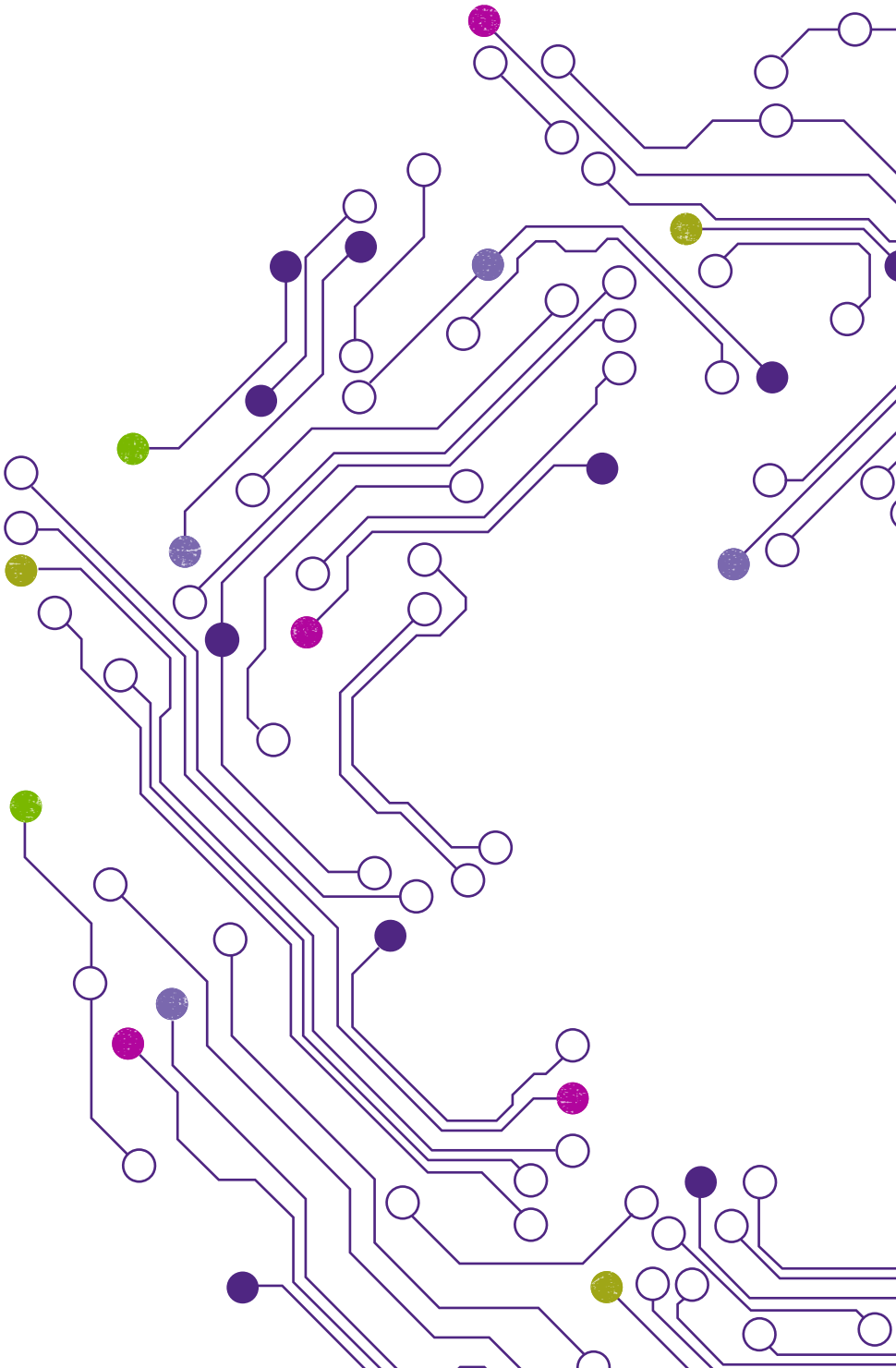
Grant Thornton

An instinct for growth™

The CFO's role in cybersecurity

CFOs play a critical role in establishing an effective cybersecurity program



ferf

financial executives research foundation

an affiliate of financial executives international

Contents

Author

William M. Sinnett
Senior Director, Research
Financial Executives Research Foundation

Contributors

Kevin Morgan
Principal, Business Advisory Services
Co-Leader, Cybersecurity
Grant Thornton LLP

Skip Westfall
Managing Director, Forensic, Investigative and Dispute Services
Co-Leader, Cybersecurity
Grant Thornton LLP

Johnny Lee
Managing Director, Forensic, Investigative and Dispute Services
Grant Thornton LLP

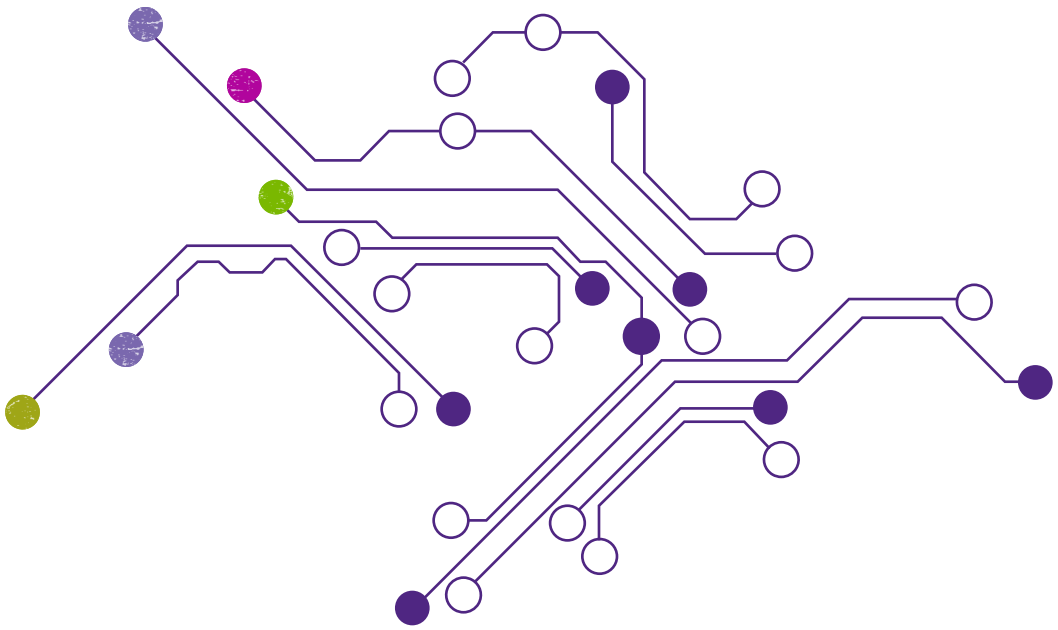
Executive summary

Organizations must comply with myriad industry standards while managing the security of both their proprietary and customer data, as well as brace for the possibility of unknown breaches and leaks. A data breach can be exceedingly costly and can jeopardize a business of any size. To help senior-level financial executives improve their cybersecurity and protect their organizations, Grant Thornton LLP and Financial Executives Research Foundation (FERF) identify critical elements of the CFO's role in protecting his/her organization from cyberattacks, as well as practical recommendations for establishing an effective cybersecurity program.

These findings are based on a survey of 98 members of Financial Executives International (FEI) and Grant Thornton clients, conducted between July and December 2014. The survey was followed by in-depth interviews of FEI members to get perspectives on a number of organizations' experiences managing cyberthreats.

Key findings include:

1. Respondents' top cybersecurity concerns include protection of data — including customer data and intellectual property (IP) — from data breaches and compliance with data security laws.
2. Either the CFO or the chief information officer (CIO) is usually responsible for the company's cybersecurity program. However, interviews revealed that collaboration between different groups is more reasonable.
3. Although the CFO is often responsible for cybersecurity, the organization's IT department typically manages the day-to-day aspects of cybersecurity. General counsel are usually involved as well, advising senior management and board members on legal responsibilities.
4. The CFO is often expected to assess cybersecurity risks, align cybersecurity strategy with business strategy and get buy-in from the board on necessary cybersecurity investments.
5. The most common impediment to developing an enterprise-wide cybersecurity strategy is a lack of understanding of cyberrisks and potential impacts of a breach.

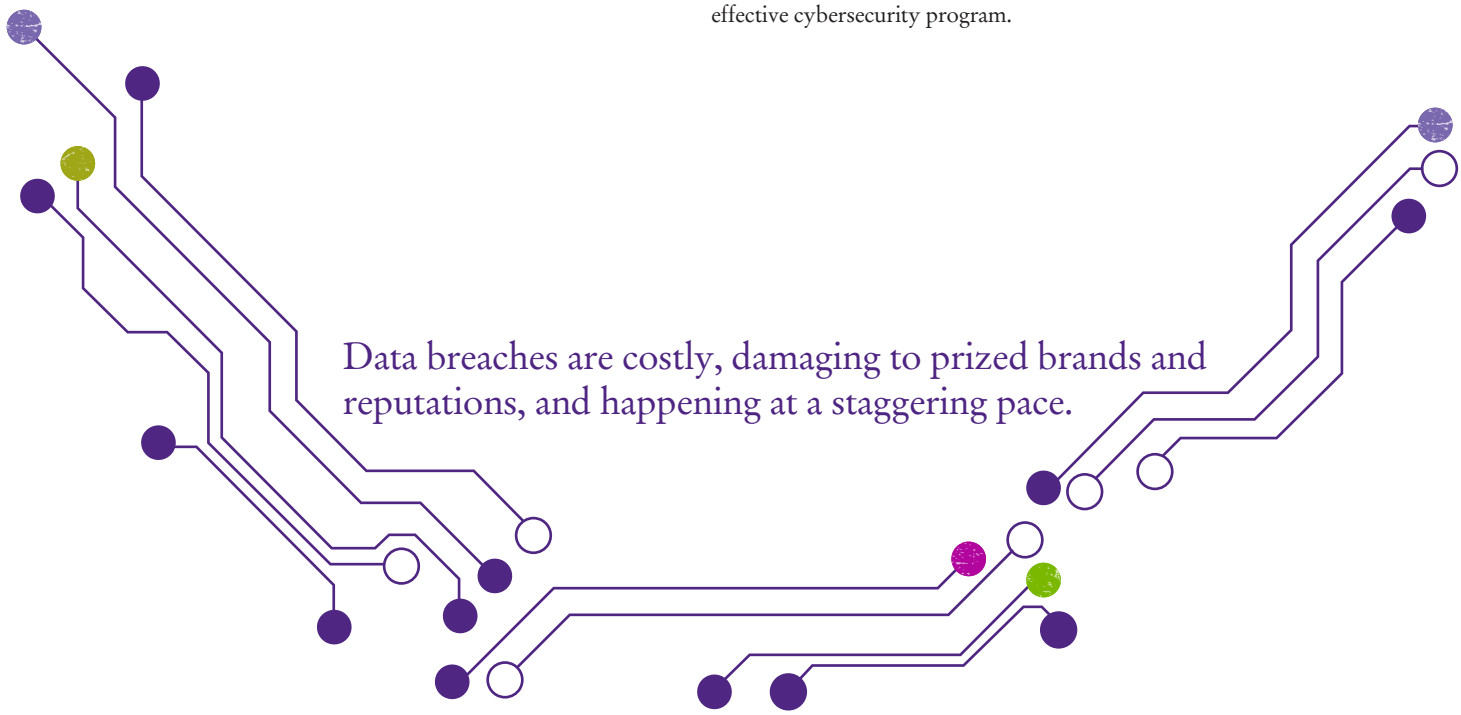


Introduction

Significant data breaches — security incidents in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual — at flagship companies are becoming nearly an everyday occurrence. At the same time, the costs related to these breaches continue to skyrocket. The Ponemon Institute's *2014 Cost of Data Breach Study: United States* puts the average cost for each lost or stolen record at $201, and the total average 2014 cost paid by organizations at $5.9 million for each data breach, up from $5.4 million in 2013. The surging costs are attributable to the "loss of customers following the data breach due to the additional expense required to preserve the organization's brand and reputation.[1]" In short, data breaches are costly, damaging to prized brands and reputations, and happening at a staggering pace.

The question is: What can companies — especially their CFOs — do about it? All data, including IP, is vulnerable to a data breach. And cybercriminals have become ever more sophisticated and continue to hone their methods at getting the data they want, whether it is trade secrets, medical records, financial data, Social Security numbers or more. Today's organizations must comply with numerous industry standards while managing the security of their data, as well as brace for the possibility of unknown breaches and leaks. While cybersecurity traditionally has been handled by the CIO and the IT function, the escalating risks have driven cybersecurity up the corporate ladder to the desk of the CFO.

Financial Executives Research Foundation (FERF), in collaboration with Grant Thornton LLP, surveyed CFOs to identify their critical role in cybersecurity, and offer insights and recommendations for establishing an effective cybersecurity program.



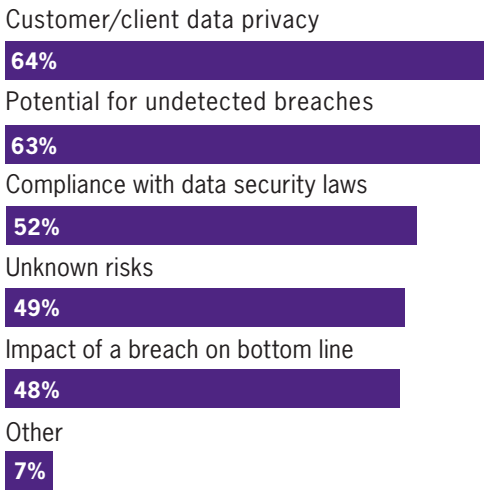
[1] "*2014 Cost of Data Breach Study: United States*," May 2014. See http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis for more information.

Top cybersecurity concerns: What is on the minds of CFOs and CIOs?

A majority of survey respondents indicate that their organizations' top cybersecurity and data privacy concerns are the protection of customer and client data (64%), followed closely by the potential for undetected breaches (63%). (See Figure 1.)

Skip Westfall, managing director of Forensic and Valuation Services with Grant Thornton LLP and co-leader of its Cybersecurity practice explains: "Protecting customer data and safeguarding against data breaches are important and necessary concerns for CFOs. However, many CFOs are insufficiently concerned and possibly even unaware of items they should be protecting, such as data that leaves the four walls of their organization when it is shared with a third party or vendor."

Figure 1: What are your organization's top cybersecurity and data privacy concerns?



Participants were able to select all responses that applied.

Concerns vary by business type

While protecting client and customer data are top of mind for most CFOs and CIOs, cybersecurity concerns vary considerably depending on the particular business. For instance, a technology CFO tends to focus on cyberthreats to IP; a marketing firm that handles third-party data worries about a breach of clients' records; and a food company CFO sweats issues such as mobile device security and phishing schemes.

Phil Roush, vice president of finance and head of internal audit at SanDisk Corp., a multinational corporation that designs, develops and manufactures flash memory storage solutions and software, says that his three primary cybersecurity concerns are protecting IP, employee data and customer data. "Our business model is based on flash memory technology, so the programs, software, design and schematics — all of that IP is critical to our company and drives our brand value," says Roush, adding that SanDisk's customer and employee data is also critical.

Paul Karras, senior vice president and CIO at Wilton Brands LLC, the leading supplier in the U.S. crafts industry, shares a litany of concerns, including phishing, social engineering malware and mobile devices: "Phishing and email attacks are extremely worrisome." An additional concern is social engineering, when rogue individuals manipulate people into divulging confidential data. "There are a lot of folks out there who pretend to be somebody that they're not, and try to win your trust so that you will disclose information to them, or release funds to them." Malware and bots are also on Karras' mind. "Any time you receive an email from somebody you don't know, and there's an offer for you to click through, you could be opening a malware site that can unleash corruption within your organization. Unless people within your organization are informed, it's very difficult to stop."

Karras adds, “We have company-issued devices, as well as people who bring their own device to work. Unless there is an effective mobile device management strategy in place, and the tooling behind it, it's very difficult to manage that.” Finally, Wilton Brands is concerned about hacked accounts. “If you don't have a strong password level control within an environment,” explains Karras, “it's easy for somebody to have a robot on the other end that can hit your login ID, and within a second have 15,000 attempts to enter into your company.”

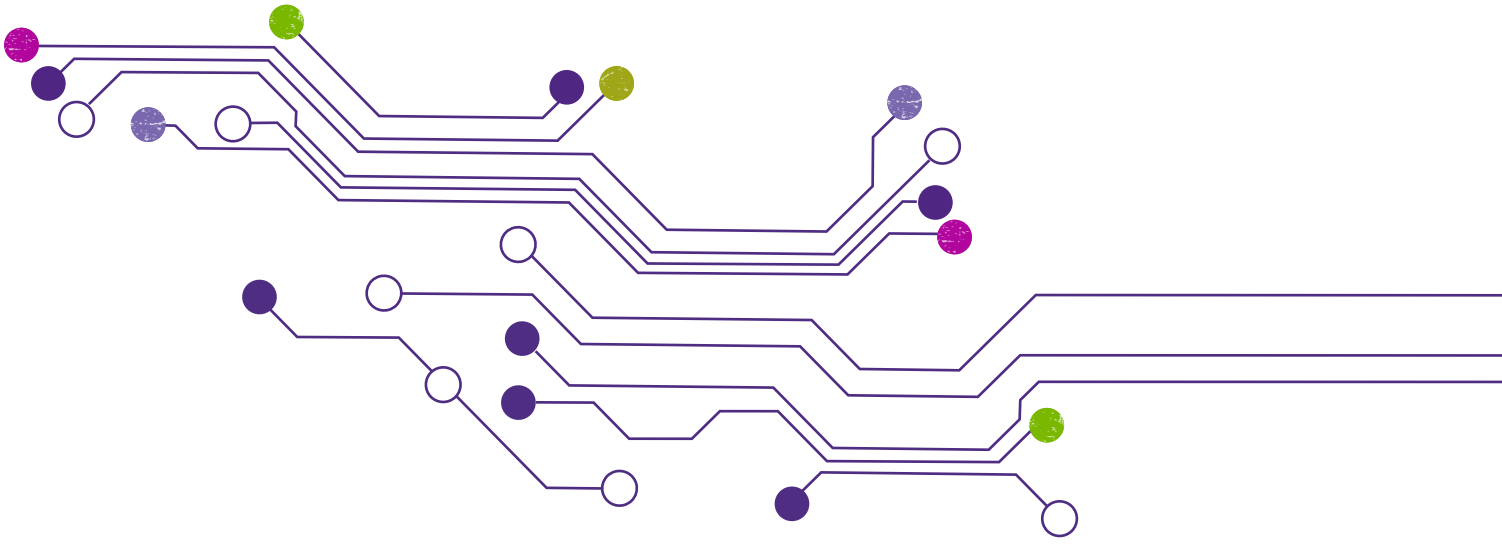
Companies that handle large amounts of data on behalf of their clients are for obvious reasons worried about data breaches that could affect clients. Gary Long, executive vice president and CFO at Ivie & Associates, a full-service global marketing company, worries about this issue. “We're a marketing agency and we work with a lot of retailers. Our concern is a data breach would impact those retailers in a negative way. We've all seen what's happened with some prominent retailers recently,” notes Long.

Doug Miller, CFO at law firm Sutter O’Connell Company, explains, “Because we deal with injuries, we have medical records, and we don't want those to be exposed to the outside. Medical information theft is much more lucrative than straight-up identity theft and is, therefore, alluring to cybercriminals.” He continues, “With a name, Social Security number and insurance identification number, a criminal can set up a fake doctor's office and start pumping in claims.”

Threats keep evolving, so CFOs can’t rest easy, says Miller. “Before it was Social Security numbers, bank account numbers and credit card information; now it's medical information. What's the next piece of information that somebody's going to want?”

Compliance is another major concern, particularly as laws governing information security continue to change. For universities, a key risk is privacy related to student records.

Judy Roy, executive vice president of finance and administration at Indiana Tech, a private university with 8,000 students, says that compliance with data security laws and student data privacy are her top concerns. “We've got a whole realm of personal data on our students that we need to keep secure — not only Social Security numbers, but names and addresses, as well as grades and payment information.”



Organizational structure around cybersecurity

Who is responsible for cybersecurity?

The CFO was most often identified as the position within the organization responsible for cybersecurity (38%), followed by the CIO at 36%. (See Figure 2.)

These responses show that CFOs are getting more involved as the advocate for strategic initiation and implementation of their organizations' cybersecurity measures — this migration is due to their unique position of internal and external visibility with their organizations. Also, they are in the best position to address the imminent scrutiny that companies may receive from the SEC and other regulators. Cybersecurity has been listed as a top examination priority for 2015 by the SEC's Office of Compliance Inspections and Examinations.

Figure 2: Who is responsible for cybersecurity?

While 74% of respondents' cybersecurity function is led by either the CFO or CIO, interviews reveal that, in fact, responsibility is often shared among more than one member of the organization, such as the chief information security officer (CISO), internal audit, CIO or general counsel, rather than one designated position. Given that the role of the CIO is to strike a balance between the budget and running a smarter business through technology implementation, a natural conflict of interest may arise between a CISO's duty of protecting the company's assets regardless of budget and the CIO's role of protecting the budget. This may, of course, differ based on the size of the organization.

Some organizations appoint a CISO to oversee cybersecurity and report to the internal audit leader or CFO. The creation of such a position can decrease the cost per record of information, in the event of a breach, by $6.59.[2]

[2] *Ibid.*

A multidisciplinary approach

Given that organizations are faced with constant cybersecurity threats, incidents and breaches, Kevin Morgan, principal of Business Advisory Services with Grant Thornton and co-leader of the firm's Cybersecurity practice, agrees that a shared approach is often best. "We recommend that the IT, general counsel and finance departments work closely together at the outset of projects to protect attorney-client privilege." Indeed, agrees Johnny Lee, a managing director in Grant Thornton's Forensic, Investigative and Dispute Services group, a former attorney, and a member of the cybersecurity leadership team. "Careful consideration should be paid to the question of privilege at the outset of these projects — even if they are assessment-oriented. These protections can be powerful if properly administered, but counsel should direct this work, and it must follow specific protocols throughout the life cycle of the project."

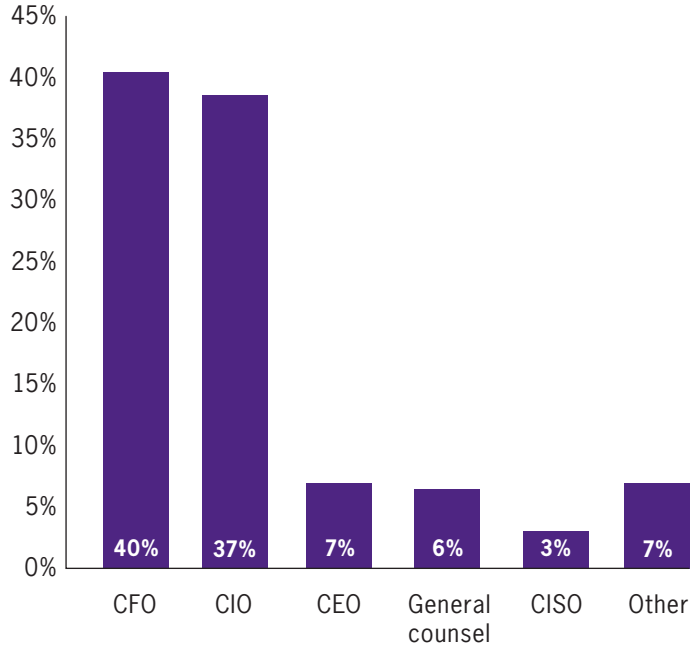
Morgan clarifies that information security incidents can constitute a variety of events, such as an unencrypted stolen laptop or smartphone, or sensitive documents in an unlocked file cabinet. While some incidents are considered breaches, incidents do not necessarily constitute a breach. "They do, however, herald a wake-up call to the organization that cybersecurity warrants immediate attention," says Morgan.

Morgan also cautions that sometimes organizational barriers, such as siloed functions, create additional challenges for companies trying to protect themselves from cyberattacks. "We recommend that organizations align the people, processes and technology that encompass its cybersecurity response structure. Then create an incident response plan that outlines roles and responsibilities."

SanDisk's Roush explains that the global information security officer in the IT organization is responsible for cybersecurity. "We [internal audit] work very closely with IT, but we design a series of audit projects within our internal audit plans that cover different aspects of security. In that way, we can provide an independent view of the security environment."

Mike Fishoff, CFO of Wilton Brands, notes, "IT leads cybersecurity at our organization, but legal is a close No. 2 because if we have any breaches or issues, those two functions work side by side."

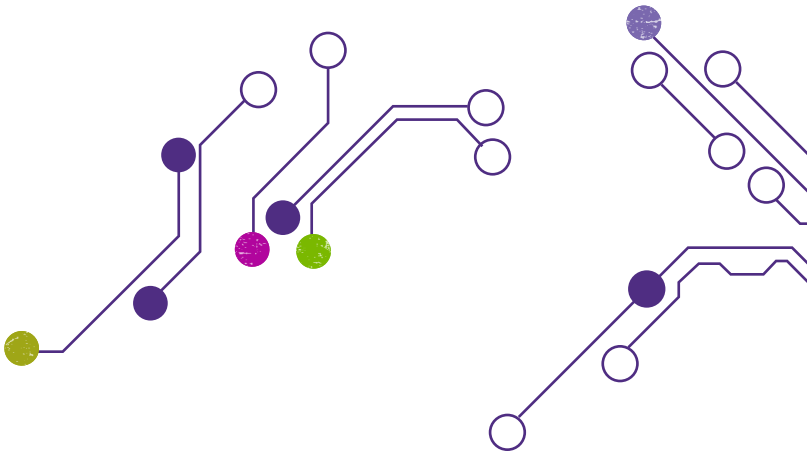
Figure 3: Who is responsible for reporting to the board about cybersecurity?



Reporting to the board

The CFO and CIO (40% and 37%, respectively) are responsible for reporting to the board on cybersecurity issues (see Figure 3). Not only should the CFO (or CIO) be reporting to the board on the organization's cybersecurity initiatives, but he/she should also be getting buy-in from the board on necessary cyberinvestments and advocating for cybersecurity resources.

While clearly boards are having discussions about cybersecurity, these statistics don't clarify how effective and engaged the board actually is. As the potential loss for each attack could range in the millions, it is imperative that boards focus closely on cybersecurity oversight, and the CFOs introduce the discussion.



At the barest minimum, boards should expect senior management — in this case, the CFO or CIO — to demonstrate that the organization has a robust cybersecurity plan in place. (The National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* provides a framework that can be used to establish this plan.)

In a roundtable conducted by the National Association of Corporate Directors (NACD) in 2013, directors agreed that it is a challenge to effectively oversee management's cybersecurity activities because of the lack of adequate knowledge. Therefore, it is essential that the board receive training on cybersecurity trends and threats, and/or nominate a cybersecurity subject matter expert to advise the board.

Given the high stakes, even though corporate directors are concerned about cybersecurity, they frequently are insufficiently knowledgeable about the subject — an opportunity for CFOs to help them understand the risks.

Roush sees education and training as one of the CFO's key cybersecurity roles. He urges CFOs to make sure board members understand the risks and educate them on what is considered sensitive information.

Interviewees report a range of perspectives about how effective their boards are when it comes to overseeing cybersecurity. In some cases, respondents say the board lacks the foundational knowledge and understanding to provide appropriate oversight. Other respondents say their board is engaged with cybersecurity threats, and receives continual updates from management on these issues.

Fishoff says that Wilton's board is engaged and that the CFO and vice president of information services jointly report to the board and the general counsel at least once a year. "Cybersecurity is a standing yearly agenda item. Obviously, if anything happens during the year — and we hope it doesn't — then we report on any incidents," explains Fishoff.

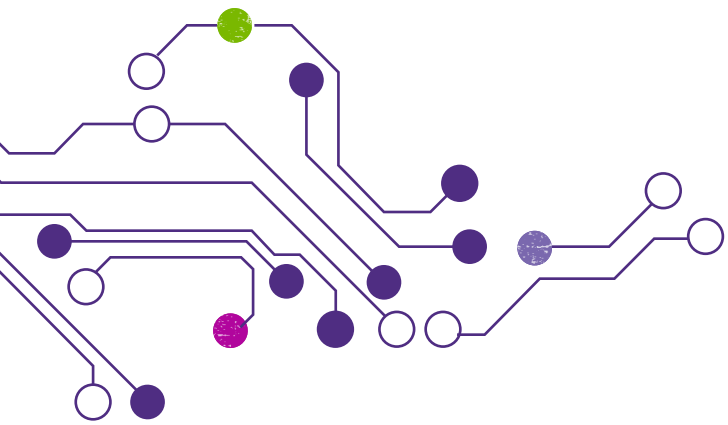
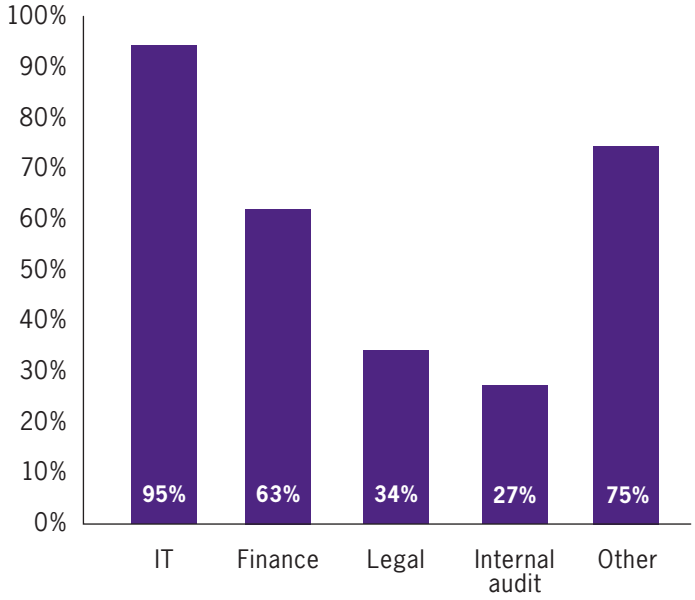


Figure 4: Which departments are involved with cybersecurity efforts?



Participants were able to select all responses that applied.

Who is involved with cybersecurity initiatives?

In the vast majority of organizations, the IT department is involved with cybersecurity (95%), followed by finance (63%) and legal (34%). (See Figure 4.)

More than three-quarters (76%) of respondents indicate that more than one department is involved. Three-quarters selected "other" and cite involvement of disparate roles, including HR, operations, the CEO, the chief risk officer and others.

Only 34% of respondents say the legal department is involved in cybersecurity efforts, which leaves ample room for improvement. Legal's involvement is essential because it plays a key role in confirming that policies are properly derived and in establishing the mechanisms that make sure organizations follow all applicable requirements. Additionally, as mentioned above, careful consideration should be paid at the outset of these projects to ensure that any privilege protections desired by the company are managed by counsel familiar with these legal nuances. The attorney-client privilege (and its related work-product doctrine) can offer protections from discovery to certain communications and analysis, but only if the work is performed at the direction of counsel in anticipation of litigation. These issues involve specific legal advice and should be discussed with counsel for the company — whether that be in-house counsel or special counsel appointed for the project.

An enterprise-wide approach

While cybersecurity was once relegated to a technical or operational issue handled by IT, a cross-departmental, enterprise-wide approach to cybersecurity is necessary, according to the *Cyber-Risk Oversight, Directors Handbook Series*, produced by the NACD. The publication suggests that cybersecurity should be evaluated and managed in the same manner as the organization considers physical security of human and physical assets.[3]

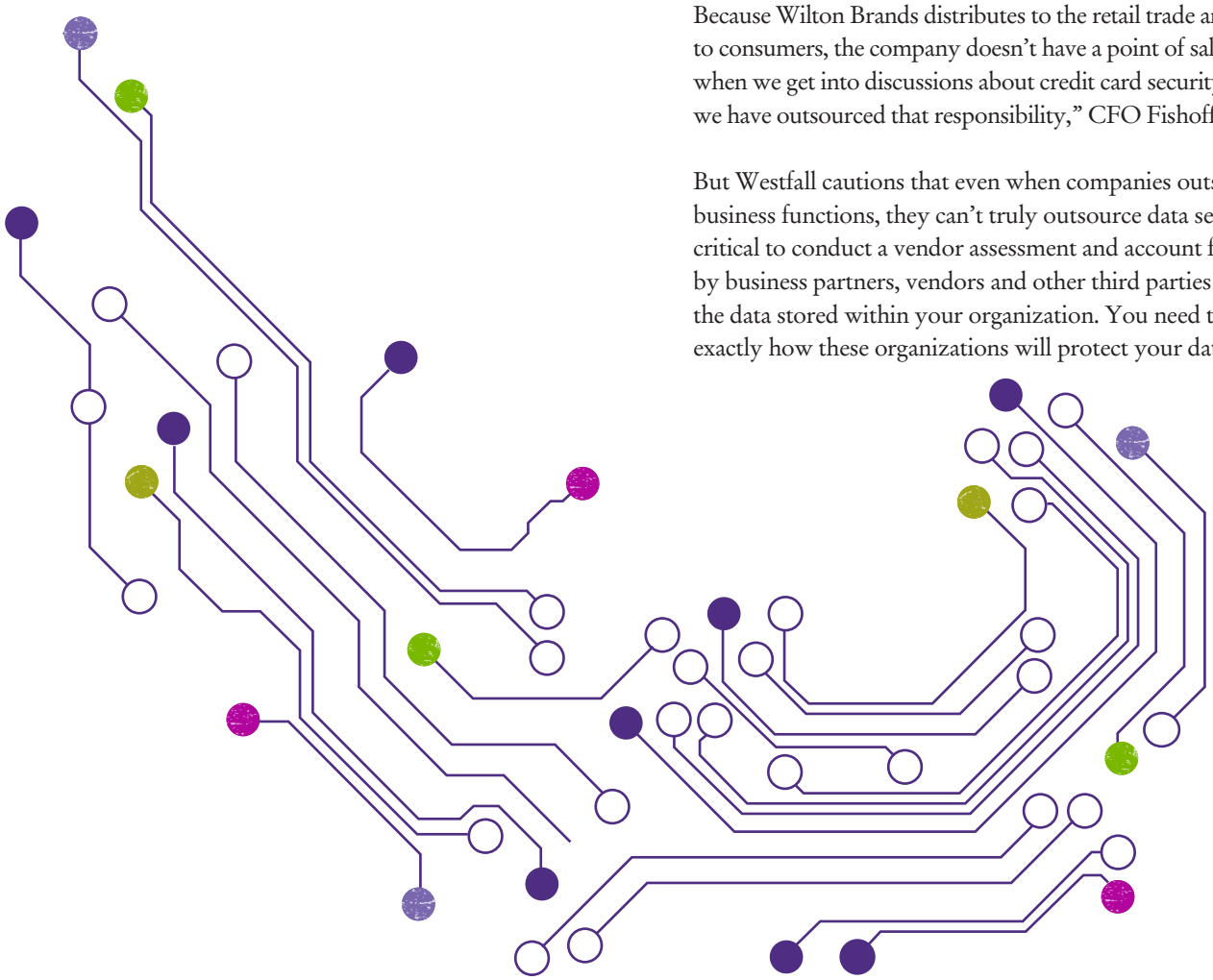
Consistent with survey findings, interviewees report that their efforts involve multiple departments. At SanDisk, the global information security officer leads cybersecurity efforts, says Roush. "But, there isn't one 'designated body' who is responsible for cybersecurity. We want to make sure we have common policies and practices, particularly within the labs. It's driven by our IT team and the global information security officer, with legal and HR departments collaborating as partners to design policies and drive actions."

At Wilton Brands, cybersecurity is a collaborative effort as well. Karras explains the role of each group within the organization:

- "IT owns the tools, such as the firewalls, antivirus software, password controls and mobile device management.
- Legal is our partner in terms of consultation, and they approve the data protection policies that we have in place. They also push out the data protection policies and report on compliance for any legal or regulatory obligations.
- HR is our change management partner, communicating to the organization in partnership with IT. And they also approve, and are consulted in terms of data protection policies, because they own a significant portion of employee information.
- Finance not only provides the funding and the resources around data protection, but they also are consulted with and approve the data protection policies."

Because Wilton Brands distributes to the retail trade and not directly to consumers, the company doesn't have a point of sale front. "So when we get into discussions about credit card security and privacy, we have outsourced that responsibility," CFO Fishoff says.

But Westfall cautions that even when companies outsource certain business functions, they can't truly outsource data security. "It's critical to conduct a vendor assessment and account for data held by business partners, vendors and other third parties — not just the data stored within your organization. You need to understand exactly how these organizations will protect your data," he says.



[3] *Cyber-Risk Oversight, Director's Handbook Series 2014* by the National Association of Corporate Directors.

Cybersecurity task forces

While establishing a cybersecurity task force is considered a best practice by many, the majority of respondents (84%) surprisingly do not have a task force in place yet (see Figure 5).

For those organizations that do not yet have a cybersecurity task force, Grant Thornton's Morgan recommends, "CFOs should establish a formal task force to help implement the strategic objectives of the organization's cybersecurity mission by reaching out and identifying the vulnerabilities in the data supply chain within their organization." Noting that the task force, at a minimum, should include IT, legal and finance, Morgan adds, "Who is involved depends on the size and vulnerability of the organization."

Those that have a task force indicate that it is made up of primarily the IT department, with support from legal, finance or other areas within the organization (see Figure 6).

Two interviewees say that their IT and legal departments are equal in their involvement in the task force. On Wilton Brands' task force, IT and legal take the lead for cybersecurity, but finance and HR are also involved.

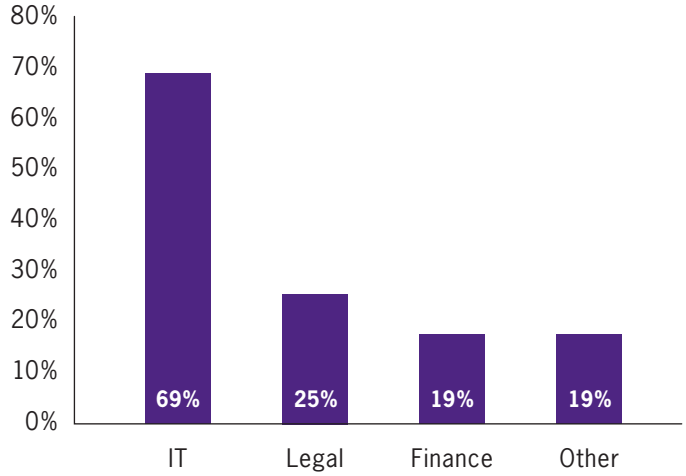
The cybersecurity task force at Ivie, likewise, involves IT and legal functions, among others. "Our general counsel has recently taken a very large interest in cybersecurity," CFO Long says, "so we now have a task force that includes the general counsel and our vice president of IT."

"Companies that have task forces, as well as those that have experienced breaches, have a much greater awareness of cybersecurity risks, and tend to have a more robust role for their legal function," says Melissa J. Krasnow, corporate and privacy partner at Dorsey & Whitney LLP.

"Preparing for cybersecurity involves being aware of the risks. Companies need to prepare and implement cybersecurity policies and procedures, which may be required by law, as well as incident response plans, which are a best practice in any event. They can be required as part of entering into a technology or other commercial transaction, including mergers and acquisitions," Krasnow explains.

Figure 5: Does your organization have a cybersecurity task force?

Figure 6: Which areas of the business are on the task force?



Strategy and practical considerations

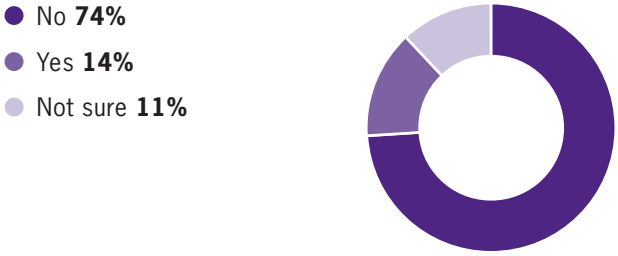
Most survey respondents (74%) have not experienced a cybersecurity breach within their organizations (see Figure 7). However, these findings are not reflective of larger data trends that show cyberattacks are on the rise.

Even if an organization has not been subject to an attack, it does not mean that efforts to secure information systems should be tabled — quite the contrary, since cyberthreats continue to be very real. Any company with data systems connected to the Internet is at risk of a breach.

Roy of Indiana Tech thinks that many organizations have a false sense of security, particularly those that have never experienced a data breach: "Many think that installing virus protection on your PC indicates that you are secure, and it is not. Cybersecurity is more than just installing software. You have to be proactive and find out if people are actively trying to intrude into your system."

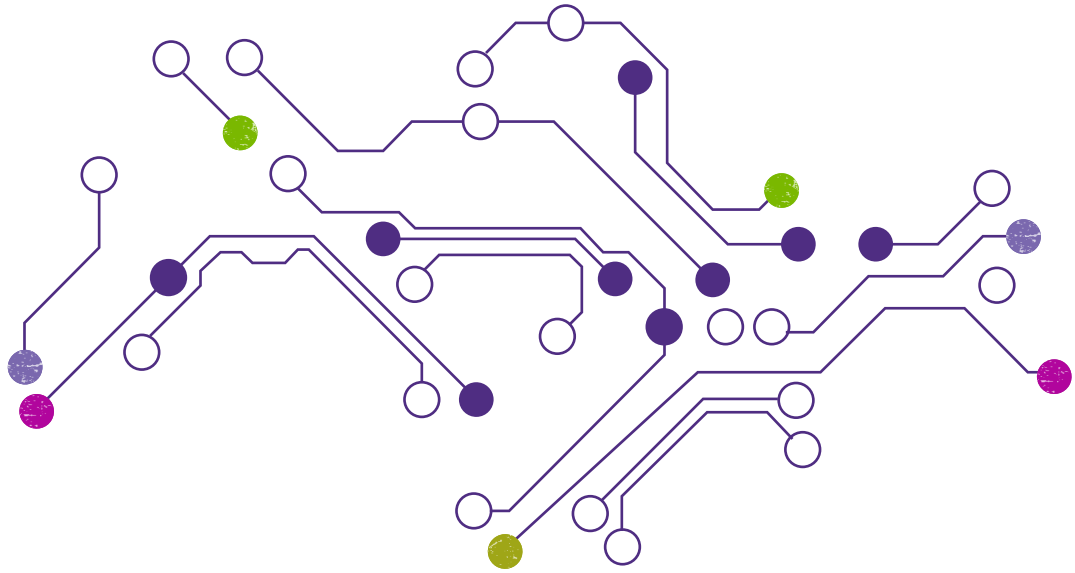
Of those that indicated a breach had occurred, 57% say their breach cost the organization less than $500,000. This amount seems nominal compared to data provided in the Ponemon report, which put average costs for a data breach at $5.9 million for 2014. The most expensive types of cyberattacks for companies to deal with, according to the Ponemon report, are malicious insiders, malicious code and web-based incidents.

Figure 7: Has your organization experienced a cybersecurity breach?



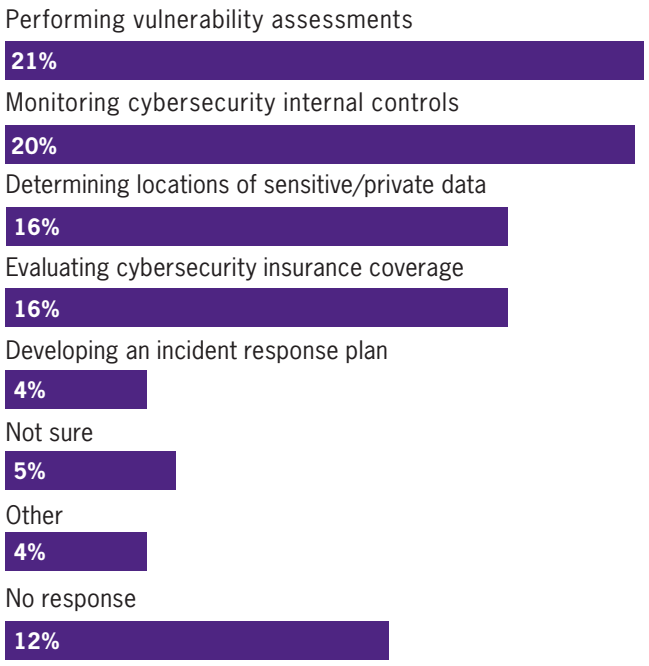
While survey respondents do not report high costs, this runs contrary to the recent and highly publicized experiences of many high-profile companies, including Sony Corp. and Target. The cyberattack on Sony resulted in an estimated loss of $1.25 billion. Home Depot suffered a data breach of 56 million credit card numbers, costing the company $33 million in 2014, after insurance payouts. Staples reported a data breach of 1.16 million customer payment cards in 2014, costing an as-yet-untallied sum. In Target's annual report, as of Jan. 31, 2015, the retailer cited net cumulative expenses of $162 million after insurance payouts related to its data breach.[4]

[4] See annual report: http://www.sec.gov/Archives/edgar/data/27419/000002741915000012/tgt-20150131x10k.htm.



What are companies doing to respond to cybersecurity risks?
Companies are doing a number of things to respond to cybersecurity risks. Atop the list, respondents are performing vulnerability assessments as a first step (21%), followed by monitoring cybersecurity internal controls (20%). (See Figure 8.) Even so, the relatively small percentages indicate that these organizations may not be doing enough to safeguard against cyberthreats.

Figure 8: What steps is your organization taking to respond to cybersecurity risks?



Participants were able to select all responses that applied.

Other practices include establishing password diligence programs, ensuring appropriate insurance coverage, encrypting laptops and mobile devices, hiring outside consultants, performing outside assessments, reviewing detection tools and joining industry consortia.

Building cybersecurity into the corporate culture is an approach embraced by Wilton Brands. Fishoff, Wilton's CFO, shares two practical examples: "When people travel to high-risk locations, they are given a separate laptop to take, so if it was compromised, it wouldn't corrupt our entire network. It enables them to be connected and do their work without creating the potential for violating our internal security. We also have a very robust password-changing process, which isn't very popular because people get lazy, but you have to enforce the rules."

Miller of Sutter O'Connell explains that his firm has encrypted all its laptops and is now encrypting mobile devices, since employees sometimes receive emails with medical records attached. "We are moving steadily toward multiple authentication and encryption on all our devices."

Roush's cybersecurity approach at SanDisk begins with education and training to build awareness. "We continue to look at the current detection tools. And we share information about a breach. It used to be that nobody would even acknowledge if they got hacked because they were afraid of how it would look. But now, companies are sharing more and more information, which is important, because the hackers may be targeting multiple firms in your industry or locations with similar security features. As we start to share information, it improves our ability to detect and respond to these situations."

Impediments to cybersecurity

The most common impediment to developing an enterprise-wide cybersecurity strategy is a lack of understanding of the risks and potential impacts of a breach (46%). (See Figure 9) This is a common issue among organizations, and unfortunately leaves valuable information exposed.

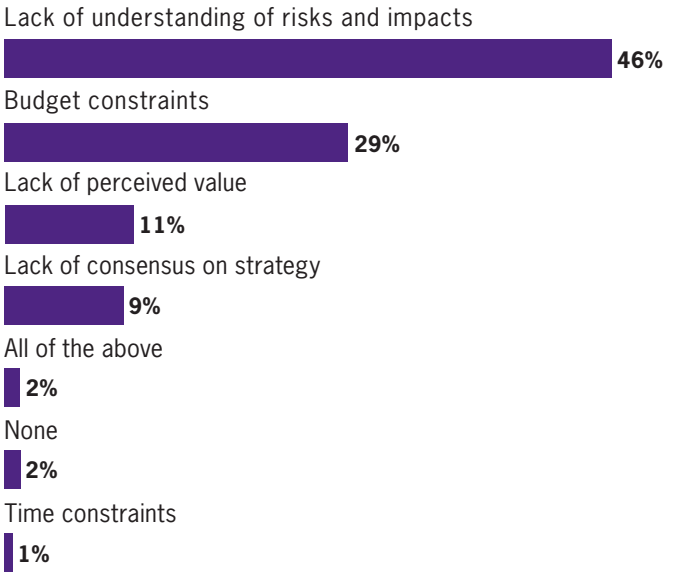
"The goal of most organizations is to get to the finish line with their product as soon as possible, and therefore see security as a hurdle or nuisance," cautions Westfall. "But it should not be ignored as the threat is very real, and only growing more so."

Interviewees share other impediments, such as decentralized environments or geographic dispersion. For example, Roush notes that SanDisk has both a decentralized environment, which can hinder developing an enterprise-wide cybersecurity strategy, as well as engineering labs in countries around the world. "When you cut across geographical borders, language barriers and historical practices, it is difficult to make sure that everyone is following the same process and procedures around cybersecurity," Roush says.

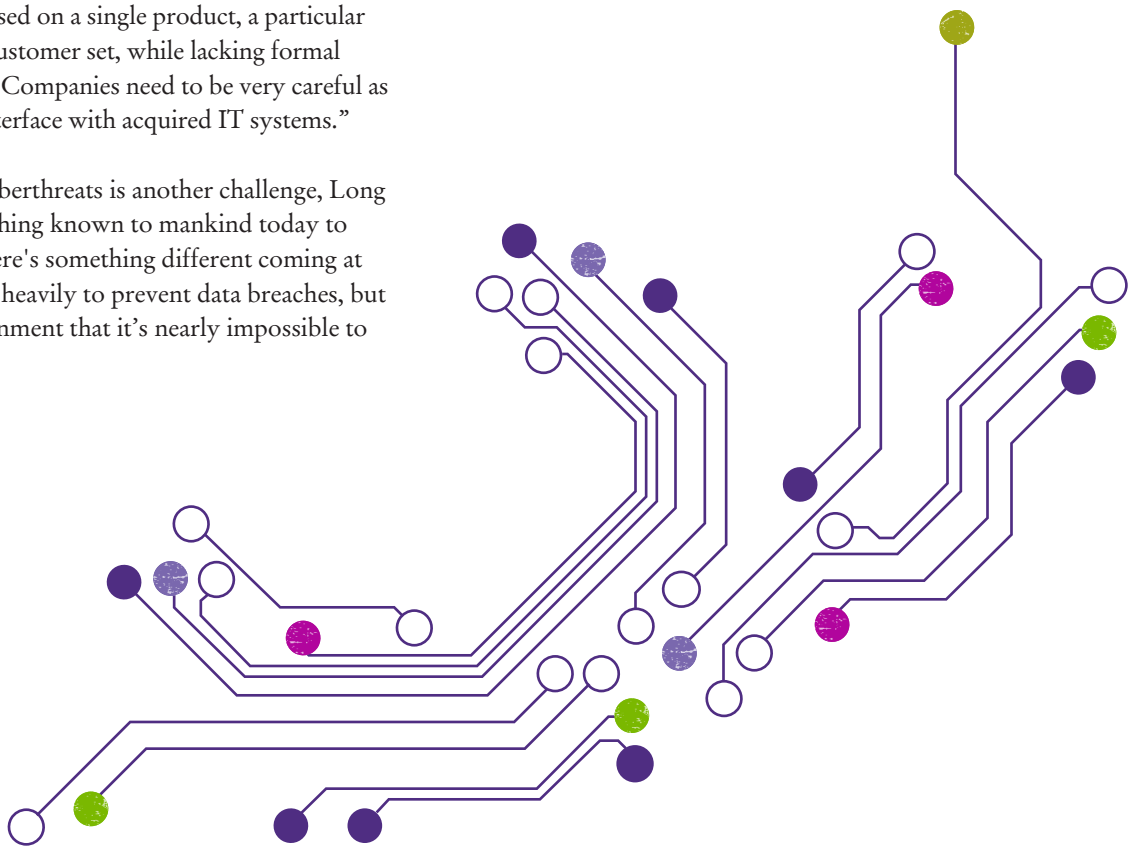
Acquisitions can be another challenge, especially startups. "Some startups pay scant attention to potential security risks," Roush notes. "They're often focused on a single product, a particular customer or a very small customer set, while lacking formal processes and governance. Companies need to be very careful as they look to connect or interface with acquired IT systems."

The changing nature of cyberthreats is another challenge, Long notes. "You can do everything known to mankind today to prevent a problem, but there's something different coming at you tomorrow. We invest heavily to prevent data breaches, but it's such a dynamic environment that it's nearly impossible to predict what's next."

Figure 9: What are the impediments to developing an enterprise-wide cybersecurity strategy?



Participants were able to select all responses that applied.



What should companies be doing?

CFOs should undertake a number of actions to help safeguard their organization against a data breach or other cyberthreat:

Map and classify data

Before the CFO can come up with an appropriate plan to protect the company's data, it's critical to know what to protect. "The CFO needs to understand how the data supply chain functions, identify where information flows through their extended ecosystems, and examine data privacy across the enterprise," says Morgan.

Determining the location of sensitive and private data is critical — the "crown jewels" for data. "My clients usually ask, 'Where is the sensitive data and how can I protect it?' Normally, the exercise begins at a business-unit level, and works up to the enterprise-wide level," Westfall advises.

That's where data mapping — making a digital inventory of where all the data resides — comes in. Data mapping can help you answer important questions like: What are the crown jewels of our business? Is IP important? Are we an information-gathering or data-hosting firm? It's important to know what the data assets are — as well as their value — in order to protect them.

Conduct a vulnerability assessment

Grant Thornton's Westfall urges companies not to overlook the common-sense approach and value to be gained from conducting a vulnerability assessment. "Vulnerability assessments help organizations understand what their internal risks are. What are the programs and operating systems in my infrastructure? Are these programs patched correctly?"

Westfall suggests that the vulnerability assessment be conducted simultaneously with a penetration test, which examines how an intruder could get into the walls of the organization. "Keep in mind that the vulnerability assessment looks only at one point in time, and therefore, you must remain vigilant in continuing assessment and staying on top of security. The timing of the assessment should be defined in monitoring cyber internal controls," Westfall says.

Develop an incident response plan

Shockingly, only 4% of respondents report developing an incident response plan. "It is critical to have an incident response plan, in contrast to a breach response plan," Westfall says. "You can have an incident that you will need to respond to quickly and efficiently, too, in order to avoid a breach. Developing a 'playbook' to avoid a breach is critical."

"A clear-cut incident response plan is a must, so that everyone within your organization can understand their roles and responsibilities," Grant Thornton's Morgan adds. An incident response plan defines what constitutes a cybersecurity incident, and provides a step-by-step process to follow when an incident occurs.

The incident response team should include representatives from all data custodians, such as HR, marketing, accounting and R&D, as well as the security officer and IT director. In some cases, it is appropriate to include any vendors or partners that have access to key data, members of the public relations team, specialized consultants and others.[5]

An effective incident response plan should:

- Identify specific risk owners and contacts within the organization
- Have clear decision-making guidelines and associated actions
- Be usable, and not overly complex
- Be tested regularly (at least once per quarter)
- Include all data loss incident types (i.e., not only intrusions)
- Outline how to help customers (including guidance, resources, etc.)

But it's not enough simply to create a response plan, notes Morgan. "Practice and testing are important too," he says.

[5] Westfall, Skip. *Unprepared organizations pay more for cyberattacks*, CorporateGovernor 2015 Winter issue. See https://www.grantthornton.com/issues/library/newsletters/advisory/2015/Incident-response-plan-reduces-cybersecurity-breach-costs.aspx for more information.

Conduct a vendor assessment
Cybersecurity demands a close look at vendor management and third-party risk, which are at the top of regulators' agendas. Companies need to account for data held by business partners, vendors and other third parties — not just the data stored within their organization. Are vendors protecting data with the same fervor as the company? To find out, it's critical to conduct an assessment of vendors' cybersecurity measures and assess their vendors' management processes.

"You'll need to determine how these organizations will protect your data, either through contractual agreements, assessments or audits. Depending on the size of your organization, your vendor management group may be able to handle this, or it might require a combined effort, with your accounting group and IT security staff working together to look at vendors," explains Morgan.

Evaluate insurance coverage
Westfall notes that participants are focusing on evaluating insurance coverage because the more costly these breaches become, the more exclusions insurance companies will include in a policy. Reviewing the coverage in detail is very important.

Create a risk profile
Many companies rely on outside consultants to test the security of their network and make recommendations. "Ivie is among them," Long notes.

"There's no way to know exactly how vulnerable systems are without having an outsider try to hack them," Westfall says. "It's useful to hire an outside firm to conduct a vulnerability assessment and penetration test (i.e., ethical hacking)."

Outside assessments are a useful tool, Roush says. "I have somebody do either an attack and penetration test or look at our network diagrams and architecture to make sure they are appropriate, and then they conduct an audit."

Based on the outside assessment report, the CFO should create a risk profile and identify the most glaring vulnerabilities. This information will help determine where to allocate resources and which areas to prioritize.

Stay on top of compliance obligations
Fast-changing compliance requirements can be daunting. Roy of Indiana Tech says: "Trying to stay compliant with all these regulations such as the Family Education Rights and Privacy Act — the HIPAA for educational institutions — with just seven people in our IT department is really difficult for us."

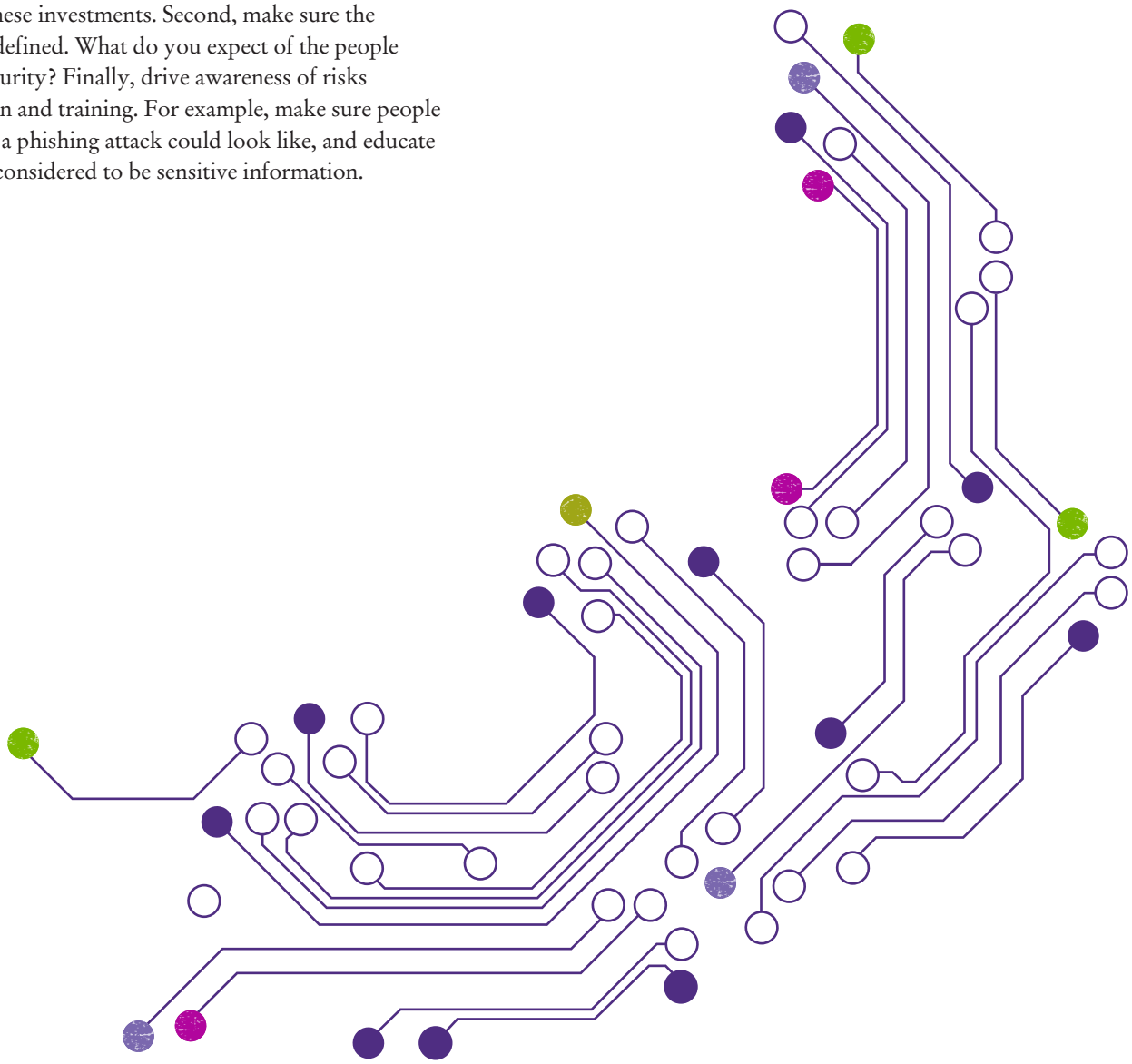
To keep up with the changing expectations, Roy and Indiana Tech's director of IT, Jeff Leichty, talk and meet regularly with peer groups from other private universities. "Jeff has an IT CIO group, and I've got a CFO group," explains Roy. "We talk about compliance issues and share best practices." The university also has cybersecurity insurance that covers costs associated with a breach.

Set cybersecurity risk management strategy

The survey data suggests that the leading way CFOs optimize cybersecurity risk management is by assessing risk and investments related to cybersecurity (40%). (See Figure 10.) In other words, what has the organization invested in most heavily (resources and/or money)? And, is the level of protection appropriate to that area's strategic importance? In most cases, this is the organization's intellectual property, since loss of this information would be severely detrimental to the organization.

Roush offers three suggestions for how CFOs can optimize cybersecurity risk management: First, get directly involved in resourcing. Understand what cybersecurity resources are being applied across the company, and what risks are being addressed with these investments. Second, make sure the goals are clearly defined. What do you expect of the people running cybersecurity? Finally, drive awareness of risks through education and training. For example, make sure people understand what a phishing attack could look like, and educate them on what is considered to be sensitive information.

Figure 10: In what ways can CFOs optimize cybersecurity risk management strategy?



Conclusion

With cyberattacks and data breaches becoming increasingly common, costly and regulated, cybersecurity has risen in its strategic importance, and has landed squarely on the desk of the CFO. As the frequent keeper of cybersecurity strategy, the CFO is expected to assess cybersecurity risks and align cyberstrategy with business strategy. This is no small task.

The key actions CFOs are expected to undertake in this role include:

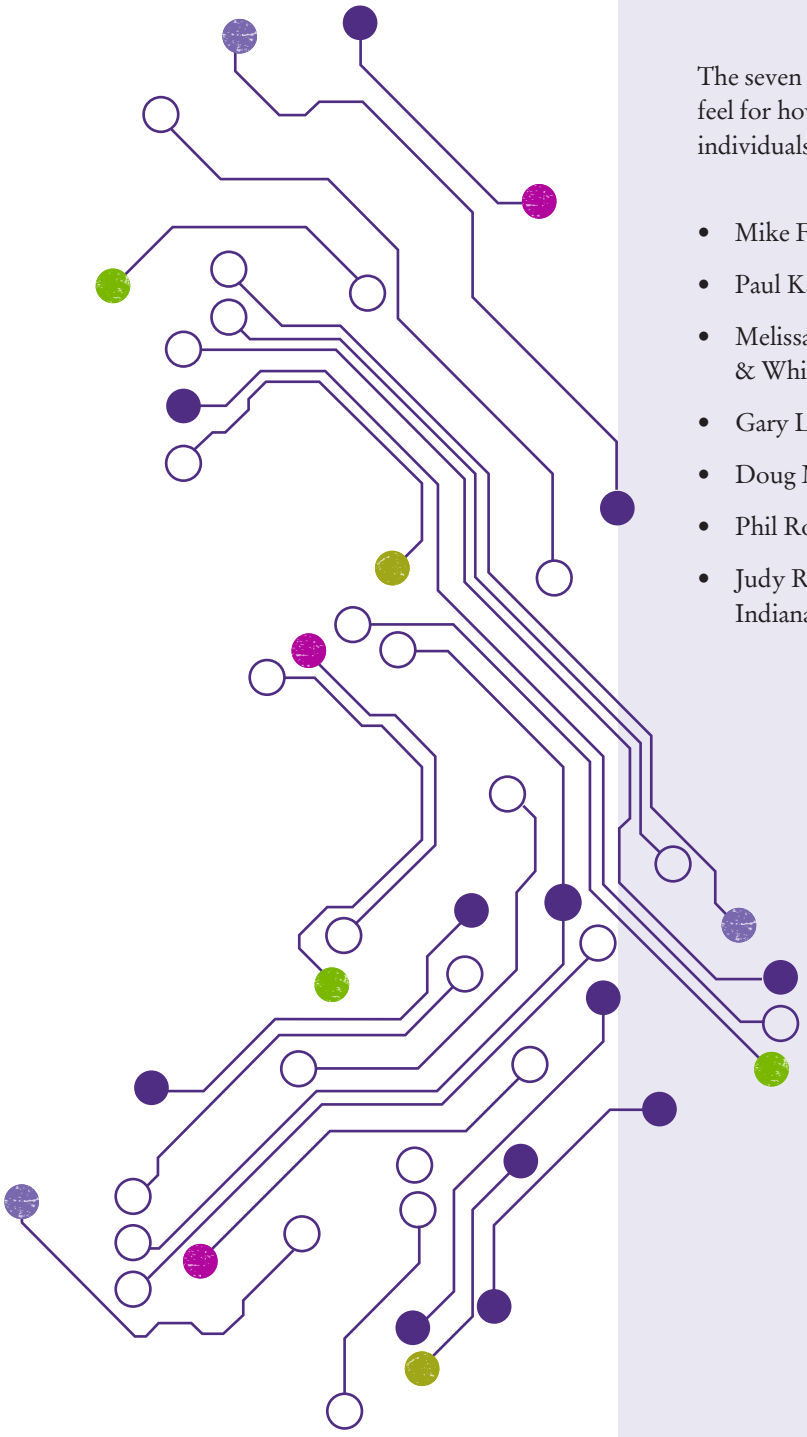
- Understand the organization's full risk universe
- Advocate for a budget to support cybersecurity preparedness
- Develop a close relationship with the CISO or CIO, if the organization does not have a CISO
- Know the relevant cybersecurity regulations and SEC expectations, which are more important than ever now that cybersecurity has become both an examination and reporting priority
- Evaluate the organization's cybersecurity insurance
- Report to the board on the organization's cybersecurity initiatives and get buy-in from the board on necessary cyberinvestments

The threats to data privacy and data security are fierce and continuously evolving.

Effective information security depends not on a single technology or strategy, but on a layered approach that needs to be monitored continually as threat patterns change, according to Vernon Habersetzer, an information security engineer with Wells Fargo.[6] "You have to assume adversaries are inside, and watch your network to see what's going on," Habersetzer said. "The average time of detection is four to six months, which is scary because there can be a lot of damage to a company in four months."

Given the seriousness of the threats faced and the obvious prominence of the CFO in these cybersecurity discussions, it's critical for CFOs to be better educated about the risks and to participate in a thoughtful dialogue with key stakeholders to ensure that the enterprise is adequately shielded from cyberthreats.

[6] 2014 FEI Leadership Summit session, "Real World Cyber Threats."



Interviewees

The seven in-depth follow-up interviews provided a much better feel for how companies are reacting to cybersecurity. The following individuals participated in these interviews:

- Mike Fishoff, CFO of Wilton Brands LLC
- Paul Karras, senior vice president and CIO at Wilton Brands LLC
- Melissa J. Krasnow, corporate and privacy partner, Dorsey & Whitney LLP
- Gary Long, executive vice president and CFO, Ivie & Associates Inc.
- Doug Miller, CFO at Sutter O'Connell Company
- Phil Roush, vice president of finance at SanDisk Corp.
- Judy Roy, executive vice president of finance and administration at Indiana Tech

Author and contributors

William M. (Bill) Sinnett
William M. (Bill) Sinnett is senior director, research, for Financial Executives Research Foundation Inc. (FERF), the research affiliate of Financial Executives International (FEI). Sinnett also supports FEI's Committee on Finance & IT (CFIT), and writes its e-newsletter, "Finance & IT News."

He can be reached at +1 973 765 1004 or bsinnett@financialexecutives.org

Kevin Morgan
Kevin Morgan is a principal in Grant Thornton's Business Advisory Services practice and the co-leader of Cybersecurity Services. Morgan advises clients regarding application development, large-scale software package implementation, complex problem-solving and predictive analytics.

He can be reached at +1 203 327 8295 or kevin.h.morgan@us.gt.com.

Skip Westfall
Skip Westfall is a managing director and the national practice leader of Grant Thornton's Forensic Technology Services group as well as the co-leader of Cybersecurity Services. Westfall specializes in providing strategic advice related to computer forensics, electronic discovery, cybersecurity and data analytics in support of investigations and civil litigation.

He can be reached at +1 832 476 5000 or skip.westfall@us.gt.com.

Johnny Lee
Johnny Lee is a managing director in Grant Thornton's Forensic, Investigative and Dispute Services group, a practice leader of Forensic Technology Services, and a member of the cybersecurity leadership team. Lee is a former attorney, as well as a management and litigation consultant specializing in data analytics, computer forensics, and electronic discovery in support of investigations and litigation.

He can be reached at +1 404 704 0144 or j.lee@us.gt.com.

About Financial Executives Research Foundation

Financial Executives Research Foundation (FERF) is the non-profit 501(c)(3) research affiliate of Financial Executives International (FEI). FERF researchers identify key financial issues and develop impartial, timely research reports for FEI members and nonmembers alike, in a variety of publication formats. FERF relies primarily on voluntary tax-deductible contributions from corporations and individuals. FERF publications can be ordered by logging onto www.ferf.org/reports.

International Standard Book Number 978-1-61509-183-6

About Grant Thornton LLP

The people in the independent firms of Grant Thornton International Ltd provide personalized attention and the highest-quality service to public and private clients in more than 100 countries. Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd, one of the world's leading organizations of independent audit, tax and advisory firms. Grant Thornton International Ltd and its member firms are not a worldwide partnership, as each member firm is a separate and distinct legal entity.

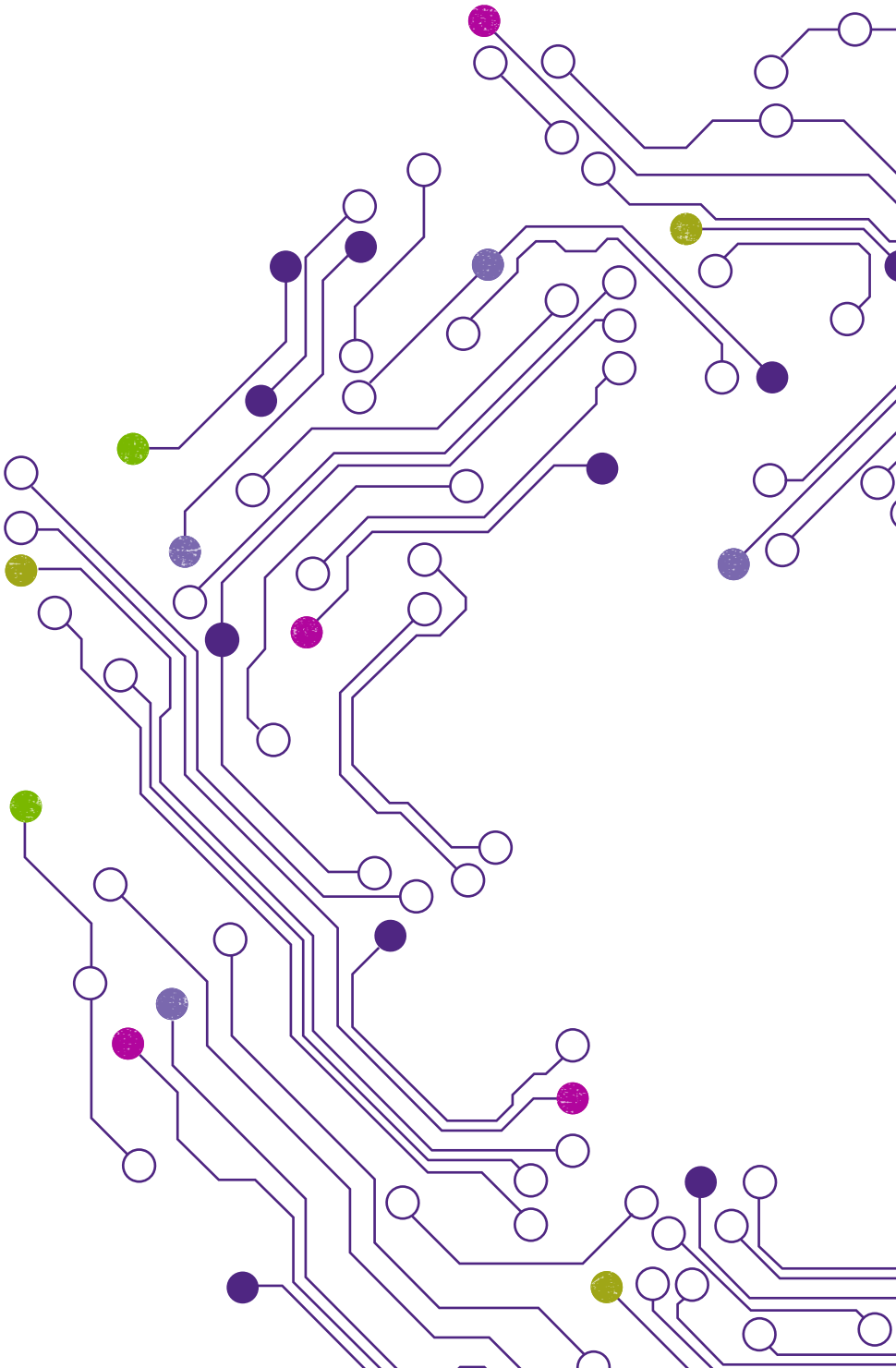
In the United States, visit grantthornton.com for details.

Financial Executives Research Foundation (FERF) gratefully acknowledges these companies for their longstanding support and generosity:

Platinum Major Gift | $50,000 +
Exxon Mobil Corporation
Microsoft Corporation

Gold President's Circle | $10,000–$14,999
Cisco Systems, Inc.
Cummins Inc
Dow Chemical Company
General Electric Co
Wells Fargo & Company

Silver President's Circle | $5,000–$9,999
Apple, Inc.
The Boeing Company
Comcast Corporation
Corning Incorporated
Credit Suisse AG
Dell, Inc.
DuPont
Eli Lilly and Company
GM Foundation
Halliburton Company
The Hershey Company
IBM Corporation
Johnson & Johnson
Lockheed Martin Corp.
McDonald's Corporation
Medtronic, Inc.
Motorola Solutions, Inc.
PepsiCo, Inc.
Pfizer Inc.
Procter & Gamble Co.
Tenneco
Tyco International Mgmnt Co.
Wal-Mart Stores, Inc.



About Grant Thornton LLP

The people in the independent firms of Grant Thornton International Ltd provide personalized attention and the highest-quality service to public and private clients in more than 100 countries. Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd, one of the world's leading organizations of independent audit, tax and advisory firms. Grant Thornton International Ltd and its member firms are not a worldwide partnership, as each member firm is a separate and distinct legal entity.

In the United States, visit grantthornton.com for details.

Grant Thornton

An instinct for growth™

Connect with us

grantthornton.com

@grantthorntonus

linkd.in/grantthorntonus