Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare

Published: 17 January 2018 **ID:** G00349114

Analyst(s): Rob McMillan, Paul E. Proctor

The failure to manage your digital risks is likely to sabotage your digital business and expose your organization to potential impacts well beyond a simple opportunity loss. The extent to which CIOs engage in digital risk management can be a crucial factor in avoiding such dangers.

Opportunities and Challenges

- Digital risk management is a business performance issue that requires business leaders to make informed choices; it's not a technical problem buried in IT.
- The complexities of digital risk management demand a structured program that supports resilience, flexibility and accountability.
- Boards have taken a deep interest in digital risk management and expect full CIO engagement.
- CIOs must be ready for the present and prepared for the future so there's an opportunity to anticipate and influence business initiatives.

What You Need to Know

- As CIOs and business leaders decide on the level of risk they're prepared to accept to pursue their business objectives, information becomes critical.
- Several components — including a charter, policy, strategy and governance process — form a digital cybersecurity program that provides the flexibility required to support business plans, inform risk trade-offs and respond to ever-changing threat environments.
- No prescriptive document an organization could follow will give complete assurance that all reasonable steps have been implemented — organizations must evaluate their own situations, and assess a number of factors to make an informed judgment about what is "enough."

Insight From the Analyst

Think It's Bad Now? The Future Will Be Worse

Rob McMillan, Research Director

Digital risk goes by many names in the Gartner client base, including digital security, cybersecurity, technology risk management and IT security. Whatever you call it, it cannot be ignored. No single, consistent term or definition is globally applicable and accurate for every organization; however, each organization should pick its terms, define them and use them consistently. Gartner uses these terms interchangeably in this document (and throughout our research) to reflect our clients' varied uses of these terms.

The convergence of IT, operational technology (OT) and the Internet of Things (IoT) means that the significance of a flaw in technology will have potentially greater implications in the physical world. These implications are already well-demonstrated by recent history, and can include impacts on human safety. Some breaches bring with them a media circus, whereas others open a generous pipeline of work for lawyers. Regulatory requirements continue to grow in volume and complexity.

Meanwhile, the race for success in the competitive world accelerates as richer digital services and feature-heavy products are developed at faster rates.

This is the world of the modern CIO, where individual executives can't do everything by themselves to safeguard their companies. They must be adept at ensuring that stakeholders are engaged, risk accountability is effectively allocated to digital resource owners and decisions are consistently based on information and consideration.

The research highlighted here gives CIOs guidance they need to succeed in this complex environment.

Executive Overview

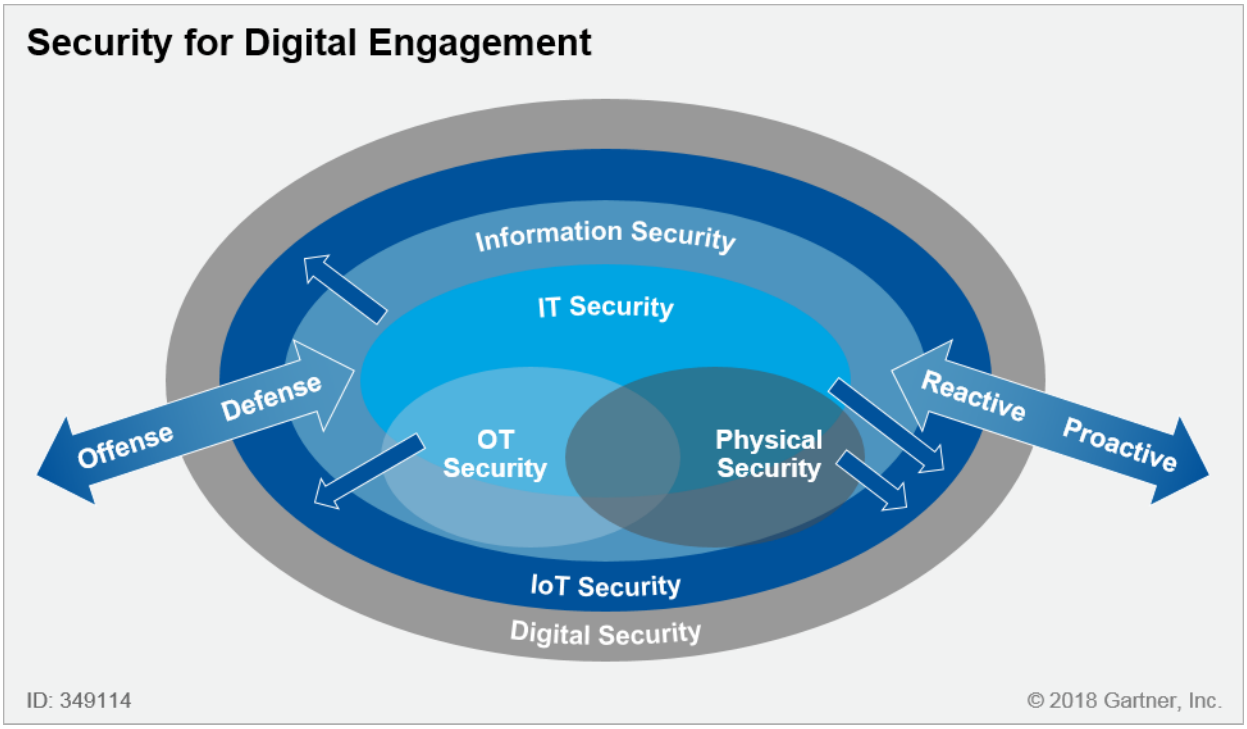
Definition

Technology risk and how we confront it is now a permanent reality that operational and strategic leaders must fully comprehend. Technological risk is no longer simply the narrow concern of technical professionals. Exposure to risk is no longer felt only in small delays or malfunctions. The evolution of business into an activity defined by digital engagement brings technology risk closer to an organization's actions and decisions. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day, often

without realizing the significance of what they're doing. The consequences of these choices can be calamitous, just as the potential of digital business constantly grows.

The CIO becomes the central agent stressing the connections between business and digital risk — connections that should be important to technical and nontechnical staff, from contributor-level staff to the board. This is a moment for CIOs to be deliberate in their implementation and communication of digital risk management issues with all of the participants in the business. With staff prioritizing the organization's measured consideration of its business plan and environmental factors, the enterprise will be positioned to cover external threats, economic conditions, social attitudes, political changes and regulatory requirements. (See Figure 1 for a depiction of interrelated security.)

Figure 1. Security for Digital Engagement



Source: Gartner (January 2018)

This research examines how CIOs can engage the entire enterprise in digital risk management efforts, and how changing perceptions of risk enable the organization to better operate with informed decision making.

Digital risk management is the integrated management of risks associated with digital business components, such as cloud, mobile, social, big data, third-party technology providers, OT and the IoT.

Research Highlights

Business Leaders Need to Make Informed Choices About Digital Risk

"CIOs can't protect their organizations from everything, so they need to create a sustainable set of controls that balances their need to protect their businesses with their need to run them. Taking a risk-based approach is imperative to set a target level of cybersecurity readiness. Raising budget alone does not create an improved risk posture. CIOs must prioritize security investments by business outcomes to ensure that the right amount of budget is being spent on the right things. Attacks and compromise are inevitable, and, by 2020, 60% of security budgets will be in support of detection and response capabilities." — Paul Proctor, Gartner vice president and distinguished analyst (see "CIOs Should Manage Technology Risk and Cybersecurity Through the Lens of Business Value").

Sadly, cybersecurity threats will continue to pervade the global economy in 2018. CIOs expect cybersecurity threats to increase and affect their organizations. In their twisted way, many cybercriminals are digital pioneers — their exploits in ransomware, for example, show that they are already operating on a global scale. They readily tap into advanced analytics capabilities to target large volumes of small victims. These security bandits are learning the same big digital lessons as the enterprises they prey on (see "The 2018 CIO Agenda: Mastering the New Job of the CIO").

What is needed now is a broad realization that this cyberintrusion phenomenon is here to stay, so crucial digital risk management decisions must be of higher quality. CIOs and business leaders must be allied and informed as they decide on the levels of risk they're prepared to accept to pursue their business objectives. Strong accountability models, in which risks rest with those that have the authority to address those risks, ensure that systemic security problems are not allowed to fester. Those decisions should then be made by the lines of business that will ultimately bear the consequences. They will subsequently use risk and cybersecurity specialists to help inform them of realistic risks and the options for managing those risks efficiently and cost-effectively (see "Institute Cybersecurity and Risk Governance Practices to Improve Information Security").

Related Research

- "CIOs Must Implement a Risk-Based Approach to Improve Business Outcomes" describes a risk-based approach to technology risk and cybersecurity issues that requires a cultural change and recognizes the impossibility of perfect protection. This case study of the Dutch National Police demonstrates that reasonable risk management can be done effectively, and this approach can measurably improve decision making and executive engagement.
- "Institute Cybersecurity and Risk Governance Practices to Improve Information Security" asserts that effective governance should be a cornerstone of security programs, and ineffective governance is the most common cause of failure. Security and risk management leaders need to implement governance capabilities that support accountability, authority, risk management and assurance.
- "CIOs Should Manage Technology Risk and Cybersecurity Through the Lens of Business Value" posits that CIOs should address technology risk and cybersecurity challenges through the lens of business value to deliver levels of protection that support business outcomes. This research helps leaders learn to treat cybersecurity like a business function.
- "How to Determine If Your Organization Practices Due-Care Security" discusses the provision of adequate information security as a corporate and government agency obligation. However, a standard to measure how, and if, this obligation is adequately addressed remains elusive. A risk management mindset that acknowledges an organization's specific — and often changing — needs must be adopted.
- "Executive Guidance: Reducing Risk Management's Organizational Drag" is based on a review of thousands of client companies. Gartner observes that progressive organizations no longer treat risk management as a discrete activity, isolated from strategy development, but, rather, as an effort central to strategic design and execution.
- "Enterprise Risk Management and Cyber Risk" is written for leaders wondering what role enterprise risk management groups play in managing cyber risk. They will then understand who at peer organizations is responsible for managing cyber risk, what role ERM plays and what every executive needs to know about managing cyber risk.
- "Building an Enterprise-Relevant Risk Assessment Process (McDonald's)" describes the concept of a fully consolidated risk assessment process. This is often perceived as extremely difficult, although valuable. This research examines how McDonald's carefully thinks through the steps to create an efficient and effective consolidated risk assessment.
- "CEB Ignition Guide to Drafting Information Risk Appetite Statements" includes documents that will help you educate business partners on the business value of creating and using an information risk appetite statement. You will be able to assess business partners' preferred risk-taking posture and write an information risk appetite statement that aligns with business partners' risk-taking posture and corporate risk philosophy.
- "Getting Serious About IT Risk Management" discusses the three imperatives every IT department should be focusing on to manage IT risks effectively. Focusing on the right risks,

improving IT's risk management practices and ensuring that IT staff understand their role in managing risk are key items for any risk management initiative.

- "Executive Guidance for 2016: Managing the Hidden Causes of Data Breaches" reflects the changes in technology, as well as the exponential growth of information collected, analyzed and stored, that cause companies to become more susceptible to data breaches. These breaches are not only costly from a financial standpoint, but harmful to a company's reputation.
- "Formalizing Interfaces Between Risk Management Functions" compares the past, when risk management functions had clearer mandates because a single function usually owned each risk type, with today, when risk management functions are more interested in how information risks are managed. This study identifies best-practice strategies for coordinating risk management activities with other risk management functions.
- "Third-Party Risk Management in the Modern Enterprise" outlines the variety of activities leaders can use to effectively manage third-party risk in the modern enterprise. Our identified best practices are organized into seven critical objectives, each applicable to individual third-party relationships.

Cybersecurity Is Complex, Requiring a Structured Program That Supports Resilience, Flexibility and Accountability

> "God is in the details." (Ironically, the origin of this saying is unclear, but has been variously attributed to Ludwig Mies van der Rohe, Aby Warburg and Gustave Flaubert.)

Organizations that rely on outdated, simplistic approaches to security program management will continue to experience inefficiency and internal disconnects, and will fail to deliver optimum business results. Those that take a more complex, but flexible, approach will position themselves for digital business success and resilience.

Related Research

- "A Practical Approach to Strategic Thinking on Risk, Urgency, Innovation and Agility for CIOs" addresses one of the greatest CIO leadership challenges in the digital age — helping enterprises embrace the concept of good strategic risks. Most enterprises express significant confusion regarding risk. This research addresses a reality for many CEOs: They claim that innovation is an important priority, yet they often struggle to clearly articulate the enterprise's approach to risk management.
- "Develop a Pragmatic Vision and Strategy for Digital Business Security" presents a comprehensive strategic vision for digital business security. This must be guided by the business, technology and threat drivers unique to the organization, and should identify a number of key elements. This research helps security and risk management leaders develop coherent digital security programs, based on a clear vision and strategy.

- "Leadership Vision for 2018: Security and Risk Leaders" discusses the security and risk management leader's role in helping the enterprise balance the risk and benefits of digital business. The enclosed slide deck is useful for your security presentations to your leadership, peers and teams.
- "CISOs Need to Understand the Components of Their Information Security Programs" describes how an information security program defines the enterprise's key information security principles, resources and activities. CISOs need to analyze, document and implement the components of a program that will enable the enterprise to deal with the challenges of cybersecurity and digital business risks.
- "Cybersecurity Charter" contains the Cybersecurity Program Charter Template, a customizable set of PowerPoint slides that you can use to create a cybersecurity program charter unique to your organization. Each slide is prepopulated, based on best-in-class charters and is accompanied by discussion notes and input instructions to help you customize.

Boards Are Interested and Expect Full Executive Engagement

As the number and impact of security breaches continues to climb, boards of directors have significantly increased their focus on information security and IT risk management. Gartner is hearing more frequently from CIOs and other IT leaderships that boards are requesting more frequent briefings on the threat and risk landscape. These discussions cover the program goals and status of the enterprise's efforts to manage IT-related business risk. Gartner survey data from March 2017 indicates that risk data regularly influences the decisions of 78% of organizations' boards of directors.[5]

> "The most important thing — and I can't stress this strongly enough — is to make sure that you present yourself credibly as a business partner who's working with the CEO, the COO and the other executives in the organization. If you aren't seen that way, you may never have an opportunity to get in front of the board." — Patricia Oelrich, Pepco Holdings (See "Gartner Fellows Interview: Patricia Oelrich, Board of Directors, Pepco Holdings, on CIOs, Their Boards and Risk Management.")

Boards expect that the organization's senior leadership has its hands on the cybersecurity tiller. With due independence in place between CIOs and CISOs, CIOs are usually under scrutiny in this respect. They are, more often than not, the senior executives with primary responsibility for the cybersecurity program.[6]

One of the CIO's tasks in this respect — in conjunction with the CISO — is to marshal the engagement and support of all significant stakeholders in the organization to ensure a business-led approach. However, only 30% of organizations do this.[7] This is symptomatic of a broader malaise, which often frustrates leadership boards.

> "Something I find pretty regularly in advising corporate leaders and in discussions at board forums is a real disconnect between the company's risk inventory — which, if there is an enterprise risk management program, is usually pretty big — and the risks that are listed in its Securities and Exchange Commission (SEC) annual report. This disconnect is frustrating for boards, because they recognize that there needs to be an integrated approach to risk management, with consistency between what the board knows about those 10 or 15 risks and what's being done about them, on the one hand, and what the company is telling the SEC and the rest of the outside world on the other. That integrated approach is the essence of the enterprise risk management strategy that the board wants for its risk oversight duties, as well as the comfort that the company is effectively managing risks to business imperatives." — Patricia Oelrich

All senior executives have a role; however, the board — or the media, or regulators — often focuses on the CIO as the first target for questioning when issues arise.

Related Research

- "Five Principles of Effective Cybersecurity Board Presentations" deals with the costly data breaches affecting major corporations, which have become a regular facet of the 24-hour news cycle, prompting heightened pressure from shareholders and regulators. As a result, corporate directors are becoming increasingly conscious of information security. This white paper arms security leaders and their teams with five principles and some practical tips for their next board presentation.
- "Toolkit: Board-Ready Slides for Cybersecurity and Technology Risk" describes a now-common practice for boards of directors to require periodic reporting and event-based updates on the state of IT risk and information security. Security and risk management leaders must provide board-relevant and business-aligned content, and these sample board presentations can help.
- "Three Questions Boards Must Ask Their CISOs" outlines three questions every board director should ask the CISO (and by extension, the CIO). It provides guidance on what responses to look for, and a cheat sheet on common security terms and definitions. CIOs can use this guide to coach board directors and improve their "cyber savviness" before security presentations.
- "2017 CEO Survey: CIOs Need to Increase CEO Technology Risk Awareness" shows that CEOs are paying attention to technology, but not always to the associated risks. This survey reveals that CIOs still have work to do in making the case for increased focus on IT risk.
- "How to Get Your CEO to Embrace Digital Risk Management" describes how organizations can improve their risk management programs and outcomes by addressing risks in the context of value, desired business outcomes and their risk appetites.
- "Top Tips for Communicating Security and Risk to Business Stakeholders" provides leaders with key communication techniques. Gartner client inquiries have made it clear that a serious challenge faced by security and risk management leaders is their inability to communicate

effectively with senior executives and other key business decision makers. This needs to be accomplished using relevant, common and simple-to-understand language.

- "A Board Narrative to Transform Operational Risk and Cybersecurity Into a Business Service" describes how risk and cybersecurity issues continue to be treated as technical problems, handled by technical people, buried in IT. Risk and security programs are perceived as cost centers aimed at protecting the organization from all possible risk and cybersecurity threats. This leads to poor investment decisions and improper expectations. Use this narrative to create a set of sustainable risk and security services that deliver defined levels of risk at defined cost.
- "Information Security Presentation Support Center: Presentation Templates for CISOs and Their Teams" discusses how frequent presentations can distract from higher-value management activities, such as functional planning and talent management. Our presentation templates and scripting guidance help CISOs and their direct reports spend less time creating presentations without sacrificing confidence or quality.

CIOs Must Be Ready for the Present and Prepared for the Future

CIOs often ask questions that can be roughly summarized as, "How much security is enough?" Frequently, an assessment of the adequacy of a security program is made using some variation of a reasonable-steps test — that is, what a reasonable person would do under the same or similar circumstances. The problem for many executives is that the notion of what constitutes "reasonable" is imprecise, depends on circumstances and changes over time. Compliance with an industry standard or satisfactory third-party audits may help mitigate consequences, but may not be a replacement for doing everything that is reasonably needed to avoid damage to the organization or to others.[8]

There is no prescriptive document any organization could follow that will give complete assurance that all reasonable steps have been implemented, and the standard of due care in a specific circumstance has been met. Each organization must evaluate its own particular circumstances, and take into account a number of factors to make an informed judgment about what is "enough."

"Adapt or perish, now as ever, is Nature's inexorable imperative." — Wells, H.G., 1945. (Mind at the end of its tether. London, W. Heinemann)

Compliance with regulation is a minimum standard, but it is not a substitute for taking all the reasonable steps. Organizations must consider all reasonably foreseeable risks. Reasonable foreseeability does not require knowing how an adverse outcome may occur, only that the outcome is a possibility. In these days of breaches spurring regular media coverage, and governments announcing regulatory reform and national cybersecurity strategies, the concept of reasonable foreseeability is expanding at a dramatic pace.

This expansion requires that organizations, usually under the direction of the CIO and CISO, have in place a suite of controls that provide a defensible mix, given the organization's risk profile. The

efficacy of these controls should be tested regularly by vulnerability assessments, penetration tests and maturity assessments. An ongoing plan for new or updated controls should be maintained to meet new risks as digital business plans evolve.

Related Research

- "How to Respond to the 2018 Threat Landscape" explains why taking action based on trends and vulnerabilities is the best step. As the monetization of exploits and security grows, patching, detection and vulnerability management are ideal ways for security and risk management leaders to face a ransomware-dominated landscape.
- "Emerging Risks Report and Monitor" uses CEB's quarterly Emerging Risks survey to capture and analyze senior executives' opinions on emerging risks and provides action-oriented insight on identifying and mitigating these risks. Review this research for an analysis of the top 10 emerging risks in key industries, with an estimate of their impact, probability and velocity.
- "The Security Processes You Must Get Right" presents a catalog of core security processes that satisfy governance and audit requirements, demonstrate value to the business, and provide a foundation for continuous improvement. They will enable enterprises to keep pace with the industrialization of IT.
- "Prepare for the Inevitable With an Effective Security Incident Response Plan" describes how advance preparation is crucial to effective incident response, but is also extremely difficult, especially in complex, distributed enterprises. Prepared organizations test various scenarios multiple times per year and engage key organizational stakeholders. This guidance helps organizations prepare relevant incident response plans.
- "CEB Ignition Guide to Building a Cyber Crisis Testing Program" will help you prepare your organization to respond to cyber crises; identify, document and remediate gaps in the organization's cyber crisis management plan; and lead cyber crisis testing at the enterprise level.
- "Toolkit: Tabletop Exercise for Cyberattack Preparation and Response" is based on the idea that security incidents are inevitable, and mistakes and/or a lack of preparation in the response can have serious repercussions. Security and risk management leaders with business continuity management responsibility can use this Toolkit to plan for and respond to the challenges of a targeted cyberattack.
- "Predicts 2018: Security and Risk Management Programs" deals with the widespread perception of the near-inevitability of cyberintrusion and how powerfully this influences the ways organizations approach risk. Security and risk management leaders are launching information security programs based on strong principles that facilitate business outcomes, organizational cohesiveness and pragmatic decisions.
- "Advance and Improve Your Mobile Security Strategy in 2018" describes how the mobile attack landscape has continued to grow and change with the increase of the number of smartphones and tablets. At the same time, bring your own device (BYOD) initiatives are proliferating in the enterprise. With the constant increase in consumer devices as enterprise tools, IT has an

opportunity to train users to protect personal and professional data from these threats by invoking the impact on their personal lives.

- "Avoiding Common Failures in Security Analytics (UnitedHealth Group)" addresses the reality that security analytics projects often fail expensively. Learn how UnitedHealth Group avoided four common failure points to build a successful security analytics program.
- "Cybersecurity Scenario 2025: Outrageous Intelligence" discusses the ways that CISOs must change how they manage and communicate about risk in the future digital business. Successful security and risk management leaders should leverage Gartner's Cognition/Sentiment Model to make better risk trade-offs and lead the conversation at the board level.

Related Priorities

Table 1. Related Priorities

Priority	Focus
Applying Project Portfolio Management with Scarce Resources to Optimize Business Value	This initiative explores evolving project portfolio management the right way, given today's dynamics. It addresses the tools, practices and skills required to maximize project portfolio value.
Managing Cost Optimization	Cost optimization is a business-focused, continuous discipline to drive spending and cost reduction, while maximizing business value.
CIO Leadership in Innovation and Strategic Business Change	In the digital era, CIOs have two jobs: business leader and IT leader. This initiative delivers to the first job, addressing how CIOs can contribute to the development of an enterprisewide strategy.
Evolving IT Financial Management Practices	IT financial management uses budgeting, metrics and other tools to support innovation, improve business and IT outcomes, and increase the credibility of the IT organization with the business.

Source: Gartner

Gartner Analysts Supporting This Trend

Jeffrey Wheatman, Research Director

Tom Scholtz, Vice President and Gartner Fellow

Sam Olyaei, Senior Research Analyst

Matt Stamper, Research Director

Wam Voster, Research Director

Related Resources

Securing Digital Business: Adapt, Transform, Scale

Prepare to meet the pace and scale of today's digital business. Take a comprehensive look at your cybersecurity, risk management and compliance strategies at Gartner Security and Risk Management Summit 2018.

Webinars

"What Every CIO Needs to Know About Technology Risk and Cybersecurity"

"Managing Risk and Security at the Speed of Digital Business"

"Develop a Pragmatic Vision and Strategy for Digital Business Security"

"How to Build Advanced KRIs That Influence Business Decision Making"

"Top Cybersecurity Trends for 2018"

"Cybersecurity Scenario 2025: Outrageous Intelligence"

"The 2018 Security Threat Landscape"

Articles

"Confront the Cybersecurity Talent Shortage"

"Former NATO Commander Says Cybersecurity Most Worrying Threat We Face"

"Link Cybersecurity to Business Outcomes"

"Cybersecurity Myths of the Industrial IoT"

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How to Get Your CEO to Embrace Digital Risk Management"

Evidence

[1] One of the most extreme examples of such damage was the Knight Capital incident, when a human error set in motion automated trades that, in effect, lost a financial company $440 million in 45 minutes.

[2] "Operating results declined due to an estimated $300 million impact from the cyberattack": FedEx, "FedEx Corp. Reports First Quarter Earnings," 19 September 2017.

[3] Report of –300 basis points (–3%) of revenue impact: Mondelez International, "Update on Cyber-Attack and Preliminary Estimates of Financial Impacts," press release, 6 July 2017; revised to –2.7% when the results were reported (–$170 million compared with 2Q16): "Mondelez International Reports Q2 Results and Increases Quarterly Dividend," press release, 2 August 2017; further revised to –2.3% of second quarter revenue, but also affecting third quarter revenue +0.6% as shipments caught up: "Mondelez International Reports Q3 Results," press release, 30 October 2017.

[4] Maersk, "A.P. Moller-Maersk Improves Underlying Profit and Grows Revenue in First Half of the Year," press release, 16 August 2017;"A.P. Moller-Maersk A/S Grows Revenue and Underlying Profit in the Third Quarter of the Year," press release, 7 November 2017.

[5] Gartner conducted its Annual Security and Risk survey in five countries between 24 February and 22 March 2017 to better understand how risk management planning, operations, budgeting and buying are performed, especially in the following areas:

- Risk and security management
- Security technologies and identity and access management (IAM)
- Business continuity management
- Security compliance and audit management
- Privacy

The research was conducted online among 712 respondents in five countries: U.S. (n = 141), Brazil (n = 143), Germany (n = 140), U.K. (n = 144), and India (n = 144).

Qualifying organizations have at least 100 employees and $50 million in total annual revenue for fiscal year 2016. All industry segments qualified, with the exception of IT services and software and IT hardware manufacturing.

Furthermore, each of the five technology-focused sections of the questionnaire required the respondents to have at least some involvement or familiarity with one of the technology domains we explored.

Interviews were conducted online and in a native language and averaged 19 minutes. The sample was drawn from external panels of IT and business professionals. The survey was developed collaboratively by a team of Gartner analysts who follow these IT markets and was reviewed, tested and administered by Gartner's Research Data and Analytics team.

A total of 294 respondents answered the question (A02), "Which of the following best characterizes the effectiveness of board-level engagement on risk in your organization?"

[6] Gartner Security and Risk (2017) above. A total of 251 respondents answered the question (A09), "In your organization, to whom does the most-senior-level person dedicated to information security directly report?"

[7] Gartner Security and Risk (2017) above. A total of 297 respondents answered the question (A03), "Does your organization have a Risk Steering Committee or Advisory Board?"

[8] In November 2013, U.S.-based retailer Target suffered an incident that resulted in the exposure of more than 40 million credit cards. Target's CFO, John Hughes, testified at a Congressional hearing. The transcript of that testimony includes an observation that, "in September 2013, our systems were certified compliant with the Payment Card Industry Data Security Standards, meaning that we met approximately 300 independent requirements of the assessment. Yet the reality is that our systems were breached." (See Congressional testimony, 26 March 2014.)

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp