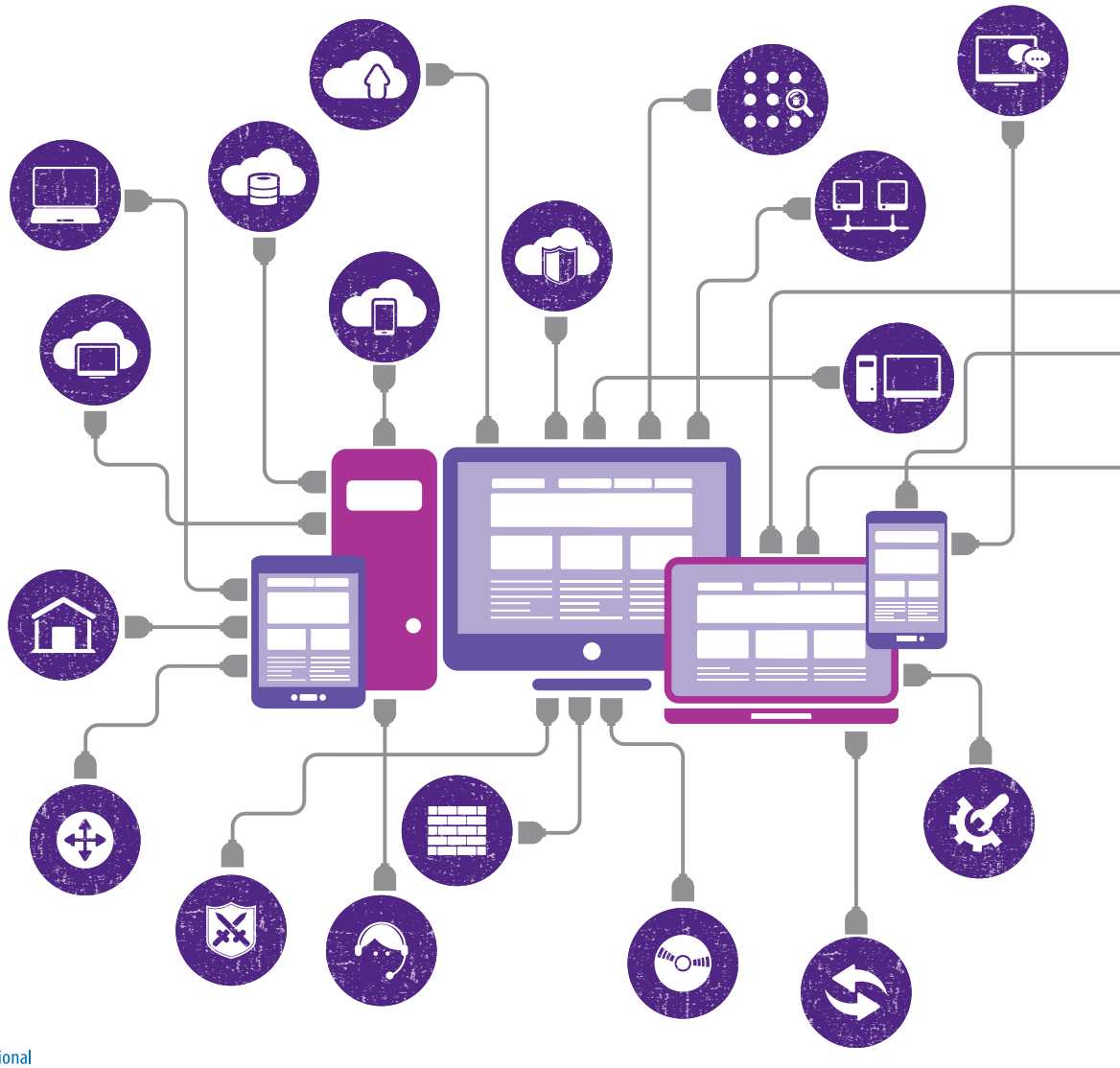
Grant Thornton

An instinct for growth™

Cybersecurity incident response:
Planning is just the beginning



ferf
financial executives
research foundation

an affiliate of financial executives international

Contents

Author

Thomas (Tom) Thompson
Manager, Research
Financial Executives Research Foundation

Contributors

Johnny Lee
Managing Director, Forensic and Valuation Services
Grant Thornton LLP

Skip Westfall
Managing Director, Forensic and Valuation Services
Grant Thornton LLP

Todd Fitzgerald
Global Director, Information Security
Grant Thornton International Ltd

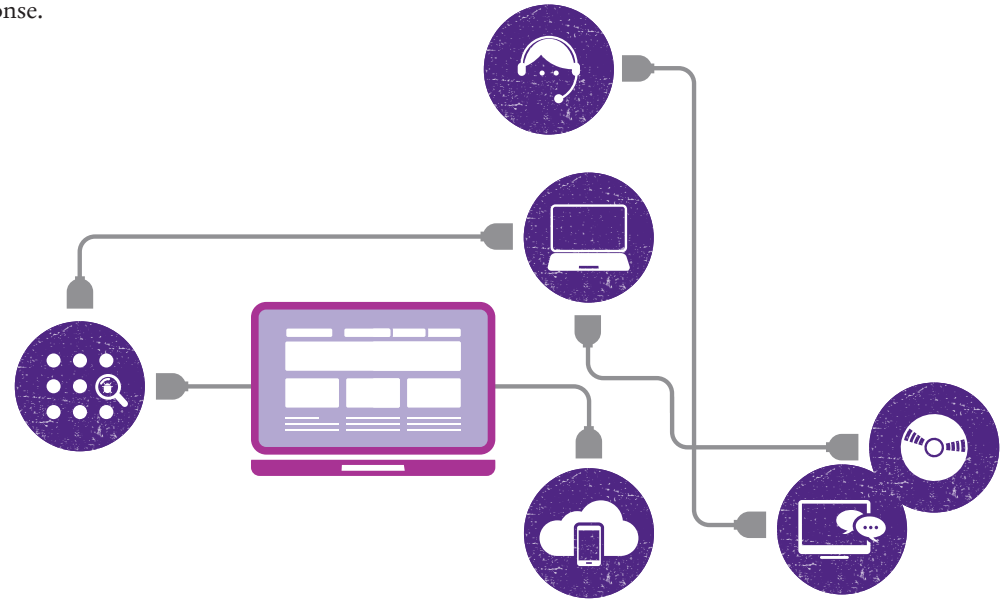
Executive summary

By now, most senior-level executives have heard that either you have had a data breach or you just don't know that you've had a data breach. Cyberattacks are now as much a part of doing business as taxes and financial statements, and they are getting expensive. According to the 2015 *U.S. Cost of a Data Breach Study*[1] by the Ponemon Institute, last year there was an 11% increase in the total cost of a data breach, to a $217 average per lost or stolen record. To be sure, those numbers are based on estimated costs of actual data loss incidents, not hypotheticals. In an effort to support senior financial executives in their cybersecurity incident planning and response, Grant Thornton LLP and Financial Executives Research Foundation (FERF) have identified several essential areas for their consideration.

This report's findings are based on in-depth interviews, conducted between August and September 2015, with 10 subject matter experts of various specializations, including legal, PR and communications, insurance, and IT security. The interviewees provided their perspectives on cyberrisk management strategies and best practices in cyberbreach response.

Key findings include:

- Simply having a cybersecurity incident response (IR) plan is not enough. It must be reviewed and updated regularly as part of a comprehensive cybersecurity incident response program.
- Regular training and exercises are important in keeping the IR plan effective. Employees can be a critical line of defense.
- Board involvement is crucial. Senior management and the board need to have open dialogue about expectations regarding risk tolerances, budget considerations, IR planning and breach response.
- General liability insurance and director's insurance most likely will not cover a cybersecurity incident. A full review of insurance should be an integral part of cyberrisk management.



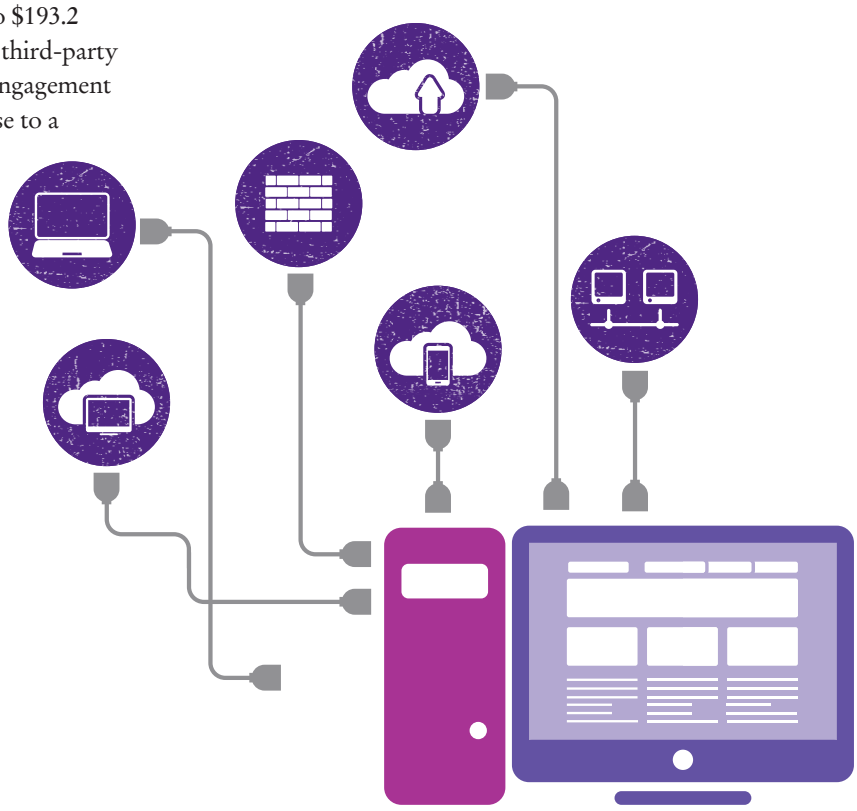
[1] Ponemon Institute. *U.S. Cost of a Data Breach Study*, May 2015.

Introduction

Today's organizations face a sobering reality. The question is no longer whether we **will** be breached but **when** we will be breached. Cybersecurity is a C-suite and board-level issue requiring a comprehensive risk management strategy, intelligent investment and integration across the organization.

While the costs associated with a data breach continue to rise, there are established best practices that can mitigate some of those costs. The 2015 *U.S. Cost of a Data Breach Study*[2] found that having an IR plan and team in place, extensive use of encryption, business continuity management (BCM) involvement, chief information security officer (CISO) leadership, employee training, board-level involvement, and insurance protection are viewed as reducing the cost of a data breach. An IR team can decrease the average cost of a data breach from $217 to $193.2 (decrease = $23.8) per lost or stolen record. However, third-party error, a rush to notify, lost or stolen devices, and the engagement of external consultants to support the IR team response to a breach increased data breach cost.

Clearly, having an IR plan and team in place, extensive use of encryption, BCM involvement, CISO leadership, employee training, board-level involvement, and insurance protection would all be considered best practices. These elements should be considered the foundation of a robust cybersecurity incident program. FERF, in cooperation with Grant Thornton LLP, spoke with several subject matter experts from a variety of fields to glean insights and recommendations for instituting an effective cybersecurity incident response program.



[2] Ponemon Institute. *U.S. Cost of a Data Breach Study*, May 2015.

Cybersecurity incident response

When determined adversaries such as hacktivists, state-sponsored actors and organized criminal syndicates set their minds on finding a way inside, every organization with valuable digitized information is at risk of having its information assets breached and its critical assets compromised. Indeed, most organizations today would do well to expand their efforts to mitigate the consequences of inevitable breaches, which likely affect infrastructure systems and compromise key data such as personally identifiable information and confidential business information. A properly drafted IR plan guides the proactive planning and management necessary to effectively react to such breaches.

It all starts with a plan

The primary objective of an IR plan is to prepare for and manage a cybersecurity incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs.[3] Unfortunately, IR plans are one of the most neglected aspects of information security.[4] Without a plan, organizations do not respond to a cybersecurity incident — they react to it, and reactions are usually based on misinformation and misunderstanding or, worse yet, fear.

To this point, Melissa Krasnow, partner and U.S. Certified Information Privacy Professional (CIPP/US) with Dorsey & Whitney LLP, noted: "While a number of companies have them [IR plans], you might be surprised by the companies that do not have them even though there is guidance about them, regulators are encouraging companies to have them, and they are a best practice. Once a company or a competitor or a business partner experiences a breach, incident or cyberattack, they develop an awareness that often galvanizes preparation, including an IR plan."

Fellow attorney Liisa Thomas, chair of the principal and data security practice at Winston & Strawn LLP, said: "Most companies have a disaster recovery plan. If a 9/11 type of event happens, they know what to do. Typically, they will dust off that plan and make sure it works for them at least once a year, if not more."

As it relates specifically to cyberincidents, Thomas continued: "A potential data breach should be treated in much the same way. An IR plan should give high-level information about how the company will handle the incident. Not all breaches are the same. Some might be cyberevents; some might be internal thefts. I've seen plans that are 30, 40 or maybe 100 pages long. Often they're very focused on specific steps that the IT department would take to contain the incident. These plans may have their place, depending on the organization. But they might not instruct those outside of the IT department — senior leadership — on what to do at a high level. I advise clients to have a shorter, high-level document. The high-level document helps not only during an incident, but also before it, raising awareness with the senior leadership about the types of decisions they're going to be asked to make. A plan like that can be used by the decision-makers to practice against, just like they would a disaster recovery plan."

[3] Bailey, Tucker; Brandley, John; and Kaplan, James. *How Good Is Your Cyberincident-Response Plan?* McKinsey & Company, December 2013.

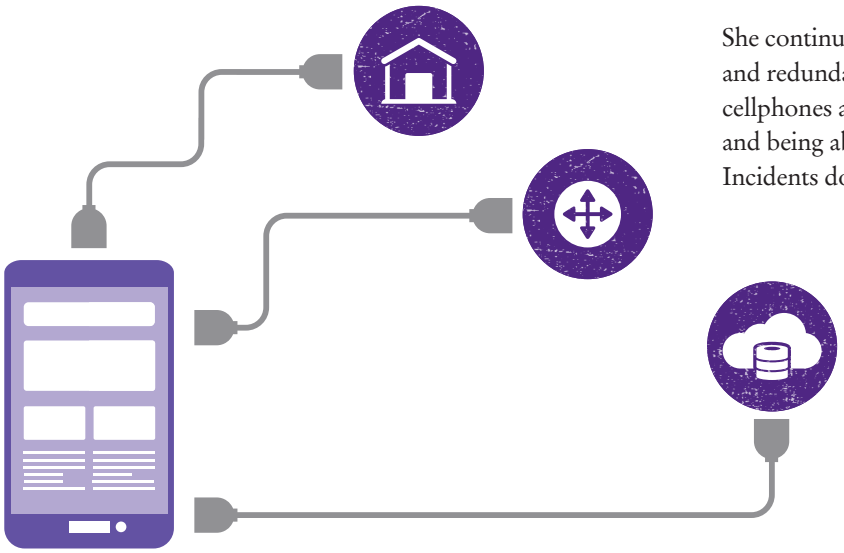
[4] Parkinson, John. "How to Respond to a Data Breach," *CFO.com*, July 14, 2015.

Johnny Lee, Grant Thornton managing director of Forensic, Investigative and Dispute Services, adds, "While the IR plan can resemble a high-level policy, it is important to note that each constituent department (IT, legal, communications, risk management, etc.) might have far more detailed protocols invoked during an incident response."

Jerry Wynne, CISO and senior director of enterprise security with Noridian Mutual Insurance, said his company does have a cybersecurity IR plan: "We are in the process of updating it again based on several breaches that have occurred within the industry in the last year. It will include some additional areas that are outside of the traditional cybersecurity IR time."

Those updates were the result of lessons learned within their industry peer group. This follows best practices, as IR plans should be revisited regularly to ensure that they don't get stale. Wynne continued, "We have a stronger legal presence on the team, and we've made sure that our privacy area and compliance areas are more heavily involved than they have been in the past."

Information security expert and former CISO Bill Barouski believes there are two aspects organizations should consider in reviewing their cybersecurity incident response plans: "I think every program, every plan should be reviewed at least annually. Then, probably every 18 to 24 months, have a third party review the plans. Any high-performing organization would want an outside view into their effectiveness."

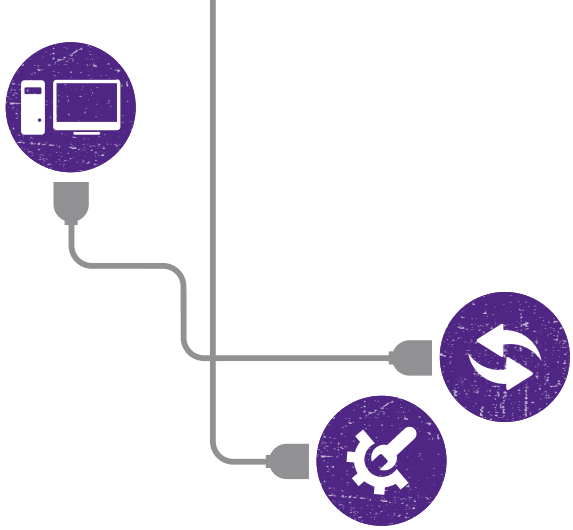


IR team

When asked who should head the response team or what departments should be included in the team, John Kennedy, corporate partner in the IT and outsourcing, privacy, and information security group at Wiggin and Dana LLP, said: "It varies by organization, but I believe a best practice is to create an IR governance committee, which should include representatives from executive management, so that decisions can be made quickly. In terms of the preparedness side and the planning and the communications chain, it will include legal, IT, risk management, human resources, public relations and, in some cases, facilities management. There may be, in addition, a compliance officer as well as a risk officer. In the end, the incident response team should represent a cross-section of key stakeholder interests that will be affected by different kinds of incidents."

Ashley McCown, president at Solomon McCown, had a few suggestions regarding which business operations should be a part of the IR team: "The CFO certainly is included; there are obviously significant financial implications in a breach, so he or she needs to be at the table. The general counsel, and as companies are getting very organized around potential cyberattacks and identifying a law firm or lawyer with expertise in cybercrimes and breaches, that person can be brought into the effort. IT clearly should be involved; HR, sometimes, if employee data and personally identifiable information are leaked. Definitely the communications department, which could include internal and external communications."

She continued: "Additionally, you want to have backups and redundancies because people go on vacation. Even with cellphones and Wi-Fi everywhere, people can be out of touch, and being able to mobilize your team quickly is essential. Incidents don't often happen at the most opportune times."



Exercises and training

Putting a plan like this together, keeping it up-to-date and exercising it periodically is a lot of work — a major reason that it doesn't always get done. But when something bad happens (and it will), having the plan available and the experience that only comes from practice will save a lot of time and potentially avoid embarrassment at best, and litigation at worst.[5]

Having a cybersecurity incident response plan is an important step, but it's only the beginning. The plan is not of much use if it only exists on paper or on a server somewhere — it must be reviewed regularly and periodically exercised. All of the interviewees stressed the importance of tabletop exercises and employee training. Additionally, as they relate to tabletop exercises, these updates should include industry-, regulatory- and technology-specific scenarios. An executive director of information security with a large insurance company noted: "We've had numerous exercises in 2015. Traditionally, we've conducted exercises focused on business continuity and disaster recovery. However, we've stepped it up this year to do more crisis management tabletop exercises to address cybersecurity threats. We engage the threat response team, which is our cross-functional IT team, to participate in cybersecurity tabletop exercises based on real-life scenarios. We exercised our plans to determine how prepared we are to respond and to determine if our response plans are well-documented."

She continued: "We've also done a tabletop with our midlevel executives, our vice presidents and other key stakeholders across the organization, to make sure plans are in place, including communication plans. Social media is going to be a big part of our response plan to make sure we handle social media issues timely and appropriately. Soon we're going to conduct an exercise with our senior-level executives so they are prepared to handle crisis management events. We are really putting a lot of effort and emphasis on tabletop exercises and preparedness as key to managing a major event."

John Kennedy, corporate partner at Wiggin and Dana, noted: "Organizations that are seriously focused on this issue are doing training directed at all employees who may be in a position to expose the company to risk by virtue of the activity that they're permitted within the company's network. We have done training sessions with hedge funds specifically for the issue of social engineering and phishing. The training was not just limited to the senior officers either; it was a room full of traders and analysts. Phishing attacks are becoming increasingly sophisticated; you hear stories where someone very high up in the organization was impersonated and a middle-management employee was duped to transfer funds or execute an order that was bogus."

Todd Fitzgerald, Grant Thornton International global director of Information Security, adds: "Training methods have to change from 45-minute slide decks to online cyberassessments, phishing simulations and interactive training to grab the end users' attention and deliver relevant 15-minute training. Only after users have been fake-phished will they really pay attention to the training where information flow and demands on our time are at all-time highs."

While there are those that will view employees as the weakest link in their organization's cyberincident preparedness, Bill Barouski, information security expert and former CISO, thinks the opposite. "Someone that is very well-trained and cyberaware is going to be far more effective than technology," he said. "People can become your strongest link."

For attorney Jason Bernstein, partner and co-chair of the data security and privacy group at Barnes & Thornburg LLP, training also means reinforcement: "If you do it once a month, people start getting kind of blind eyes, like a parent talking to a 16-year-old. With the IT directors and CIOs that I talk to, it's constant education. It does not matter how high- or low-level you are at this; these phishing attacks have gotten so good, and there are so many nuances in them that it's real easy to just click on them."

[5] Parkinson, John. "How to Respond to a Data Breach," *CFO.com*, July 14, 2015.

Board involvement

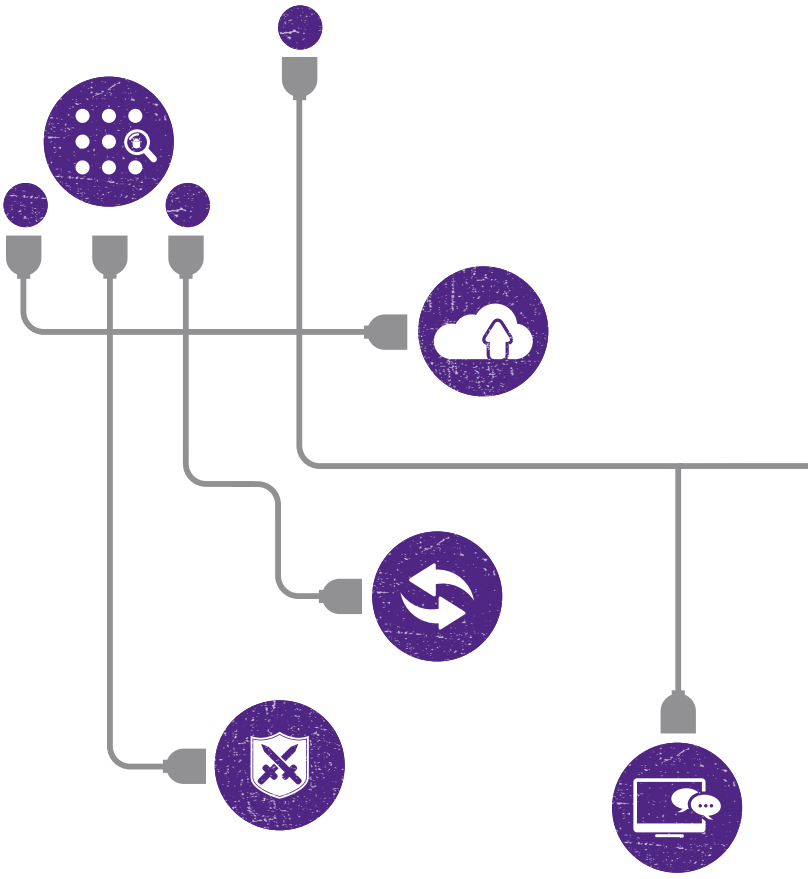
With recent high-profile legal cases involving board members making headlines, boards need to be more than just aware of cybersecurity incident response, they need to be involved in the IR planning. As Melissa Krasnow, partner and CIPP/US with Dorsey & Whitney LLP, pointed out, "The intersection of cybersecurity and corporate governance is an area that's developing and where awareness continues to increase."

She continued: "IT is in the middle of all this, and increasingly is being called upon by the board of directors and executives. Some companies are being transparent about their cybersecurity, for example stating, 'Here's where we're lacking in our security, and here's what we need to do to address it,' and providing steps that should be considered. Company ethics and culture may transcend legal requirements about how a company handles things. It's interesting to see this dynamic play out."

Unfortunately, the reality is that boards are often focused on other competing priorities. The former CISO of a large educational system noted that there was limited support at the board level: "If they did get involved, it did not trickle down to me. To my knowledge, senior management did not have much expectation from the board relating to cybersecurity. The board was focused on other topics."

However, other boards are very involved in cybersecurity. The executive director of information security with a large insurance company said the board in her organization takes this issue very seriously: "It's considered in every board meeting now. My boss is the chief information security officer, and he reports to the CIO. Every quarter, they have to give an update regarding not only IT in general, but also cybersecurity threats. The board is very interested and they do care, and I think it's helping to drive our investments in security, which is a good thing."

From the senior management perspective, she continued, "[t]he expectation of the board is to drive awareness. The board sets the tone so senior management and the end users know that it's important that security and the controls work properly."



Cyberinsurance

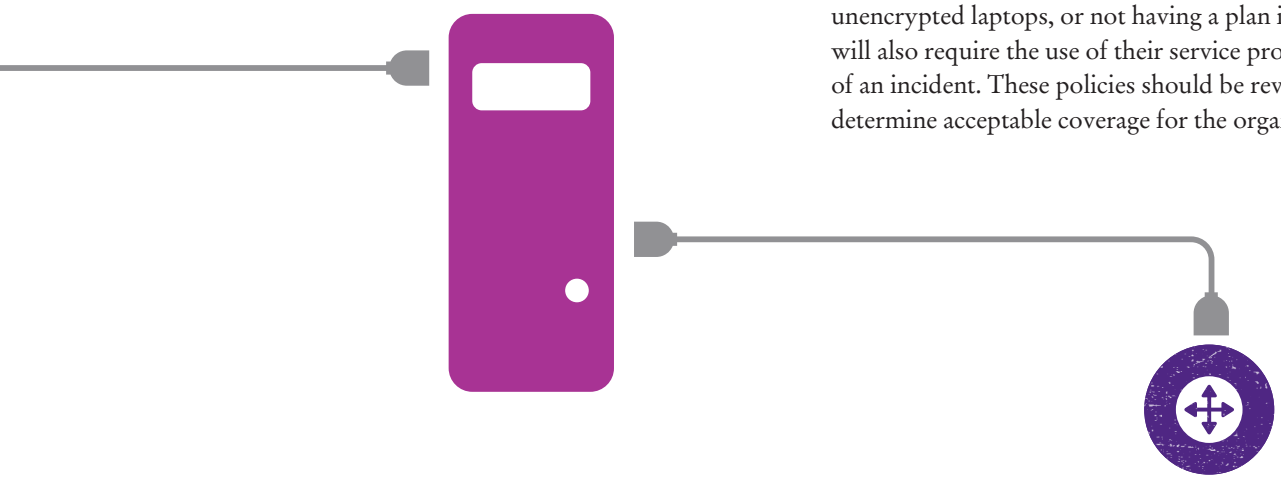
Given that cybersecurity is all about risk assessment and management, no cybersecurity IR program would be complete without a review of an organization's existing insurance coverage. Do not just assume the company's general liability or directors insurance coverage will suffice. That said, there are certainly some companies that are ahead of the curve. Jerry Wynne, CISO and senior director of enterprise security at Noridian Mutual Insurance, said his company has been carrying cyberliability insurance for several years: "We went down the road of cyberinsurance after recognizing the potential liability. The discussion focused on the financial impact a breach would be to the company and to everyone involved. In the end we decided that we really had to have cyberinsurance, so we've been maintaining that for about five years."

Nolan Wilson, Southeast region leader of professional risk solutions at AON, notes: "Probably more do not purchase [cyberinsurance] than do, even though it's such a big topic today. I think from a general liability perspective, it's more and more common to see a specific exclusion for access or disclosure of confidential and personal information. It's critical to not just assume that you have insurance that will cover a specific incident, and to make sure that you're looking at the policy and any exclusions that it might have."

John Kennedy, corporate partner at Wiggin and Dana LLP, noted more policy review: "Companies are paying much more attention to it. At least some of them are waking up to the fact that commercial general liability (CGL) policies and other kinds of standard policies do not address cyberrisk. We do a fair amount of work in the insurance sector, so we've actually worked with insurance companies on how to draft cyberinsurance policies, but also how to draft cyberrisk exclusions from their CGL policies."

Kennedy continued: "Companies just don't seem to pay the same degree of attention to the risk of loss to their information assets as they do to their tangible assets, and therefore may not understand that data loss is not covered. Or if you outsourced something and that third-party provider lost your data, your policies may not cover that. Insurance provisions have gotten very detailed and demanding. Customers are telling their vendors or their suppliers that they've got to carry all these types of cyberliability coverage, criminal cyberliability coverage, etc., in addition to the other types of insurance."

Todd Fitzgerald, Grant Thornton International global director of Information Security, also notes: "Cyberinsurance is an important tool to mitigate risk; however, this cannot be a substitute for having reasonable controls and an adequate IR program. Many policies have exclusions for not having minimum controls, such as an exclusion for losses due to unencrypted laptops, or not having a plan in place. Some policies will also require the use of their service providers in the event of an incident. These policies should be reviewed carefully to determine acceptable coverage for the organization."



Third-party risk

Just because an organization's systems do not suffer a breach does not mean its information cannot be compromised. Third-party or vendor risk is another key area of consideration for a company's cybersecurity IR program. Are they protecting data with the same fervor you are? To find out, it's critical to conduct an assessment of your partners' cybersecurity measures and assess your 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. For more insight, see Skip Westfall's article "Unprepared Organizations Pay More for Cyberattacks," originally published in Grant Thornton's CorporateGovernor newsletter on Feb. 4, 2015. The former CISO of a large educational system said he instituted vendor security and a vendor assessment questionnaire: "Anytime a new vendor would come on board, we would have them complete the questionnaire and we would make a risk recommendation whether or not to proceed. Now the organization could always accept the risk, but IT would at least make some recommendation based on our vendor security review."

Bill Barouski, information security expert and former CISO, noted: "I think this has started to get more attention in the last 18 months. Any large, extended enterprise will have a very wide array of third-party vendors and partners. They're saying, 'We need to take a holistic view of cyberrisk across the entire enterprise, including contractors, vendors, partners, etc.' so I see a lot of energy around this topic, especially in the financial services industry."

Ashley McCown, president of Solomon McCown, commented: "In business in general, we are hearing more about companies requiring verification from third-party vendors to show what systems and processes they have in place to protect data. I think that's becoming much more commonplace."

An executive director of information security with a large insurance company said her company has spent a lot of time looking at third parties because incidents can occur outside your systems but have implications for your company: "Many times it had to do with a third party either having some kind of entry point into your system, or just the fact that we're sharing our data with third parties. So we have a strong, robust third-party vendor management program. We look at it from a privacy, security and legal perspective. But we know it's really working with our procurement department, as well as our business partners, to have a strategy of what type of information lends itself to be hosted externally with third parties and the criticality of the business. So we're putting a lot of criteria and strategy around our third-party vendor management to make sure we're providing the right oversight."

She continued: "If vendors have access to critical and/or confidential information, we require what's called a minimum security requirements document that's a part of the contract, like an addendum, and one of our requirements is data security at rest, in addition to many other things. It seems like the industry has shifted, and a lot of companies and third-party vendors — at least the ones that deal in health care information — are taking it seriously and adhering to that requirement."

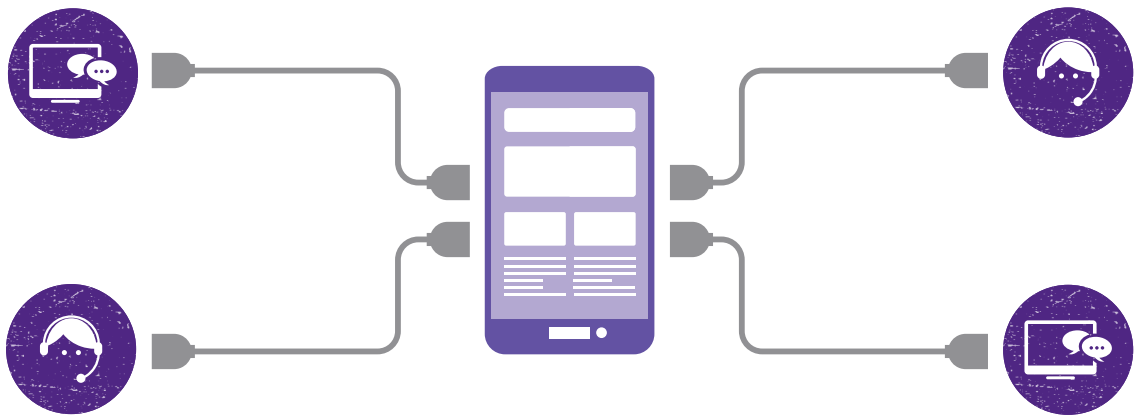
Communications

PR and communications must be an integral part of any cybersecurity incident response plan. This is the area of expertise of Ashley McCown, president of Solomon McCown, and she summed this up perfectly: “Social media is a game changer in our world in terms of how quickly information and/or rumors can spread. Now hackers will often be the ones that go onto a blog or other social channels to put it out there that they've hacked an organization or company. So then the clock starts ticking. Someone's going to tell the story, and you want that someone to be you and your company and not other people.”

Bill Barouski, information security expert and former CISO, noted: “What I've observed, increasingly so, is the sooner you're able to provide clear and unambiguous information, the sooner you reduce the attention, uncertainty and the number of news stories. By nature, if the public doesn't believe you're being straightforward or cooperating, the scrutiny and intensity increase. But I think you've seen in the last two years how firms are much quicker to announce what they do know even without full understanding of what's happened.”

While putting out a public communication statement following a breach is important, Jason Bernstein, partner and co-chair of the data security and privacy group at Barnes & Thornburg LLP, did provide some words of caution: “A lot of times when we're talking about a small company, they don't have a PR firm, certainly not a PR firm that knows how to deal with data breach communications. Part of what we do in our role is to help manage this whole process, and one of the things that a PR firm and certainly the client tends to do in terms of communication is say, ‘We are guilty, we're sorry, mea culpa.’ We try and advise them on what they should be saying or not to say just yet.”

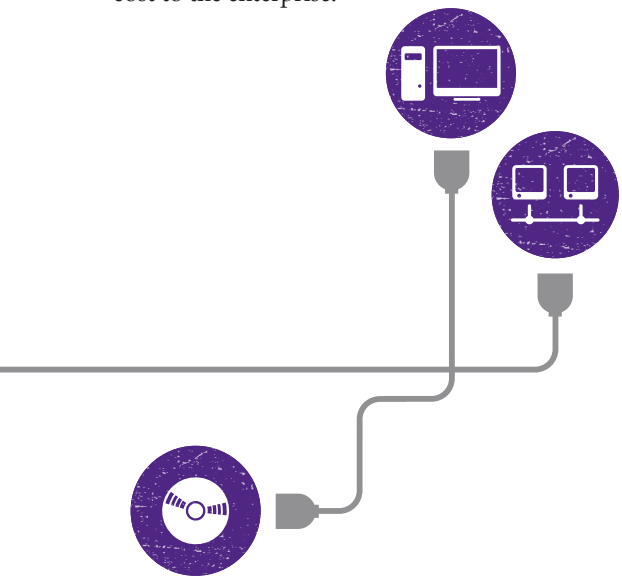
He continued: “One key to managing communications is to communicate early and clearly what you do know, and that you will provide more details as they become available. In a major breach incident, it’s not a good idea to release information that is not confirmed. Delaying an initial announcement makes the public suspicious of your motivations. But restating the facts later is likely to be more damaging. So managing that communications process is a balancing act. And, in the big picture, the way the company handles communications will be remembered long after the breach is fixed and individuals have been taken care of, and this is the key to minimizing damage to the company’s brand reputation and regaining trust.”



Conclusion

Hardly a day goes by without cyberattacks and data breaches grabbing media headlines. No company, organization or even government is immune. That's the bad news. The good news is that companies can use these events to bolster their own cybersecurity incident response. Once again we consider those factors that can reduce the cost of a data breach. Some of the most valuable investments companies can make seem to be an IR plan, extensive use of encryption, the involvement of business continuity management, the appointment of a CISO with enterprise-wide responsibility, employee training, board-level involvement and insurance protection.[7]

Prevention through implementing reasonable controls is still very important; however, these controls are point-in-time and, even if implemented correctly 100% of the time, there are new threats and exploits that are emerging. There will always be a gap between the implemented controls and the resources available to a determined attacker. Thus, planning for this situation by implementing an IR program is critical to reducing the risk and cost to the enterprise.



The risks of cyberattacks span functions and business units, companies and customers. Given the stakes and the challenging circumstances related to becoming cyberresilient, making the decisions necessary can only be achieved with active engagement from the CEO and other members of the senior management team.[8] Cybersecurity is not a check-the-box-and-you're-done issue. It requires a commitment of time and resources. It's too late to start planning for a breach once a breach has taken place. Start planning now; best practices begin with a cybersecurity incident response plan as part of a comprehensive IR program.

Key areas of consideration in cybersecurity incident response planning include:

- Who is a part of the cybersecurity incident response team? Who will lead that team?
- How often will the cybersecurity incident response plan be reviewed?
- Does the company perform tabletop exercises and testing of employee cyberreadiness?
- What training is/will be provided to all employees on cybersecurity?
- What are the board of directors' expectations regarding cybersecurity and cyberreadiness planning?
- Is your organization adequately insured to cover data breaches?
- Has your company identified its third-party risks?
- Who will be the company spokesperson to communicate in the event of a breach?

[7] Ponemon Institute. *U.S. Cost of a Data Breach Study*, May 2015.

[8] Bailey, Tucker; Kaplan, James; and Rezek, Chris. *Why Senior Leaders Are the Front Line Against Cyberattacks*, McKinsey & Company, June 2014.

Interviewees

Ten in-depth research interviews provided insights into how companies are reacting to cybersecurity. The following subject matter experts participated in these interviews:

- Bill Barouski, information security expert and former CISO
- Jason Bernstein, partner, data security and privacy group, Barnes & Thornburg LLP
- John Kennedy; corporate partner, IT and outsourcing, privacy, and information security group; Wiggin and Dana LLP
- Melissa J. Krasnow, corporate partner and CIPP/US, Dorsey & Whitney LLP; Governance Fellow, National Association of Corporate Directors
- Ashley McCown, president, Solomon McCown
- Liisa Thomas, chair, privacy and data security practice, Winston & Strawn LLP
- Nolan Wilson, Southeast region leader, professional risk solutions, AON
- Jerry Wynne, CISO and senior director of enterprise security, Noridian Mutual Insurance
- Anonymous, executive director of information security with a large insurance company
- Anonymous, former CISO of a large educational system

Author and contributors

Thomas (Tom) Thompson
Thomas (Tom) Thompson is manager of research at FERF, the nonprofit research affiliate of Financial Executives International (FEI). Thompson specializes in qualitative and quantitative research methodologies, and has authored more than 60 executive reports and white papers. He earned a BA in economics from Rutgers University and a BA in psychology from Montclair State University. Prior to joining FERF, Thompson held positions in business operations and client relations at NCG Energy Solutions, AXA-Equitable and Morgan Stanley Dean Witter.

He can be reached at +1 973 765 1007 or tthompson@financialexecutives.org.

Johnny Lee
Johnny Lee is a managing director in Grant Thornton's Forensic and Valuation Services practice, a practice leader of the Forensic Technology Services group, 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.

Skip Westfall
Skip Westfall is a managing director in Grant Thornton's Forensic and Valuation Services practice, the national practice leader of the Forensic Technology Services group, and the co-leader of the Cybersecurity practice. 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.

Todd Fitzgerald
Todd Fitzgerald is a global director of Information Security for Grant Thornton International Ltd, providing strategic information security leadership for Grant Thornton member firms supporting 40,000 employees in more than 130 countries. Fitzgerald is also an information security author specializing in information security leadership and governance issues.

He can be reached at +1 630 873 2720 or todd.fitzgerald@gti.gt.com.

About Financial Executives Research Foundation Inc.

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 non-members 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.

The views set forth in this publication are those of the authors and do not necessarily represent those of the FERF Board as a whole, individual trustees, employees or the members of the Research Committee. FERF shall be held harmless against any claims, demands, suits, damages, injuries, costs, or expenses of any kind or nature whatsoever except such liabilities as may result solely from misconduct or improper performance by FERF or any of its representatives.

International Standard Book Number 978-1-61509-194-2

About Grant Thornton LLP

Founded in Chicago in 1924, Grant Thornton LLP (Grant Thornton) 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. In the United States, Grant Thornton has revenue in excess of $1.3 billion and operates 57 offices with more than 500 partners and 6,000 employees. Grant Thornton works with a broad range of dynamic publicly and privately held companies, government agencies, financial institutions, and civic and religious organizations.

"Grant Thornton" refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. Please see grantthornton.com for further details.

Financial Executives Research Foundation gratefully acknowledges these companies for their support and generosity:

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

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

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

This content is not intended to answer specific questions or suggest suitability of action in a particular case. For additional information about the issues discussed, contact a Grant Thornton LLP professional.

Grant Thornton

An instinct for growth™

Connect with us


grantthornton.com


@grantthorntonus

linkd.in/grantthorntonus