Deloitte.
University Press

Cyber risk in consumer business

Deloitte offers a complete portfolio of services to help complex organizations establish their cyber risk appetite, design and implement Secure.Vigilant.Resilient. programs, and assist in the ongoing management, maintenance, and adaptation of their programs as the business and threat environments change. Contact the authors for more information, or read more about our cyber risk services at https://www2.deloitte.com/us/en/pages/risk/solutions/cyber-risk-services.html.

COVER IMAGE BY SAM FALCONER

CONTENTS

Understanding cyber risk in consumer business

INNOVATIVE technologies are helping to fuel an unprecedented rise in consumer expectations. For today's businesses, harnessing emerging technologies in order to redefine products, services, and consumer experiences is often the new cost of doing business. Technology investment, however, can drive more than just profit potential. Widespread initiatives around customer analytics, cloud integration, connected devices, and digital payment technology are likely leaving businesses increasingly exposed to cyber threats.

Some threats, such as credit card fraud and identity theft, are becoming all too familiar in today's marketplace and can be significantly detrimental to customer trust and brand reputation. Other risks, such as those related to food safety and intellectual property theft, appear to be escalating, leaving many businesses (and their customers) in unfamiliar territory.

Businesses that have direct contact with consumers, such as retailers, restaurants, and consumer product companies, should consider taking the proper precautions to mitigate cyber risk during this period of digital transformation. Their growing technology footprint, along with the accelerating pace of change in business, may have a dramatic impact on the breadth and complexity of the cyber risks consumer businesses will likely need to address over the next decade.

Building upon our previous cybersecurity research in manufacturing,[1] Deloitte launched the Cyber Risk in Consumer Business Study to assess current challenges faced by companies in the consumer products, retail, restaurant, and agribusiness sectors. Using a combination of an online survey and in-depth interviews, we gathered opinions from over 400 chief information officers (CIOs), chief information security officers (CISOs), chief technology officers (CTOs), and other senior executives in these sectors.

The results of this study are designed to help consumer businesses engage their senior leadership teams and boards in deeper conversations on how to make their businesses secure, vigilant, and resilient. Applying lessons learned from this study can help businesses:

Be secure: Take a measured, risk-based approach to what is secured and how to secure it. This includes managing cyber risks as a team and increasing preparedness by building cyber risk management strategies in the enterprise and emerging technologies as they are deployed.

Be vigilant: Monitor systems, applications, people, and the outside environment to detect incidents more effectively. This includes developing situational awareness and threat intelligence to understand harmful behavior and top risks to the organization, and actively monitoring the dynamic threat landscape.

Be resilient: Be prepared for incidents and decrease their business impact by improving organizational preparedness to address cyber incidents before they escalate. This also includes capturing lessons learned, improving security controls, and returning to business as usual as quickly as possible.

Six areas of focus for consumer business companies

MANY businesses are leveraging innovative technologies to help enhance the customer experience, build loyalty, and, perhaps most importantly, remain competitive in a digital world. However, companies should consider balancing their expanding digital footprints with a growing focus on cyber risk. Emerging technologies are often attractive avenues of opportunity for cyber criminals looking to expose weaknesses in an organization's digital ecosystem.

The road forward will likely not be an easy one. Consumer businesses face numerous challenges as they attempt to handle the complex issues of cyber risk. As such, we have identified the following six themes that companies should consider:

- **Executive-level engagement:** For many organizations, the responsibility for preventing, managing, and recovering from cyber incidents tends to be highly fragmented. Consumer businesses should consider gaining a better understanding of the cyber risk landscape in order to establish a more effective structure to own this critical issue across their organizations. There is also a significant opportunity to strike a more effective balance between investing in the right advanced technologies to move businesses forward while ensuring that in doing so, they are not opening themselves up to increased cyber risk.
- **Customer trust:** Today's businesses may be skating on thin ice when it comes to potential consumer backlash from cyber breaches. Longitudinal research across thousands of US consumers reveals a heightened state of uncertainty around data security over the past decade. Businesses should not only consider how perceptions of uncertainty about the privacy of personal information may impact future purchase decisions but also assure their customers that they are taking appropriate steps to mitigate cyber risk.
- **Connected products:** The future success of connected products is likely dependent not only on the technology that facilitates connectivity but also on consumer trust, which can drive demand. The rapid growth of connected products not only presents numerous potential benefits to consumer businesses and their customers but can also increase cyber risk. It is essential that consumer businesses ensure the security of connected products if both businesses and consumers are to reap their benefits.
- **Payments:** Emerging payment technologies are enabling businesses to elevate the customer experience by streamlining and, in many cases, reinventing the payment process. Companies

Our previous research, *Cyber risk in advanced manufacturing*, identified six key cyber risk challenges facing the advanced manufacturing industry. Many of these themes, including **executive-level engagement**, **talent and human capital**, **intellectual property**, and **connected products**, were found to be strong areas of focus and concern among consumer businesses. However, consumer businesses also face two unique areas of cyber risks, **customer trust** and **payments**, which can be critical to their evolving cybersecurity landscape.

We believe these themes are critical to consumer-facing businesses' ability to capture and protect the value associated with this new frontier of technology, while appropriately addressing dynamic cyber risks over the longer term.

that are able to leverage emerging payment technologies while maintaining a focus on the security of these platforms will be positioned to gain from their implementation. Technologies such as emerging payment systems that provide new and efficient customer experiences are also being targeted by cyber criminals.

- **Intellectual property:** Intellectual property (IP) drives a company's innovation, competitiveness, and growth. The evolving nature and rising incidence of IP theft require a comprehensive cyber risk approach around identity and data access management.
- **Talent and human capital:** An organization's ability to effectively and efficiently manage cyber risk should be part of its culture. Talent can be the weakest link in the cyber landscape. In order to mitigate this risk, it is imperative to attract, train, and retain top cyber talent while implementing educational programs for all employees on the role they play to minimize risk across an evolving digital landscape.

Executive-level engagement

Driving engagement with C-suite executives to help mitigate cyber risk

Executive-level involvement with cyber risk management, including prevention, mitigation, and recovery, is critical to the success of cyber risk programs. C-suite executives can set leading policies and procedures. But for many organizations, the management of cyber risk initiatives tends to be fragmented due to the growing threat vectors companies are experiencing (figure 1). To help mitigate potential cyber risk incidents and further align business stakeholders, consumer businesses, led by C-suite executives, should consider understanding the cyber risk landscape and defining organizational ownership. Consumer businesses could benefit from

Figure 1. Top cybersecurity initiatives (percentage of businesses driving each initiative)

Note: Sample sizes: n(overall)=402, n(consumer products)=150, n(restaurants)=100, n(retail)=100.

Source: Deloitte analysis.

82 percent of consumer businesses have not documented and tested cyber response plans involving business stakeholders in the past year.

29 percent of businesses lack clarity on the roles and responsibilities of individuals during an actual cyber breach.

their C-suite executives taking a more proactive role regarding the cyber risk issues their companies face and the current gap between perception and reality in terms of their organization's cyber preparedness. There may also be significant opportunity to strike a more effective balance between investing in the right advanced technologies to move their businesses forward, while ensuring that, in doing so, they are effectively managing any new risks that may follow in their wake.

Some consumer businesses may be operating with a false sense of confidence about cyber risk

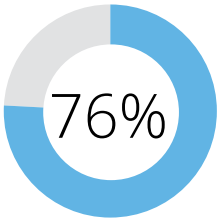
Over three-quarters of the executives interviewed report being highly confident of their ability to respond to a cyber incident, yet they simultaneously cite many issues that critically impair their ability to effectively respond to cyber incidents that could be addressed by more involvement from C-level and board executives (figure 2). This paradox suggests many companies operate with a false sense of security.

Wargaming can help C-suite executives mitigate cyber risk

Executives were also questioned about the challenges they face when responding to an *actual* cyber breach. Their responses echo what they said about the concerns they face when trying to establish effective programs (figure 3).

These challenges can be addressed and planned for through **wargaming exercises**. Cyber wargaming is an interactive exercise that immerses participants in a simulated cyber risk incident, followed

Figure 2. Cybersecurity preparedness



FEEL ADEQUATELY PREPARED FOR CYBER INCIDENTS, HOWEVER...

82% Have not documented and tested cyber response plans involving business stakeholders within the past 12 months

Only 46% Perform war games and simulations on a quarterly or semiannual basis

25% Report lack of cyber funding

21% Lack clarity on mandate, roles, and responsibilities

Q30. How prepared is your company for the next cyber crisis event?

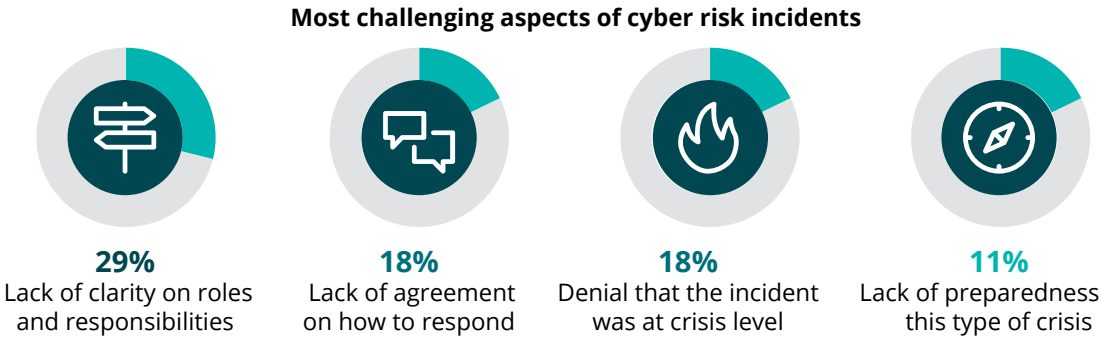
Q26. Does your organization have an incident response plan, and has it been tested within the last 12 months?

Q37a. How often does your organization perform the following cybersecurity initiatives?

Q25. What are the most important challenges your organization faces to establish/maintain an effective cybersecurity program?

Source: Deloitte analysis.

Figure 3. Reacting to a breach



Q28. What was the most challenging aspect of the severe cyber incident/crisis your company experienced in the past 12 months?

Source: Deloitte analysis.

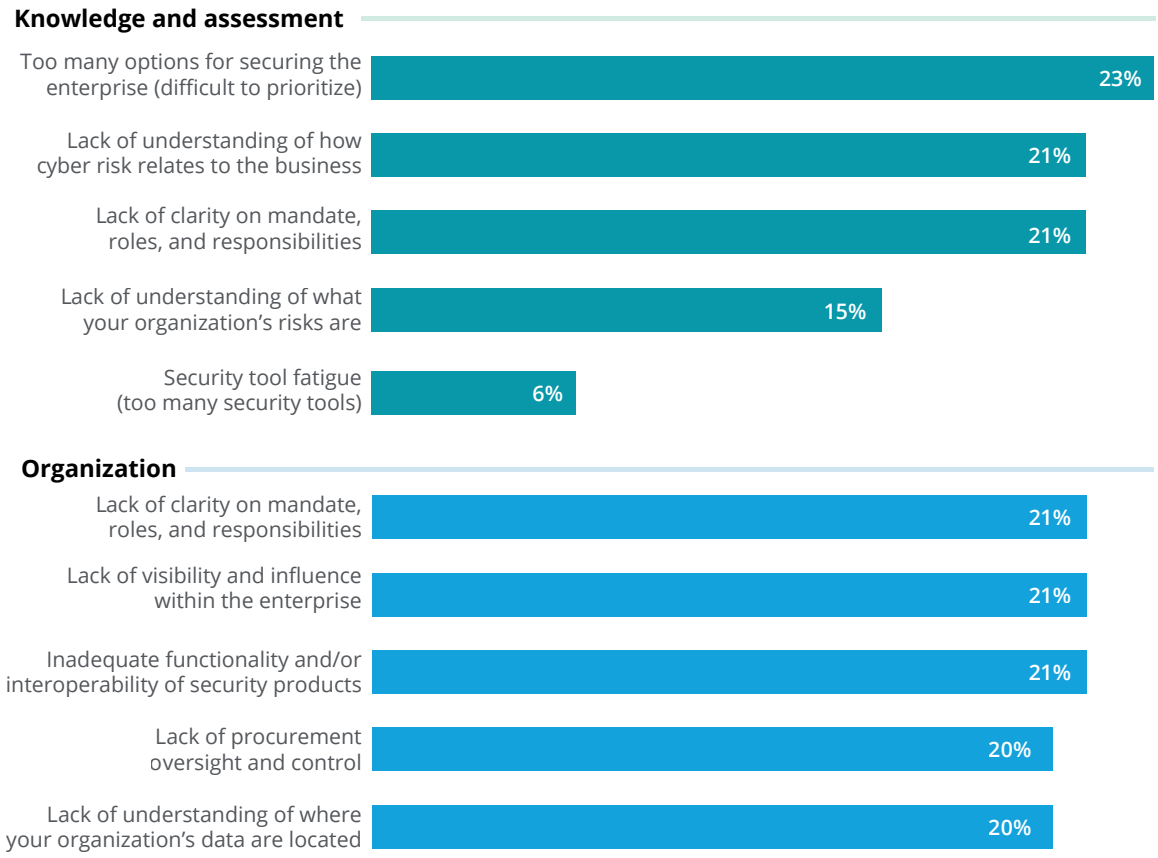
by a documentation of what did and did not work, thus exposing potential loopholes in the individual company's overall response protocol. In comparison with traditional cyber threat preparedness assessments, which focus on evaluating technology controls and the completeness of incident response plans, cyber wargames bring the experience of responding to a cyber risk attack to life. Some benefits of wargaming and related simulations include bringing disparate stakeholders together to test their mettle in making business decisions under pressure and to work as a focused team deploying specific tools and techniques.[2]

Despite the benefits of wargaming and other simulations, only 46 percent of consumer businesses perform them on a quarterly or semiannual basis. Organizations not engaged in cyber breach simulations are missing an opportunity to be better prepared, should they experience a cyber incident.

Solving organizational challenges is often paramount to effectively managing cyber risk

Organizations face many operational issues that compromise their ability to manage cyber risk effectively and efficiently. Executives were asked to identify the most important challenges they face when establishing and maintaining an effective cybersecurity program. Lack of funding emerged as a top concern, along with a lack of clarity on both the cyber mandate as well as roles and responsibilities (figure 4). Note that this is consistent with the challenges they face when responding to an actual breach (as highlighted in figure 3 above), where lack of clarity around roles and responsibilities during a

Figure 4. Challenges in establishing effective cyber risk programs (percentage of businesses citing challenge)



Q25. What are the most important challenges your organization faces to establish/maintain an effective cybersecurity program?

Source: Deloitte analysis.

breach was a top concern. This suggests these are systemic issues in cyber risk management.

Only 9 percent of consumer businesses participating in our survey report having had a breach in the past 12 months. This is considerably lower than the reported incidence rate in the manufacturing sector (39 percent) and suggests that although consumer businesses may not feel they are in imminent danger, in fact, the level of incident risk likely remains high, as one executive expressed during an in-depth discussion:

> I would say we're pretty vulnerable. Right now, for many CPG manufacturers and third-party sellers, there's a big move to cloud . . . 90 percent of brand sites are now sitting on Microsoft Azure or cloud systems. As you move off-site, your legacy tools and processes no long apply or transfer to the cloud. . . . The way we engage [with customers] has changed the last few years. [We're a] bit more vulnerable than other industry verticals that have been at this. . . . We're just doing it . . . we're trying to catch up.

Media reports on cyber incidents have helped put a spotlight on the need for cybersecurity initiatives, helping cyber executives request more funding for future programs. In requesting additional funds, however, cybersecurity executives could benefit from taking a comprehensive and systematic approach to the topic and being careful to avoid the

appearance of overreacting to specific incidents. As one executive we spoke to put it:

> One way to get money in security is to experience a breach or an embarrassing audit, or have a leadership team that understands risk along with a security team that can convey security concerns in a way that resonates. For example, "Here is our security posture . . . our gaps . . . and what we should do about it . . . and we have a plan in place to address it."

Helping ensure full executive leadership involvement in cyber risk management

Full executive commitment is needed to coordinate the specific needs of all the departments touched by cybersecurity issues. Study participants were asked about both day-to-day management of cyber risk and which stakeholders are involved in the event of an actual breach. Of specific concern to participants was that the management of cyber risk lacks representation from a broad range of stakeholders across organizations.

In our survey, we learned that in day-to-day management of cyber risk, CIOs are primarily responsible for cybersecurity functions, followed by CISOs. CIOs own strategy, budgeting, and board reporting (66 percent); program measurement and reporting (59 percent); and incident response (55 percent). However, in the event of a cyber breach, only 76 percent of consumer-facing businesses report CEO or equivalent involvement. Involvement from other C-suite executives is even lower: Only 48 percent of chief financial officers (CFOs) are present, and 28 percent each of chief risk officers (CROs) and chief marketing officers (CMOs). Similarly, board-level engagement is low, at only 40 percent.

Given the importance of marketing to consumer-facing businesses, and the need to help ensure consumer trust and brand reputation, which can be impacted during a cyber breach, the involvement of only 28 percent of CMOs seems low. However, according to the cyber executives with whom we spoke, there is growing involvement from CMOs, who are taking an interest in protecting personally identifiable information (PII) and brand websites, in particular.

Given that many companies are now selling directly to consumers, and accessing social media data is becoming common, consumer businesses are starting to collect more PII data such as credit card information, cell phone numbers, online and offline addresses, and birth dates. Thus protecting PII is no longer just the responsibility of CIOs and CTOs but of CMOs as well. As one cyber executive we interviewed indicated:

> [I] met with the CMO last week about PII that is starting to build in our cloud system. If we have people's birthdays, email and home addresses, and if we follow up about gifts after an event, [we are open to vulnerability]. All [the] marketing cloud app vendors we work with know they need to be compliant and give assurances. [My CMO] is very concerned if there is a breach of these things, even if inadvertently by [an] employee, or [due to an] insecure cloud. So this is a big topic here.

With the potential of tarnishing a brand's reputation, hacking of product websites (which tend to be cloud based without cloud application firewalls) is another growing concern among the executives we interviewed. There can be greater potential for hackers to access internal information or spread false content. For many larger consumer product companies with multiple products, each with an individual website, this issue is compounded. Further, if it's a global organization, there will be country-specific sites for the same product, thus exponentially increasing the possibility of hacking.

Staying competitive in a digital world

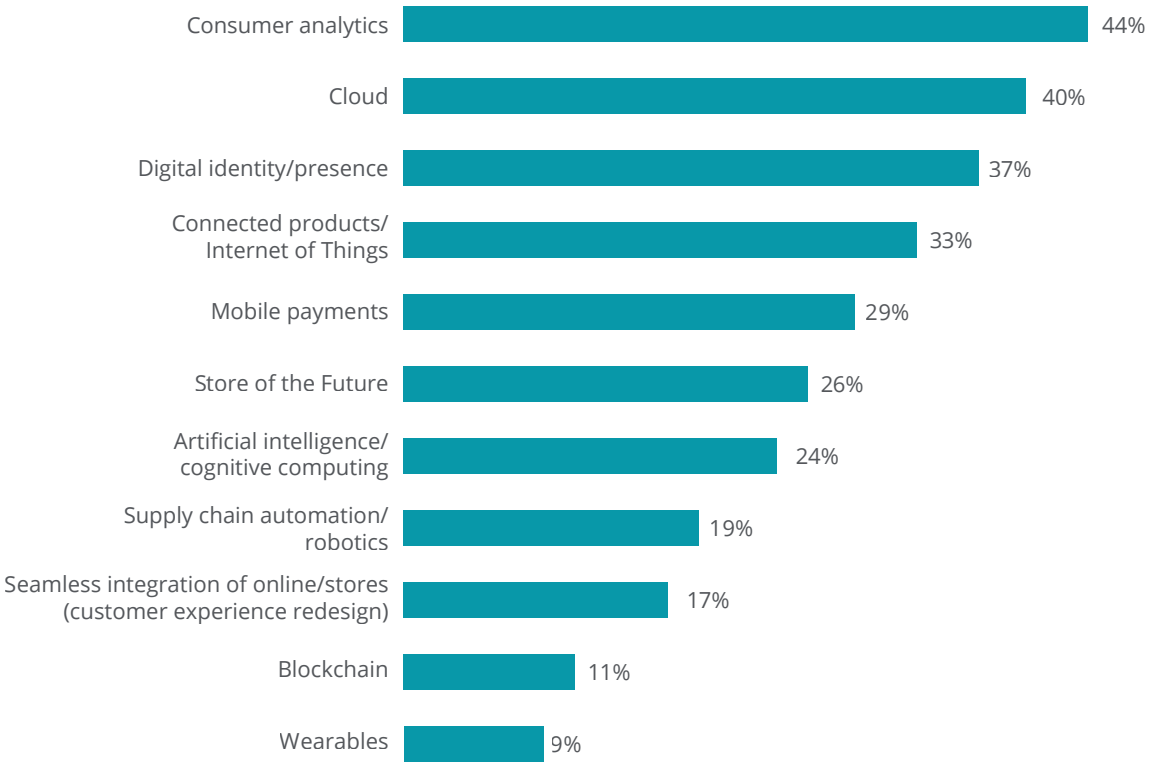
Often, to stay competitive in today's marketplace and effectively compete in a digital world, many consumer businesses are pursuing a wide range of technology-based initiatives that can increase the opportunity for cyber risk. Many C-suite executives are in a strong position to help ensure there's a

strong balance between the rapid adoption of technology and appropriate cyber risk management.

For example, executives were asked to list their strategic initiatives critical to business leadership. The second-highest initiative was "technology-enabled innovation to enhance value proposition." In addition, cyber executives were asked to list the technologies they are investing in to support their initiatives (figure 5). Importantly, we learned that to make their strategic initiatives a reality, thus contributing to overall business goals, effective cybersecurity management is likely critical. This is because strategic initiatives translate to investments in a number of advanced technologies such as the cloud, digital identity and presence, connected products, and mobile payments. However, many consumer businesses are developing and deploying these technologies at a record pace. If not properly managed, this adoption potentially opens the door to increased cyber risk.

Further, the fact that consumer analytics tops the list of planned technology investments (figure 5) implies that consumer businesses are doing whatever they can to capture and leverage as much consumer data as possible. The unintended consequence of this data collection is that it increases the potential cyberattack surface, as these data are not only valuable to the company but can also be monetized by attackers. In fact, the danger of theft goes well beyond customer PII to include spending patterns, location data, time spent in stores, and even abandoned online shopping carts, as obtaining any of these customer data can provide a strong motive for a cyberattack.

Figure 5. Planned technology investments to support strategic initiatives (percentage of businesses investing in each technology)



Note: Sample sizes: n(overall)=402, n(consumer products)=150, n(restaurants)=100, n(retail)=100

Source: Deloitte analysis.

Executive engagement playbook

HOW CAN BUSINESSES ENGAGE WITH C-SUITE EXECUTIVES TO DEVELOP A BUSINESS-DRIVEN CYBER RISK PROGRAM?

Often, C-suite executives are in the best position to oversee the direction of their organizations, particularly as it relates to changing attitudes and behavior around cybersecurity. There are several approaches to further engaging C-suite executives in cyber risk management:

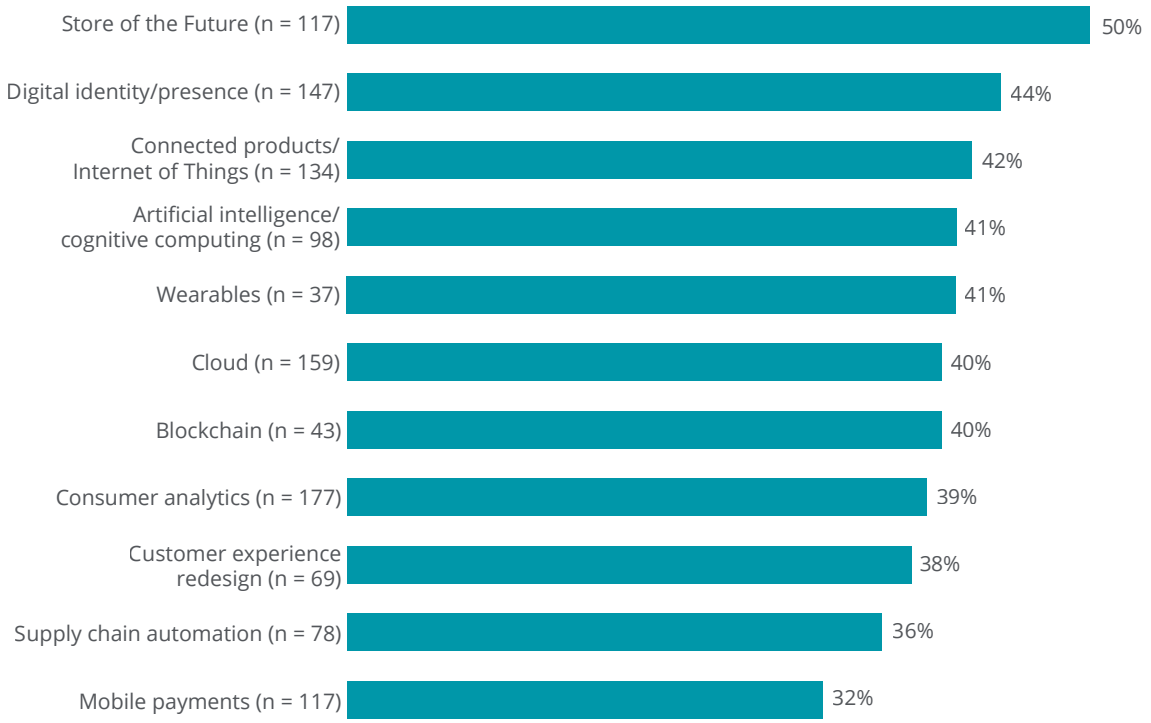
- **Establish a cross-functional C-suite-level committee** with board representation dedicated to cyber risk.
- **Review the cyber breach incident management framework**. Establish escalation criteria to include C-suite executives and board members.
- **Share results of enterprise cyber risk assessments** and their impact on business outcomes in the areas of sensitive data protection and connected products.
- **Establish a dashboard of cyber risk indicators** and trending to support continued dialogue around strategic investments designed to improve cyber maturity across the organization.
- **Provide executive- and board-level updates** that include results of broad employee awareness and resiliency efforts, such as lessons learned from wargaming simulations and tabletop exercises. Topics to address include transparency on the most likely cyber risk events a company may experience, key mitigation and incident response strategies, and continuous opportunities identified.

Customer trust

Harmonizing business imperatives

The future may look bright for businesses determined to push the limits of technology. Big data analytics are forming the bedrock for personalized experiences that drive lifetime customer loyalty. Mobile functionality has the potential to create seamless in-store and online shopping and buying experiences. Connected products offer consumers improved, "smarter" lifestyles and unlock new ways for businesses to minimize operational inefficiencies. Digital innovation, however, comes with more than just profit potential. Popular technology initiatives among today's businesses include leveraging consumer analytics (44 percent), transitioning to cloud-based technologies (40 percent), producing connected products (33 percent), and implementing mobile payments (29 percent). All of these technologies require greater aggregation and storage of sensitive customer information across a growing array of new touchpoints (figure 6).

Figure 6. Percentage of companies with mature cybersecurity programs in place to address emerging risks*



Q16. Which technologies/initiatives is your organization investing in to support strategic initiatives?
Q17. Has your organization considered cybersecurity risks for these key technologies?

** Among those employing these technologies.*
Note: The sample varies for the sectors as the question was asked to the respondents based on their option selection in figure 1.

Source: Deloitte analysis.

Many businesses appear to be prioritizing swift (and often profit-generating) innovation over cybersecurity. While leveraging emerging technology has commonly opened new value streams, executives surveyed revealed that these technologies also increase their cyber risk. For example, only 30–40 percent of executives surveyed that are currently investing in platforms such as consumer analytics, cloud integration, and mobile payments said they have mature programs in place to address related risks (figure 6).

Innovation and cyber risk are often inextricably linked. For businesses, prioritizing one over the other can jeopardize the increasingly close relationship companies have with their customers, particularly because new technology initiatives can take advantage of an exceptionally broad portfolio of data types. These data types may expose consumers to much more than stolen credit cards and identity theft.

Food safety provides a good example. Our intricate food system is becoming increasingly connected. A variety of players, including food and beverage companies, agribusinesses, restaurants, and transportation companies are commonly leveraging connectivity to create more efficiency in the complex process of feeding millions of people worldwide. This increasingly connected food ecosystem, however, can open up new ways for cyber criminals to do harm, which can jeopardize customers' health and cause potentially irreversible harm to brand reputation. Many restaurants investing in digital supply chain and food storage technology, for example, may be opening new pathways for cyber criminals to tamper with food quality. Malicious actors targeting agribusinesses could manipulate the amount of chemicals put into food, causing widespread illness and, potentially, death.

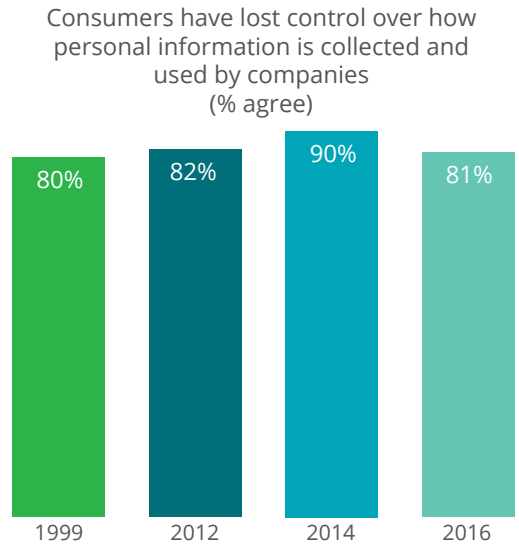
Concerned consumers can be unforgiving when it comes to cyber breaches

Today's businesses may be skating on thin ice when it comes to potential consumer backlash from cyber breaches. Longitudinal research across thousands of US consumers reveals a heightened state of uncertainty around data security over the past decade. In 2016, roughly 80 percent of US consumers felt they have lost control over how their personal information was being used by companies (figure 7).[3] This sentiment has remained relatively unchanged since 1999, despite high-profile breaches over the past decade.

This long-standing mistrust represents an opportunity for consumer businesses to tackle this issue head on and perhaps create a competitive advantage by being more transparent with (1) how and where they collect customer data; (2) what they do with those data; and (3) how they protect the data. By investing in cybersecurity capabilities, consumer businesses can increase their chances of upholding this trust and enhancing their brand.

Businesses should also consider how uncertainty about the privacy of personal information may impact future purchase decisions—particularly when it comes to the businesses consumers choose to buy from. Today's consumers are not short on options, and switching brands is often as easy as downloading a new app.

Figure 7. Consumers feel that they have lost control over how companies use their personal information



Source: Deloitte analysis.

Consumers already demonstrate they can be unforgiving with businesses who neglect their data. In this heightened state of unease, customers remain vigilant, and efforts to mitigate their own risk often translate to cautionary or even punitive actions and behaviors, such as decreasing online and offline engagement with brands they perceive to be a risk. Over the past 12 months, 31 percent of US consumers deleted specific apps on their smartphone, and 27 percent avoided specific websites to mitigate their own cyber risk. Some consumers, while only a small amount, did not buy a certain product or purchased the same product from a different brand (figure 8).

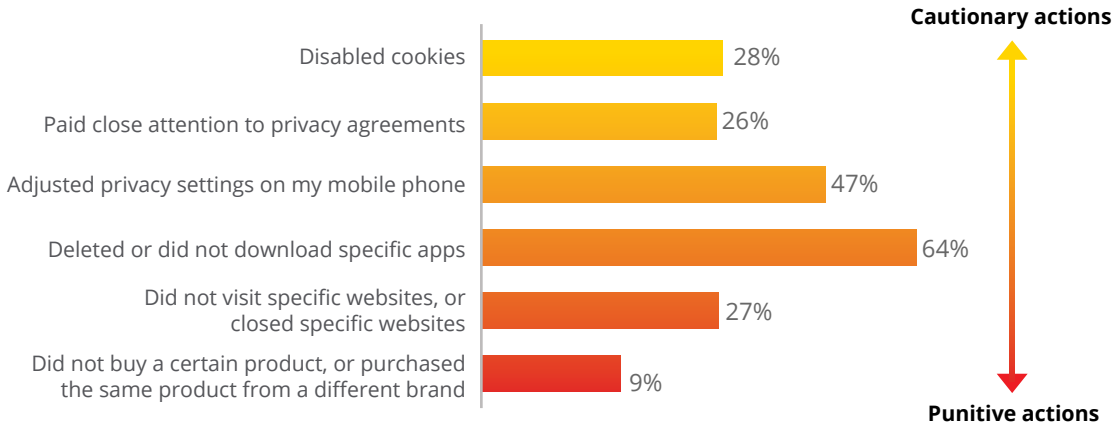
The potential consequences of underestimating trust

The consumer product industry offers an example of the growing importance (and challenge) of maintaining customer trust in the digital age—particularly within the rapidly growing market of connected products. In physical stores and online, many of today's consumers are finding themselves in new and unfamiliar territory. Products that have remained relatively unchanged for decades, such as thermostats, door locks, and even kitchen appliances such as refrigerators, now often come outfitted with Web connectivity. This new generation of products can offer consumers new, cutting-edge functionality, while also offering businesses a new frontier for revenue growth.

So far, demand for many types of connected devices, including fitness trackers and smart home devices, remains healthy.[4] However, tapping into this segment's full, long-term growth potential hinges largely on consumer trust. Many consumers must feel confident these products not only operate flawlessly but also that they do not develop into new gateways for criminal activity. As products such as smart door locks become installed in more homes, for example, they will likely gain the attention of cyber criminals looking to exploit potential weaknesses. Contributing to growing concern, emerging cyber risks continue to rattle the health care industry, as security weaknesses in connected devices such as heart monitors make front-page news.[5] Continuous news of breaches through these devices can not only threaten sales of a particular product or brand but

Figure 8. Consumers taking action to avoid data breach

In the past 12 months, did you do any of the following due to concerns over data privacy?



Source: Deloitte, SSI, and JD Power, consumer privacy study presented at Next2017 Conference, May 9–10, 2017, New York.

also tarnish the broader perceptions consumers have of connected products in general—jeopardizing billions in future sales growth.

Consumer product companies may be underestimating the importance of building consumer trust around cybersecurity and digital innovation. In fact, when thinking about potential cyber incidents, consumer product companies in our survey seem to be primarily concerned about production disruptions (48 percent) and loss of intellectual property (42 percent), while significantly fewer (16 percent) are concerned about tarnishing brand perceptions related to trust.

In a competitive marketplace, the immense pressure to hit aggressive production goals in order to gain "first-mover advantage" in emerging-product categories may be casting a shadow over the importance of building positive, long-term customer perceptions around connected products. Ultimately, in this environment, cyber protection around connected products is not as robust as it should be. In fact, nearly a third of consumer businesses participating in our survey do not feel their current cyber risk initiatives and practices around connected products are effective.

Reimagining cybersecurity as a potential competitive advantage

Regardless of industry, many consumer-facing businesses are fighting similar uphill battles. Staying relevant in today's marketplace often requires companies to roll out technology initiatives on tight timelines and budgets—which can add to the challenges of mitigating cyber risk. But businesses cannot afford to neglect cybersecurity. Companies need to think about how decades of underinvestment in cybersecurity will impact long-term growth. Data protection is something consumers have come to expect, and investments in security can create a competitive advantage in today's world of growing cyberattacks.

Consumer trust playbook

HOW CAN YOU BUILD CONSUMER TRUST KEEPING CYBERSECURITY IN MIND?

Many organizations are adopting new technologies, whether consumer analytics or connected products, with a goal of generating new revenue streams. While we often see heathy adoption of these services and products by consumers, long-term adoption will likely depend on a brand's ability to invoke consumer trust. This could be a golden opportunity for businesses to build brand differentiation in the marketplace by embracing cybersecurity as a foundational principle to build that consumer trust. Ways this might be accomplished include:

- **Build a reputation for protecting consumer information and privacy**: It is important to let your consumers know that protecting their information and privacy is taken very seriously. Communicate the steps taken to keep their information secure. Educate consumers on cybersecurity as it relates to the use of your products and services. Own shared responsibility with consumers regarding the potential legal implications of connected products.
- **Build security up front in your products and services**: Every time, as an organization, you think about developing a new product or

service for growth, embed security in the forefront as you think about designing the functionality of the product or service. This can be a foundational element of developing customer trust. You want your product or service to be world class. Part of that expectation includes not having that product or service be exploited by criminals, causing harm to your consumers.

- **Be transparent with your consumers and give them control**: Many consumers are willing to share their information with you for some control on how the information is used. Be transparent about how their information will be used and shared. Make it easy for your consumers to have a say in the process so they can control the flow of information. Implement strong processes to honor their requests.
- **Manage your business associates and third-party vendors**: In today's world, where lines between the enterprise and outside are blurring, consumer information is often shared with third parties, or products and services are sourced from them, which can jeopardize reputation and hence consumer trust. Mandate that third-party vendors follow the same cybersecurity standard as your organization to establish that you are serious about building consumer trust.
- **Know your consumers, but also know how to protect that knowledge**: Understand what you collect from your consumers and why. Understand where and how that information flows in your organization and beyond. Make responsible choices; limit the collection of information to what you need for business, and then contain and protect it.
- **Consumer experience trumps everything**: Managing cyber risk is a core component of consumers' experience. Having a bad experience because of a cyber incident will likely erode your brand and consumer trust. Elevate the role of cyber risk, and embed it as a job responsibility for key C-suite executives such as the chief customer experience officer, CMO, and others who are directly responsible for your brand and consumer engagement.

Connected products

Connected products can have unlimited potential—including for increased cyber risk

The adoption of connected products is expected to grow dramatically in the coming years. Though estimates of growth in connected devices vary considerably, Gartner suggests that there will be an estimated 20.8 billion of them by 2020, and others suggest that the number could be as high as 31 billion.[6] However, the future success of connected products may depend not only on the technology that facilitates connectivity but also on consumer trust, which can drive demand.

The rapid growth of connected products presents not only numerous benefits to consumer businesses and their customers, but also increased cyber risk. That's because many connected products rely on advanced technologies such as the cloud to store information, as well as on mobile payments to facilitate transactions. Along with the benefits of ever-increasing connectivity, cybersecurity vulnerabilities are growing more common as companies increase the points of entry to their systems, opening the door to breaches that can arise anywhere across the entire connected ecosystem—from consumers to third-party vendors.

The potential downside of connected products

In our survey, we learned that executives are not confident about the security of connected products: 32 percent do not believe their cyber risk management program is effective in maintaining their strategy to develop and market connected products.

It's no surprise, then, that consumer-facing businesses report a variety of concerns around their deployment of connected products, with 74 percent of those who deploy connected products citing changing regulatory requirements as their top concern (figure 9).

Operational risk can also be introduced by connected products. In an increasingly connected world, consumer business ecosystems are exposed to greater risk that a cyber incident can have a direct impact on core business operations. This may include impacts such as supply chain disruption, interruption of retail store sales, or e-commerce

Figure 9. Biggest concerns around connected products

"Thinking about your company's focus on connected products, how concerned are you with each of the following cyber threats?" (% very or extremely concerned)

Source: Deloitte analysis.

32 percent of companies do not believe their cyber risk management program is effective at maintaining their strategy to develop and market connected products.

site malfunctions. As adoption of connected products goes up, so does dependence on the Internet of Things (IoT) in general—and, therefore, the cyber risk associated with it. Because of this, consumer businesses need to broaden their approach to cyber risk management from just data protection, risk avoidance, and incident response to ensuring sustainable operations.

Connected products present a major challenge for cybersecurity executives due to both the growing number of connected devices as well as their rapid development and deployment. Some cyber executives tell us they never know where the threat will come from, making it extremely hard to put the right safeguards in place. As one industry executive we spoke with put it:

> With regard to where the industry is going with the Internet of Things, [the] question is how we will secure this stuff. It's a big part of our short-term future. Just making sure we have a good handle on understanding what the devices are, how people are using them, and how to secure them—there's a lot of work to be done. In the industry, we need to spend a lot of time on this in the future. Just keeping up with this stuff is challenging enough.

Let's not forget the unlimited potential of connected products

Connected products enabled by IoT can make possible a world where everything and everyone is potentially connected—consumers, retailers, and consumer product companies. Connected devices can offer consumer-facing businesses and their customers limitless potential to reap benefits such as enhanced customer experience and customization of products and services.

INNOVATIVE APPLICATIONS FOR CONNECTED DEVICES

Technology meets the fashion industry with clothing made from app data. In addition to the use of LEDs and near-field communication (NFC), global technology and fashion players revealed examples of the intersection of fashion and connectivity at New York Fashion Week in February 2017. While garments were not connected to the wearer, the design process was. Fashion designers leveraged personal app data collected via smartphone to create digitally tailored, custom-made clothing based on the wearer's environment, including his or her habitual routes, activity level, and the typical temperatures in the wearer's area. This information, known as context signals, was passed through an algorithm to inform clothing design.[7]

The Store of the Future. At a "Store of the Future" event at London's Design Museum in April 2017, e-commerce brands displayed connected clothing racks, touchscreen-enhanced mirrors, and sign-in stations that helped bridge the gap between online and brick-and-mortar retail. For example, customers were able to scan their smartphones upon entering a retail location to allow sales assistants to view their profiles, including what items they might have previously bought or saved to an online wish list. Connected clothing racks recorded which items customers physically picked up, storing this information in apps that customers could later swipe left or right to edit their selections. Smart mirrors allowed shoppers to request items in another size, browse online alternatives, and even pay without leaving the dressing room. Retailers also demonstrated holographic displays that enabled customers to create and order custom shoes, experimenting with different leathers, skins, and colors.[8]

For companies that deploy connected devices, the data these devices collect can be invaluable, providing a window into consumer preferences and enabling consumer-facing businesses to optimize customer experience and innovation. But how this information is collected, stored, and analyzed can make both users and consumer businesses more vulnerable to cyber risk.

Though consumers' top-of-mind uses for connected products tend to focus on health and well-being applications, many consumer-facing businesses are investing in creative, new ways to deploy connected products—for instance, in fashion and retailing (see sidebar "Innovative applications for connected devices"). That said, these applications will need to be properly secured in order for them to be successful.

A tale of two toys: Connected products' upside and downside potential

Even connected toys can potentially deliver value to their end users—or, conversely, steal proprietary information when device manufacturers do not take the necessary steps to secure the data they capture. These types of breaches can be problematic for device manufacturers, considering that children today have many of their own connected devices. In these cases, securing connected devices may no longer be just a cybersecurity issue, but a concern about the actual physical and emotional security of the children who use them for fun and entertainment.

At the 2017 Consumer Electronics show, a leading toy manufacturer introduced the world's first interactive doll, which can play games and tell stories as well as listen to and learn what children are interested in. The information collected is uploaded to the cloud and continually updated via the doll's Wi-Fi capabilities. The doll comes to know the child's preferences, likes, and dislikes, and then incorporates this knowledge into its conversations, thus having the potential to be the child's friend.[9]

But interactive toys can have their downside as well: Too much information can be shared and/or used inappropriately. A recent example involves a teddy bear manufacturer whose collection of 2.2 million voice recordings of children and their parents may have been exposed to a data breach; the data compromised also included email addresses and password data for more than 800,000 accounts.[10]

Connected products playbook

HOW CAN CONNECTED PRODUCTS BE SECURED?

Generally, it's essential that consumer businesses ensure connected products' security if both the businesses and their customers are to reap benefits from these products. This can be accomplished through multiple efforts, including:

- **Create a comprehensive, holistic inventory of the connected products attached to the network** to help identify potential points of entry and vulnerabilities.
- **Assess the value-add for new connected product functionality prior to release**. Each new feature set can bring additional risk to both the consumer and the organization; both may require increased protection from malicious intent. The value-add of any given feature set should outweigh the cost of securing these features. Otherwise, the organization's appetite for cybersecurity measures may fall short of the level of investment required.
- **Engage actively with legal** to ensure that customer agreements clearly state both the company's and the consumer's roles and responsibilities with respect to matters such as the ownership of the data collected by connected products and the actions to be taken in the event of a breach. It's important to be clear and up front about any responsibilities the customer may have to help effectively manage cyber risks.
- **Consider security-by-design principles and strong application security.** Consumers are not always able to update firmware, and they sometimes neglect to do so even when updates are available. The expectation is that

consumer businesses will produce products that are secure immediately off the assembly line, or they may potentially suffer negative impacts on operations, brand, functionality, or regulatory compliance.

- **Remember that old-school data protection hygiene still applies to the new age of connected products**. Much of the information collected by products today may be deemed private and/or confidential. As with any such data, data collected by connected products should be protected upon collection, while in transit, and when stored on both the device and the data store. Additionally, privacy and data use policies, including policies related to cross-border data transfer, should be updated to reflect the new age of 24/7 data collection in homes, on roads, on persons, and otherwise.
- **Evaluate the scope of other enterprise efforts**, such as cyber threat monitoring and wargaming/resiliency exercises, to determine whether these efforts are comprehensive enough to cover top cyber risks related to connected products.

Payments

Emerging payment technologies are attracting many forward-looking businesses—and opportunistic cyber criminals

Emerging payment technologies can enable businesses to elevate the customer experience by streamlining—and in many cases reinventing—the payment process. While NFC and other mobile payment technologies have existed for quite some time, consumers finally seem to be warming up to ideas such as using their smartphone as a wallet, signaling a mainstream shift in how payments are made. In fact, the mobile wallet market, valued at approximately $594 billion in 2016, is expected to skyrocket to $3,142 billion by 2022, with a compound annual growth rate of around 32 percent between 2017 and 2022.[11] Companies that are able to leverage emerging payment technologies while simultaneously maintaining the security of their payment platforms will be best positioned to gain from these investments.

Many restaurants, retailers, and other consumer-facing businesses are racing to stay ahead of the mobile payment trend. Thirty percent of executives

Less than one-third (32 percent) of executives investing in mobile payment solutions feel they have mature security controls in place around the technology.

in our survey highlighted customer experience as a top strategic priority for their organization, and for many, investing in mobile payment technology is a key part of that initiative. Indeed, three in ten executives cited mobile payments as a top technology initiative.

While businesses continue to explore how mobile payment technology can transform the in-store experience, and many are incorporating automatic payment technology into their apps, relatively few are building in adequate protection. Our study revealed that only 32 percent of executives at companies implementing mobile payment technology feel they have "mature" cybersecurity programs in place. Leaders should remember that the same technologies they employ to provide new and efficient delivery channels for their customers are also being used aggressively by hackers and criminal elements. Cyber criminals will likely probe emerging payment systems because they aren't as protected as some others.

Keeping up with the evolving payments landscape

The constant evolution of payment technology requires perpetual cyber vigilance. The long-awaited

roll-out of EMV chip technology, for example, was one win in the battle against cybercrime and fraud. However, businesses should not feel a false sense of security. Ultimately, ploys such as EMV "chip-and-PIN" technology will likely not eradicate payment fraud, but simply shift the type of fraud that occurs as cyber criminals look to exploit new weaknesses.

In order to keep up with change, effective cybersecurity programs should allocate sufficient budget toward developing new and maintaining existing security controls. Executives in our survey indicate they are currently allocating roughly one-third of their total cyber budgets to developing new and maintaining existing security controls.

Vulnerability around payments is on the rise as consumers begin to embrace third-party payment vendors

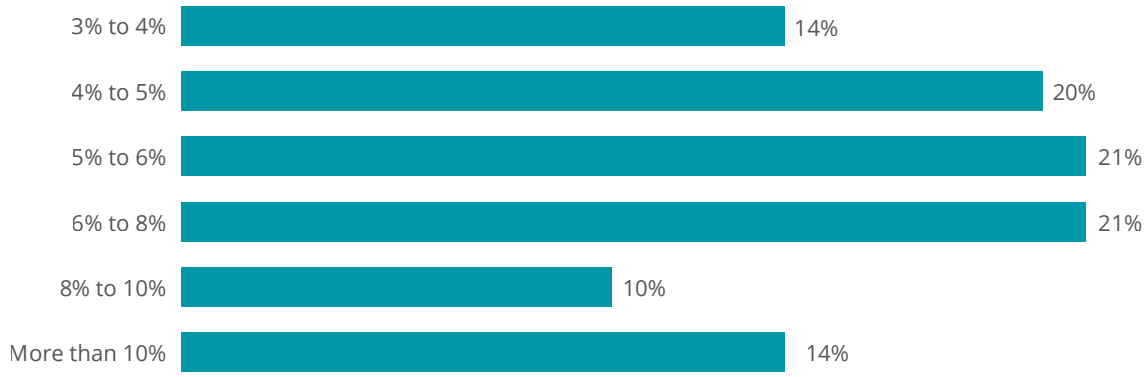
Many consumer businesses are increasingly leveraging digital payment technology from companies that specialize in electronic payments. This reliance on third parties can create all-new hurdles in the world of cybersecurity. Businesses can invest heavily in their own cybersecurity initiatives, but it can be all for naught if a third-party vendor creates a weak link in the chain. While many consumer businesses appear extremely confident in the third-party vendors they work with, our survey indicates that only a few regularly review and test their vendors' cybersecurity capabilities.

Franchisees heighten a brand's cyber vulnerability

For many brands, particularly in the restaurant and hospitality sectors, geographic expansion is key to growth. While franchising can give brands an effective way to scale, it can also create a variety of cybersecurity issues. Despite appearing to be big, global brands on the surface, many franchisees operate more like small to medium-sized businesses, and cybersecurity spending often takes a back seat to profit-related initiatives.

Often, franchisees assume that criminals are after the "big guys," businesses that handle thousands of payments daily. This false assumption can actually make franchisees more susceptible to breaches because they generally don't make cybersecurity a top priority. Restaurant organizations provide an excellent example. With limited funding for cybersecurity (figure 10), many restaurant franchisees outsource their point-of-sale (POS) systems to third-party service providers, which may not always adhere to best security practices.

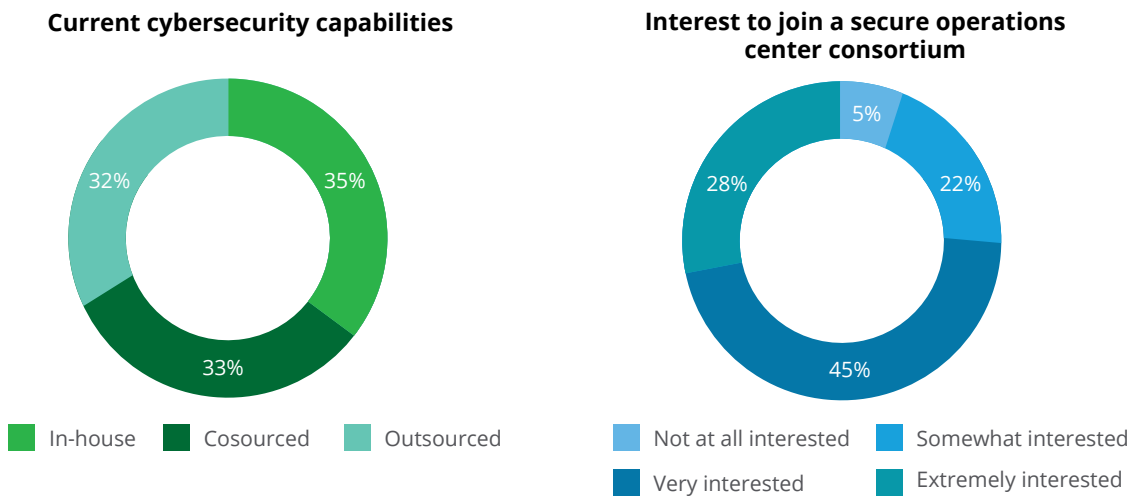
Figure 10. Cybersecurity budgets (as a percentage of annual IT budget)



Note: Sample sizes: n(overall)=400, n(consumer products)=149, n(restaurants)=99, n(retail)=100.
Excludes agribusiness.

Source: Deloitte analysis.

Figure 11. Cybersecurity outsourcing and interest in joining a secure operations center consortium (restaurants only)



Q11. How much of your current cybersecurity capabilities are outsourced, in-house, or cosourced?
Q10. How interested would you be in joining a restaurant/retail industry secure operations center consortium?

Source: Deloitte analysis.

Outsourcing cybersecurity services has often been an effective way for restaurant franchisees to make the most of limited cybersecurity budgets. As a group, the restaurants we surveyed either outsourced or cosourced nearly two-thirds of their cybersecurity capabilities (figure 11). Particularly when it comes to monitoring and logging capabilities, restaurant organizations surveyed are very interested in joining collaborative cyber consortia that could allow them to effectively pool resources with other participating restaurants.

Payments playbook

HOW CAN CONSUMER BUSINESSES ENSURE PAYMENTS ARE SECURE?

It's critical to both businesses and consumers that payment systems be safe and secure. Businesses can take several steps to accomplish this:

- **Consider establishing a formal governing body** responsible for organizational payment security and compliance.
- **Keep applicable business units and functions informed** of and included in discussions about payment security.
- **Perform a scoping exercise** to map out the life cycle of payment transactions, and fully understand both the technologies and business units involved (such as card-present transactions, call centers, automated clearing house transactions, e-commerce, and back-office functions such as accounting and finance).
- **Review contractual agreements with third-party providers** such as acquiring banks. Understand your organization's compliance obligations (such as PCI DSS) as they relate to your payment environment.
- **Implement processes and technologies** that help to keep an accurate, up-to-date inventory of payment endpoints (such as POS devices).
- **Perform regular vulnerability scans** and keep payment technologies up to date with the latest security patches.
- **Log and monitor suspicious activity** regarding the health and security of your payment technologies.
- **Document and test response plans** in the event of unplanned payment outages or data breaches.

Intellectual property

The potential devastating impact of an IP breach: Cyber theft and loss of IP

While losing customer data during a breach can rattle customer trust and tarnish brand image, losing intellectual property (IP) could threaten a company's future. IP drives innovation, competitiveness, and growth for any business, and it can constitute more than 80 percent of a single company's value today.[12] For a consumer product company, IP might be critical information about a new line of products or the product formulation on which the company was built. For a restaurant, it might be the secret ingredient to an amazing recipe.

Intellectual property rising as a top data concern

Deloitte's study on cyber risk in advanced manufacturing revealed that IP was a top data concern among the executives surveyed—second only to financial theft.[13] This rising concern over IP theft is mirrored among consumer businesses, even though the general public, when thinking of consumer business companies, tends to focus on more familiar cybercrimes such as credit card theft and theft of other PII. Forty-two percent of the food and beverage executives we surveyed, for instance, were concerned with cybercriminals trying to steal proprietary product information such as food recipes and product codes.

42 percent of food and beverage executives are concerned with cybercriminals trying to steal proprietary product formulation information such as food recipes and product codes.

Rising concern around IP theft among consumer businesses isn't without reason. IP theft is on the rise across the board. According to a recent Deloitte poll, the number of IP cyber theft incidents is expected to increase over the next 12 months.[14]

The evolution of IP theft

The rising concern around IP theft may largely stem from the evolving nature of breaches. Historically, IP theft primarily took the form of disgruntled employees running away with physical documents, computer disks, or prototypes. Wrongdoers had either direct knowledge of or were able to gain physical access to trade secrets to perpetrate the crime. In contrast, in a digital world, IP thieves can operate from anywhere in relative anonymity, making the pool of possible suspects both broad and deep. The list of potential perpetrators may indeed include insiders such as current and former employees, but it also includes competitors, recreational hackers, and even nation-state actors.

The emerging ecosystem of connected products is just one example of a technology that can change the shape of modern IP theft. While connectivity offers new ways for businesses to create value, it may also create new opportunities for information to be accessed and compromised.[15] In fact, our respondents cited IP theft as the top concern around continued investment in connected devices, beating out concerns over theft of customer information, product disruption, and negative impacts to product safety (see figure 9 in the discussion on connected products).

The evolving nature and rising incidence of IP theft likely requires a comprehensive cyber risk approach around identity and data access management, taking into consideration who can access certain information, where and how the information is stored, and the application of security controls at the data layer itself. Unfortunately, identity and access management is often a weak link in an organization's cybersecurity chain. The executives we surveyed cited "data and access management" as the least mature element of their company's cybersecurity program—ranking below seven other attributes, including compliance and program management, application security, and cybersecurity strategy (figure 12).

Intellectual property playbook

HOW CAN INTELLECTUAL PROPERTY BE SECURED?

Securing IP is commonly challenging, as there is no silver bullet. History shows that traditional security measures such as perimeter security are necessary, but still not fully effective. A fundamental shift in approach is necessary to apply security controls in a layered fashion that considers both internal and external risks and threats. In other words, this approach should consider not only who might attack from the outside and what technologies they might employ, but also who on the inside—such as rogue employees or third-party contractors—might have the motive, means, and opportunity to steal IP.

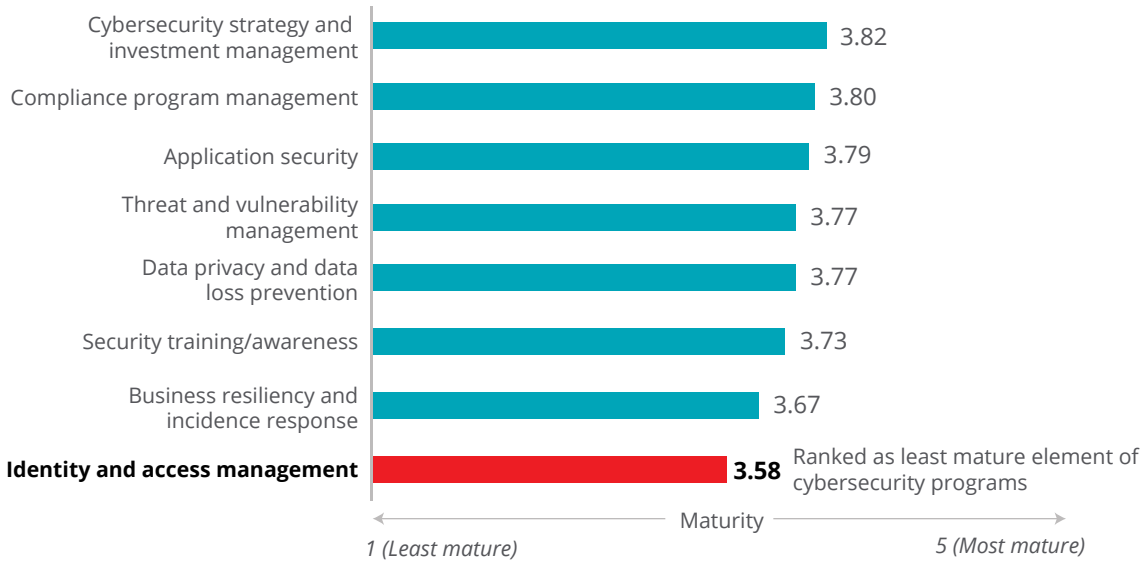
It is often recommended that organizations apply security controls at the data layer itself (the "inside out" security model) in addition to other basic capabilities such as perimeter security, vulnerability management, application security, and so on. Data protection from the inside out focuses on three important principles:

- Inventorying, classifying, and maintaining sensitive data and corresponding assets
- Implementing preventative and detective data protection capabilities at the data layer
- Reducing the value of sensitive data if and when they are compromised

Actions to consider taking in this regard include:

- **Inventory and classify IP at the source** and among the corresponding systems that store and process the IP. Determine who uses the IP, including other departments and third parties, and assess how widely it is distributed.

Figure 12. Cybersecurity program maturity



Source: Deloitte analysis.

- **Implement IP protection capabilities at the data layer**. Once IP is identified and tagged, apply security controls at the data layer itself, whether the IP is stored in documents or in databases. These controls could include preventative solutions such as digital rights management (DRM) as well as detective solutions such as data loss protection, data access governance, and database activity monitoring. Develop an overall strategy to protect the IP, and select tools that complement each other and cover the risk holistically.
- **Reduce the value of sensitive data to the cybercriminals**. This is perhaps the most important principle in inside-out security, and it is based upon the premise that the question is not "if," but "when," IP will become exposed. One way to reduce the value of sensitive data is to encrypt or obfuscate the data to render it difficult to use when compromised. A second method is to securely destroy sensitive data when they are no longer necessary for legitimate legal or business purposes. In all cases, protecting sensitive data is a complex challenge that requires a holistic and comprehensive data protection strategy, executive support, and investments in time, talent, and funding. Implementing individual data-centric solutions in a siloed manner without integration can lead to critical gaps in an organization's security.

Additional strategies companies may employ to protect IP can include:

- Implementing global network segmentation strategies
- Establishing strong central guidance on IP protection policies and procedures
- Continuously monitoring for IP-related threats
- Training high-risk employee groups that frequently handle sensitive IP on cyber awareness, tailoring the training to their specific roles
- Using secure sites to share IP as needed—with key suppliers and subcontractors, for example—as opposed to sending the information out in an uncontrolled manner

Organizations may also need to make strategic business decisions based on their risk tolerance for IP protection risks when evaluating the types of business activities they may or may not be willing to undertake in emerging markets.

Talent and human capital

Be purposeful in addressing talent-related challenges

An organization's ability to effectively and efficiently manage cyber risk depends on its culture. Talent can be the weakest link in the cyber landscape. Throughout this report, we've addressed opportunities for consumer businesses to manage cybersecurity through increasing executive-level engagement, building customer trust, safeguarding information exchanged by connected products, protecting IP, and securing payment systems. But to be successful in these areas, it is often critically important to have the right employees focused on the right tasks to mitigate cyber risk. To do this, an organization should be purposeful in addressing talent-related challenges around cyber risk—specifically, by attracting, training, and retaining top cybersecurity talent, and by delivering frequent education on new approaches to cybersecurity in light of the evolving nature of cyber threats.

25 percent of survey respondents cite lack of available talent and finding talent with the right skill set as a challenge.

Only 25 percent provide cyber awareness training to executives, employees, and third-party vendors on a quarterly basis.

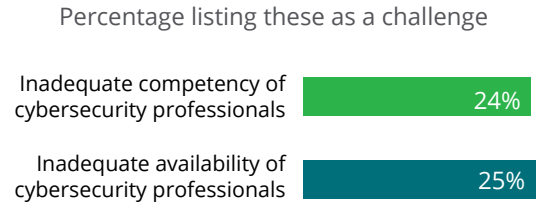
The challenges of attracting, training, and maintaining cybersecurity talent

Attracting the right talent emerged as an issue in our survey when we asked about the top challenges of establishing and maintaining an effective cybersecurity program (figure 13). The consumer businesses we surveyed reported significant hurdles related to two issues: the availability of cybersecurity talent (since cyber professionals are in high demand), and finding talent with the right skill set. Cybersecurity executives we spoke with expressed frustration around recruiting talent, aptly expressed by one executive:

> Companies can't hire enough [cyber talent]. It's hard to scale a team. We are looking to augment our team.

Unfortunately, availability is only part of the problem. Once cyber talent has been identified and hired, challenges may arise around training and retaining that talent, as some cybersecurity professionals may not perceive the training to be leading-edge or challenging enough. And there's always the

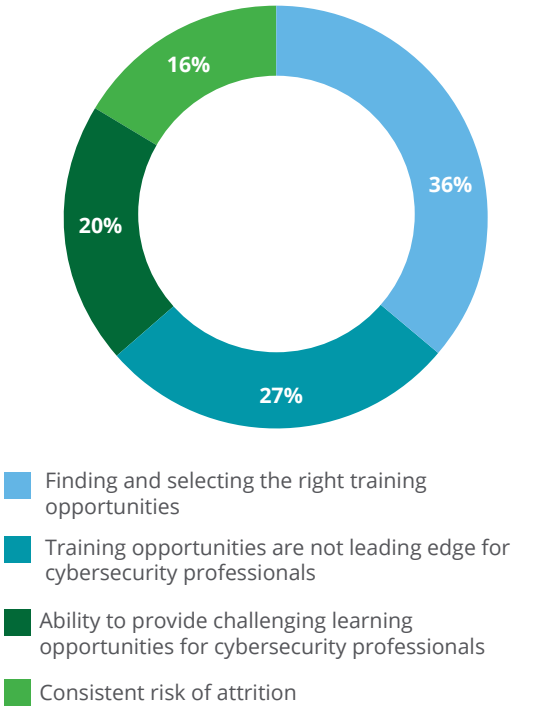
Figure 13. The talent gap in cybersecurity



Q25. What are the most important challenges your organization faces to establish/maintain an effective cybersecurity program?

Source: Deloitte analysis.

Figure 14. Issues in developing cybersecurity talent



Q48. What is the most challenging issue with respect to developing cybersecurity talent?

Source: Deloitte analysis.

risk of attrition, an issue reported by 16 percent of our respondents (figure 14).

In our in-depth discussions with cyber executives, we learned that the difficulty of hiring and retaining top talent is often related to the varying appeal of working for a tech company versus a consumer business. Simply put, many consumer businesses do not have the same cachet as do tech companies, which tend to offer higher compensation and more sophisticated technological training and learning opportunities. Often, tech companies tend to be located in appealing cities or tech hubs, which many younger cybersecurity professionals find especially attractive. As one executive said:

> [We are in] a hot job market; it's very competitive. I think hiring external people is difficult, even though we are a big company. It may be that our compensation is not as high as others'. What we've done is added roles in our teams, and we look for existing people in related functions to train by developing them from within—taking someone from other IT disciplines and training them. [Cyber] is a hot thing, so some people may be interested in training up. For us, that is a safer development strategy than external hire.

Consumer business companies acknowledge the need to invest in training and development of their employees. Training internal staff on security awareness and cyber risk should likely be a priority, with companies in our survey rating their maturity level in this area only 3.73 on a five-point scale (figure 12).

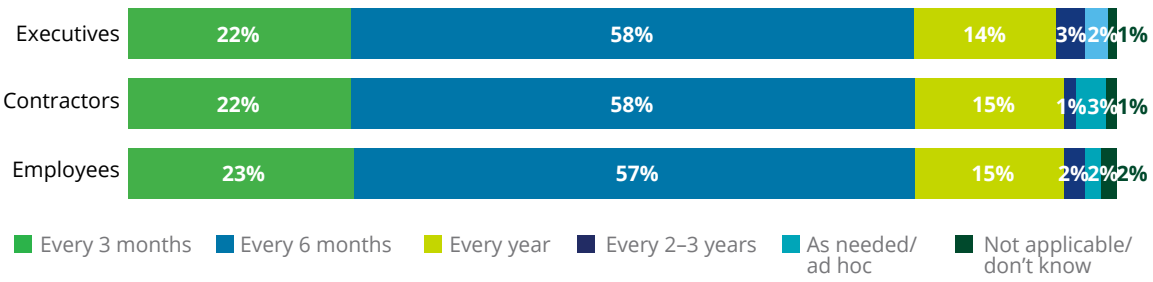
Managing insider threats is often a priority

The threat from employees within the organization is also a concern for many consumer businesses. The damage done by an internal agent can be devastating, depending on what information the employee has had access to. Reflecting this, managing insider threats is a top-five cybersecurity initiative among 26 percent of the executives who participated in our study. Our discussions with cyber executives suggest that many executives view insider threats to be more often due to employee error than malicious intent; yet these internal threats can be as potentially devastating as external threats. One executive commented:

> Human error does lead to security issues, so we have to ensure [security] around identity access management. If people have elevated access that they don't need, you open yourself up to risk. So we have tried to address this by [implementing] network-monitoring, compensating controls to prevent error. If you have human error, these [types of controls] can reduce risk.

Despite concerns around insider threats, the frequency with which organizations train contractors, executives, and employees on cybersecurity

Figure 15. Frequency of cybersecurity training received by employees, executives, and third-party vendors



Source: Deloitte analysis.

remains relatively low (figure 15), supporting our view that talent can often be the weakest link in the cybersecurity landscape.

Employing third-party vendors can increase cyber risk

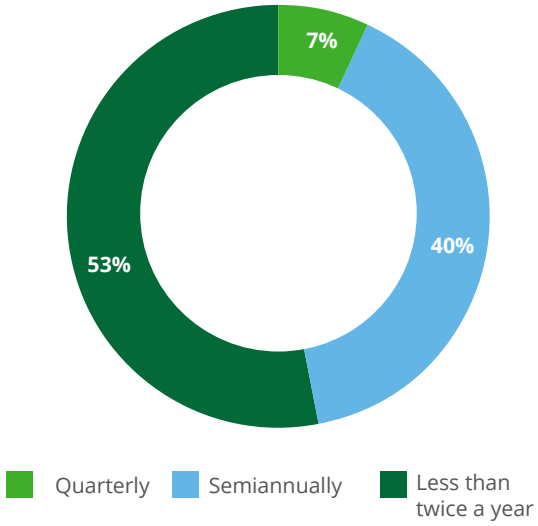
With the difficulties companies experience in hiring and training internal cyber professionals, outsourcing to third-party vendors can help companies integrate new technologies such as cloud, mobile payment, and e-commerce solutions into their businesses. However, this can open new cyber risk possibilities if relationships are not managed correctly, from onboarding through frequent assessments. It is an area of concern, then, that third-party risk assessment is infrequent, with only 7 percent of those surveyed conducting third-party risk assessment quarterly (figure 16).

Creative approaches to cybersecurity

In addition to formal preparedness efforts focused on internal security, companies commonly train their employees on how to secure their personal information, based on the rationale that if employees understand the personal threats to themselves, they will be more vigilant at work. Topics addressed tend to be more basic, but they are some of the fundamentals of cybersecurity, such as identity and password protection, using secure Wi-Fi networks, identifying and deleting suspicious emails, W-2 fraud, and safe use of mobile devices. As one executive commented:

> [T]here's only so much [security and training tools] can do. You can implement IP controls and processes, but you are only as successful as users. They are the weakest link. So [we are] trying to elevate awareness and maturity of user base and bring along the organization through the journey as well.

Figure 16. Frequency of third-party risk assessments



Q37(c). How often does your organization perform an assessment of high-risk third parties?

Source: Deloitte analysis.

In our in-depth discussions with cybersecurity executives, they spoke about the informal networking events they attend with other cyber professionals to stay apprised of developments in cyber risk. Many participate in local CISO discussion groups to share learning related to cyber breaches. Meetings may also include guest presentations on key topics such as presentations by FBI cybersecurity experts. Participants are anonymous, as are the examples they share.

Recognizing the need to develop top cyber talent, China launched cybersecurity talent training nationwide in September 2016.[16] This could serve as a model for the United States and other countries hoping to advance cyber risk management. An education official at the 4th China Internet Security Conference in August 2016 stated that the country needs at least 500,000 cybersecurity experts, but only about 8,000 such majors graduate each year. Authorities at Wuhan, the capital of central China's Hubei Province, announced plans to both double the number of scholarships for students pursuing cybersecurity as well as run special recruitment for "maverick geniuses," as part of nationwide efforts to train cybersecurity talent. The Chinese government has not only established an innovative evaluation system that prioritizes practical and entrepreneurship training, it will also offer twice the salary and research funds to the best cybersecurity experts.

Talent and human capital playbook

WHAT CAN BUSINESSES DO TO OPTIMIZE TALENT AND HUMAN CAPITAL?

Leadership can set the tone at the top to promote a security culture, through proactive, organization-wide engagement, implementing measurable cybersecurity learning and awareness programs, and encouraging their employees' behaviors that protect the organization and its people from a pervasive security breach. More specifically, this can be accomplished by:

- **Establishing a dedicated cybersecurity function** led by the CISO with skilled cybersecurity staff in place to protect sensitive assets, monitor security threats, and be ready to respond to breaches that may occur. The development of cybersecurity workforce strategies can be accomplished by assessing workforce needs and skill gaps, recruiting skilled talent for well-defined cybersecurity management roles, providing specialized training as needed to further enhance employee skill sets, and creating a productive, results-driven environment to retain talent.
- **Establishing a cross-functional team of key stakeholders**, including information technology, operations technology, research and development, finance, marketing, and risk. Identify and socialize the risk framework with this team to define key mitigation strategies and clearly identify ownership for implementation.
- **Performing regular internal phishing tests** as an assessment and awareness tool to help employees better identify these attacks when they occur.
- **Ensuring the organization regularly recognizes cyber risk behaviors**, trends, and cyber threats to the organization.
- **Providing learning and awareness opportunities** in the form of frequent, small bites of

information while leveraging multiple delivery channels (digital, classroom based, and so on).

- **Simulating real-life threat scenarios** with a cross-section of the executive leadership team to periodically perform knowledge checks and assess real threat management preparedness. Evaluate results of various simulation tests to gauge effectiveness, and to incorporate lessons learned into iterative awareness and learning programs.
- **Developing and implementing a comprehensive third-party risk program**. In light of the dependence on third-party vendors to implement advanced cybersecurity programs and increasing decentralization of operating units, it's prudent to mandate consistent third-party governance standards. The focus of third-party engagement is progressively shifting toward value, reflecting organizations' recognition of the strategic opportunity that third parties can create for them.
- **Defining requirements for third-party cybersecurity vendors up front** in key contracts, and making sure companies have the right to audit using those requirements.
- **Increasing monitoring and assurance activity related to third parties**. Consumer businesses would benefit from third-party risk management programs that also help ensure that third-party access to the company's network, systems, or data fulfills cybersecurity requirements.
- **Visiting third-party locations** to gain assurance about third-party management.

Conclusion

THROUGHOUT this report, we've highlighted the challenges and potential opportunities consumer businesses face related to cybersecurity. In order to capture the business value associated with innovative technologies and the cybersecurity initiatives that many companies are pursuing, businesses should remain secure, vigilant, and resilient. A few thoughts on where to potentially begin include:

- **Set the tone:** Set the right tone at the top for cybersecurity management in the organization. Cybersecurity initiatives should be appropriately supported by the leadership team and executive-level management to accomplish key cyber risk objectives.
- **Assess risk broadly:** Perform cyber risk assessments that cover the entire enterprise and connected products. If prior assessments have been conducted, review the scope to confirm it was inclusive of all possible risks. Make sure the risk assessment addresses the principles around being secure, vigilant, and resilient.
- **Socialize the risk profile:** Share the results of the risk assessment along with the recommended strategy and road map with executive leadership. Engage in a dialogue as a team about the business impacts (including potential dollars lost as well as damage to brand reputation and consumer trust) of key cyber risks. To address those risks, discuss how to prioritize resource allocations across the secure, vigilant, and resilient areas commensurate with your organization's risk tolerance, posture, and capabilities.
- **Build in security:** Evaluate top business investments in emerging technologies and connected products. Confirm whether those projects are aligned with the cyber risk program. Determine whether cyber talent is part of the project teams to help them build in cyber risk management and fail-safe strategies on the front end.
- **Remember data are an asset.** In consumer businesses, data are a strategic asset; product formulations, consumer data, and such are invaluable to companies who must build relationships with their customers. This likely necessitates a tighter connection between business value associated with data and the strategies to protect them.
- **Assess third-party risk:** Inventory mission-critical third-party relationships. Evaluate strategies to address the third-party risks that coincide with these relationships.
- **Be vigilant with monitoring:** Be vigilant in evaluating, developing, and implementing your company's cyber threat monitoring capabilities. Determine whether and how quickly a breach in key areas in the company would be detected. Remember to extend cyber threat detection to connected products.
- **Always be prepared:** Increase organizational resiliency by focusing on incident and breach preparedness through wargaming exercises. Engage IT as well as key business leadership in these exercises.
- **Clarify organizational responsibilities:** Be crystal clear with the executive leadership team on organizational ownership responsibilities for key components of the cyber risk program. Make sure there is a clear leader on the team with the responsibility to bring it all together.
- **Drive increased awareness:** Make sure that employees are appropriately aware of their responsibilities to help mitigate cyber risks related to phishing or social engineering, protecting IP and sensitive data, and appropriate escalation paths to report unusual activity or other areas of concern.

ENDNOTES

1. Deloitte, *Cyber risk in advanced manufacturing: Getting ahead of cyber risk*, 2016, https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html#.
2. Deloitte, "An introduction to cyber war games," *Wall Street Journal—CIO Journal*, September 22, 2014, http://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/.
3. Deloitte, SSI, and JD Power, consumer privacy study presented at Next2017 Conference, May 9-10, 2017, New York.
4. Zion Market Research, "Global smart home market will reach USD 53.45 billion by 2022," *Global Newswire*, January 20, 2017, https://globenewswire.com/news-release/2017/01/20/909668/0/en/Global-Smart-Home-Market-will-reach-USD-53-45-Billion-by-2022-Zion-Market-Research.html.
5. Associated Press, "U.S. warns of security flaw that could allow hackers control of heart devices," *CBS News*, January 10, 2017, http://www.cbsnews.com/news/cybersecurity-flaw-that-could-allow-hackers-control-of-heart-devices-united-states-warns/.
6. Amy Nordrum, "Popular Internet of Things forecast of 50 billion devices by 2020 is outdated," *IEEE Spectrum*, August 18, 2016, http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.
7. Kyle Wiggers, "Google partnered with H&M-backed fashion startup Ivyrevel to build customised 'data dresses,'" *Business Insider*, February 7, 2017, http://www.businessinsider.com/google-partners-with-hm-ivyrevel-for-coded-couture-project-2017-2?IR=T.
8. Robert Williams and Jeremy Kahn, "Inside the retail store of the future: Online retailer Farfetch is bringing technology to the shop floor to blend internet and in-store experiences," *Bloomberg*, April 24, 2017, https://www.bloomberg.com/news/articles/2017-04-24/online-retailer-farfetch-and-the-retail-store-of-the-future.
9. Blake Morgan, "Five easy to understand examples of The Internet of Things," *Forbes*, January 27, 2016, https://www.forbes.com/sites/blakemorgan/2016/01/27/5-easy-to-understand-examples-of-iot-and-customer-experience/#4841b95b366c.
10. Ellie Burns, "The IoT era: A connected world where even teddy bears pose a threat," *Computer Business Review*, February 28, 2017, http://www.cbronline.com/news/cybersecurity/breaches/IoT-era-connected-world-where-even-teddy-bears-pose-a-threat/.
11. Zion Market Research, "Global mobile wallet market will reach USD 3,142.17 billion by 2022," *Global Newswire*, January 19, 2017, https://globenewswire.com/news-release/2017/01/19/909307/0/en/Global-Mobile-Wallet-Market-will-reach-USD-3-142-17-billion-by-2022-Zion-Market-Research.html.
12. Ocean Tomo, "2015 annual study of intangible asset market value," March 5, 2015.
13. Deloitte, *Cyber risk in advanced manufacturing*.
14. Deloitte, *Intellectual property theft expected to rise*, 2016, https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/intellectual-property-expected-to-rise-deloitte-poll.html.
15. Deloitte, *Cyber risk in an Internet of Things world*, 2015, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html.
16. Cao Siqi, "China launches cyber security talent training nationwide," *Global Times*, September 20, 2016, http://www.globaltimes.cn/content/1007158.shtml.

ABOUT THE AUTHORS

Sean Peasley

Sean Peasley is a partner with Deloitte & Touche LLP and serves as the Consumer and Industrial Products leader for the Cyber Risk Services practice. He has more than 30 years' experience in helping clients to become Secure.Vigilant.Resilient.™ by helping organizations address cyber risk challenges. He is experienced in cyber risk management, cyber threat intelligence, cyber wargaming, identity and access management, privacy and data protection, and business resilience.

Kiran Mantha

Kiran Mantha is a principal at Deloitte Advisory and leads Cyber Risk Services for the Retail and Distribution sector. With over 17 years of experience, he helps corporations manage complex business and information risks. Mantha is involved in several industry groups from an eminence perspective and promotes cyber risk awareness among retailers.

Vikram Rao

Vikram Rao is a senior manager in Deloitte's Advisory business with over 15 years of experience. He is a leader in Deloitte's Cyber Risk Services practice, which helps clients to be Secure.Vigilant.Resilient.™ He has helped *Fortune* 100 companies in various consumer business sectors with evaluating their cyber risks and has advised executives on investment strategies to bolster their cybersecurity posture.

Curt Fedder

Curt Fedder is a senior manager at Deloitte Services LP's Center for Industry Insights and leads market research for consumer products. With expertise in consumer research, and a focus on brand equity, customer satisfaction, and advertising, Fedder has led consumer research groups in consumer products and retail organizations. He has published articles in the *Journal of Advertising Research* and *Quirks Marketing Research*, and presented at market research industry conferences.

Marcello Gasdia

Marcello Gasdia is a manager within Deloitte Services LP's Center for Industry Insights, and is the research lead for Travel, Hospitality, and Services. He leverages primary research experience to study consumer behavior and marketplace trends across several travel sectors—including hotels, airlines, ground transportation, and restaurants.

CONTRIBUTORS

Rob Goldberg, Advisory principal, Deloitte & Touche LLP

Gregg Schmidtetter, Consumer Products Cyber Risk Services leader, Deloitte & Touche LLP

Vikram Kunchala, Advisory managing director, Deloitte & Touche LLP

Gina Pingitore, Managing director, Deloitte Center for Industry Insights

Ryan Robinson, Industrial Products and Services research leader, Deloitte Center for Industry Insights

ABOUT THE DELOITTE CENTER FOR INDUSTRY INSIGHTS

The Deloitte Center for Industry Insights is the research division of Deloitte LLP's Consumer and Industrial Products practice. The center's goal is to inform stakeholders across the consumer business and manufacturing ecosystem of critical business issues, including emerging trends, challenges, and opportunities. Using primary research and rigorous analysis, the center provides unique perspectives and seeks to be a trusted source for relevant, timely, and reliable insights.

To learn more, visit www.deloitte.com/us/cb and www.deloitte.com/us/manufacturing.

ACKNOWLEDGEMENTS

The authors would also like to thank the following professionals who have contributed to the publication of this study:

Leslie Ament, Retail research leader, Deloitte Center for Industry Insights, Deloitte Services LP

Linda Chen, Strategic marketing professional, Deloitte Center for Industry Insights, Deloitte Services LP

Linda Clemmer, Travel, Hospitality, and Services marketing leader, Deloitte Services LP

Joanna Wrobel Cullinan, Advisory strategic marketing professional, Deloitte Services LP

Ashley Dunham, Retail marketing leader, Deloitte Services LP

Shweta Joshi, Senior analyst, Deloitte Center for Industry Insights, Deloitte Support Services India Pvt. Ltd.

Sarah Katz, Advisory strategic marketing professional, Deloitte Services LP

Charlie Kirby, Advisory manager, Deloitte and Touche, LLP

Robert Libbey, Market Research, Deloitte Center for Industry Insights, Deloitte Services LP

Beth Ruck, Senior communications manager, Deloitte Services LP

Paula Spoto, Consumer Products marketing leader, Deloitte Services LP

Jagadish Upadhyaya, Assistant manager, Deloitte Center for Industry Insights, Deloitte Support Services India Pvt. Ltd.

CONTACTS

Sean Peasley
Consumer and Industrial Products leader for Cyber Risk Services
Partner
Deloitte & Touche LLP
+1 714.334.6600
speasley@deloitte.com

Kiran Mantha
Retail & Distribution leader for Cyber Risk Services
Principal
Deloitte & Touche LLP
+1.212.436.6155
kmantha@deloitte.com

Vikram Rao
Senior manager
Deloitte & Touche LLP
+1.617.437.3950
vikrao@deloitte.com

Curt Fedder
Consumer Products research leader
Deloitte Center for Industry Insights
Senior manager
Deloitte Services LP
+1.773.680.4952
cfedder@deloitte.com

Marcello Gasdia
Travel, Hospitality, and Services research leader
Deloitte Center for Industry Insights
Manager
Deloitte Services LP
+1.212.436.3839
mgasdia@deloitte.com

 Follow @DU_Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

About Deloitte