e.g., provide excellent service)
Standards	HR and specific functional teams	Dictate whom you hire and what they are responsible for (e.g., the marketing group is responsible for delivering world-class service)
Procedures	All employees	Provide step-by-step guidelines for employees; clarifies what needs to be done to meet standards
Guidelines	All employees	Provide recommendations based on industry best practices

Expert perspective on Process



Michael Markulec
Vistage Chair, Partner
and Co-Founder, Harbor
Technology Group

Bring discipline to IT practices

Companies need to put basic defensive strategies in place and have good processes and procedures. Backing up data should be routine. Too often, we just put some random measure in place and move on to the next task. We wouldn't treat our financial reports with the same lack of discipline that we treat our communications systems.

A comprehensive set of IT security policies is required to comply with regulatory frameworks (such as HIPPS, PCI DSS, NIST 800-53). Additional policies provide guidance for your IT staff on security operations. At a bare minimum, you need an acceptable use policy. But you can't just write policies; that's only one-third of the job. The other two-thirds is providing training and enforcing policies.

We task our controller with producing a report on our financial data each month. Certainly, you can do the same thing on the IT side. You can do it in a very low-budget spreadsheet kind of way, or you can bring technology to bear if you think it is appropriate.






TECHNOLOGY

Make smart technology choices.

When it comes to cybersecurity solutions, SMBs have a lot of options. These include:

- **Antivirus software.** Defends against most types of malware.
- **Endpoint security solutions.** Cost about the same as anti-virus software and can be more effective.
- **Firewalls.** Provide an added layer of protection by preventing an unauthorized user from accessing a computer or network.
- **Data back-up solution.** Can recover any information lost.
- **Encryption software.** Protects sensitive data, such as employee records, client and customer information, and financial statements.
- **Two-step authentication or password-security software.** Reduces the likelihood of password cracking.

However, a monetary investment in technology is only one part of the equation. Technology has to work in concert with your people and processes and in accordance with your overall cybersecurity strategy. As you work out this balance, keep the following in mind:

-  **Choose service providers with strong security.** Every company that serves your company — such as a firm that manages your payroll — has to have good security to keep you secure.
-  **Get application controls.** With application controls, companies can program their computers to only run a preapproved set of business-essential programs (e.g., Microsoft Word, Excel and Firefox). When these controls are implemented, viruses can't run.
-  **Apply the concept of minimalism to staff computers.** A lot of computers come pre-installed with free versions, lite versions or trial versions of programs. Uninstall the ones you don't use. This removes “toeholds” for hackers and makes your computer more slippery.
-  **Get a second multifunctional printer.** Here's the logic: If your company's printer breaks down while IT is dealing with a major cybersecurity issue, the company can continue to function — and IT can be free to work on the issues that really matter for your business.
-  **Remember that antivirus software won't protect you from everything.** Attackers are often a step ahead of the latest antivirus software, so don't let that be your only form of defense.

Q: How much should I spend on cybersecurity?

A: It varies dramatically by company and risk tolerance. However, a good rule of thumb for SMB CEOs is to spend about 1-1.5% of your time thinking about cybersecurity and spend about 1-1.5% of your revenue on security measures.

Michael Markulec

Partner and Co-Founder, Harbor Technology Group

**Mike Foster**

Founder and CEO,
The Foster Institute

How you manage patches is critical

CEOs can ensure their company has a best-practice approach to addressing security vulnerabilities through patches. A patch is a piece of software that's designed to update, fix or improve a computer program or operating system. Software companies produce these patches in the form of downloadable programming code, and they are only effective if they are installed across a company's network. If your company does not have a patch on every single computer, attackers can infiltrate your systems quickly.

There are three steps that guide the successful application of patches. First, the patch should be tested in an environment that is similar to your company's environment, such as through desktop virtualization. The patch should be tested to make sure it doesn't break systems including Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) and all other systems on the network. Second, IT resources should practice uninstalling the patch. That way, if the patch crashes the network, there is a known process to remove the patch. Third, IT should ensure the patch is applied in stages; that is, it is installed on few computers initially, and then expanded to a quarter of the computers, next on half of the computers, and finally on all of the computers. Patches are essential. They are one of the best ways to ensure your company's computers are protected.

A success story in cybersecurity

The CEO of a third-generation family business — a company that produced circulars and flyers for Sunday newspapers — was working late on a Friday night. All of a sudden, the CEO's computer went black and a message appeared on her screen: "We have all of your company's data. Pay us \$50,000 in Bitcoin, or you'll never get your data back."

The CEO panicked. She thought, "The company that my grandfather founded — and my father handed to me — is going to go out of business on my watch. All of my 75 employees are going to lose their jobs."

She contacted the director of her IT department to share the bad news, but received good news in return. Two weeks prior, the IT director explained, the technology team had backed up all of the company's files to a third-party source. Over the weekend, the team was able to restore all of the lost data. And by Monday morning, the company was back in business.

Part IV: Best practices

No matter where your company's cybersecurity program stands today, your work is not yet done. "Security is a journey, not a destination," says Muniz. "You don't become secure. You continue to be secure."

"The data show that many SMBs are at the beginning of their cybersecurity journey," says Petrik. "As you start or continue on your journey, consider these questions and recommended actions to help make sure your employees, your business and your customers are secure."

Current state of SMBs	Question for CEOs	If yes, then...	If no, then...
38% of SMBs have a current and active cybersecurity strategy.*	Do you have a cybersecurity strategy?	Have a cybersecurity expert review your strategy, ideally every six months.	Take inventory of your assets so you can start to develop a risk profile that will determine your strategy.
67% of SMBs work with an external partner to manage their cybersecurity.*	Do you work with a professional cybersecurity specialist?	Review their qualifications. Check for certifications such as Certified IS Security Specialist (CISSP), Certified IS Auditor (CISA) and Certified Ethical Hacker (CEH).	Look for specialists who have certifications such as Certified IS Security Specialist (CISSP), Certified IS Auditor (CISA) and Certified Ethical Hacker (CEH).
51% of SMBs buy cybersecurity insurance.**	Do you have cybersecurity insurance?	Make sure you're meeting best practices in terms of people, process and technology. Otherwise, if you get attacked, you will need to prove that you have done your due diligence in terms of security. The insurance company may deny your company's claim, citing its lack of security.	Don't buy insurance until you've built a strong cybersecurity program. In the event of an attack, you will need to be able to prove that you did everything in your power to protect the security of your company. Otherwise, the insurance company may find you liable for the attack.
27% of companies are fully compliant with cybersecurity regulations such as NIST, PCI, SOX and HIPAA.**	Is your company compliant with security regulations?	Continue to review regulations on an annual basis to ensure that your company is abiding by best practices in cybersecurity to remain compliant.	Make compliance a top priority, and not just because it helps protect your company against a breach. Noncompliant companies may face legal ramifications in the event of a cyberattack.

* Source: Q4 2017 Vistage CEO Confidence Index survey, n = 1,377

** Source: Q1 2018 Vistage CEO Confidence Index survey, n = 1,707





Executive summary

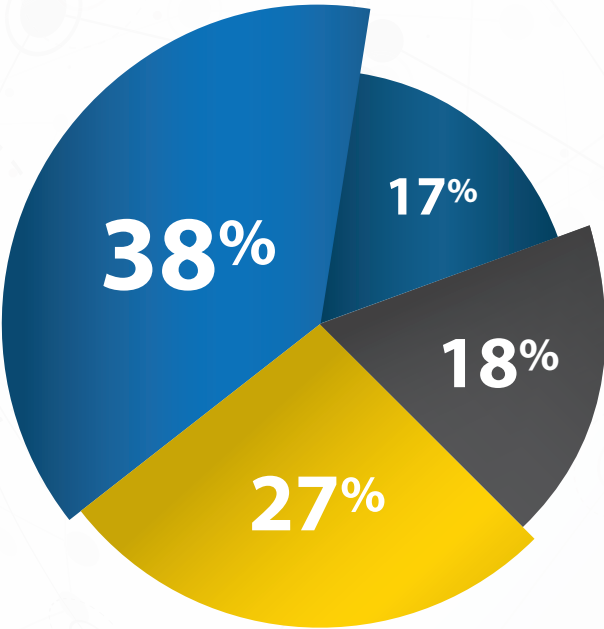
If you maintain customer, employee or financial data, you are a target for cyberattacks. If you use technology to communicate, store data, or connect with suppliers or customers, you are exposed. Because of their size and lack of IT resources, SMBs are especially vulnerable, and hackers know it. Choosing to completely ignore the threat of cyber — as 27% of SMBs do — is equivalent to not wearing a seatbelt: You might get away with it, but you might not. It's a risk you choose to assume.

- If you are among the 38% of SMBs who have an active cyberstrategy in place, you must remain diligent. Cybercriminals are working full-time to create new threats, viruses and other nefarious ways to compromise your systems. Maintain and update your plan at least every six months, and continuously educate your people. Accept the fact that you will always be spending money to protect your customers, employees and data.
- If you are among the 18% of SMBs whose cybersecurity plan is “in development,” expedite the process.
- If you are among the 17% of SMBs with a plan that’s not current, fast-track an update. Cyberthreats are growing, evolving and becoming more sophisticated.
- If you are among the 27% of SMBs without a cybersecurity strategy, the liability — legal or otherwise — still exists. Consciously deciding to not protect or defend your systems, applications and data is putting your customers and your employees at risk.

The data, insights, expert perspectives and framework provided in this report can help you get started. Just as you may have an outside legal counsel or CPA, consider engaging a cybersecurity professional for additional support. Only you can decide to ignore the realities and risks of living in the Information Age without security.

Does your company have a defined cyber-risk strategy that is documented and communicated to executive leaders?

-  Yes — strategy is current and reviewed at least annually
-  Yes — but the strategy is not current and does not have a scheduled review cycle
-  No - but we are actively working on a cyber-risk strategy
-  No - our organization does not have a defined strategy



Contributors



Ken Barnhart

Founder and President, Highground Cyber, Inc.

Ken Barnhart is an experienced business owner, CEO and IT executive. His current company, Highground Cyber, has been named one of the top 10 fastest-growing cyber companies. CIO Magazine recognized Ken's Smart and Safe Framework as one of the top 20 cyber security solutions for the middle market, and this assessment has been used by many Vistage members. As a speaker and cyber champion, Ken educates boards of directors, CEOs, and small business owners about how to improve their "cyber posture," using the language of business to discuss cyberthreats and the role and responsibility of business leadership. Ken also serves on the advisory board for the Global Cyber Security Summit, is a decorated combat veteran of the Desert Storm/Desert Shield Gulf War, and is co-founder and chairman of the board for the Center for Cyber-Resilience.



Mike Foster

Founder and CEO, The Foster Institute

Mike Foster is the founder and CEO of The Foster Institute. He has earned numerous certifications, including Certified Ethical Hacker, Certified Information Systems Auditor, and Certified Information Systems Security Professional. For the past 20 years, Mike has consulted with hundreds of companies regarding IT best practices for increasing productivity, profits and protection, and has helped CEOs, owners and executives understand and trust their in-house and outsourced IT professionals. Renowned for his IT expertise, Mike is a professional speaker, author of "The Secure CEO: How to Protect Your Computer Systems, Your Company, and Your Job," and has provided expert commentary for publications including USA Today, Forbes Magazine and The New York Times.



Joe Galvin

Chief Research Officer, Vistage

As chief research officer for Vistage, Joe Galvin is responsible for providing Vistage members with the most current, compelling and actionable thought leadership on the strategic issues of small and midsize businesses. Joe is an established thought leader and analyst who has researched and presented to business leaders around the world on customer management, world-class sales performance, and CRM and sales force automation technology.



Michael Markulec

Vistage Chair, Partner and Co-Founder, Harbor Technology Group

Michael brings decades of entrepreneurial and leadership experience to Harbor Technology Group, where he and his partners have developed a set of cybersecurity services tailored to small and midsize businesses. Michael's expertise on cyber policy and the global threat landscape has been leveraged by corporate leaders (Bank of America, Goldman Sachs, Hartford Insurance) and government officials (DoD, Veterans Affairs, Executive Office of the President, NATO, UK Ministry of Defense). As a speaker, Michael presents on a variety of networking and security topics.

**Joey Muniz****Security Architect, Cisco**

Joey Muniz is an architect at Cisco Systems and a security researcher with extensive experience in designing security solutions and architectures for Fortune 500 corporations and the U.S. government. Joseph's current role gives him visibility into the latest trends in cybersecurity, from both leading vendors and customers. Examples of Joseph's research include his RSA talk titled "Social Media Deception," which has been quoted by many sources (search for "Emily Williams Social Engineering"), as well as his articles in PenTest Magazine regarding various security topics. Joseph runs The Security Blogger website and is the author of and contributor to several publications covering various penetration testing and security topics. You can follow Joseph at thesecurityblogger.com and @SecureBlogger customer management, world-class sales performance, and CRM and sales force automation technology.

**Anne Petrik****Director of Research, Vistage**

As director of research, Anne Petrik leads the design, deployment and analysis of member surveys for Vistage, capturing the sentiment and practices of the Vistage CEO community. This analysis, in collaboration with perspectives from experts and partners, helps create insights for SMB CEOs through the thought leadership published by Vistage.

**Thomas A. Stewart****Executive Director, National Center for the Middle Market**

Thomas A. Stewart is the executive director of the National Center for the Middle Market, based at The Ohio State University. Previously, he served as chief marketing and knowledge officer for Booz & Company (now Strategy&) and was the editor and managing director of Harvard Business Review. He recently published the book "Woo, Wow, and Win: Service Design, Strategy, and the Art of Customer Delight" (co-authored by Patricia O'Connell).

About Vistage Worldwide

Vistage Worldwide is an organization designed exclusively for high-integrity CEOs and executive leaders who are looking to drive better decisions and better results for their companies. Our members — 22,000 strong in more than 20 countries — gather in trusted, confidential peer advisory groups where they tackle their toughest challenges and biggest opportunities. CEOs who joined Vistage in the past five years grew their companies 2.2 times faster than average small and midsize U.S. companies, according to a 2017 analysis of Dun & Bradstreet data.

Learn more at vistage.com.

About our research

Vistage curates subject matter from our community and collaborates with top thought leaders to create unique content. Vistage executives access actionable, thought-provoking insights from the Wall Street Journal/Vistage Small Business CEO Survey and Vistage CEO Confidence Index results, as well as national and local economic trends. Since it began in 2003, the Vistage CEO Confidence Index has been a proven predictor of GDP, two quarters in advance. Vistage provides the data and expert perspectives to help SMB CEOs make better decisions.

Learn more at vistage.com/confidenceindex and vistageindex.com.

About the National Center for the Middle Market

The National Center for the Middle Market is a collaboration between The Ohio State University's Fisher College of Business, SunTrust Banks Inc., Grant Thornton LLP and Cisco Systems. It exists for a single purpose: to ensure that the vitality and robustness of middle-market companies are fully realized as fundamental to our nation's economic outlook and prosperity. The center is the leading source of knowledge, leadership and innovative research on the middle-market economy, providing critical data analysis, insights and perspectives for companies, policymakers and other key stakeholders to help accelerate growth, increase competitiveness and create jobs in this sector.

Learn more at www.middlemarketcenter.org.

About Cisco

Today's cybersecurity experts use up to 50 vendors to protect their networks. Multiple vendors and multiple products lead to needless complexity and to gaps in threat defense. Cisco security products work together. They deliver effective network security and incident response. And they boost IT productivity through automation.

We have integrated a comprehensive portfolio of security technologies to provide advanced threat protection. Our technologies include next-generation firewalls, intrusion prevention systems (IPS), secure access systems, security analytics and malware defense. We offer web and email security, network security and cloud security. All this is backed by in-depth threat and malware intelligence. Let us help you keep a step ahead of the latest cyberattacks.

To learn more about Cisco's threat-centric approach to security, visit cisco.com/go/security.

