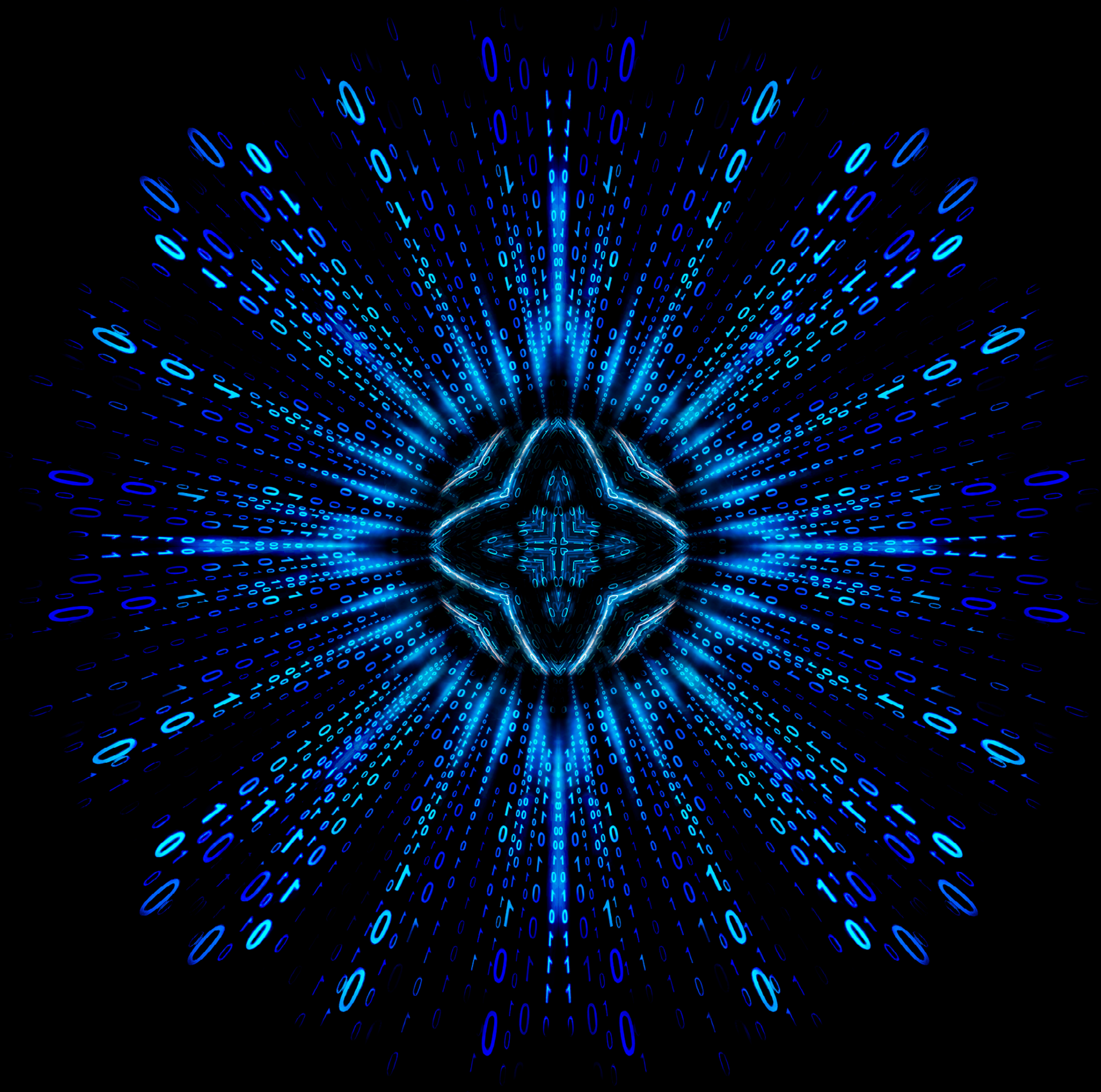
Deloitte.



# Take the lead on cyber risk

How to move from now to
next-level security

Cyber Risk

# Risk powers performance.

Digital transformation and the use of exponential technologies are creating unprecedented opportunities for businesses. Every new opportunity also presents new threats, and one of the biggest is cyber risk. The most successful businesses will go beyond traditional risk management—simply avoiding or mitigating a cyberattack—to taking strategic, calculated risks to maximize the benefit from advances in technology.

Cyber risk is already a huge challenge and it's growing rapidly. According to a recent report, by the year 2020 the world will need to cyber-defend 50 times more data than it does today.[1] And with new risks emerging daily, organizations must constantly devise new cyber strategies and defenses as attackers figure out how to get past the cybersecurity that is currently in place.

In order to be successful, organizations need a robust cyber strategy that will enable them to be secure, vigilant, and resilient when faced with constantly evolving cyberthreats. We believe that adopting this approach is a key step in helping leaders continue to identify risks and responses—and even to use risk as a way to power performance at their organizations. Deloitte's Cyber Risk professionals around the world can guide you on that journey.

To learn more, please visit us at www.deloitte.com/cyber.

Regards,

Sam

Sam Balaji
Global Risk Advisory Business Leader

[1] Cybersecurity Ventures, 2016 Cybersecurity Market Report, http://cybersecurityventures.com/cybersecurity-market-report/ Accessed 9 May 2017

# Table of contents

# Introduction

## For organizations of every shape and size, it's no longer a question of *if* you will be attacked, but *when* (and *how*).

The digital revolution is happening and there is nothing you can do to stop it. Nor should you try. In the months and years ahead, digital innovations and exponential technologies will be key drivers of growth and success, providing unprecedented opportunities for your organization to create value and competitive advantage.

But to thrive in a digital future, you need a robust cyber strategy that can help your organization become secure, vigilant, and resilient. Hope is *not* a strategy.

Cyber capabilities must do more than address the threats that exist *now*. As exponential technologies drive digital disruption, they introduce entirely new kinds of cyberthreats and amplify existing ones—requiring additional *next-level* capabilities that companies must start building now.

Cyber risk is not an information technology (IT) issue, it's a business issue—and a strategic imperative. Risk, security, and business leaders must constantly strive to understand the opportunities and risks associated with digital innovation, and then strike a balance between the need to protect the organization from cyberthreats and the need to adopt new business models and new strategies that capitalize on digital technology and lay the groundwork for future success.

The good news is that while digital disruption and cybersecurity present serious challenges, those challenges are not insurmountable. By understanding what needs to be done—and mustering the courage and foresight to tackle the challenges head-on—you can take charge of your cyber fate and become a digital disrupter, instead of getting disrupted by the competition.

# The changing landscape of cyber risk

In the World Economic Forum's Global Risk 2017 report,[2] cyber risk is recognized as one of the top commercial risks, alongside the economy, the environment, and geopolitics. Digital technologies and innovation are growing exponentially, accelerating cyber risks, creating new attack vectors, and greatly expanding the attack surface that organizations must patrol and defend.

The internet and mobile connectivity continue to be increasingly vital to every aspect of how we live, work, and do business, opening up endless and growing opportunities for cyberattacks. Meanwhile, cyberthreats are becoming increasingly sophisticated, malicious, and well-funded—constantly raising the bar on cybersecurity.

[2] World Economic Forum, *The Global Risks Report 2017, 12th Edition,* http://www3.weforum.org/docs/GRR17_Report_web.pdf
Accessed 9 May 2017

Key factors reshaping the cyber landscape:

**Dissolving perimeter:** Innovations such as Hybrid IT, Cloud, and digital ecosystems are blurring the boundaries between organizations and dissolving the network perimeter an organization must defend.

**Exponential technologies:** Increasing use of exponential technologies—such as robotics, automation, 3D microchips, cognitive intelligence, and agile development—are changing the velocity of business and technology innovation. This accelerates cyber risks and can complicate cyber programs, which are often structured around traditional IT development approaches and timelines.

**Mobile networks:** Mobile isn't just a new feature that organizations must offer to their customers. For a growing number of consumers—particularly millennials—mobile is a way of life. For them, it's not just another channel; it's the only channel that matters. As such, mobile is creating fundamentally new buying behaviors. It also greatly increases the attack surface for cyberthreats, since mobile networks are by nature geographically vast and fluid.

**Internet of Things (IoT):** Whether it includes smart sensors in a "smart factory" (Industry 4.0) or a remote connection to an insulin pump, the IoT is expected to have a positive and transformative impact on our lives. However, it also opens up a whole new world of devices to be exploited. This can temper the growth or acceptance of these technologies.

**The changing nature of business:** Innovative organizations are creating new digitally enabled revenue and delivery models that create cyber challenges at every level, starting at the top with business strategy.

**Artificial intelligence (AI):** Artificial intelligence is beginning to supplement or replace human experts. This can lead to greatly improved capabilities and reduced costs; however, it also creates new risks, such as chatbots that go rogue and behave inappropriately.

**Collaborative platforms:** Software that integrates social networks into business processes can help foster innovation, but it also increases an organization's exposure to risks from external sources.

These factors will change our world, creating market opportunities beyond the imagination. Yet they will also give rise to new kinds of cyberthreats that are impossible to fully anticipate.

# Moving from now to next-level cybersecurity

Even threats an organization thinks it has under control today could threaten it again in the future as those threats evolve and grow in sophistication and complexity. For example, distributed denial of service attacks have been around for many years, yet they are now more prevalent, deceptive, and sophisticated than ever—often being used as a ploy to divert attention from secondary attacks such as data exfiltration, physical attacks, or the implanting of ransomware.

To protect itself from both evolving and emerging cyberthreats, an organization needs to ensure it has established basic cyber capabilities that can protect it from today's threats right now, while at the same time investing in next-level capabilities that can protect it from whatever threats might emerge in the future. These now and next-level capabilities fall into three broad categories:

### Secure.

Your actual defenses against an attack, including everything from cyber strategies to policies and procedures to systems and controls.

### Vigilant.

Your early warning systems, which enable you to identify potential threats before they hit, and to quickly detect attacks and breaches as they occur.

### Resilient.

Your ability to respond quickly to attacks, and to bounce back quickly with minimal impact on your organization, reputation, and brand.

The pages that follow take a closer look at each of these categories, discussing the now and next-level capabilities your organization needs to keep itself safe—today and in the future.

# Secure

## Enhancing risk-prioritized controls to protect against known and emerging threats, and to comply with industry cybersecurity standards and regulations

"Secure" refers to an organization's actual defenses and all their associated components and capabilities. Like fences and locked doors in the physical world, these are the mechanisms that actually keep bad guys out. In cyber terms, "secure" includes capabilities such as: infrastructure protection, vulnerability management, application protection, identity and access management, and information privacy and protection.

### Where you should be now

#### Integrate cyber strategy with business strategy

In a digital world, cyber strategy and business strategy go hand-in-hand. Although business objectives are paramount, it is no longer possible to develop effective business strategies and business models without thinking about how they will be affected—and in many cases enabled—by digital technologies, and how the organization will protect itself from cyberthreats. Even the most creative and brilliant business strategy in the world is worthless if an organization can't figure out how to secure the required operations from cyberattacks.

The time for an organization to consider the impact and mitigation of cyberthreats is in the beginning, when developing its strategy—not months or years later when the organization has already begun implementing the required systems and processes and has committed vast resources to pursuing a particular course of action.

## Identify and protect your crown jewels

Although a comprehensive cyber strategy that provides full protection for everything within an organization might sound great in theory, in practice, it just isn't feasible. Cyberthreats are infinite, but cybersecurity budgets and resources are finite. This means setting priorities, with your "crown jewels" at the top. These include:

- **People:** Key individuals that might be targeted.
- **Assets:** Systems and other assets that are crucial to your business and operations.
- **Processes:** Critical processes that could be disrupted or exploited.
- **Information:** Data, information, or intelligence that could be used for fraudulent, illegal, or competitive purposes.

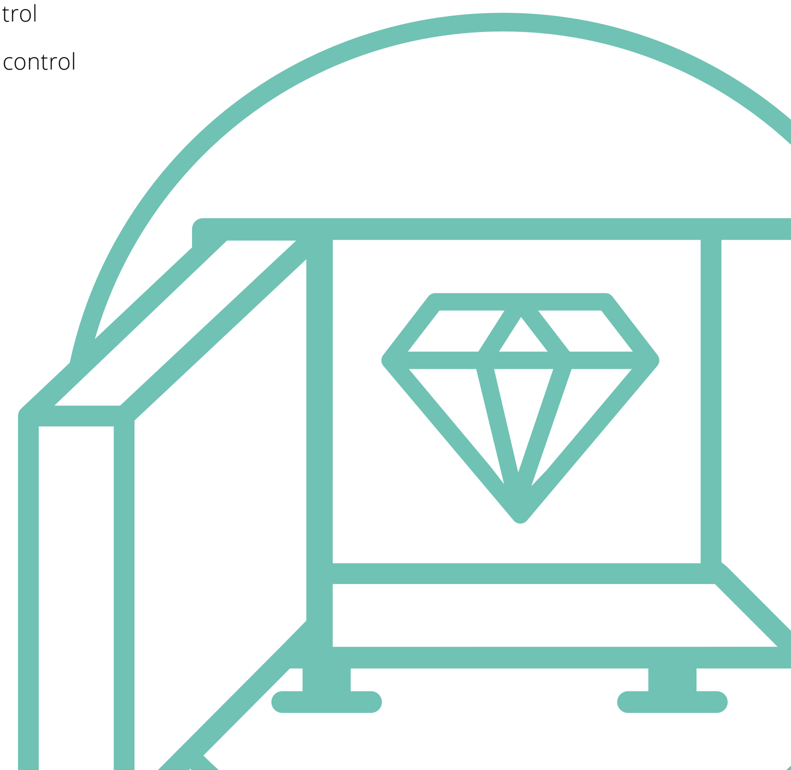
Organizations that don't explicitly design their strategies around these crown jewels often end up allocating their resources haphazardly, investing too much in areas that aren't very important while investing less in what matters most, leaving these areas dangerously vulnerable.

After identifying your crown jewels, the next step is to assess the threats to which they are most vulnerable, and then identify and close any security and control gaps that could leave them exposed.

## Develop a strong cybersecurity framework

After creating an overall strategy that protects your crown jewels, the next step is to develop a framework that integrates cyber strategy with business strategy. As with cyber strategies, the specific details of every cybersecurity framework are unique to each organization. However, the framework typically includes some standard elements:

- Strategy and operating model
- Policies, standards, and architecture
- Cyber risk culture and behavior
- Cyber risk management, metrics, and reporting
- Lifecycle management
- User access control
- Role-based access control
- Privileged-user access control



## Taking cybersecurity to the next level

### Embed cybersecurity into everything from the beginning

Cybersecurity has traditionally been treated as an IT issue and tacked onto IT applications and systems almost as an afterthought. But in a digital world, this back-end approach just isn't good enough. Instead, organizations need to make cybersecurity part of their DNA, weaving it into everything they do from the outset. As noted above, integrating cyber strategy with business strategy is critical. Also, since most organizations now execute their business strategies by operating as an extended enterprise, it is essential to consider cybersecurity when building and working with an ecosystem of suppliers, vendors, and partners.

Cybersecurity also needs to be an integral part of application development. Today's developers rely heavily on approaches like Agile and DevOps that emphasize speed and collaboration, enabling them to push out applications much faster—which is a digital imperative. However, this speed to market means security measures may suffer, as proper controls and security features may not get built in at each phase. In fact, many developers still view cybersecurity requirements as an inhibitor or roadblock to getting things done quickly and efficiently. This is a conflict that needs to be addressed as organizations raise their cybersecurity capabilities to the next level.

Fortunately, there is an emerging trend to embed security into DevOps—which itself is a combination of development and operations—essentially turning DevOps into SecDevOps. And while the terminology might be a bit awkward, the idea of formally integrating security with development and operations is a big step in the right direction.

### Develop better ways to manage data

Data is a precious resource that is growing exponentially as people and organizations around the world embrace all things digital. This precious resource needs to be carefully managed to keep it safe while harvesting its full value.

One key to success is information lifecycle management (ILM), which is a comprehensive approach to managing and securing all aspects of data and information, from acquisition to disposal—and everything in between.

This is a situation where more is not necessarily better, since the more data you have—and the longer you keep it—the greater your attack surface, risk exposure, and legal liability. Also, the challenge of managing data is becoming larger and more complex every day. Data volumes are growing faster than ever, driven by increased mobile use and the rise of IoT. And the data is increasingly complex, with numerous formats (both structured and unstructured) and numerous sources (including third-parties).

As with the overall cyber strategy, it's important to focus on protecting the data and information that is most critical. Organizations that try to secure all of their information assets are setting themselves up for failure. However, the same is true if an organization focuses on its crown jewels but makes the mistake of trying to protect those critical assets from every possible threat.

Ultimately, success in this area hinges on setting the right priorities: identifying your most critical assets, and then protecting those assets from the most critical threats.

# Vigilant

## Sensing, detecting, and predicting violations and anomalies through better situational awareness

Vigilance is an organization’s early warning system. Like security cameras and a guard at the front desk, capabilities in this area help sense, detect, and predict threats before they become attacks, attacks before they become breaches, and breaches before they become crises.

### Where you should be now

#### Be situationally aware

Vigilance starts with understanding your adversaries—who might attack and why—and then building situational awareness to stay a step ahead. Many organizations think they can achieve the necessary awareness through automated threat intelligence reports, which are essentially just newsfeeds of emerging threats and issues. Unfortunately, true vigilance requires much more than that. Instead of settling for generic knowledge of the current threat landscape, you need to understand your organization’s unique cybersecurity context—including what it most needs to protect, and where it is most vulnerable.

In particular, organizations should strive to establish continuous situational awareness—the ability to detect changes in a business’s footprint that could change its risk posture. Examples of such changes include: mergers, acquisitions, alternative delivery models (e.g. offshoring), new vendors, or even outsourcing strategic functions such as legal counsel.

When innovating, it’s a good idea to bring security teams in early to conduct ongoing system reviews that can help identify and address unexpected impacts to the threat landscape. Also, robust monitoring processes make it possible to stay constantly aware of what is going on across the entire cybersecurity environment. Are you still secure? Are you currently under attack? Have you been breached? A surprising number of organizations are victims of an attack or a breach without ever realizing it.

### Pay attention to your entire ecosystem

Suppliers, vendors, partners, and even customers can all be points of entry for an attack—which means that even if an organization itself is highly secure, it could still be vulnerable. After all, a chain is only as strong as its weakest link.

To stay aware, conduct ongoing cybersecurity assessments of your ecosystem to ensure outsiders are not creating unacceptable risk exposure. Also, be part of the solution, sharing information with ecosystem partners and fostering collaboration to fight common adversaries.

It is also essential to constantly monitor for suspicious or atypical activities, wherever they might occur. Although external attacks get most of the headlines, the fact is many of the biggest cyberthreats are internal—originating from within an organization or its extended enterprise. These internal incidents can be even more damaging than attacks from the outside, yet they tend to be kept quiet. Also, in some cases, the damage is done without malicious intent, but is simply the result of carelessness or poor controls and procedures.

## Taking cybersecurity to the next level

### Use advanced technologies to pro-actively identify and hunt down threats

Leading organizations harness the power of AI, cognitive learning, deep analytics, correlation technologies, and threat intelligence to develop advanced levels of situational awareness—enabling them to anticipate and identify potential new threats before they emerge.

Deep analytics and correlation technologies can help an organization understand how an attack was launched, what types of attackers are using it, and what entry points are being targeted. These technologies also enable predictive threat detection, helping to anticipate and mitigate future threats that may evolve from current threats as attackers find ways to circumvent existing security mechanisms.

Threat intelligence is the province of trained CTI (cyberthreat intelligence) professionals, who monitor a wide variety of information sources—including the dark web, malware reports, and online activity—to find risks specific to your organization. These professionals monitor and learn from attacks perpetrated against other organizations, and then apply that accumulated intelligence to help you protect the areas at greatest risk within your organization.

In addition to monitoring, mature intelligence teams actively hunt for new threats. If, for example, a team uncovers a new malware stream, it can build an analytical model to detect new instances and iterations of the malware. From there, it can create algorithms and automated processes to hunt down the emerging threats before they can do harm.

Success in this area requires a deep understanding of the business through direct engagement and integration. By building these advanced threat detection capabilities into core business processes, you can operationalize threat intelligence across the entire organization—putting responsibility for detecting and managing cyber risks closer to the source. This distributed, action-oriented approach becomes increasingly important as your attack surface expands and cyberthreats become more widespread and difficult to detect.

### Understand and address exponential threats

Exponential technologies and digital disruption are taking organizations into new and uncharted territory. This shift will present exciting new market opportunities; however, it will also greatly increase the attack surface and present new risks that are unfamiliar and difficult to predict. The one thing we can safely assume is that many of those new risks will be very different from what organizations have faced in the past, and as such will require new and different approaches.

Most organizations today are at least dabbling with exponential technologies, looking for ways to expand the business, dramatically improve efficiency and effectiveness, and create a lasting competitive advantage. But once an exponential technology reaches critical mass, the pace of change skyrockets and it can be hard to get in front of the rapidly emerging threats.

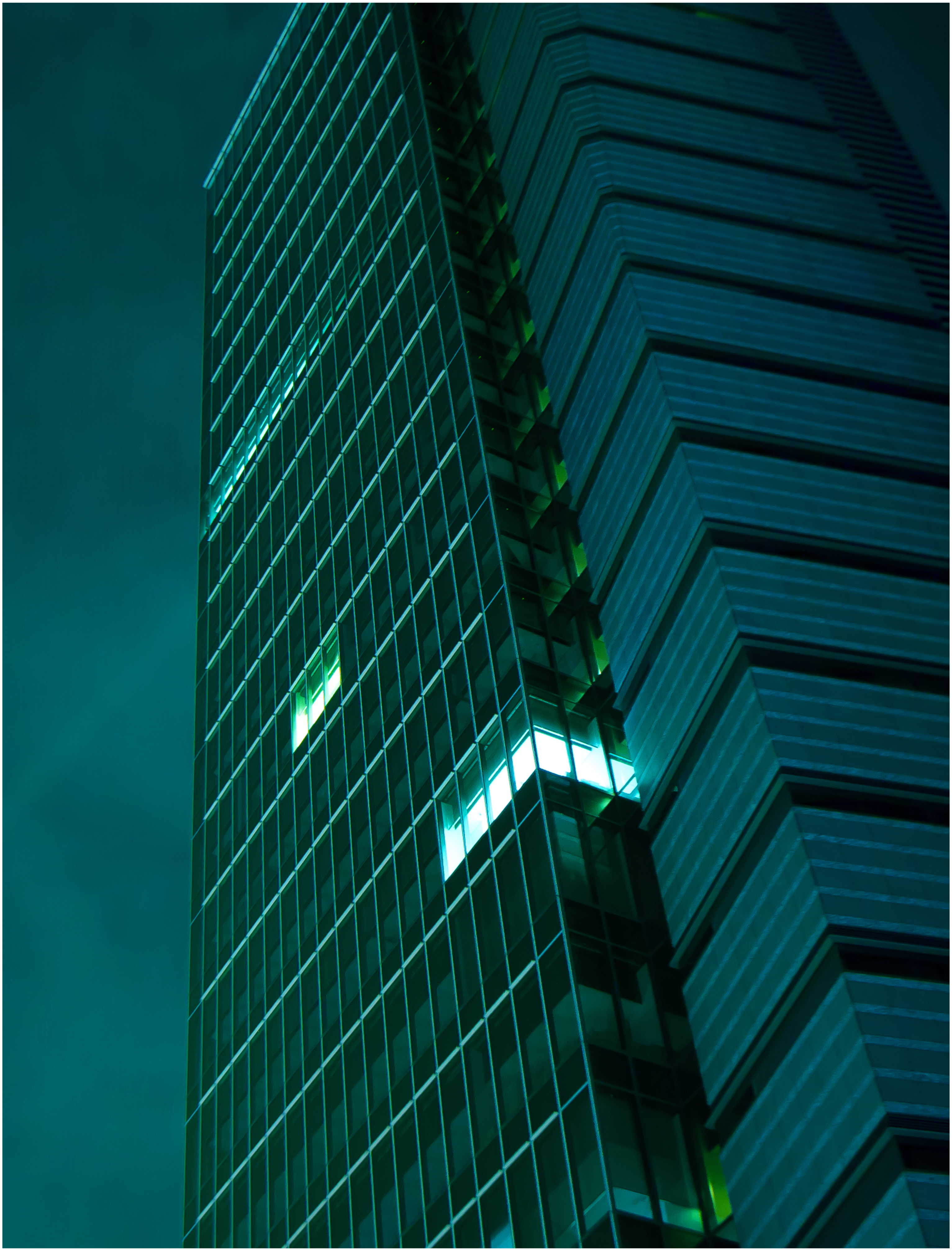
It's time to start giving serious thought to the cybersecurity impacts of exponential technologies and digital disruption, and to begin building the capabilities needed to stay safe. This will require even more forward-looking vigilance than usual, since you are trying to anticipate emerging threats from innovations and technologies that are themselves still emerging. However, this futuristic view will enable you to make smarter, more informed decisions in the short term, and to build a long-term foundation of capabilities flexible enough to contend with tomorrow's.

## When you can't go at it alone

Many organizations struggle to implement advanced analytics and threat intelligence on their own, particularly if they have limited internal resources and expertise.

Outsourcing some or all of your cybersecurity needs to a managed security services provider (MSSP) can be a practical way to extend the capabilities of in-house resources and talent. MSSPs offer a wide range of services, including threat-monitoring, proactive detection of risk events, intelligence, surveillance, and advanced analytics.

It might also be useful to establish or join a CTI sharing community. These communities aim to help organizations improve their vigilance posture in a variety of ways, including: enabling cross-sector sharing with similar organizations; leveraging cybersecurity expertise; facilitating open group discussions; improving compliance with regulatory requirements; developing a funding framework; and initiating government relationships. Think of CTI communities as fighting fire with fire. After all, cyber attackers leverage online communities to strengthen their attacks; shouldn't you be doing the same to strengthen your defenses?



# Resilient

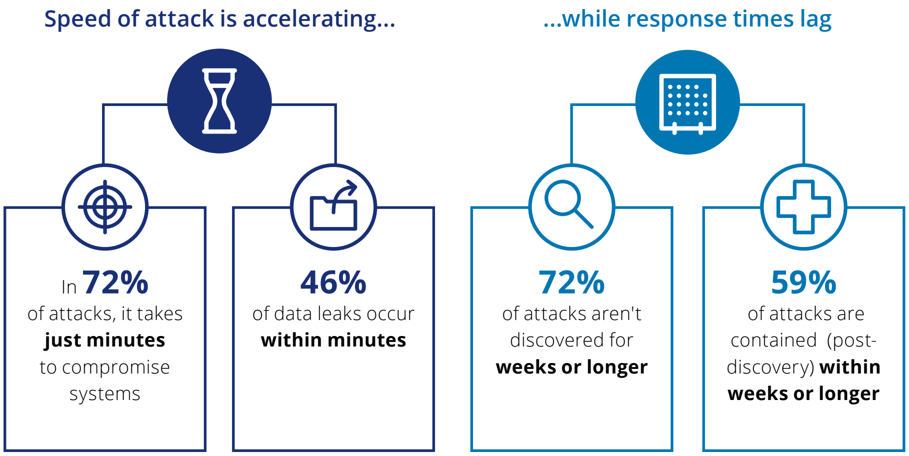
## Being able to quickly return to normal operations and repair damage to the business

Resilience is an organization's ability to manage cyber incidents effectively—responding quickly to minimize the damage from an incident, and getting its business and operations back to normal as quickly as possible.

No matter how much money and effort you spend strengthening your cyber defenses, at some point an attack will get through. When that happens, what will you do?

In the middle of an attack, there is no time to lose; each passing minute leads to more and more damage (see diagram below). Yet many businesses remain largely in reactive mode when it comes to managing cyber incidents and the resulting repercussions. In fact, according to a recent survey by Nasdaq and Tanium, more than 90 percent of corporate executives say their organizations are not prepared to handle a major cyberattack.[3]

### Anatomy of a cyberattack


Speed of attack is accelerating...

In **72%** of attacks, it takes **just minutes** to compromise systems

**46%** of data leaks occur **within minutes**

...while response times lag

**72%** of attacks aren't discovered for **weeks or longer**

**59%** of attacks are contained (post-discovery) **within weeks or longer**

**Time is of the essence**

[3] Tom DiChristopher, "Execs: We're Not Responsible for Cybersecurity" (April 2016), CNBC, http://www.cnbc.com/2016/04/01/many-executives-say-theyre-not-responsible-for-cybersecurity-survey.html Accessed 9 May 2017

To be resilient, you need a plan. You also need to establish effective governance and oversight to coordinate plans and response activities across all stakeholders—including board members and business leaders outside of IT. For most organizations, this comprehensive approach will require a mindset shift from thinking of cyber breaches as an IT risk to understanding that cybersecurity is a strategic business issue and should be addressed as an integral part of the organization's disaster recovery planning.

The preparation process is continuous—develop, test, evolve, repeat—with the goal of having a response plan that constantly matures and improves to keep pace with emerging threats and changes to the organization's threat landscape.

## Where you should be now

### Start with a resiliency plan

The middle of a crisis is no time to be figuring out things from scratch. An effective resiliency plan needs to be developed well in advance, and should be clear and concise enough that people can quickly understand it when the bullets are flying, yet detailed enough to be immediately actionable. Typical elements include:

1. **Governance:** Establish cross-functional coordination, documentation, and stakeholder communication.
2. **Strategy:** Create a strong and aligned organizational strategy for dealing with cyber incidents, including executive, board, and customer communications.
3. **Technology:** Understand the technical elements of incident response and breach documentation. (What forensics will be conducted? Does the team have processes in place to log incidents and perform incident analysis with the support of IT operations?)
4. **Business operations:** Create integrated business continuity and disaster recovery processes, which include proactive communications. (What is the plan for operational resilience during a cyber incident?)
5. **Risk and compliance:** Ensure the resiliency plan includes involvement with risk and compliance management, such as dealing with regulators, legal counsel, and law enforcement.

### Put yourself to the test

Once an organization has a solid plan in place, it needs to conduct ongoing drills and simulations in a controlled environment so everyone can be 100 percent confident that the plan works. These tests and practice sessions include wargaming, red-teaming, and compromise assessments.

*Wargaming* involves simulating the moves and countermoves that would be involved in an ongoing cyber incident. This enables an organization to see its response plan in action and to identify gaps that need to be closed. Business leaders are assigned to manage various components of a simulated breach to test how well they would respond in a live situation. Often, participants don't know the situation is only a simulation, giving organizations the opportunity to honestly and accurately assess how quickly teams respond, whether the board is engaged, and how decisions are made. In many countries, such as throughout Europe and in Canada, this includes decisions about informing the privacy commissioner, a recently established regulatory post created by new laws requiring organizations to report any data breaches that cause "significant harm" to individuals.

*Red-teaming* involves sanctioned covert hacking—typically initiated and approved by an organization's executives or board—to test defenses and uncover weaknesses. Many organizations don't realize how easily their cyber environment can be compromised, and won't really believe it unless presented with proof. A strong red team attack can provide such evidence—often stealing client data without even breaching the core network. Once the red team has breached security, they can then assess how quickly and effectively the organization's defensive team (the blue team) identifies and responds to the attack. Traditionally, red and blue teams have operated completely separate from one another. However, a growing number of organizations are now also using purple teaming, in which red and blue teams collaborate to share information and learnings.

*Compromise assessments* are another valuable tool, typically used when an organization suspects it has been breached but isn't sure, and needs to know if there is still a criminal presence in its system.

All of these tests, individually and collectively, provide critical insights about an organization's resiliency strengths and gaps, which can help drive improvements in governance, cyber incident escalation, communications strategy, executive awareness, cyber response capacity, and horizon-scanning. The test results can further drive home the point by demonstrating the vulnerability in tangible terms: how much money was "lost," what data was "corrupted," etc.

Testing will almost certainly make an organization stronger and more resilient; however, it shouldn't be conducted haphazardly or as a one-off exercise. Wargaming and simulations should be performed annually, while red-teaming needs to be an ad hoc but ongoing activity. Organizations should also update their overall cyber resiliency plan at least once a year, testing, evaluating, and evolving it as needed in response to changes in the threat landscape.

## Taking cybersecurity to the next level

### Develop threat and situation-specific playbooks

For extreme threats, especially those that involve an organization's crown jewels, it's a good idea to develop playbooks in advance that are tailored to specific situations and threats. These playbooks outline the series of events that are likely to occur as a particular type of attack unfolds—and what actions should be taken to minimize damage and get a step ahead of the attack.

In a crisis, every moment counts—and missteps can be disastrous. Threat and situation-specific playbooks enable you to plan thoughtfully and carefully without the pressure of a crisis, so you can respond more quickly and effectively when an attack occurs. They also encourage a broad view of potential threats, so you can set clear priorities and focus on those that matter most for your organization, instead of making the common mistake of focusing the lion's share of time and resources on defending against whatever attack was most recently in the headlines.

### Develop a one-response approach

The ultimate goal for a cyber resiliency plan should be to develop a one-response plan approach to breach management. Too many organizations, even those that consider themselves focused on resiliency, have a multifaceted response strategy with too many disconnects between its numerous moving parts.

A one-response approach means being able to launch a cohesive response, incorporating legal, insurance, cyber, and forensics in a coordinated effort.

# The human element

Despite the focus on technology and innovation, effective security still requires individuals who can bring deep expertise and a strategic perspective to the cyber fight. Tools are important, but attackers are masters at circumventing them. To be effective, cybersecurity requires a combination of people, processes, and technology.

## The art and science of cybersecurity

Cybersecurity is both art and science. Attacks are best stopped by dedicated specialists who have mastered the art of cybersecurity and not only have the ability to apply the appropriate preventive tools, but can also understand attackers' motivations, and possess both the tactical and business acumen to align cyber strategy with business strategy. Unfortunately, such skills are in short supply these days, leaving many organizations struggling to assemble the pool of qualified cyber talent necessary to keep themselves safe.

Tools and software for cybersecurity are becoming increasingly sophisticated, which can help an organization do more with less. However, they are not an adequate substitute for true human experts, who can often detect anomalies and threats that a software program alone would miss.

## Role of the CISO

The chief information security officer (CISO) is a key player in the cybersecurity effort. CISOs need to be organizationally empowered to contribute to strategy, which means they must have a seat at the strategy table and fully understand the organization's priorities from both a technical and business perspective.

Cyber strategy affects all areas of your business and must now be seen as a business risk, not just an IT issue. It's up to the CISO to drive this transformation. Of course, that's often easier said than done.

Improving cybersecurity is a major challenge that places CISOs in a difficult paradox. According to a recent survey of CISOs, 61 percent feel that cybersecurity is a core expectation of them and the IT function. At the same time, 33 percent feel that the business views security and risk management as a compliance chore, a cost to the business, or an operational expense.[4]

In cyber-mature organizations, CISOs have significant authority and are seen as strategic advisors by the board, management, and employees. Because their organizations recognize cybersecurity as a business risk that needs to be collectively solved, these CISOs can be less tactical and more transformational and strategic, focusing on higher-level risks such as those associated with launching new products and applications, or sharing information across the extended enterprise.

[4] Deloitte University Press, Navigating Legacy: Charting the Course to Business Value—2016–2017 Global CIO Survey (2016), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-cio-survey-2016-2017-full-report.pdf Accessed 9 May 2017

# Taking the lead on cyber risk

As the economy becomes increasingly knowledge-based, digital disruption and exponential technologies will be key drivers of growth and performance, providing unmatched opportunities for organizations to create value and competitive advantage. But in order to capitalize, they will need to fully embrace digital innovation—and the cyber risk that comes with it.

To succeed, you need to tackle cyber risk head-on—developing and implementing a robust cyber strategy that can make your organization secure, vigilant, and resilient. Such a strategy must not only address the threats that exist now, but also the next-level threats that have yet to emerge.

The good news is that while cyber risk is a serious and growing challenge, it is not insurmountable. Although hope is not a strategy, the situation is far from hopeless. In fact, we are already seeing positive changes in the way leading organizations are responding to the cyber imperative.

In addition to improving their overall capabilities for managing cyber risk—which includes expanded roles and scope for the CISO and risk function—cyber-mature organizations are working to embed cyber awareness into the very fabric of their organizations. Also, they are beginning to leverage smart technologies to detect, predict, and mitigate risks, while at the same time recognizing that cybersecurity is both art and science, and that even the most sophisticated tools cannot replace the creativity, insight, and judgment of human experts.

Cyber risk is not an IT issue, it's a business issue. As such, risk, security, and business leaders must constantly strive to balance the need for strong cybersecurity and the strategic needs of the business.

By understanding what needs to be done—and gathering the courage and foresight to take the lead on cyber risk—your organization can take charge of its own cyber fate and position itself as a digital disrupter, rather becoming one of the disrupted.

# Appendix A: Key takeaways to move from now to next-level security

## Secure

### Now

- Integrate cyber strategy with business strategy
- Identify and protect your crown jewels
- Develop a strong cybersecurity framework

### Next-level

- Embed cybersecurity into everything from the beginning
- Develop better ways to manage data

## Vigilant

### Now

- Be situationally aware
- Pay attention to your entire ecosystem

### Next-level

- Use advanced technologies to proactively identify and hunt down threats
- Understand and address exponential threats

## Resilient

### Now

- Start with a resiliency plan
- Put yourself to the test (wargaming, red-teaming, compromise assessments)

### Next-level

- Develop threat and situation-specific playbooks
- Develop a one-response approach

# Appendix B: Key elements of a cyber strategy

Tomorrow's challenges are different than today's. How can you stay ahead?

To ensure an organization is able to withstand a cyberattack, it must have a solid cyber program in place, and this starts with building a strong foundation. Here are the key elements of a strong cyber strategy:

### 1. Strategy, management, and risks

Incidents like the WannaCry ransomware attack reminds us that the cyberthreat landscape is constantly changing. Cybersecurity requires a continuous improvement mindset and a conscious effort to ensure that cybersecurity controls are in place to address the primary threats to an organization. Having a strong cyber strategy means that the organization can effectively assess and understand the risks it faces, and it has an actionable plan to implement the controls necessary to protect itself.

### 2. Policies and procedures

An organization's policies and procedures translate its cyber strategy into meaningful responses and behaviors. These often include defined roles and responsibilities for who handles what in the event of a major cybersecurity incident, and defines the steps to be taken to manage the situation and limit the damage. The most secure organization will rehearse its response procedures on a regular basis and have incident response plans to ensure a coordinated response to different types of incidents.

### 3. Technical defenses

Technical defenses and other protective controls often represent an organization’s first line of defense against cyberthreats. There are numerous technical solutions that can be leveraged to protect the organization from threats, from firewalls and basic malware protection to specific solutions for identifying and nullifying insider attacks. Whatever solutions an organization chooses to leverage, it must have a clear understanding of its cyberthreat landscape to determine where the most effective investments should be made. Also, an organization’s technical defenses should be continuously reviewed to ensure that they remain appropriate in an evolving threat environment.

### 4. Monitoring and situational awareness

All organizations must balance their protective and detective security controls. Protective security controls are generally part of an organization’s first line of defense. In the event that an attack successfully penetrates the network, the focus then turns to the organization’s detective capabilities to establish how the attacker succeeded and what assets have been compromised; only with effective monitoring and situational awareness can the organization start to activate response procedures to limit the damage. However, organizations that are truly vigilant have such strong monitoring and situational awareness that they can recognize threats and potential attacks before the latter even have a chance to penetrate the network.

### 5. Vendor security

Most organizations make use of external vendors to deliver services or provide inputs. A close partnership with these vendors is often necessary, but this also exposes the organization to additional cyberthreats. For example, an organization buying software from an external vendor is dependent on the strength of the vendor’s security controls to ensure that the software contains no malicious code. Understanding the role of external vendors in an organization’s cybersecurity ecosystem enables the organization to apply the appropriate technical and contractual controls to limit its exposure.

### 6. Employee awareness

No matter how good your technical controls are, the role of employees in ensuring cybersecurity will always remain important. When an email arrives from an unknown sender with a suspicious attachment, an employee’s decision to open the attachment or delete and report the email could be the difference between normal operations and a major cybersecurity incident. Training and awareness are crucial to developing an appropriate cyber risk culture that drives the correct behaviors.

# Contacts

## Authors

**Marc MacKinnon**

**Partner, Cyber Risk Services**
mmackinnon@deloitte.ca

**Mark Fernandes**

**Partner, Cyber Risk Services**
markfernandes@deloitte.ca

## Global contacts

**Nick Galletto**

**Global and Americas Cyber Risk Leader**
ngalletto@deloitte.ca

**Chris Verdonck**

**EMEA Cyber Risk Leader**
cverdonck@deloitte.com

**James Nunn-Price**

**Asia/Pacific Cyber Risk Leader**
jamesnunnprice@deloitte.com.au

### Deloitte has been widely recognized as a market leader, including these recent independent analyst reports:

**Deloitte ranked #1 globally in Security Consulting Services, based on 2016 Market Share revenue by Gartner**
Source: Gartner, Market Share Analysis: Security Consulting, Worldwide, 2016, Elizabeth Kim, June 2017.

**Deloitte named a global leader in Security Operations Consulting by ALM Intelligence**
Source: ALM Intelligence; Security Operations Center Consulting 2016; ALM Intelligence estimates
©2016 ALM Media Properties, LLC. Reproduced under license

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook,  LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2017. For information, contact Deloitte Touche Tohmatsu Limited.