Cybersecurity as a growth advantage

Authors

Joel Barbier

Lauren Buckalew

Jeff Loucks

Robert Moriarty

Kathy O'Connell

Michael Riegel

Key Insights

- In an era of digital disruption, the C-suite needs to begin viewing cybersecurity differently—beyond its traditional "defensive" role.
- As Mike Dahn, head of data security and industry relations at Square, Inc., put it, "I think it's really important that we stop thinking about security as a defense-centric approach that is sold by fear, uncertainty, and doubt. We need to start thinking of it as an enabler that supports innovation … and helps the business go forward."
- A new Cisco study[1] indicates that an increasing number of executives are doing just that.
- Thirty-one percent of the survey's 1014 respondents (senior finance and line-of-business executives) believe the primary purpose of cybersecurity is **growth enablement**. Sixty-nine percent still see the main purpose as risk reduction.
- Forty-four percent consider cybersecurity a **competitive advantage** for their organization. Fifty-six percent perceive it as a cost of doing business.
- Executives recognize the critical link between cybersecurity and *digitization*—the movement of operations, processes, and business functions onto a single, re-engineered digital operating model.
- There's a lot at stake. Cisco has identified **414 use cases** that will drive $7.6 trillion in Digital Value at Stake[2] globally over the next decade.
- More than three-quarters of this amount involves **cybersecurity as a growth enabler**.
- Unfortunately, many companies are missing out. Our research reveals that 71 percent believe **cybersecurity risks hinder their innovation**. Thirty-nine percent have **halted a mission-critical initiative due to cybersecurity concerns**.
- Uncertainty about cybersecurity is also causing companies to delay critical digital initiatives. These initiatives can be key differentiators in an increasingly competitive economy.
- Companies need to follow the example of the **"Secure Digitizers,"** who are strongly committed to growth through digital business models and offerings—with cybersecurity as an essential foundation.

> The digital economy is not just a digitized version of the current economy. Part of that discussion is cybersecurity, both in terms of the threats, but also thinking about what it can enable.
>
> – Adriaan Bouten, CEO and Founder, dPrism

Introduction

Disruptors now harness the power of digital to create new sources of value that reduce costs, improve the customer experience, and scale their offerings.[3] Digital disruptors also enjoy a decided innovation advantage over established companies: they are better able to identify new opportunities, and move faster to take advantage of them.[4]

In this intensely competitive environment, startups and agile firms are overturning incumbents with digital business models, products, and services.[5]

All companies are being pulled toward the center of a "Digital Vortex," which is characterized by exponential change and the blurring of industry lines.[6] Companies must adapt, or their odds of being displaced—or even put out of business altogether—markedly increase. A recent study by the Global Center for Digital Business Transformation, an IMD and Cisco initiative, predicts that four out of 10 leaders in each industry will be displaced by digital disruption within the next five years.[7]

Established companies can compete and thrive in the Digital Vortex by finding "value vacancies"—market opportunities ripe for exploitation by digital disruption—and by adopting digital strategies that take the fight to disruptors.[8]

Digital transformation, however, requires a strong cybersecurity foundation. With this foundation, companies will have the confidence to implement digital processes and technologies that fuel innovation and growth. Without it, companies may hesitate to start digital projects—stifling their innovation potential and opening the door to digital disruptors.

Anxiety Is Growing on Boards and in the C-Suite

Most C-suite leaders are still thinking about stopping threats when they could be thinking about the tangible growth that cybersecurity excellence makes possible. As the number of cybersecurity breaches rapidly escalates,[9] the once-startling admission that millions of records have been compromised by outside hackers has become terrifyingly commonplace.

Senior executives are taking notice: 87 percent said they are concerned about the potential for cybersecurity breaches at their companies. Nearly half are "very concerned." Some 41 percent are "much more concerned" than they were just three years ago.

This anxiety reaches far beyond the IT organization. CEOs and boards of directors are considered most accountable for major cybersecurity incidents (see Figure 1), but executives in charge of enterprise risk, chief information security officers (CISOs) and CIOs, and department heads all share the accountability when things go wrong.

Financial and line-of-business executives told us that cybersecurity has become a board-level concern. Audit committees in particular are probing their companies' cybersecurity weaknesses as part of their fiduciary responsibilities. Cybersecurity has become a pillar of enterprise risk management, along with financial risk and safety/security. Thus, audit committees are demanding that executives responsible for enterprise risk management—such as CFOs[10] and chief risk officers—be held accountable for cybersecurity.

Business executives must rely on those who understand the technical side of cyber risk—their CIOs or, in some cases, CISOs—to provide trusted guidance and advice. As Cisco research has shown, 46 percent of IT spending is now controlled by line-of-business

Methodology

About the Survey

In October 2015, we conducted an online survey of 1014 C-level executives, VPs, and directors. More than one-third had financial roles and cybersecurity financing influence; the remainder came from a mix of line-of-business domains. Respondents represented Australia, Brazil, Canada, China, France, Germany, India, Japan, the United Kingdom, and the United States.

We also conducted qualitative interviews with 11 experts; all were senior executives (current and former) with extensive cybersecurity experience, and two were cybersecurity consulting experts.

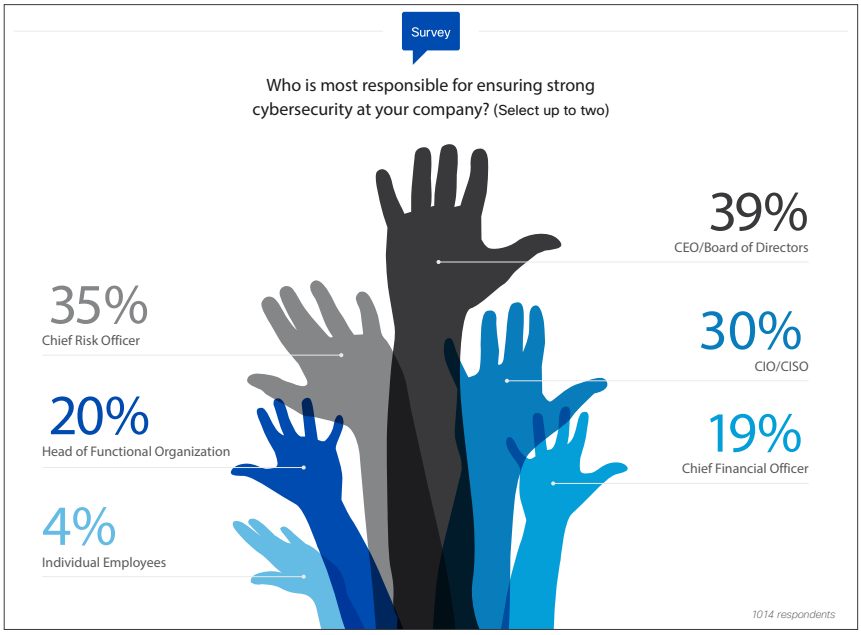


Figure 1
Cybersecurity accountability extends all the way to the top

Source:
Cisco, 2016

executives[11], who are also responsible for the company's sources of revenue and critical operations. Ultimately, when a company releases a new product or a mobile app, a line-of-business executive is responsible for its development and execution, a fact these executives acknowledge. Fifty-four percent of line-of-business executives say that key stakeholders, such as customers, hold them accountable for cybersecurity "to a great degree."

Because breaches cause immense damage, senior executives feel responsible for preventing them.

The average cost of a cybersecurity breach is large and increasing—reaching $3.79 million in 2015, up from $3.52 million in 2014.[12]

The repercussions extend far beyond the costs that are easiest to calculate, such as incident response, forensic investigation, internal audits, and communications. According to the financial executives we surveyed, lost business stemming from the erosion of consumer trust was the most feared consequence (see Figure 2). When customers avoid doing business with a company because they fear their accounts could be vulnerable to cyber threat, millions in revenue can be jeopardized.

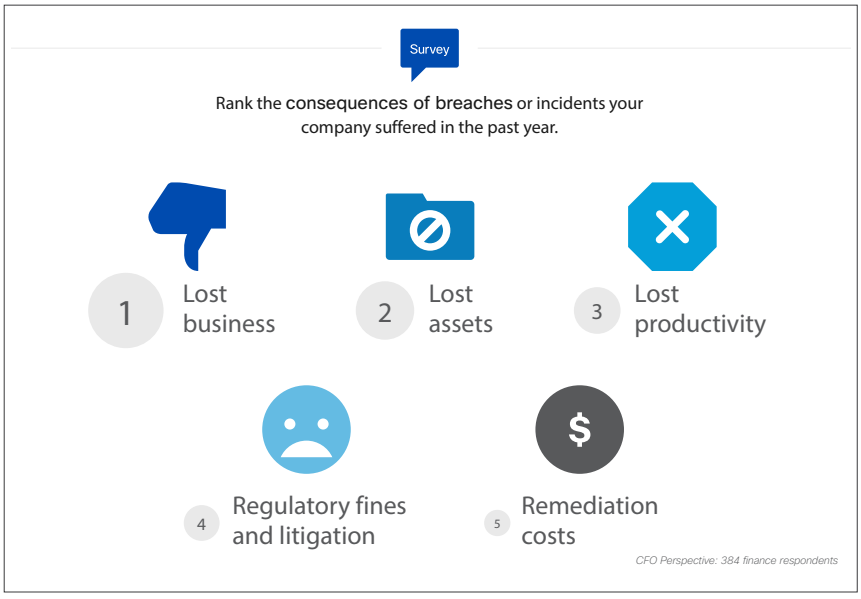


Figure 2
The consequences of breaches are far-reaching and devastating

Source:
Cisco, 2016

Regional Insights

Cybersecurity Strategy Responsibility Varies by Country

In China and India, the chief risk officer is most likely to have primary responsibility for cybersecurity (as indicated by 44 percent of respondents in each country).

In Brazil, Canada, and the United Kingdom, it is the CEO / board of directors that is most responsible.

The United States was the only country surveyed in which the CIO/CISO took the top spot (37 percent), with the CEO / board close behind (36 percent).

The CFO was named the responsible party in 19 percent of companies interviewed globally. In China, 29 percent of firms consider the CFO responsible, more than any other country surveyed.

Customer data was considered the most critical to secure by line-of-business executives, and the reason is clear. Lost or compromised customer data is a catalyst for a host of negative consequences. Companies can expect the threat of lawsuits, fines, increased regulation, and remediation costs, in addition to lost business. Executives were nearly unanimous (92 percent) in expecting increased scrutiny from regulators and bankers. Recent announcements show that a new wave of rules is coming.[13]

When customer information is breached, the consequences can be profound across industries. For example, if a retailer suffers a data

breach, customers won't feel comfortable sharing personal information. As a result, the retailer won't be able to offer the analytics-driven, hyper-relevant experiences in-store and online that shoppers expect. Those customers will switch to a retailer that can provide better customer experiences driven by secure data.

Executives also fear that strategic assets like intellectual property and other confidential information can be vulnerable. The financial and human resource investments that companies expend on innovation must be factored into the total cost of a data breach. So, too, must be the loss of competitive position when rival companies steal the details of products and plans.

Executives also mentioned the importance of safeguarding financial data, business processes, formulae, and contracts with suppliers. They are well aware of the damage lost or diminished assets can inflict on their company. Many fear where threats may come from: 27 percent identified industrial espionage as a top concern.

Inadequate Cybersecurity Stifles Innovation and Competitiveness

An often overlooked, but critically important implication of cybersecurity weakness is *how it can impact a company's innovation and growth*. This particularly applies to the development of digital offerings and business models.

In our study, a stunning 71 percent of executives said that concerns over cybersecurity are impeding innovation in their organizations. Thirty-nine percent stated that they had halted mission-critical initiatives due to cybersecurity issues (see Figure 3).

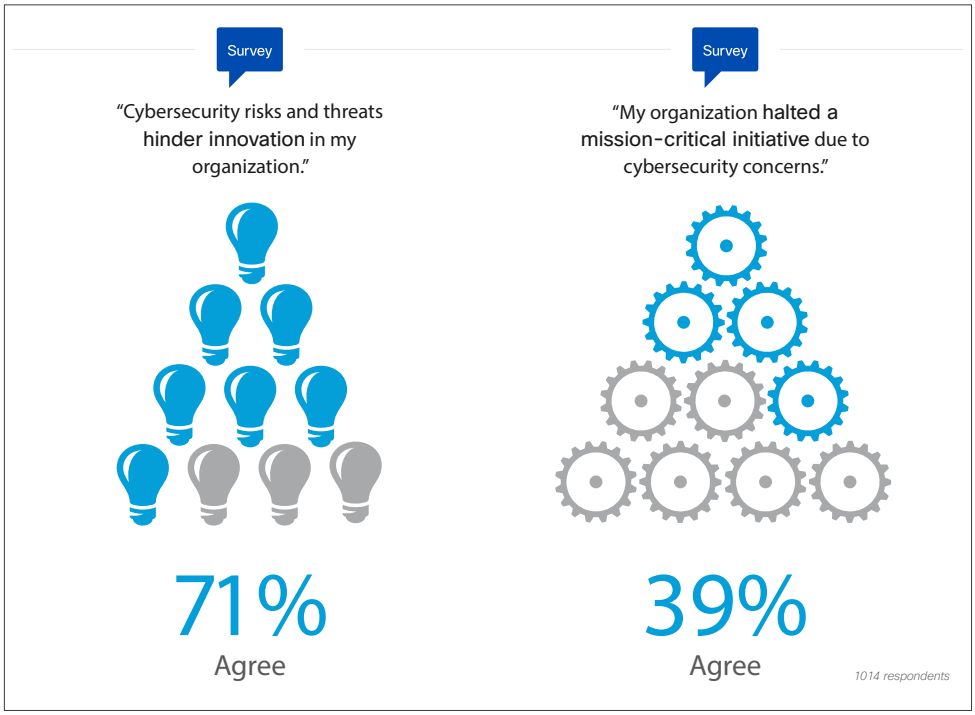


Figure 3
Lack of cybersecurity cripples innovation and slows business

Source:
Cisco, 2016

The study found no strong correlation between geographical location and the impact of cybersecurity concern on innovation. The perceived threat of cybersecurity weakness to innovation was greatest among respondents from India, China, the United Kingdom, and Canada, while it was lowest among U.S. respondents. India and Brazil had the highest percentages of respondents who said their organization had halted a mission-critical initiative due to cybersecurity concerns.

Among industries, the perceived threat to innovation was highest in technology products, business services, retail, and banking. It was lowest in hospitality/travel/entertainment and manufacturing/consumer packaged goods. Business services had stopped the most mission-critical initiatives due to cybersecurity concerns, followed by technology products and education.

Several industries have already experienced high levels of digital disruption. Leaders in digital businesses are acutely aware of the risks and benefits of implementing digital products and services. They are also more likely to recognize the link between weak security and lost innovation.

Cybersecurity weakness is a "silent disease" that impedes firms' ability to innovate at precisely the time they can least afford it—when they are being drawn into the Digital Vortex,[14] where digitization, disruption, and exponential change are the "new normal."[15] Many companies suffer from this malady, but few are aware that they have it. Left unattended, cybersecurity weakness can be fatal in the Digital Vortex.

In the Digital Vortex, disruptive firms typically have three key advantages over established companies: their abilities to 1) innovate, 2) move quickly, and 3) reward experimentation (see Figure 4). To match both the pace and effectiveness of startups, established companies must boost their innovative capabilities. Yet, 60 percent of our survey respondents indicated that their organizations are reluctant

> "Our biggest concern with cybersecurity breaches is not as much the direct financial impact as the indirect. What would it do to us from a reputational standpoint? What if customers decide that we're not worthy of their trust and stay away?"
>
> —Greg Kleffner, CFO, Stein Mart

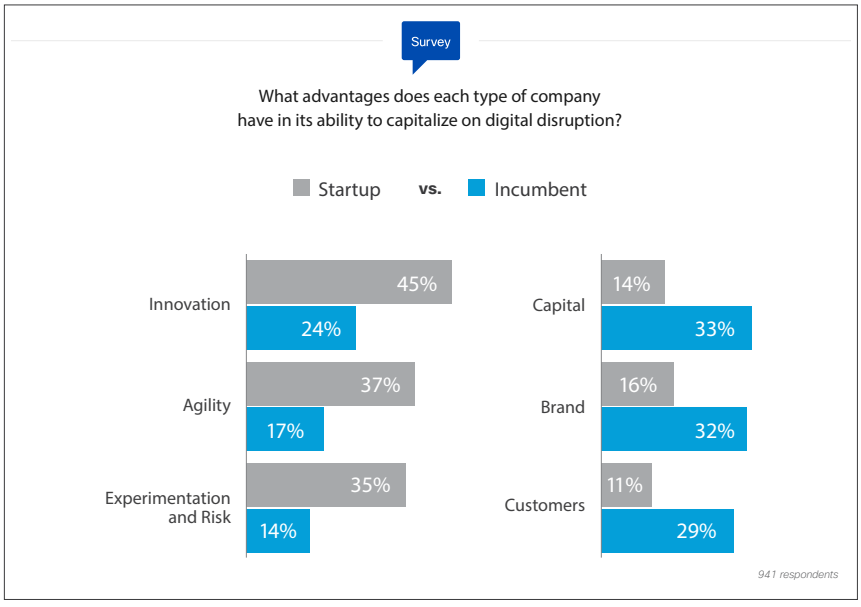


Figure 4
Incumbents have advantages, but need to learn from startups

Source:
Global Center for Digital Business Transformation, 2015

to develop digital products and services because of the potential cybersecurity risks.[16] Unfortunately, these are the very products and services they need to compete with disruptors.

While cybersecurity concerns can hinder the pursuit of some digital business models and innovations, many firms believe they must move forward, or be left behind by digital disruptors and other agile competitors. In fact, 73 percent of survey respondents admitted that they often embrace new technologies and business processes, despite the cybersecurity risk.

Subpar cybersecurity leaves companies in the worst possible competitive position: not innovating fast enough to compete, yet not safe enough from cyber attack despite delaying digital innovations.

For more insights, please visit
cs.co/cyberAB

"Innovations are moving forward, but probably at 70–80 percent of what they otherwise could if there were better cybersecurity tools..."

—Robert Simmons, CFO

Executives Know Cybersecurity Enables Growth, Yet Are Underinvesting in This Area

The imperative to digitize products, services and business models is clearly recognized by senior business leaders. Sixty-nine percent of executives said digitization is "very important" to their company's current growth strategy. They also recognize that cybersecurity is a vital foundation for their digital growth strategies: 64 percent cited it as a "significant" driver of the success of digital products, services, and business models (see Figure 5).

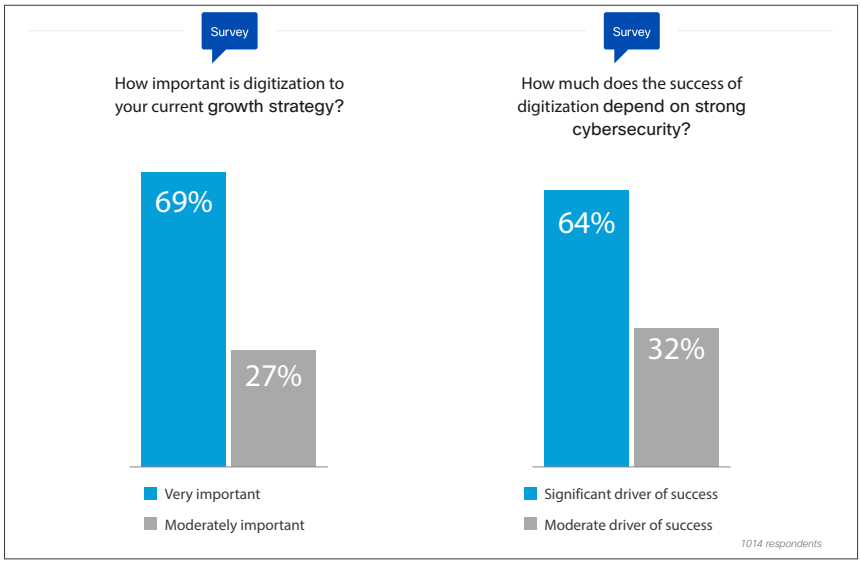


Figure 5
Executives understand the connection of cybersecurity to digitization and growth

Source:
Cisco, 2016

Given the tight connections among cybersecurity, digitization, and innovation, cybersecurity excellence is increasingly being viewed as a driver of business value. According to our survey, nearly a third of executives (31 percent) already make this linkage: they view "enabling growth" as the *primary* purpose of cybersecurity. Meanwhile, 69 percent of executives see the main purpose of cybersecurity as "reducing risk."

Similarly, 44 percent of executives see cybersecurity as a competitive advantage for their organization, while 56 percent view it as a cost of doing business. Changing perceptions—moving from viewing cybersecurity investments strictly as "defensive," to also seeing them as "enabling" greater innovation—can boost corporate competitiveness.

Among countries, the "growth enablement" sentiment was strongest in China, India, and Canada (see Figure 6), while respondents from India, China, and Brazil were most bullish about cybersecurity as a competitive advantage. These views undoubtedly reflect the sharp rise in digital adoption among emerging countries like China, India, and Brazil. In fact, according to recent Cisco analysis, emerging countries will drive nearly one-third of global private sector digital value by 2024.

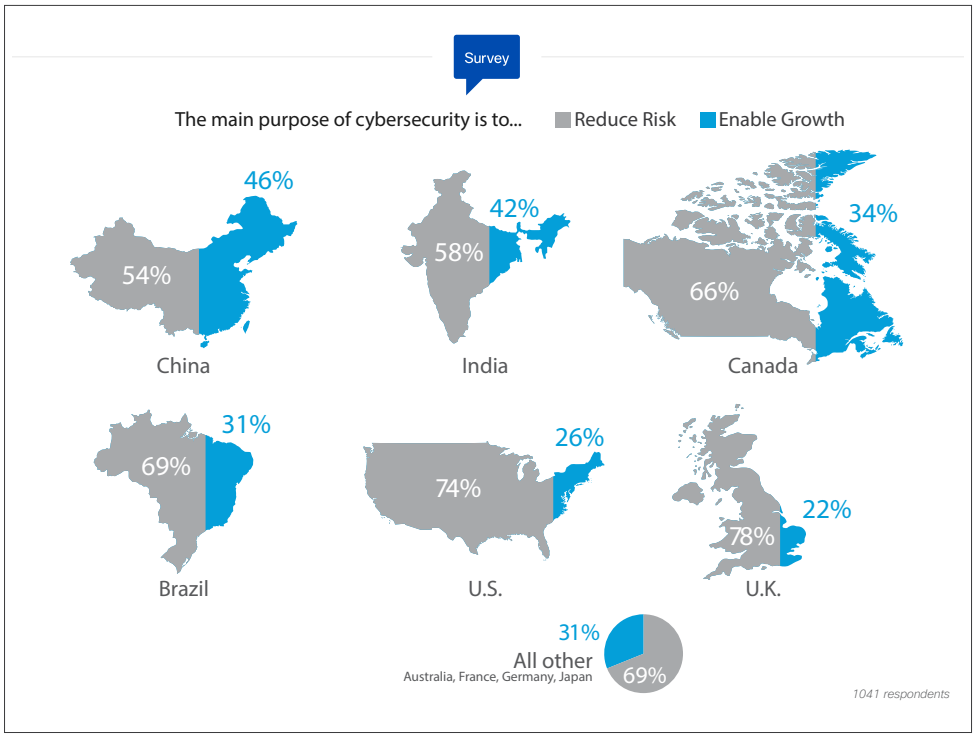


Figure 6
Globally, almost one-third of executives associate cybersecurity to growth

Source: Cisco, 2016

Among industries, mining & utilities, retail, and transportation / logistics had the highest percentages of respondents viewing cybersecurity as a growth enabler (see Figure 7, next page). This shows that executives in nearly all industries understand both the need to accelerate innovation and the critical linkage of cybersecurity to digital products *and* services.

Firms that turn cybersecurity excellence into true competitive advantage can innovate faster and more fully pursue the sort of digital transformation that allows

"Evolving from thinking of cybersecurity as a necessary evil to a strategic advantage sets you apart."

—Former VP of Human Resources, Fortune 100 Bank

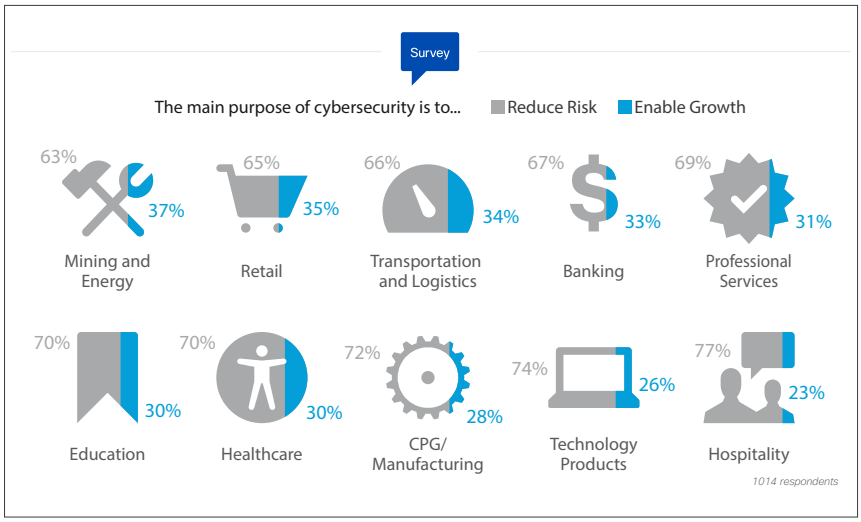


Figure 7
Growth enablement sentiment is strongest in mining/energy, retail, and transportation/ logistics industries

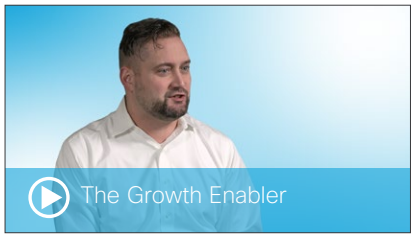
Source: Cisco, 2016

them to respond nimbly to rapidly changing markets. This agility makes them more effective and drives enhanced financial performance.

Cybersecurity excellence also gives firms the opportunity to differentiate their brands by conveying a strong perception of customer trust. When prospects and customers trust that security and privacy breaches will not occur, that trust becomes an important brand attribute—similar to quality, cost, and customer experience. Firms can then achieve competitive advantage by promoting this capability to prospects and customers.[17]

These benefits are beginning to impact how finance executives invest in cybersecurity. Today, the "ability to enable business growth" accounts for one-third of the decision criteria weighed when considering cybersecurity investments. Defensive criteria such as threat protection and regulatory compliance account for the remainder (see Figure 8, next page). As companies come to recognize that cybersecurity excellence can boost agility, operations, and digital fluency, we expect that "growth enablement" will become a more influential factor in the investment decision.

Although Gartner predicted a decline in corporate IT budgets during 2015, [18] companies are placing a new priority on cybersecurity investments. Eighty-seven percent of companies say they are increasing cybersecurity spending in the next year—41 percent "significantly." Financial executives we interviewed said that it is becoming easier to get cybersecurity projects funded because the benefits are understood better.



For more insights, please visit cs.co/cyberMD

Figure 8
Cybersecurity's potential to spur growth is an important criterion in investment decisions

Source: Cisco, 2016

"There's not a rule book here.... You've got to look at the crisis-level potential of the risks, as well as the growth opportunities. I think the allocation formula is something we struggle with."

—Robert Simmons, CFO

Companies would invest even more in cybersecurity, however, if they could quantify the value of its benefits. In fact, 81 percent of financial executives said they would be "much more" or "moderately more" likely to increase their cybersecurity spending if they had a better way to measure these business outcomes.

Our respondents acknowledged they struggle to find the right metrics. Although 88 percent of companies use defined metrics such as "top-line growth" and "profitability" to quantify the contribution of cybersecurity to positive business benefits, just 42 percent find these metrics "very effective." This falls far short of what companies demand when justifying costly strategic investments to their management and stakeholders.

As a result, most companies are likely underinvesting in cybersecurity. In fact, our survey respondents said that underinvestment is one of the biggest management challenges they face, along with keeping pace with the rapidly evolving digital business environment and ineffective enforcement of cybersecurity protocols.[19]

For more insights, please visit cs.co/cyberRS

Cybersecurity Enables Innovation and Growth from More Than 400 Digital Use Cases

Cisco has identified 414 digital use cases that will drive $7.6 trillion in Digital Value at Stake over the next decade (see "Placing a Value on Security" for details).

To capture your share of this value, you must get the defensive side of cybersecurity right first. Seven specific defensive use cases will deliver $1.8 trillion in Digital Value at Stake over the next 10 years. These include protection of intellectual property, reduction of compromised data (both internal and customer information), increased business uptime and reduced network downtime, protection of financial assets, safeguarding of sensitive government/national/political information, and preservation of business reputation.

The biggest opportunity, however, comes from making cybersecurity the critical foundation of 407 digital use cases that enable innovation and growth. Cisco estimates that these digital use cases will drive $5.8 trillion in Digital Value at Stake from 2015–2024 (see Figure 9).

How did we determine this value?

Our study revealed that cybersecurity vulnerabilities and concerns are making many organizations reluctant to pursue digital products and services. In some cases, cybersecurity worries are forcing them to halt mission-critical initiatives entirely.

This has a quantifiable cost—the value private and public sector organizations are "leaving on the table" by ceding digital innovation to more nimble competitors. We measured the degree to which these concerns are preventing organizations from realizing the value of more than 400 potential digital use cases over 10 years (2015–2024).

Based on the degree of cyber risk associated with each use case, the analysis assumed various degrees of adoption lag—ranging between one and five years. The higher the risk, the longer it takes to address

Placing a Value on Security

Digital Value at Stake is based on two components: 1) entirely new sources of value emanating from digital investments and innovations; and 2) value shifting among companies based on their ability (or inability) to harness digital capabilities.

Cisco calculated the Digital Value at Stake by taking a "bottom-up" approach using the sum of the value created by more than 400 private and public sector digital use cases over the next 10 years (2015–2024). Value at Stake is based on net value: for each use case, we considered both benefits and costs.

Our use cases reflect the projected result of a business application of technology—in this case, business transformation driven by the digital economy/digitization. This differs from typical "case studies," which represent the actual results of the application of technology. Cisco's Digital Value at Stake calculation encompasses both industry-specific and cross-industry use cases.

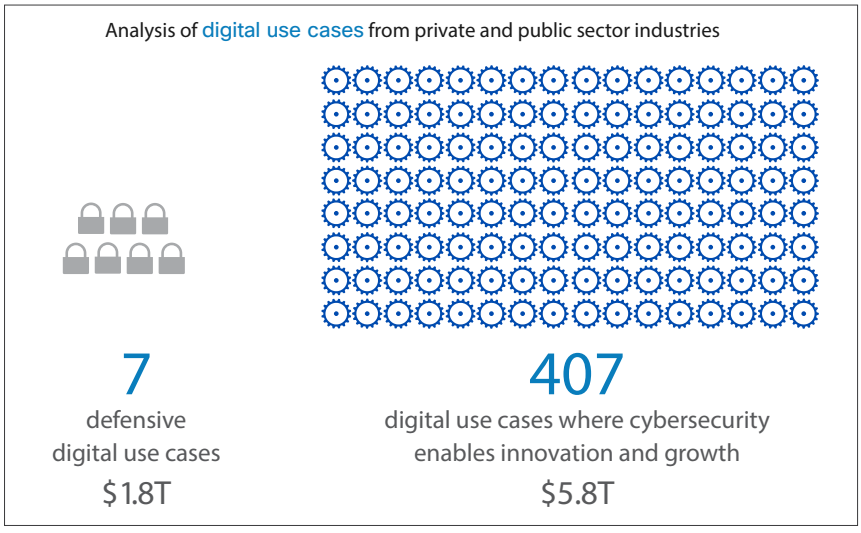


Figure 9
76% of cybersecurity's digital value is tied to innovation and growth

Source:
Cisco, 2016

and overcome perception issues. This risk could inhibit growth initiatives that rely on digital capabilities—and slow the pace of innovation and digital transformation.

Therefore, our admittedly conservative $5.8 trillion "growth" estimate would be even larger if it weren't for cybersecurity fears that will cause some companies to delay digital projects.

Manufacturing

Consider the manufacturing industry, for example. Figure 10 shows the potential impact of cybersecurity risks and adoption lags related to the seven use cases that will drive most of this industry's Digital Value at Stake over the next decade. All of these use cases require manufacturers to instrument their operating environments with digital capabilities related to the Internet of Things, analytics, and more. Manufacturers must have confidence in their cybersecurity to do this. If not, they will miss out on value.

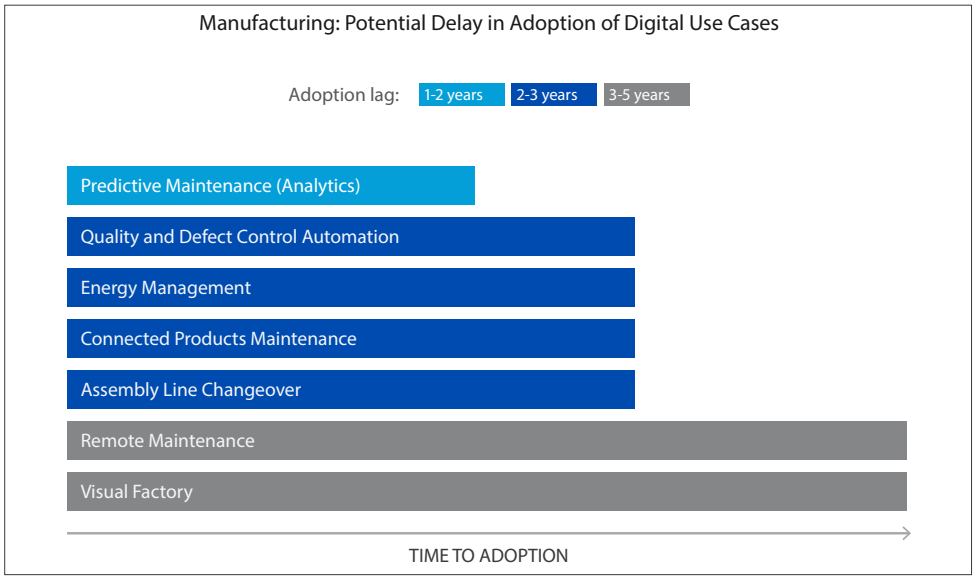


Figure 10
When cybersecurity concerns delay digital initiatives, growth potential and market position suffer

Source: Cisco, 2016

Analytics-driven predictive maintenance is a critical digital use case for manufacturers to implement in order to remain competitive. Most manufacturers, however, do not have the expertise to run—yet alone write—the algorithms needed for predictive maintenance. As a result, they are looking to their partners (machine builders, controls vendors, and so forth) for this capability. This could be either on-premise, or off-premise in a cloud-delivered offering—a new and scary concept for manufacturers.

Based on the perceived level of cybersecurity risk associated with this use case, we estimate a one- to two-year adoption lag for manufacturers. Looking at it another way, if cybersecurity concerns cause manufacturers to delay implementation of this particular use case, it could take them one to two years to catch up to competitors who have already adopted it. By delaying implementation, manufacturers miss out on capturing their share of the estimated $418 billion in global Digital Value at Stake that predictive maintenance (analytics) will drive over 10 years. As a result, they lessen their ability to innovate and grow.

At the other end of the spectrum is the *remote maintenance* use case.

Remote maintenance sometimes requires that companies open their networks to outside vendors. These vendors need to access the company's machinery and data so they can identify and resolve issues. Historically, machines have not been connected to internal networks. Therefore, the idea of providing Internet-based access to machines represents a paradigm shift for many companies' business operations. Operators, however, recognize the need for remote maintenance: it can minimize machine downtime by allowing companies to fix problems over the network, versus having to send a repair expert to a specific location.

Centralized remote maintenance systems carry high levels of risk because breaches can cause significant system downtime. For example, hackers could wreak havoc on a factory's control and automation systems, posing large competitive challenges if undetected for an extended period of time. Consequently, Cisco estimates that it could take up to five years to address and overcome perception issues associated with cybersecurity weakness for the remote maintenance use case. The result is a weakened market position and stifled growth.

The following examples show how cybersecurity helps create value in other industries:

Financial Services: *Mobile Payments*

Financial institutions are built on customer trust. In particular, the mobile payment business depends entirely upon consumer confidence. Firms must be able to prevent security breaches—and detect and remedy them quickly if they occur. Mobile-payment security breaches can result in downtime, lost revenue, diminished business reputation, retribution costs to remedy the damage, and loss of financial data.

What's at stake? With the proper cybersecurity capabilities in place, mobile payments will generate as much as $396 billion across industries from 2015-2024.

Retail: *In-store Analytics*

In the retail industry, in-store analytics is about improving workforce efficiency through dashboards, real-time information, operational analytics, workforce management tools, and shopping analytics. Cybersecurity is a key enabler: information quality and privacy are critical to ensure the source of insights is robust and the information has not been compromised.

A potential security breach could result in loss of customer information, as well as tainted data. Customers could also lose confidence about sharing personal data with the retailer, making analytics less informative and pervasive.

With the proper cybersecurity foundation, in-store analytics has the potential to generate $285 billion in digital value from 2015-2024.

Oil & Gas: *Oil-spillage Control*

When digital oil-control systems are inaccessible, oil spills can go undetected for extended periods of time. Many of these remote systems are not

connected. Or, they're connected "on demand," which can cause a delay from the time an issue occurs to when it's resolved. The results are increased litigation, cleanup, and system-downtime costs.

Cisco has determined that cybersecurity plays a "defining" role in the oil-spillage control use case. As a result, cybersecurity concerns could result in a three- to five-year adoption lag.

With the right connections and cybersecurity practices, oil-and-gas firms can "light up" their "dark" (unconnected) assets and grab part of the $16 billion in digital value that oil-spillage control will drive from 2015-2024.

Innovation, value, and growth all depend on organizations' ability to build cybersecurity *into the foundation* of their digital strategies. Our study uncovered a new market segment—the *Secure Digitizers*[20]—that seems to be doing this more effectively than anyone else.

Secure Digitizers Capitalize on Cybersecurity and Compete To Win

To compete more effectively with disruptors and improve their cybersecurity, established companies must pursue digital business *transformation*.

True digital transformation means *organizational change* driven by digital technologies and digital business models. It gives established companies the opportunity to redefine the way they create value for customers, and to change their operations and value chains to deliver in a more agile fashion. Companies can use digital technologies—most notably Big data and analytics, IoT, and cloud computing—to make the types of exponential improvements that give disruptors such marked advantages.

Digital transformation also demands that organizations build cybersecurity into their plans from the earliest stages.

For example, mobile payments company Square includes cybersecurity experts in all of phases of its product design. Advanced cybersecurity is considered an essential criterion, rather than being "bolted on" at the end of product development. The same is true when the company designs new internal processes. Nothing is done at Square without cybersecurity experts actively collaborating with executives and designers. In essence, digital transformation allows companies to build new, digitally enabled processes that do the job better, with cybersecurity baked in from the start.

Most of the executives we surveyed understand that further digitization of their business gives them the opportunity to improve cybersecurity while redesigning their business processes to make them more agile. In fact, 69 percent said that cybersecurity concerns have made them more willing to pursue their digital agenda.

New Market Segment

'Secure Digitizers' Show the Way

Over a quarter of Cisco's survey respondents are pursuing digitization with particular urgency—partly because they understand that digitization *can improve their cybersecurity*.

This market segment, which we've dubbed the "Secure Digitizers," is strongly committed to growth through digital business models and offerings, with cybersecurity as a critical foundation. As a result, they tend to manage cybersecurity more proactively than our other respondents. They are also much more likely to measure the business impact of security across multiple fronts.

Secure Digitizers have higher confidence in the security of three key digital capabilities: Big Data/analytics, cloud, and the Internet of Things. This confidence makes them more willing to pursue digital offerings, thereby accelerating innovation and time to market.

By emulating the Secure Digitizers, firms can tackle cybersecurity challenges, innovate with greater confidence, and improve their competitive position.

"Digital transformation can make you more secure if you build cybersecurity into your business processes right from the start."

—President, Cybersecurity Consulting Firm

A subset (28 percent) of all respondents, however, is pursuing digitization with particular urgency. This group understands that it can improve cybersecurity through digital transformation. These "Secure Digitizers" appear best positioned to contend with digital disruptors and outcompete other incumbents because they are strongly committed to growth through digital business models and offerings (see Figure 11 and "'Secure Digitizers' Show the Way" on previous page).

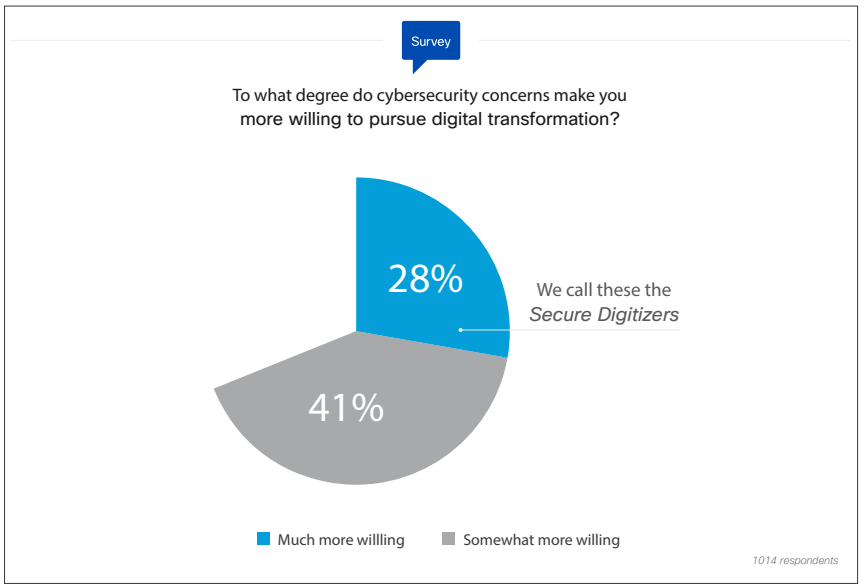


Figure 11
Cybersecurity demands prompt some companies to accelerate their digital transformation

Source:
Cisco, 2016

Ninety-five percent of all Secure Digitizers say that digital is very important to their current growth strategies, and 89 percent believe it will be "much more important" for growth in the next two years, compared with 58 and 35 percent, respectively, for other established companies.

Secure Digitizers are much more engaged in cybersecurity issues than their peers: 66 percent strongly agree that cybersecurity is their responsibility, versus 31 percent of their peers. In part, this is because the CEO, corporate board, and other key stakeholders hold them responsible for cybersecurity issues, even though they do not hold IT or technical roles.

Because Secure Digitizers rely heavily on digital business models and offerings to drive growth, they recognize that cybersecurity concerns can hold back innovation, and hinder growth. Thus, they are taking aggressive steps to improve their cybersecurity as they transform themselves.

As a result, they undertake digital projects with greater confidence. This allows them to innovate faster and capture a greater share of Digital Value at Stake. In fact, 62 percent of Secure Digitizers report they are performing much better than their peers in terms of revenue from new products and services. Only 33 percent of non-Secure Digitizers can make the same claim.

How To Make Cybersecurity the Foundation of Your Digital Strategies

In an era of constant disruption and continual innovation, the ability to use cybersecurity as a means to improve strategic agility and operational excellence will serve as a key differentiator for companies hoping to accelerate their growth. When thinking about how your company's cybersecurity practices can evolve, consider these best practices of the Secure Digitizers:

1. Turn cybersecurity into your growth advantage. Secure Digitizers take ownership of cybersecurity: 80 percent are "very concerned" about cybersecurity, compared to 36 percent of all others; 83 percent are expected to assume responsibility for cybersecurity "to a great degree," compared to 39 percent of all others; and 66 percent strongly agree that "as a leader, I consider cybersecurity to be my responsibility," compared to 31 percent of all others.

   As a result, their approach to cybersecurity is more proactive. For example, 66 percent employ dedicated cybersecurity resources, compared to 42 percent of other respondents; 65 percent provide funding for cybersecurity initiatives, versus 41 percent of all others; and 65 percent actively incorporate cybersecurity tools and best practices into their operations, compared to 47 percent of all others (see Figure 12).

For more insights, please visit cs.co/cyberSD

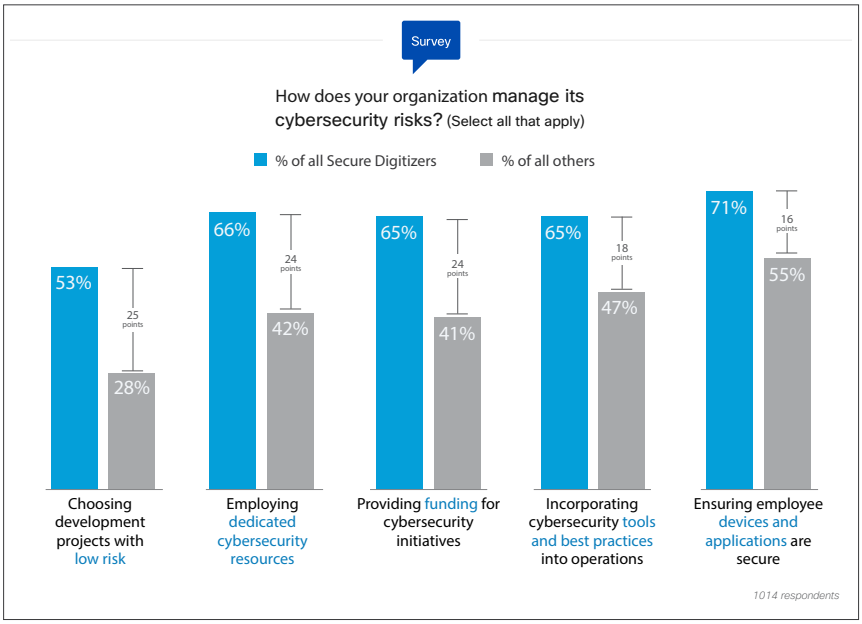


Figure 12
Secure Digitizers manage cybersecurity more proactively

Source:
Cisco, 2016

2. Mitigate risk by choosing projects with a high opportunity-to-risk ratio, not just a low-risk profile. Secure Digitizers take more risks, but the rewards outweigh the costs.

   Fortunately, there are many digital use cases with a high opportunity-to-risk ratio—starting with cybersecurity itself. Other mature digital capabilities that are already delivering proven value include remote collaboration, Center of Excellence support functions, improved oil-recovery efficiency (oil and gas), omnichannel capabilities and sales-and-service transformation (financial services), and predictive maintenance analytics (manufacturing).

   As Mike Dahn, head of data security solutions at Square, explained, "A lot of the times we talk about cybersecurity risk, but really, one of the things that we could be talking about is security enablement.

   "With the explosion of devices, we have both a potential risk but also a potential opportunity, he continued. "I think that the risk is always going to be present. We should be aware of it, but we need security minds to start thinking away from the old model of defense-centered thinking into the new model of security enablement. That's really the heart of innovation, where we start looking at products and instead of saying, 'How do I need to secure them?' we say, 'How can these products be used to secure us?'"

   Secure Digitizers feel more prepared than our other respondents to address cybersecurity challenges in three key digital technology areas—analytics, IoT, and cloud computing. As a result, Secure Digitizers are far more confident about incorporating digital technologies into their business processes and offerings (Figure 13).

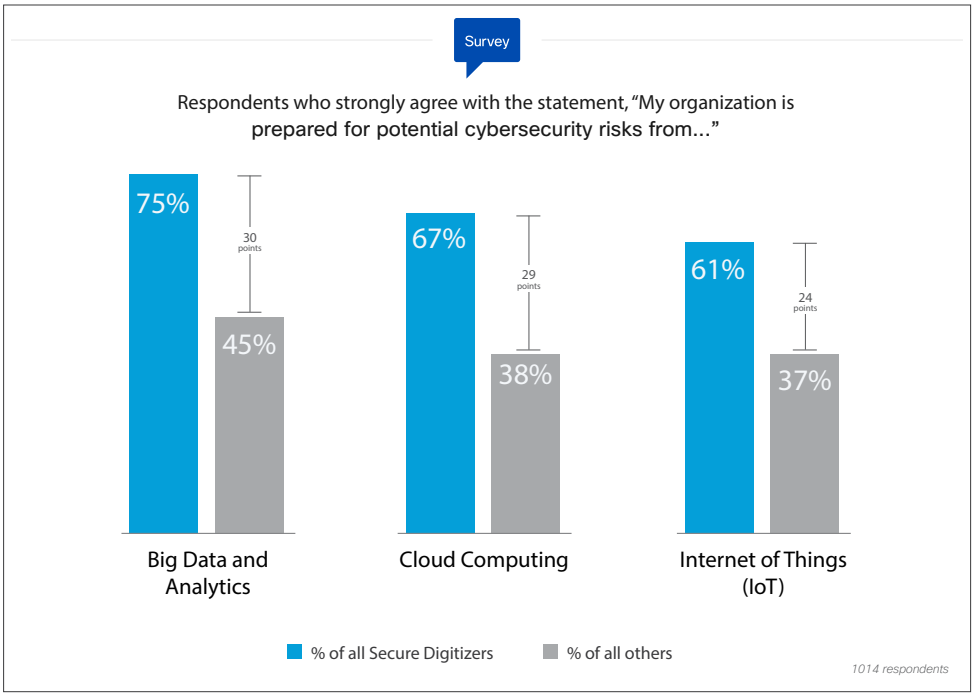


Figure 13
Secure Digitizers are much more confident in the security of their digital strategies

Source:
Cisco, 2016

3. Re-engineer digital processes with cybersecurity as the foundation. Cybersecurity itself is an engine for digital business transformation. As they evolve, companies must identify insecure technologies—and the business processes they enable—and replace them with new ones that integrate cybersecurity from the very outset. Secure Digitizers already do this far better than more established companies (see Figure 14). As Adriaan Bouten, CEO and founder of dPrism, pointed out, "If you don't deal with cybersecurity from the get-go, you will have a 'job and a half' fixing it later."

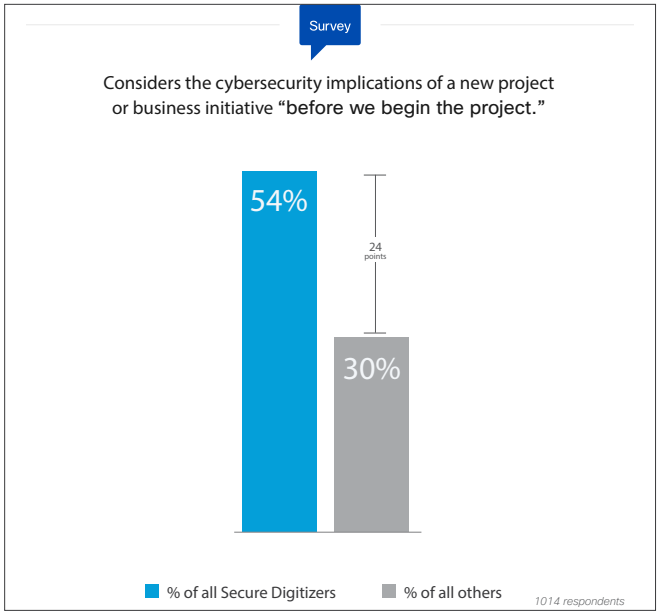


Figure 14
Secure Digitizers understand that cybersecurity is foundational

Source:
Cisco, 2016

4. Institute cybersecurity expertise at all levels of the company. The same proactive measures that help companies excel in cybersecurity can also boost product development, risk resilience, threat analysis, and response in other parts of your business. This argues for the inclusion of cybersecurity expertise in many disparate functions of your company, and for a mind-set that anticipates cyber threats in order to inform other aspects of your company's strategic planning and operations.

   "Ownership spans from the board all the way to the cleaning crews and everyone literally in between," explained CFO Robert Simmons. "This is not the domain of IT anymore. I think the sooner companies can come to that realization, the better position they'll be in to put these sort of programs in place for the current digital age."

5. Measure what you treasure. Seventy-five percent of Secure Digitizers have very detailed processes for determining the effectiveness of cybersecurity initiatives on their functional organizations, versus 21 percent of other companies. These processes measure a wider range of inputs, including the effect on digital assets and the right level of cybersecurity investment (see Figure 15, next page).

   Measuring the impact of cybersecurity protections makes executives more aware of threats to the company's operations and strategic assets. It helps build the case for additional investments to enhance protections.

   Sixty-five percent of Secure Digitizers say they can measure these business benefits "very effectively." That's something only 30 percent of other companies claim. This helps explain why more than twice as many Secure Digitizers expect to increase cybersecurity spending in the next year (64 percent versus 31 percent).

For more insights, please visit
cs.co/cyberMD2

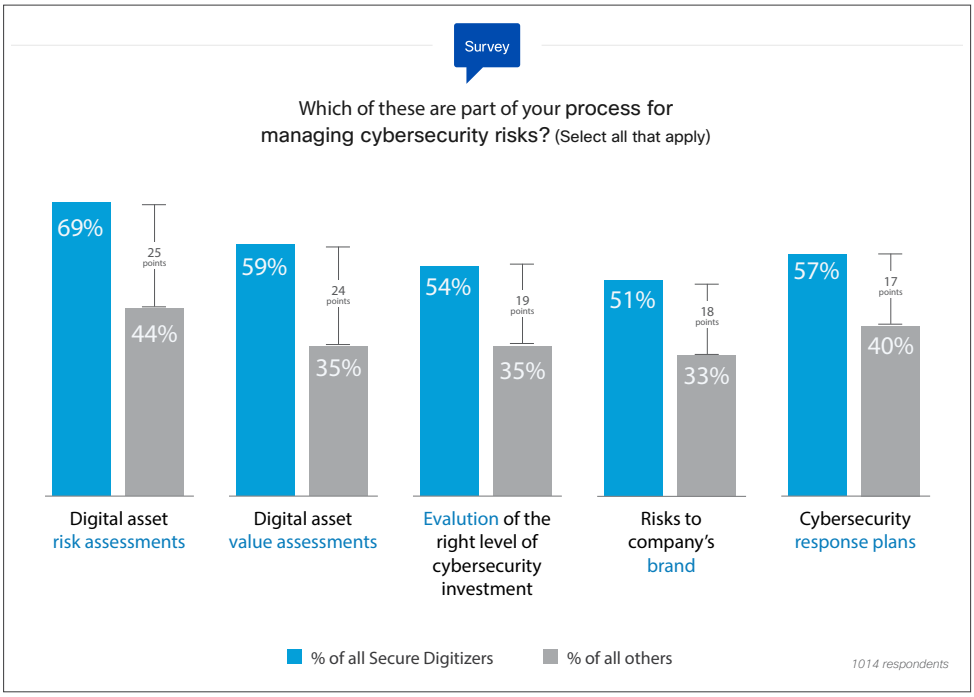


Figure 15
Secure Digitizers are much more confident in the security of their digital strategies

Source:
Cisco, 2016

To understand how much to invest, businesses need to measure the value of what they are protecting:

"It's about understanding the risks associated with protecting the information that needs to be protected, but also understanding the value of that information to the organization should it fall into the wrong hands," explained Steve Durbin, managing director of the Information Security Forum. "You're starting from the standpoint that says, 'There is a very good chance we'll lose some of my information at some point in time. How valuable is it? How difficult do I now need to make it for people to gain access to it from outside the organization? That then translates into your resource focus and your spend associated with protecting that information."

Effective measurement requires a methodology that quantifies both the gains and losses associated with cybersecurity. Too often, firms fail to establish objectives that consider both the desired performance and the unintended consequences of the changes that new digital business strategies create.[21]

In an era of digital disruption, digital products and services are the necessary path to growth, even survival. Yet, because of sub-par cybersecurity practices, many companies are in a tough position: not innovating with the speed and confidence they need to win—and, due to competitive pressure, experimenting without the right cybersecurity practices in place. All the while, nimble disruptors—less burdened by legacy IT systems, and more likely to invest in cybersecurity as a growth enabler—speed ahead.

By following in the footsteps of the Secure Digitizers, you can boldly pursue digital innovations and increase your growth in the digital era.

"When you launch a new initiative, cybersecurity is included in your business case and project management process. You've got to hit all the buttons. You'll have milestones for data security. You'll have compliance people involved. Everyone has to sign off."

—Former VP of Human Resources, Fortune 100 Bank

1. To understand how medium- and large-sized firms incorporate cybersecurity into their businesses, we conducted an online survey of 1014 directors, VPs, and C-level executives in October 2015. Over a third (38 percent) of respondents had financial roles and cybersecurity financing influence. The remaining 62 percent of respondents came from a mix of line-of-business domains. They were moderately or very informed of cybersecurity strategy and practices in their companies, but were not in information technology or information security departments. The executives came from the following countries: Australia, Brazil, Canada, China, France, Germany, India, Japan, the United Kingdom, and the United States. In addition, we conducted qualitative, hour-long telephone interviews with 11 experts sourced from the GLG expert network. All were very senior executives (current and former) with extensive cybersecurity experience at established companies, in both finance and line-of-business roles. Of them, two were cybersecurity consulting experts.
2. Digital Value at Stake is based on two components: 1) entirely new sources of value emanating from digital investments and innovations, and 2) value shifting among companies and industries based on their ability (or inability) to harness digital capabilities (in essence, value moving from "losers" to "winners").
3. By "offerings," we mean the products and services companies provide. Sometimes, these offerings do not neatly conform to the typical definition of a product or service, and traditional business models. For example, digital disruptors are introducing offerings with unique consumption models, and via business models in which the offering itself is free, and revenue is generated by related activities. For an in-depth examination of the sources of value digital disruptors are creating, and the business models they are using to create them, see New Paths to Customer Value: Disruptive Business Models in the Digital Vortex, Global Center for Digital Business Transformation (the DBT Center), an IMD and Cisco initiative, November 2015.
4. In contrast to startups and other agile digital disruptors, "established companies," or "incumbents," have large numbers of employees, tend to have traditional value chains, and own more of their own productive assets than startups. Cisco's survey focused exclusively on established companies: all of them had at least 500 employees. Eighty-three percent were enterprises with at least 1000 employees, including 19 percent with at least 10,000 employees.
5. By "digital," we mean the convergence of multiple technology innovations that are enabled by ubiquitous, high-speed connectivity. These technology innovations include Big Data and analytics, cloud computing, the Internet of Things (IoT), mobility, social media, and machine learning. For the definition of "digital" and related terms, we use Defining the Digital Vortex, developed by the DBT Center.
6. We define "digitization" as generating or converting information that can be used and shared by digital technologies. Digitized information is the foundation of digital business processes and business models. See "Defining the Digital Vortex," DBT Center, December 2015
7. The Digital Vortex: How Digital Disruption Is Redefining Industries, Global Center for Digital Business Transformation, June 2015.
8. Disruptor and Disrupted: Strategy in the Digital Vortex, Global Center for Digital Business Transformation, November 2015.
9. In 2014, over a billion records were compromised, up 54 percent year-on-year, largely due to massive retail breaches. In the first half of 2015, the number of breaches increased 10 percent versus 2014H1, but overall number of records compromised was down 41 percent to 246 million records. Gemalto, September 2015; ZDNet, January 2016.
10. "Data and Dollars: The Role of the CFO in Cybersecurity," Steve Durbin, Managing Director, Information Security Forum, Connected Futures.
11. Fast IT: Accelerating Innovation in the Internet of Everything Era, Cisco, 2014.
12. "2015 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2015.
13. "Businesses Braced for Bout of Regulation on Cyber Security," Financial Times, and "New York Bank Regulator Details Cybersecurity Regulations," The Wall Street Journal, November 2015.
14. "The Digital Vortex: How Digital Disruption Is Redefining Industries," Global Center for Digital Business Transformation, June 2015.
15. In another study, when asked "What keeps an organization from being innovative?" 28 percent of respondents answered "Belief that innovation increases security risk." See "Risk & Innovation in Cybersecurity Investments," Ponemon Institute LLC and Lockheed Martin, April 2015.
16. This finding aligns with those of a recent study conducted by Ping Identity ("Secure Access for the Digital Enterprise," Ping Identity, 2015), which revealed that security is the top challenge to adopting digital technologies for 51 percent of enterprises, and that 78 percent of enterprises delayed their move to cloud due to security concerns.
17. "Seven Ways CEOs Can Apply Digital Business for Competitive Advantage," Hung LeHong, Gartner, June 2015.
18. According to Gartner, worldwide IT spending declined in 2015.
19. When asked to identify their biggest cybersecurity management and policy challenges, 32 percent of Cisco's survey respondents selected "Inability of cybersecurity policy to keep up with the pace of business change"; 27 percent selected "Lack of the right metrics to determine cybersecurity effectiveness"; 26 percent selected "Insufficient investment in cybersecurity"; and 24 percent selected "Ineffective enforcement of cybersecurity policies." Increased cybersecurity investment overall is not a cure-all: to maximize value, companies must prioritize investments in initiatives that have defined metrics for success, and that are managed effectively.

Acknowledgments

The authors gratefully acknowledge the contributions of the following people to the development of this paper: Debbie Abbott, Caroline Ahlquist, Sara Aiello, Kevin Bandy, Ruba Borno, Kristine Briggs, John Choi, Lynne Cox, David Goeckeler, Dan Gould, Gene Hall, Amy Henderson, Lisa Lahde, Rob Lothman, James Macaulay, Melissa Mines, James Mobley, Bryan Palma, Robert Pepper, Caroline Robertson, John Stewart, Ann Swenson, Greg Thomas, Virgil Vidal, Michael Zielenziger, and Elisabeth Zornes

20. Secure Digitizers are a new market segment identified by Cisco as part of this research study. Market segmentation involves dividing a broad target market into subsets of businesses that have, or are perceived to have, common needs interests, behaviors, and priorities.
21. "Using Risk-Adjusted Value Management to Close the Strategy Gap and Gain Competitive Advantage," Michael Smith and Paul E. Proctor, Gartner, December 2015.

C45-BCI0416-00 04/16