Harvard Business Review
ANALYTIC SERVICES

Pulse Survey

MANAGING CYBER RISK

Understanding the Opportunity

Sponsored by

JLT

SPONSOR PERSPECTIVE

An illusion of control pervades businesses when it comes to managing cyber risks. As cyber attacks grow in scale and severity, no organization—not even those whose core business is handling volumes of data and that have invested heavily in cyber-security—are immune. Why do most organizations remain exposed to the business impact of cyber events? To attempt to answer this question, JLT sponsored a survey that was administered to corporate executives by Harvard Business Review Analytic Services.

The research findings confirmed our observations—a critical element in mitigating the business impact of cyber risk is to approach it strategically.

The survey found that there is almost a universal agreement among corporate executives that the financial impact of cyber risks will continue to rise. There is also broad support from boards and senior management for improving cybersecurity and organizational awareness. More organizations are training employees about cybersecurity and allocating budgets and resources to it. Even so, a small percentage considers their organizations well prepared for cyber risks. What is the piece that is missing in our efforts?

Despite greater awareness, support, and resources devoted to cybersecurity, organizations continue to be exposed to cyber events. The Harvard Business Review Analytic Services research offers a telling reason for this: few organizations are treating cyber as a strategic business risk.

In the research, respondents said they are concerned about cyber risks harming their day-to-day operations, future business prospects, relationships, and reputation. Those are exactly the kinds of risks that require a strategic focus and the involvement of business leaders at all levels of an organization.

It is our hope that this research will be a starting point for organizations to redefine cyber as a strategic business risk and begin to approach cyber risks differently, and to maximize opportunities to mitigate this growing threat.

MICHAEL D. RICE
CHIEF EXECUTIVE OFFICER
JLT SPECIALTY USA

MANAGING CYBER RISK
Understanding the Opportunity

It Can Happen Here

Cyber threats are multiplying, and coming from all sides. And they are costly.

In June, the digital security solutions supplier ESET discovered a malware known as Win32/Industroyer that was capable of carrying out an attack on power supply infrastructure. It was likely involved in the December 2016 cyber attack on Ukraine's power grid that halted power to Kiev for over an hour. Then in September, Equifax revealed that hackers gaining access to the company's systems had potentially seized personal data including Social Security and driver's license numbers for 143 million Americans.

As these examples suggest, even large, sophisticated, data-centric organizations can learn—abruptly—that they have only an illusion of control over cybersecurity. To better understand how organizations worldwide are responding to threats from cyber attacks and breaches, and in particular the degree to which they are incorporating these issues into their strategic planning, Harvard Business Review Analytic Services surveyed 278 individuals in a wide range of industries, roughly evenly split between large organizations with 10,000 or more employees and those with fewer. SEE METHODOLOGY, PAGE 16 Harvard Business Review Analytic Services also conducted one-on-one interviews with a group of thought leaders in the field.

Larger organizations, the survey found, are more alert to the issue: 65% regard cyber attacks and breaches as a significant or very significant threat to their reputation compared with less than half (46%) of smaller organizations. In neither group, however, are most organizations fully prepared for a cyber attack or breach. Only 14% of respondents from smaller organizations agreed that their employer is fully prepared, but even among their counterparts from larger organizations, only 39% agreed. FIGURE 1 The study yielded other key findings:

- Survey respondents are concerned about their ability to respond despite putting structures in place to address cybersecurity issues, and many lack the resources to make those structures work optimally.
- Cybersecurity threats pose risks not just to daily operations but to the organization's broader strategic goals.
- However, many organizations are not approaching the issue strategically to create effective, cross-functional responses to this business risk.
- Most organizations do not understand the magnitude of the threat that cyber attacks and breaches pose and are not calculating the possible cost of such attacks.

HIGHLIGHTS

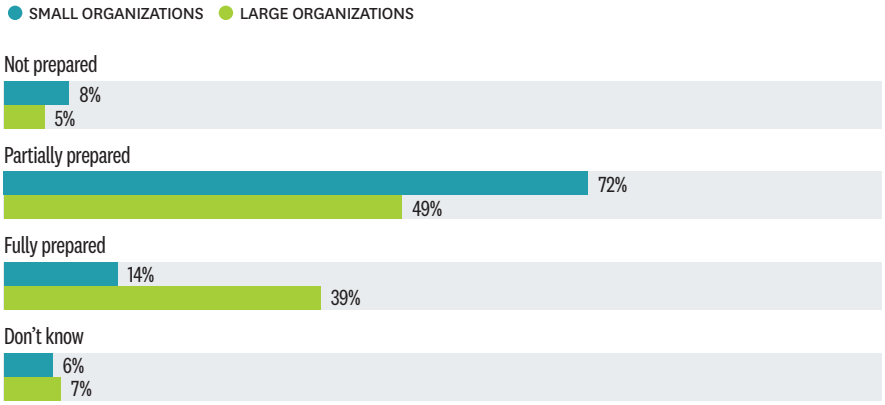
85%
OF SURVEY RESPONDENTS SAID THEY EXPECT THE FINANCIAL IMPACT OF CYBER ATTACKS AND BREACHES TO RISE IN THE NEXT ONE TO TWO YEARS.

ONLY 23%
RESPONDENTS HAVE ADOPTED A FORMAL STRATEGIC PLAN TO ADDRESS BUSINESS RISKS FROM CYBER ATTACKS.

FIGURE 1

LESS THAN PREPARED

In your view, how well prepared is your organization to respond to a cyber attack or breach?



SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

RESPONDENTS SEE CYBER ATTACKS AND BREACHES AS THREATS NOT JUST TO THEIR DAY-TO-DAY OPERATIONS BUT TO THEIR FUTURE BUSINESS PROSPECTS, RELATIONSHIPS, AND REPUTATION.

As a result, few organizations are achieving "maturity in cybersecurity," which includes training all levels of the organization, including employees and first-line leaders, to detect and respond to risks; establishing a strategic plan for cybersecurity; and incorporating cybersecurity into the organization's vision and risk appetite statements.

This must change. As reliance on digital technology continues to grow, businesses will only see their vulnerability increase. One recent estimate placed the average cost of a future global attack at around $53 billion, although estimates range as high as $120 billion.[1] Under one scenario, a single malicious hack taking down a cloud service provider could deliver anywhere from $15 billion to $121 billion in losses.[2]

Cybersecurity is both an operational and a strategic business risk of the highest order and a threat to the organization's competitiveness; its customer and client relationships; its ability to function, possibly for long periods; its ability to capitalize on the opportunities the digital age would otherwise afford it; and its bottom line. And concern is rising.

Threats Are Serious and Growing

Overwhelmingly, survey respondents regard cybersecurity threats as serious and growing—and expressed concern about their ability to respond to a major attack. Eighty-five percent expect the financial impact of cyber attacks and breaches to rise in the next one to two years. The survey found little variation between larger and smaller organizations on this point. FIGURE 2

Respondents see cyber attacks and breaches as threats not just to their day-to-day operations but to their future business prospects, relationships, and reputation. More than three-quarters mentioned reputational damage (79%) and disruption of business operations (75%) as significant or very significant risks, followed by increased legal and regulatory costs (60%), lost business and/or investment opportunities (58%), and risk convergence and cascading effects (57%). Large percentages of

respondents also cited lawsuits or the threat of lawsuits (52%), damage to supplier and other third-party relationships (51%), inability to capitalize on present and future digital innovations (42%), and product liability (42%). Any and all of these consequences of a cyber attack or breach could have a negative effect on the company's earnings and share price.

Most organizations are taking some measures to create an organization-wide response to cyber threats. Three out of five respondents (60%) say their organization has developed and implemented a risk model or models. Most are not yet taking the next step and calculating the cost, however. Only 40% have attempted to quantify the business impact, in financial terms, of cyber attacks and breaches—while 29% have not and 31% of respondents to this question said they don't know. And, most troubling, almost one-third (29%) said applying resources to cyber-security risks is not regarded as clearly worth the investment, indicating that while most organizations aim to create a stronger response in the years ahead, many others will fall behind.

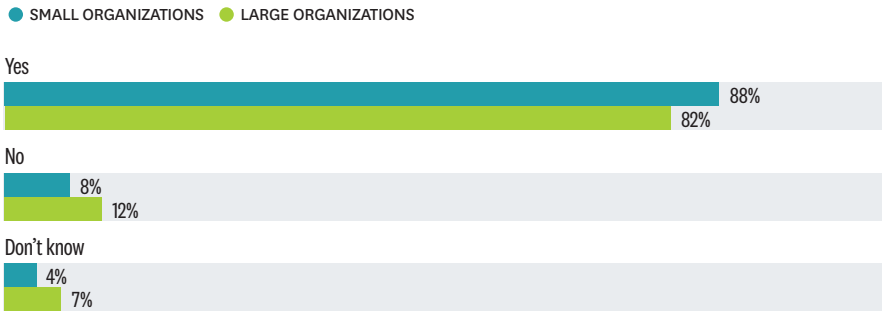
A clear pattern emerges from the survey findings and interviews: larger organizations are both more concerned and more likely to be taking action to prevent, mitigate, and respond to cyber threats.

"Where are we in the evolution of cyber risk management? Organizations that are defending against real-time threats and reporting effectively through the CISO [chief information security officer] to the board are more toward the sophisticated end of the scale," says the chief technology officer at a data security firm. "Smaller companies are still reactive, while larger companies have more structure and are more proactive."

FIGURE 2

FINANCIAL IMPACT RISING

Do you expect the financial impact of cyber attacks and breaches to rise in the next one to two years?



Numbers may not total 100% due to rounding.

SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

Failure Points

The challenge they all face is formidable. Cyber attacks have many more channels to penetrate than previously, both within the organization itself and between its suppliers, customers, and the myriad other digital users with which it interacts. Cyber threats that exploit failure points can create cascading risks at all levels—across national and global economies, across industries, and within companies themselves. Substantial numbers of respondents cited malware (52%), attacks (such as spear-phishing) that trick the user into providing sensitive information (41%), ransomware (33%), and breaches due to human error (33%) as having affected their organization in the past one to three years. Respondents expect these four categories to increase at the fastest rate in the next few years as well.

Perhaps more troubling, some threats that respondents cited less frequently are expected to loom much larger in the years ahead. Counterfeit goods, pirated software, and theft of trade secrets cost the U.S. economy as much as $600 billion annually, an amount comparable to the current yearly level of U.S. exports to Asia, the independent Commission on the Theft of American Intellectual Property concluded in a 2017 review.[3] Yet only

As disruptions become more frequent, governments and supranational bodies are **under pressure to enforce standards** aimed at curbing them.

21% of survey respondents said that theft of intellectual property or other confidential information has affected their organization in the past three years, and less than half (42%) said this threat is increasing. The same is the case for DDoS attacks (from 16% to 21%), attacks targeting third-party resources (e.g., cloud service providers, from 9% to 28%), attacks targeting IoS devices (from 1% to 15%), internal attacks (from 6% to 14%), and attacks aimed at causing broad economic disruption (e.g., attacks on electrical grids, from 7% to 14%).

Social media may be among the next big threats as well, one interviewee adds, because of the ease with which criminals and pranksters can set up fake social media accounts, impersonating executives at the organization. Another cites the cloud: "I don't know that people fully understand what it means, and we really rely on our vendors" to use cloud-based computing services carefully.

In addition, cyber threats are generating legal and regulatory risks. As disruptions become more frequent, governments and supranational bodies are under pressure to enforce standards aimed at curbing them, the EU's General Data Protection Regulation (GDPR) being the most recent example. Companies that do not comply may face fines and other penalties—even when the problem did not originate with them.

Leadership Deficit

Many organizations are putting structural elements in place to address cybersecurity threats. More than three out of five respondents (62%) said their organization has a CISO—although the figure is much higher for larger (74%) than for smaller (50%) organizations—and 75% said they have an IT/information officer who is a primary sponsor or champion of the organization's cybersecurity strategy. Other executives/functions that play key roles include the chief security officer (35%), risk management (32%), finance/CFO (25%), compliance (22%), and legal/general counsel (22%). FIGURE 3

While top leadership is paying attention, it still may not be focused in the right direction, or giving the threat sufficient weight. "If the CEO and CIO are evaluating their cyber investment, and if their company wasn't attacked last year, they could conclude that they're doing great," says Alex Blau, vice president at ideas42, a New York-based nonprofit that studies and develops solutions based on behavioral science. "But they may have just been lucky or already had an invasion that they just didn't know about." Instead, the C-suite should "think about cybersecurity as an insurance policy. If your power generation system goes off-line from an attack, how long does it take you to get it back up? What are the costs associated with stopped operations? How much are you willing to invest to manage that risk?"

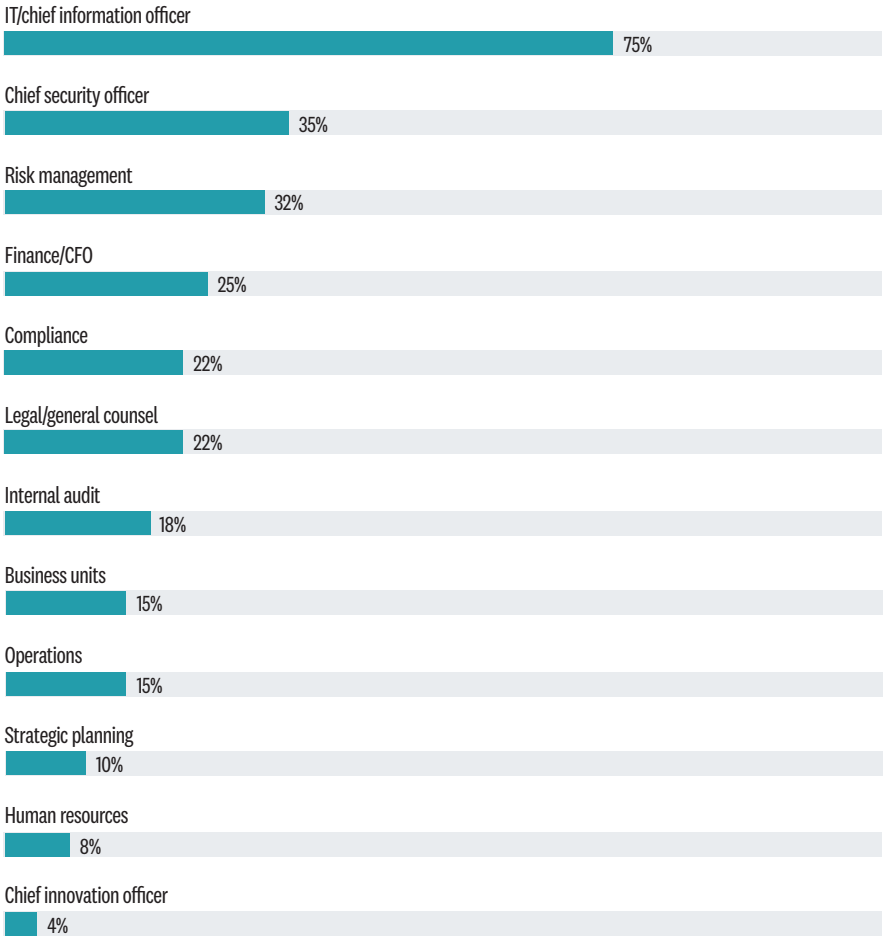
"Information security is a people and process issue, not a technology issue," says the CISO at a large global professional services firm. "The biggest thing you can do is to drive awareness of the risks and implications of an individual's actions." Getting the C-suite and board involved and committed to promoting more robust cybersecurity is critical, he says, "because it has a trickle-down effect on the rest of the organization."

The CTO argues that the importance of cybersecurity is such that companies should have a board member dedicated to overseeing it. While few companies are going this far, many are taking steps to keep cybersecurity issues in board

FIGURE 3

CYBERSECURITY CHAMPIONS

Which executives are the primary sponsors or champions of your organization's cybersecurity strategy?



SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

BOARD-LEVEL ATTENTION IS CRITICAL TO OBTAINING THE FOCUS AND RESOURCES CYBERSECURITY NEEDS WITHIN THE ORGANIZATION ITSELF.

members' line of sight. "I update the board three times a year, along with an educational session once a year," says the CISO at a large insurance company. "I also update them on any major incidents and issues; they've been actively engaged in determining whether we have the right resources dedicated to cybersecurity."

Board-level attention is critical to obtaining the focus and resources cybersecurity needs within the organization itself, and in this respect, most are making progress, the survey indicates. Less than one in five respondents (17%) said support at the C-suite and board levels is lacking. And while nearly half (49%) said their organization lacks the resources to properly address cybersecurity risks, almost two-thirds (64%) said it has increased the budget and resources it allocates to cybersecurity in the past three years and more than one-third (35%) said it plans to do so in the next one to two years. The numbers are much higher at larger than at smaller organizations, however. FIGURE 4

Many companies are **struggling to improve** internal collaboration and integration around cybersecurity threats.

What they are not doing in great numbers is pushing cybersecurity strategy and awareness deeper into the organization itself, where many attacks and breaches take place—and can be prevented. Only 15% of respondents said their organization's business units are primary sponsors of cybersecurity, and only 15% cited operations. This suggests that at most organizations, responsibility for cybersecurity is not being pushed down to the operational levels. Many companies are struggling to improve internal collaboration and integration around cybersecurity threats. More than one-third (38%) of survey respondents said internal collaboration at their organization is not sufficient. Only 20% said their functional teams (e.g., CISO, compliance, general counsel, CSO, procurement) are very integrated, and 37% said they are somewhat integrated—and the numbers are much lower for smaller than for larger organizations. More than one in four (27%) said these functions are only minimally integrated or not integrated. FIGURE 5

Some organizations, however, are pulling together key cybersecurity functions into a coordinated team to protect against cyber attacks and breaches. At a large global professional services firm, legal, compliance, and the CISO meet monthly, and the three functions keep in touch regularly in between. "Everyone helps to move the ball forward on all of our programs," the firm's CISO says. The insurance company has a six-member cybersecurity committee representing all the major functional areas and reporting directly to the chairman. The committee meets monthly to review policy and budgets for cybersecurity. "Ten percent of the budget is flexible, so that we can reallocate depending on how risks change, without going through a full budget process," the CISO notes.

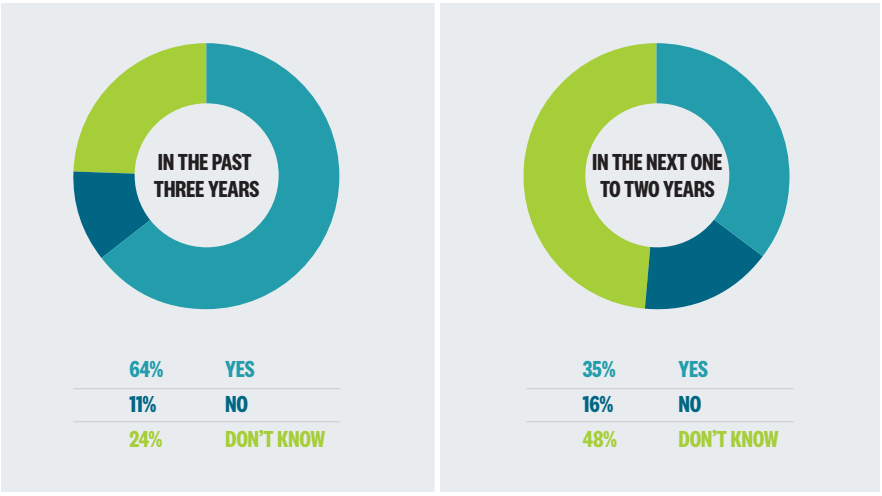
Defining the role of the CISO itself can be difficult; many come from a largely technical background and lack experience in business operations, according to Blau. At the same time, the C-suite and board often fail to consider the larger perspective the CISO can bring.

"They're seeing the CISO too often as a technical resource rather than integrated into the organization's broader risk concerns, combining operational thinking with business savvy," says Blau. "CISOs often have trouble getting boards and the executive suite to make the kind of investment they feel is necessary, especially in communicating how not acquiring or replacing a critical piece

FIGURE 4

CYBERSECURITY BUDGETS RISING

Has your organization increased the budget and resources it allocates to cybersecurity?

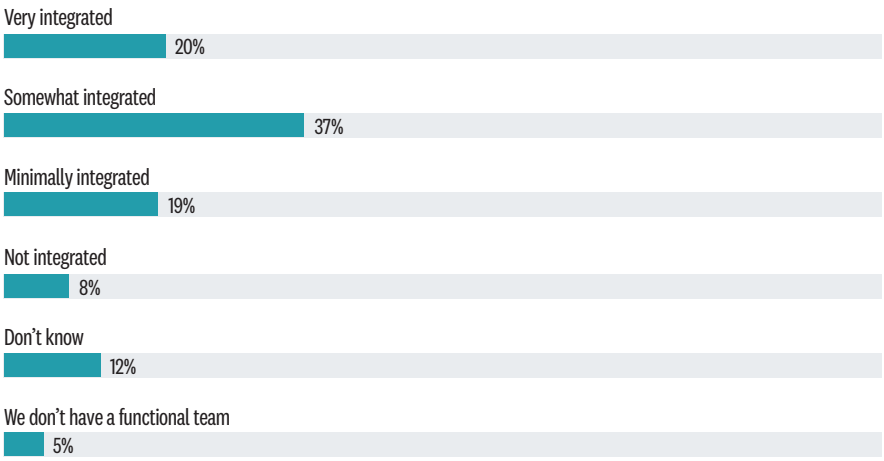


SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

FIGURE 5

STRUGGLING TO IMPROVE INTERNAL COLLABORATION

How integrated is your organization's functional team (e.g., CISO, compliance, general counsel, CSO, procurement) in protecting against cyber attacks and breaches?



Numbers may not total 100% due to rounding.

SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

of software might impact broader organizational risks the company may face."

Collectively, the survey findings suggest that many organizations still regard cybersecurity as a discrete problem to be delegated to IT specialists and compliance executives, rather than a business risk that must be addressed at every level. This creates problems—often catastrophic ones—not only for the organization itself but for its clients and customers when new products and services don't reflect best practices in cybersecurity.

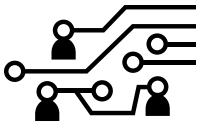
In May, for example, the WannaCry ransomware infection caused $8 billion in economic damage in more than 100 countries, while the NotPetya attack a month later could cost $850 million,[4] including disruption to the global operations of Merck; shipping giant A.P. Moller-Maersk, which estimated its own total cost of addressing the attack would be in the $200 to $300 million range;[5] and FedEx, which analysts forecast could see its earnings eroded by somewhere between 50 cents to $1 per share.[6]

"Fix It and Forget It" Won't Work

Cyber threats can't be pigeonholed as a technical risk; restricting the organization's response to patching weak points after breaches occur encourages a "fix it and forget it" approach, insufficient for a world where new weapons are being manufactured all the time. Repairing breaches, diagnosing them, and protecting against future attacks are insufficient when not done consistently. Likewise, while taking inventory of its digital assets helps the organization identify and respond to attacks, it's of little help when the inventory isn't updated regularly.

The technology that organizations rely on may itself bear some of the blame, says Blau, when they don't make sure that robust security features are embedded in it. Even improved security programs designed to block viruses and malware can contribute to the problem when they turn back automated tools intended to find and neutralize common flaws.

THE WANNACRY RANSOMWARE INFECTION CAUSED $8 BILLION IN ECONOMIC DAMAGE IN MORE THAN 100 COUNTRIES.



CREATING A STRONG COLLECTIVE RESPONSE TO CYBERSECURITY THREATS BEGINS WITH IDENTIFYING INTERNAL AND EXTERNAL VULNERABILITIES.

Creating a strong collective response to cybersecurity threats begins with identifying internal and external vulnerabilities that undermine the organization's capacity to anticipate and respond to specific threats. Internal vulnerabilities, like organizational complexity, are structural, often with very little technology component. External weaknesses, like interconnectivity with clients, vendors, and the digital marketplace, are both organizational and technological.

Our survey identified eight internal areas of vulnerability that half or close to half of respondents cited as significant or very significant:

- Organizational complexity (50%)
- Siloing of cybersecurity planning and response within the CIO and/or IT functions (49%)
- Inefficient, fragmentary, or sporadic data inventory and monitoring processes (48%)
- Failure to regularly update inventory of vulnerabilities (47%)
- Fragmented data management systems (46%)
- Lags in discovering and reporting cyber attacks (46%)
- Failure to patch publicly disclosed flaws promptly (45%)
- Failure to track employee access to data within the organization and manage growth in access points (44%)

Survey respondents rated the most significant external vulnerabilities even higher than those they recognized internally:

- Changing nature and motivation of attackers (68%)
- Changing types of attacks (65%)
- Increased sharing of information (65%)
- Interconnectivity with broader internet infrastructure (e.g., through customers and suppliers, 57%)
- Laxity or misuse of systems by third parties (51%)

There are plenty of steps that organizations can take—and, in many cases, are taking—to overcome these vulnerabilities. One large global professional services firm phishes groups of employees every month and places individuals on a list if they respond—"not a list you want to be on," says the firm's CISO. Conversely, employees who practice good cybersecurity are praised, encouraging others to work themselves into the virtuous circle.

Organizations with a wide network of suppliers and third-party relationships must treat these counterparties' vulnerabilities as their own. At the large insurance company, which engages a community of some 5,000 vendors, "we teach them cybersecurity, share intelligence and best practices, and give them mandatory controls they must implement," says the CISO. "We bring them together once a year for teaching, publish a newsletter, and send them relevant information continuously."

More comprehensively, the CTO says, organizations can shift from a strategy of responding piecemeal to cyber threats and breaches to one of "looking for the good." For some of its more "document-heavy" clients, the company takes every document it receives, transfers it to a new representation, and rebuilds it and regenerates it as a new document, eliminating any unwanted code—along with the need to search for any one strand in particular.

Companies need to update their controls often and shift to relying more on unconventional approaches, says the CISO. At his company, "we drop all inbound email from every newly registered domain, because that's where phishing originates from; every 24 hours, cyber criminals change their domains." The company has also automated much of its cybersecurity effort, using algorithms to scan for abnormal activity and implement controls to protect against them. "More and more security controls in the next five years will be driven by algorithms," he says. "It's the only thing with the scale and speed." As a result, "I'm teaching data professionals to be data

"More and more security controls **in the next five years** will be driven by algorithms," says the CISO at a large insurance company.

scientists—because that's where we're finding the answers."

Yet the survey results suggest that a significant share of organizations do not have a structural or procedural framework in place that enables them to detect cybersecurity vulnerabilities and address them proactively; at the same time, the constantly evolving nature of cyber threats and the ever deeper interconnection between their systems and those of third parties represent a severe challenge even to organizations that have integrated cyber risk into their strategic and risk appetite visions.

Achieving Maturity in Cybersecurity

As noted earlier, 85% of survey respondents said they expect the financial impact of cyber attacks and breaches to rise in the next year to two years. To rid themselves of the "fix it and forget it" mentality and develop a mature cybersecurity strategy, corporate leaders must act on the understanding that cyber threats not only create data risks and technical flaws, but also pose fundamental business risks.

Even organizations that have the tools and technical capabilities to address cyber threats may not be able to do so if they lack the organizational characteristics needed to make the best use of them. Maturity in cybersecurity is defined by three criteria: training and performance evaluation, strategic planning, and leadership and vision. The survey questioned respondents about their organization's maturity according to each of these criteria, ranking them from Level 1 to Level 5, the highest being Level 5.

Survey results indicate that while most organizations are making progress according to each of the three criteria, few have made cybersecurity a responsibility at the employee level, few have embraced it as an element of organizational strategy, and few have defined it as an area of business risk—the key factors meriting a Level 5 rating. Larger organizations are further along the maturity curve according to each of the three criteria.

Training and performance evaluation: The first step in developing a robust cybersecurity process is to identify critical vulnerabilities in the supply chain, including contractors and other suppliers, and understand how they overlap and combine, converge and cascade across the business structure—creating, in effect, a "cyber supply chain" that generates new threats at a deeper level. This is not possible unless all levels of the organization, including employees and first-line leaders, are trained and aware of the risks. FIGURE 6

Demonstrating how important this is, the CTO points to the data breach that resulted in the theft of credit card information from 70 million Target customers in 2014. A refrigeration, heating, and air-conditioning subcontractor was found to have unwittingly provided the gateway. He also notes a client that suffered an attack that began with delivery of a CV to a receptionist. The attackers "were specifically targeting her as a way into the organization," he says. "The CEO and executives would have had the training, so attackers are shifting their attention to the lower levels."

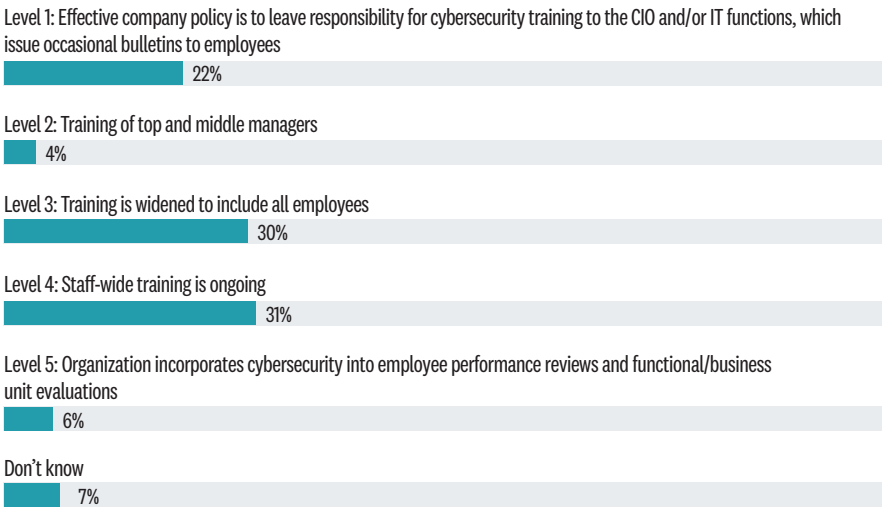
Happily, organizations have made perhaps the most progress at pushing cybersecurity training and awareness down into the employee base. More than two-thirds (67%) of respondents said their organization is at Level 3 or higher, which means it includes all employees in cybersecurity training, while more than one-third (37%) are

Organizations have made perhaps the most progress at **pushing cybersecurity training** and awareness down into the employee base.

FIGURE 6

CYBERSECURITY MATURITY: TRAINING

Which of the following best describes how your organization trains employees in cybersecurity?



SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

at Levels 4 or 5, which means they conduct ongoing, staff-wide training.

Only 22% of respondents said their organization leaves responsibility for cybersecurity training to the CIO and/or IT functions, with only occasional bulletins to employees (7% said they don't know). Very few (6%) incorporate cybersecurity into employee performance reviews and functional/business unit evaluations, however.

Only 18% of larger organizations are still at maturity Level 1 and Level 2, compared with one-third (33%) of smaller organizations.

Strategic planning: Understanding cyber threats and how to respond to them begins with modeling those risks, just as one would a natural disaster, and then developing response scenarios. A key task of leadership is to quantify the impact of cyber threats, for example in terms of EBITDA or EPS, to determine which pose the greatest threat and where risk capital should best be allocated. This helps executives better conceptualize cyber attacks as a business threat and respond to them as such. It also facilitates creating a financial impact model that evaluates the risk from cyber attacks—just as the organization would for other business threats. FIGURE 7

One interviewee notes that his firm regularly inventories the risks to which it's exposed and maps threat vectors to those risks to determine the likelihood of an event and quantify the loss of cash or other potential impact: "Can we make a change in our processes? If so, are we going to mitigate it? Transfer it? Remove it? Do we change our policies? Our controls? Our insurance?"

At the large insurance company, "we measure costs in both labor time and expense," says CISO. "Then we do a trend analysis to see what types of incidents suck up the most. Ransomware attacks are the most expensive, due to the need for patching, monitoring, and dealing with impact."

While most organizations have formalized aspects of cybersecurity practice, few have adopted a formal strategic plan to address cyber threats. Almost four out of five respondents (79%) at least have policies in place for responding to cyber attacks, and more than half (54%) at least have adopted a strategic plan to address them proactively along with a strategic definition of cybersecurity. (The company updates its strategic plan every three years.) More than one-third (37%) model cyber risks and quantify their business impact. ("There's a challenge to putting an ROI to cyber

FIGURE 7

CYBERSECURITY MATURITY: STRATEGY

Which of the following best describes your organization's cybersecurity strategy?

SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

risks," comments one interviewee. "A lot have tried, but the amount of time and effort may not be worth it.") However, only 23% have adopted a formal strategic plan to address business risks from cyber attacks.

Lawmakers and regulators, responding to concerns about consumer data security, are providing the impetus to do more. The GDPR, due to go into effect next May and applying to all companies doing business in the EU, includes stringent data privacy rules and imposes sanctions of up to 4% of annual worldwide turnover in the preceding financial year in cases of noncompliance. "A lot of companies had their heads buried in the sand, but GDPR is a catalyst," says the CTO. "Companies are starting to be more strategic, at least to meet the minimum requirements."

More than one-third (34%) of smaller organizations are still at maturity Level 1 or Level 2 for cybersecurity strategic planning, compared with just 18% of larger organizations.

Leadership and vision: Leadership must center on the C-suite and engage the board as well as the heads of all functions with responsibility for cybersecurity, from data security to finance. Moreover, the cybersecurity committee mustn't be isolated from other parts of the organization's risk management effort. It should be represented on the risk management team, Blau argues, the CISO and the rest of the risk management team can contextualize cyber risks in the wider strategic perspective. In its preparations for the succession of hurricanes that hit the East Coast in September, for example, a large insurance company allocated some of its risk management budget to advise employees and clients on fraudsters masquerading as charities for hurricane survivors. FIGURE 8

Inattention to cybersecurity is now very rare. Only 8% of respondents said the board, C-suite, and other senior executives are not focused on cybersecurity risks; only 28% said responsibility for addressing these is confined to the CIO and/or IT functions. Yet, as discussed earlier, relatively few organizations are establishing a coordinated, strategic response.

While over half (56%) said at least some cybersecurity responsibilities are assigned to functional areas and business units, only 38% said the board

FEW ORGANIZATIONS HAVE ADOPTED A FORMAL STRATEGIC PLAN TO ADDRESS CYBER THREATS.

IN ONLY 21% OF ORGANIZATIONS HAVE THE BOARD AND C-SUITE DEFINED CYBERSECURITY AS AN AREA OF BUSINESS RISK.

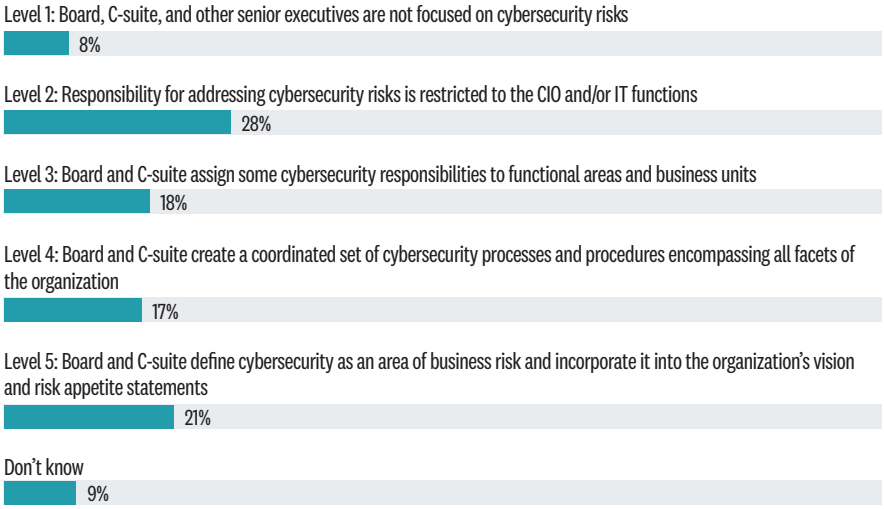
and C-suite have created a coordinated set of cybersecurity processes and procedures encompassing all facets of the organization. In only 21% of organizations have the board and C-suite defined cybersecurity as an area of business risk and incorporated it into the organization's vision and risk appetite statements.

Once again, larger organizations are making more progress. Almost half (45%) of respondents at smaller organizations said theirs is still at Level 1 or Level 2 for maturity in cybersecurity leadership and vision, compared with 23% of larger organizations.

FIGURE 8

CYBERSECURITY MATURITY: LEADERSHIP

Which of the following best describes your organization's leadership approach to cybersecurity?



SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

Opening the Way to Opportunity

Cyber threats are not insoluble and they can be defended against. But the solution must start with a clear understanding of how the threats themselves can affect every part of the organization's business, not just aspects of its technology architecture.

Organizations that do so can proceed with greater confidence in the security of their operations and revenue flow and move with greater assurance to exploit the opportunities to differentiate themselves that heightened concern with data security provides. "We use it as a point of differentiation and a competitive advantage," says an interviewee at one data-intensive company.

This is especially true for any consumer products or consumer-facing company. "Data security is a credence value," says Blau. "Consumers will eventually expect security to be embedded in the quality of the product." But understanding and enforcement vary greatly. "We've seen examples where firms have red and blue teams testing their defenses to understand what's not working. But we're concerned, especially with the Internet of Things, that a lot of products don't have great security functionality—maybe not even a consumer help line."

At the vast majority of organizations we surveyed, cybersecurity is no longer an afterthought; indeed, the past three years have seen a surge in new allocation of budget and resources to this critical risk area. Most are aware of the specific risks they face; of their vulnerabilities, both internal and external; and of the potential of cyber threats to damage their future business success. Most have taken at least first steps to create a chain of responsibility for cybersecurity and are enlisting key executives to devise solutions. Larger sections of the employee base are being trained and made aware of cyber threats.

However, smaller organizations are making slower progress and have made fewer of the institutional changes—e.g., installing a CISO, increasing employee training, involving the board in cybersecurity decision-making, creating a strategic plan for data security—than have larger organizations. More than half (56%) of respondents said their organization lacks the resources to properly address cybersecurity risks, compared with 42% of larger ones. Some experts anticipate that legal and regulatory spurs like the GDPR will help to push smaller companies further along the path to maturity. FIGURE 9

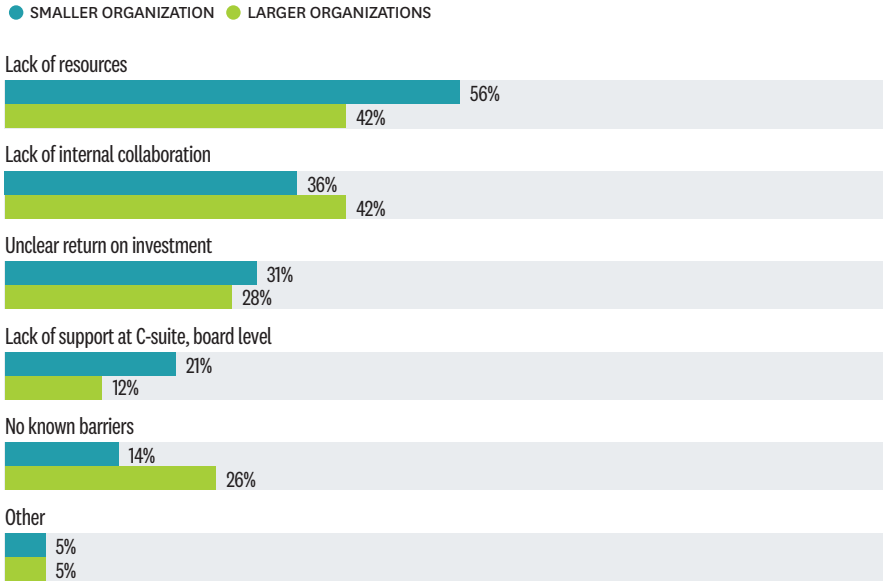
AT THE VAST MAJORITY OF ORGANIZATIONS WE SURVEYED, CYBERSECURITY IS NO LONGER AN AFTERTHOUGHT.

MORE THAN HALF (56%) OF RESPONDENTS SAID THEIR ORGANIZATION LACKS THE RESOURCES TO PROPERLY ADDRESS CYBERSECURITY RISKS, COMPARED WITH 42% OF LARGER ONES.

FIGURE 9

CYBERSECURITY PITFALLS

What are the most significant obstacles to properly addressing cybersecurity risks at your organization?



SOURCE: HARVARD BUSINESS ANALYTIC SERVICES SURVEY, AUGUST 2017

Integrating the key functions around cybersecurity is critical to developing strong processes and solutions, as discussed earlier; however, most organizations are failing to do so. This goes for larger organizations (only 38% say these functions are very integrated) as well as smaller ones (13%). This may be the biggest obstacle to creating a more strategic approach to cybersecurity. Yet at most organizations, coordination is still rudimentary and responsibility is not being pushed down to the business unit level. This is especially the case at smaller organizations. And while half or more of all organizations surveyed are on the road to creating a more strategic approach, few have defined cybersecurity as an area of business risk or incorporated it into their overall strategic plan.

They will have to try harder, says the CTOo: "Progress is being made, but attackers have made lots of progress as well."

INTEGRATING THE KEY FUNCTIONS AROUND CYBERSECURITY IS CRITICAL TO DEVELOPING STRONG PROCESSES AND SOLUTIONS.

METHODOLOGY AND PARTICIPANT PROFILE

A total of 278 respondents completed the survey: 252 came from the HBR audience of readers (magazine/enewsletter readers, customers, HBR.org users); 26 came from client-sourced lists.

SIZE OF ORGANIZATION

ALL RESPONDENTS' ORGANIZATIONS HAD 500 OR MORE EMPLOYEES.

46% 10,000+ EMPLOYEES

14% 5,000-9,999 EMPLOYEES

40% 500-4,999 EMPLOYEES

SENIORITY

20% EXECUTIVE MANAGEMENT OR BOARD MEMBERS

45% SENIOR MANAGEMENT

31% MIDDLE MANAGEMENT

4% OTHER GRADES

KEY INDUSTRY SECTORS

OTHER SECTORS WERE EACH REPRESENTED BY 8% OR LESS OF THE RESPONDENT BASE.

18% FINANCIAL SERVICES

17% TECHNOLOGY

15% PROFESSIONAL SERVICES/ CONSULTING

10% HEALTH CARE

JOB FUNCTION

OTHER FUNCTIONS WERE EACH REPRESENTED BY 6% OR LESS OF THE BASE.

15% IT

13% GENERAL/ EXECUTIVE MANAGEMENT

9% CONSULTING

8% SALES/BUSINESS DEVELOPMENT

7% RISK MANAGEMENT

REGIONS

45% NORTH AMERICA

33% EMEA

18% ASIA/PACIFIC

4% REST OF WORLD

Endnotes

1 Cited in Suzanne Barlyn, Global cyber attack could spur $53 billion in losses: Lloyd's of London, Reuters, July 17, 2017. https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB

2 "Counting the Cost: Cyber Exposure Decoded," Lloyd's and Cyence, Emerging Risks Report, 2017

3 National Bureau of Asian Research, "Update to the IP Commission Report," Commission on the Theft of American Intellectual Property, 2017. http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

4 Cited in "Cyber 'Worm' Attack Hits Global Corporate Earnings," Reuters, August 2, 2017. http://fortune.com/2017/08/02/cyber-worm-attack-corporate-earnings/

5 Lee Matthews, "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million," Forbes, August 16, 2017. https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#5859539e4f9a

6 Mary Schlangenstein, "FedEx's TNT Reels From June Cyberattack as Damage Lingers," Bloomberg Technology, July 17, 2017. https://www.bloomberg.com/news/articles/2017-07-17/fedex-says-tnt-systems-may-never-fully-recover-from-cyberattack

Harvard Business Review
ANALYTIC SERVICES

hbr.org/hbr-analytic-services