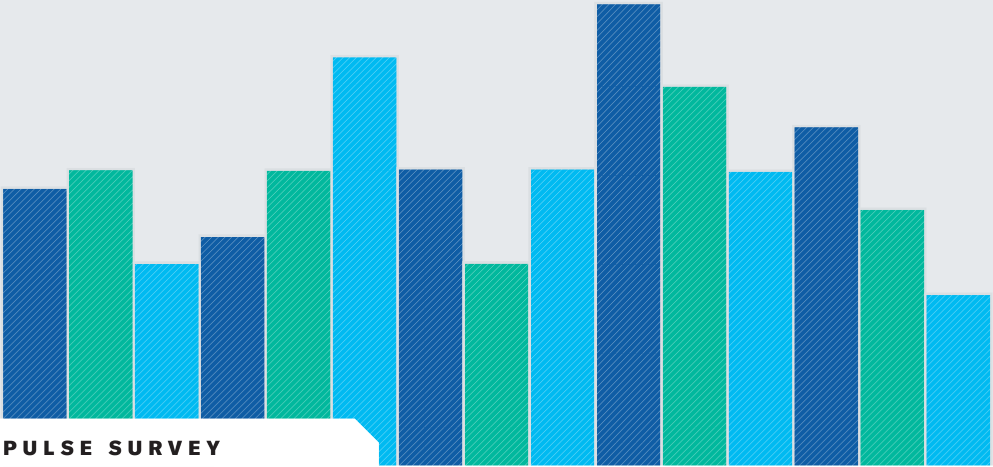
Harvard Business Review
ANALYTIC SERVICES



PULSE SURVEY

Cybersecurity in the Era of Intelligence and an Expanding Attack Surface

Sponsored by

DXC TECHNOLOGY

SPONSOR PERSPECTIVE

In a matter of months, businesses have witnessed the emergence of a new normal in the way they share and protect their data. The Covid-19 crisis accelerated changes that were already underway, such as digitization of processes, the proliferation of mobile devices, and remote access to sensitive information. These changes, along with the growing complexity of IT estates, have created an expanded attack surface for opportunistic cybercriminals.

Companies today are struggling to balance the business benefits with the security risks of implementing new technologies such as the cloud, artificial intelligence (AI), and machine learning. These tools offer great potential for new insights, efficiencies, and levels of performance but can also expose vulnerabilities within IT systems.

Working with some of the world's largest companies on their move to the cloud and hybrid environments, we see the challenges posed by these seismic shifts every day. DXC Technology sponsored this research by Harvard Business Review Analytic Services to see how companies are responding to these challenges and opportunities. The survey and interviews provide insights into perceptions about protection against online attacks, securing remote work, and the implications of new technologies.

We've identified several core principles to guide companies as they navigate this new cybersecurity landscape:

- As security perimeters become more fluid, we can no longer rely on the old models that focused on securing a traditional network infrastructure. We must build security around the data itself, for example, with zero trust models that focus on securing data rather than network segments.
- It's critical for companies to know their IT estates, identifying where their most critical assets reside as well as key interconnections and dependencies.
- Organizations should build security into every new technology and process they implement, rather than treating it as an afterthought. Advanced analytics and AI make it easier to analyze complex, voluminous data and event records and detect potential threats quickly and effectively.
- Despite the best security measures, there's a high probability every organization will experience a breach at some point, so organizations should develop a cyber resilience strategy that helps them recover from incidents quickly, with minimal damage and disruption.

It's easy to make errors or omissions when rushing to implement new processes and technologies. As we move from crisis mode to more strategic planning, I encourage you to use this report as a springboard to assess your preparedness and cyber resiliency.

Read on to gain invaluable insights, and stay on top of the latest threats with DXC's Security Threat Intelligence Report at dxc.com/threats.

Mark Hughes
President, Security
DXC Technology

Cybersecurity in the Era of Intelligence and an Expanding Attack Surface

The Covid-19 crisis has delivered a new era of cyber threats. As the coronavirus spread and led to economically punishing lockdowns, companies rushed to move whatever operations they could online. Cybercriminals saw opportunity in that flight to digital. With legions of employees working from home and business processes quickly digitized, corporate IT systems and data stores suddenly grew in size and complexity, offering an expanded and more enticing "attack surface."

Have companies managed to rise to this security challenge? A new survey by Harvard Business Review Analytic Services of 332 executives at organizations around the world shows that many are aware of the information security risks today and report robust efforts to secure data. Some 43% of executives believe their organizations are well protected from online attackers—a level of confidence experts say is far too high given the capabilities of sophisticated hackers—while 52% rate the inability to detect and prevent data theft as a high or very high security concern for their organizations. **FIGURE 1**

Clearly, companies continue to struggle to balance opportunities created by new technologies and massive amounts of data, and the huge security risks they create. If they are to seize the business potential, they must raise their cybersecurity game, refresh their security strategies, and harness for security the same powerful new technologies they are beginning to use to boost their businesses—data analytics, artificial intelligence (AI), machine learning (ML), and automation. They must also address vulnerabilities that have been introduced by the crisis-driven, but likely lasting, move to remote work.

HIGHLIGHTS

52% of executives say **automation is very important** to their security operations.

43% believe their organizations are **well protected** from online attackers.

34% say their organizations **assess risk and build in new security measures** every time or nearly every time they undertake initiatives to expand the collection and use of data.

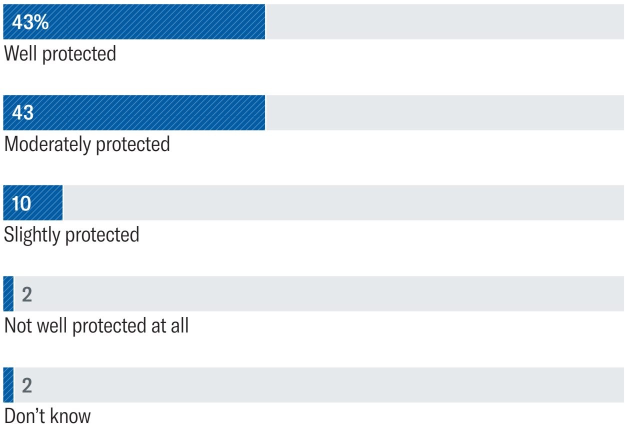
> “We’ve embarked on a new normal, and we are going to see the continuation of financial constraints on many C-suite leaders,” says Lakshmi Hanspal, global chief security officer at Box Inc.

FIGURE 1

A False Sense of Security?

Determined and advanced attackers can penetrate even the best-protected organizations

How protected from online attackers do you believe your organization is ?



Source: Harvard Business Review Analytic Services survey, March 2021

“We’ve embarked on a new normal, and we are going to see the continuation of financial constraints on many C-suite leaders,” says Lakshmi Hanspal, global chief security officer at Box Inc., a cloud content management services company based in Redwood City, Calif. “There’s going to be incentive to drive efficiency and deliver on results. So automation ... is going to be leveraged as a multiplier and provide frameworks to combat these risks.”

However, organizations must beware the potential for an arms race. Data systems capable of making important decisions, be they security or business decisions, are bound to become targets of attack themselves. Organizations must move carefully into this new arena, lest they create even more new opportunities for attackers.

This Harvard Business Review Analytic Services report explores the security challenges that accompany an expanding attack surface and aims to explain what companies can do to mitigate their risk. It provides insights into how organizations are successfully managing these challenges, identifies best practices, and offers recommendations about how to better secure company data in this new era.

The Security Implications of Remote Work

During the Covid-19 crisis, companies significantly expanded their digital capabilities as they fought to keep their businesses alive. Companies quickly ramped up online marketing and sales and invented or extended work-from-home protocols for staff since in-person interactions with customers and colleagues were suddenly impossible.

Most respondents to the survey say that due to Covid-19, the pace of digital transformation efforts at their organizations accelerated (83%), collection and use of data expanded (80%), and employees’ ability to work from home increased (86%).

Fortunately, that expansion was, for the most part, accompanied by attention to security. Despite widespread financial stress, 41% of executives say their IT security team’s staffing and resources increased somewhat or significantly as a result of Covid-19 (28% and 14%, respectively), while 44% report that there was no change. Nearly half of respondents (49%) say security measures at their organization were tightened when staff began to work from home and remain tight today, while another 29% say security measures were eased to get staff up and running from home but have been tightened since. **FIGURE 2**

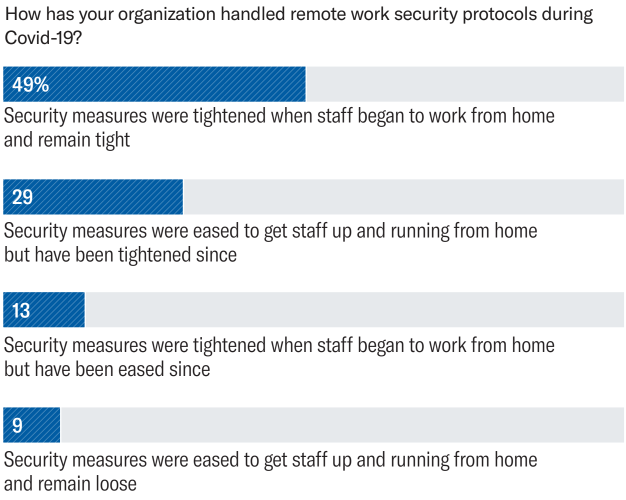
“For sure, most companies weren’t prepared for the security implications of everyone working from home,” says Avivah Litan, a distinguished vice president analyst at research firm Gartner. “They weren’t ready to secure all of these desktops that weren’t in their headquarters, so they had to expand all their programs for [virtual private networks] and remote security and authentication and change policies of who could work from home.”

To manage the equally swift move to online-only business, many companies hurriedly adopted software-as-a-service (SaaS) technologies, expanded cloud-based storage, and onboarded new partners and suppliers—very often while short on staff and resources. Hurry, change, and disruption can mean confusion, omissions, and mistakes that create openings that cybercriminals are masters at exploiting. And they are attacking companies indiscriminately, Hanspal says, adding, “Everyone’s a target.”

FIGURE 2

Executives Believe Remote Security Is Tight

Companies have taken the security of remote work seriously



Source: Harvard Business Review Analytic Services survey, March 2021

> Hurry, change, and disruption can mean confusion, omissions, and mistakes that create openings that cybercriminals are masters at exploiting.

Companies are now facing a volume and velocity of attacks difficult for anyone to sustain. Phishing attacks—scam emails with dangerous links often used to steal credentials for cloud-service accounts—doubled in 2020, according to the Anti-Phishing Working Group's fourth-quarter 2020 report; and when these attacks had Covid-19 themes, they were more effective, Verizon reports. Attempted malware attacks rose by 358% and ransomware by 435%, a February 2021 study by cybersecurity firm Deep Instinct shows. Meanwhile, companies became more concerned not only about direct attacks but also about attacks on suppliers whose systems could be used to infiltrate them.

The top risk for most companies right now is a type of phishing called business email compromise (BEC), says Brenda R. Sharton, a Boston-based partner and co-chair of the global privacy and cybersecurity practice at law firm Dechert LLP, because successful attacks are costly. In this type of attack, scammers get access to email accounts, often of senior executives, using phishing emails or computer intrusion techniques. Then they impersonate the executive and try to divert funds using bogus vendor invoices or by changing wiring instructions on deal payments. In 2020, companies filed complaints to the FBI about BEC attacks that cost them an astronomical $1.8 billion, finds the "2020 Internet Crime Report" by the FBI's Internet Crime Complaint Center.

Ransomware attacks, which can begin with phishing and password theft, are also becoming more targeted and costly in both data and financial terms. Attackers used to simply break into companies, encrypt their data, and hold it for ransom, Sharton says. But now, they are exfiltrating the data first. "They're getting so bold," she says. In a case she had last May, extortionists demanded "to speak to an executive within a half hour or they were going to start dumping all of the company's files on the dark web."

As of May 2020, extortionists typically demanded $3 million to $5 million, says Sharton, who has handled more than 500 data breach investigations in her career. But ransoms escalated through 2020 and into 2021. Attackers seem to be going after larger, richer companies, and Sharton has heard of demands as high as $60 million. This spring, emboldened extortionists even disrupted critical commodity supplies and prices by attacking and shutting down gas pipeline operator Colonial Pipeline Co. in May and meat processor JBS USA Holdings Inc. in June. Colonial Pipeline reportedly paid $4.3 million in ransom, $2.3 million of which the U.S. government successfully recovered, and JBS reportedly paid $11 million.

Security Awareness but Inconsistent Action

Most executives are aware of information security risks, particularly those related to company data and remote work. "I think that there's much higher awareness [of security] than there was three or five years ago," says Sharton, who specializes in data breaches. "In the beginning, it was just the IT people worrying about it and trying to get people to hear them. Then it was the C-suite—probably five years ago, you'd have CEOs and CIOs all over it. Now, you've got boards who are asking for cybersecurity updates."

Importantly, companies appear to have absorbed years of experts' entreaties to weigh security carefully when deciding whether to collect and use more data. Forty percent of executives surveyed say that cybersecurity and risk management are prioritized somewhat more (15%) or much more (25%) than expanding data collection and data use at

> Companies appear to have absorbed years of experts’ entreaties to weigh security carefully when deciding whether to collect and use more data.

their organizations. Combined, that’s notably more than the 24% who say data collection and use is more prioritized than security. Another 33% say the two needs are equally prioritized.

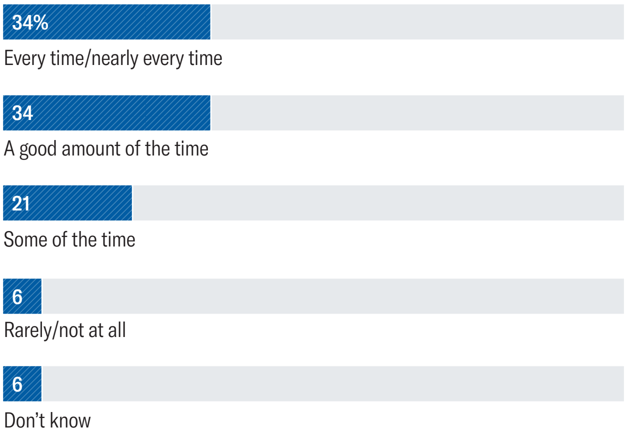
Meanwhile, about half of respondents (52%) say the inability to detect and prevent data theft is a high or very high organizational security concern. A similar share of respondents note high concern regarding unsecure networks and software (49%), which can lead to data theft, and increased IT network expansion and complexity (49%), a key impact of remote work and the trend behind the expanding attack surface.

FIGURE 3

Security Too Often an Afterthought

Assessing risk and building security into new data initiatives is not yet routine

How regularly does your organization assess risk and build in new security measures before expanding data collection and data use initiatives?



Source: Harvard Business Review Analytic Services survey, March 2021

These executive concerns are being felt at cloud services companies. Hanspal says customers now quiz Box on how it’s handling their data and preventing breaches. And they’re demanding built-in security, digital privacy, compliance, and resilience, which is pushing cloud companies to up their security games.

Executives are also concerned about security risks related to remote work, a key driver of IT network expansion and complexity. Here, two-thirds of executives cite phishing attacks and other email scams (68%) and malware and viruses (67%) as high or very high security risks, in line with the top concerns of experts.

However, despite awareness and recognition of the importance of prioritizing data security, there remains a gap in actually achieving it. Only 34% of respondents say their organizations assess risk and build in new security measures every time or nearly every time they undertake initiatives to expand collection and use of data. Another 34% say they do so a good amount of the time. But over a quarter (27%) say they only do so some of the time or rarely or not at all. **FIGURE 3**

Chris Ulliott, chief information security officer at NatWest Group, a large Edinburgh, Scotland-based financial services firm, says companies should consider security every time they embark on a new data project, though what controls they apply will vary based on the data and threats to it.

The survey suggests there may be less of a security gap when it comes to remote work. Awareness of security risks is fairly high, and most executives say work-from-home security is tight now. However, executives may, again, be overconfident. Remote or hybrid work arrangements are likely to be an enduring feature going forward. Indeed, most of the survey respondents (81%) expect to have more ability to work from home in the future than they did before Covid-19. Organizations should take time now to examine whether their work-from-home measures are, in fact, sufficient for the long haul and make any necessary changes.

Securing Data in a Remote Work Future

Companies are now beginning to focus on a post-Covid-19 future. “We see that organizations are truly starting to dust off from the pandemic mode and move from crisis mode to strategic mode,” Hanspal says.

Business leaders are now tasked with trying to figure out how to support work inside and outside the office, meet customer and partner demands for digital interfaces and services, and manage the related security risks and privacy challenges.

Organizations long relied on “systemic controls” for security, Hanspal explains, like locked office locations, hard corporate network perimeters, protected virtual private

> "If you understand what your data flows are and where the information resides and what the threats are to that, you can then put proportional controls in the right places and have some confidence that you're protecting what really matters," says Chris Ulliott, chief information security officer at NatWest Group.

networks for road warriors, and trusted corporate devices managed by the security team. But those controls have gotten progressively less effective. Today, an overwhelming number of devices connect to corporate networks and access corporate information, including employees' personal devices, and many companies are moving to more flexible cloud-based platforms. As a result, more companies are looking to build security around the data itself, rather than rely on so-called trusted devices, an approach that requires a comprehensive understanding of their specific risks and layers of protections.

Organizations must protect their people and educate them. They need processes for understanding business risk and for attack detection, response, protection, prevention, and "the rinse, repeat of that," Hanspal says. And they need technology tools that enable all those processes.

Perhaps the most important processes for organizations to get right today are those related to data. Companies need to know what data they are using, map how it flows through company systems, and identify where security risks crop up as a result. "If you understand what your data flows are and where the information resides and what the threats are to that, you can then put proportional controls in the right places and have some confidence that you're protecting what really matters," NatWest's Ulliott says.

A data-centric approach enables secure remote work, he adds. Since well before Covid-19 struck, most NatWest employees worked remotely some of the time. To do so safely, "we don't have data residing remotely. We have technologies that take you to the data," Ulliott says. "That gives me some more really robust boundaries that I can police and enforce and protect."

To support remote work, Hanspal says Box has worked with customers to employ a number of existing but underused security strategies. Among them are "device trust" processes whereby companies grant devices privileges to view, download, print, or share data based on their security and internet connection. Another is data-centric malware protection, which looks for malicious attacks "at the point of sharing, at the point of upload, at the point of collaboration," rather than when potential attacks might reach an endpoint, she says.

Hanspal also advocates anomaly and threat detection, technology that looks for unusual activity compared to normal behavior and blocks it. For example, if an employee tries to download data from a computer in a country she has never operated in before, the system flags it as a potential security breach and stops the download.

Companies can change business processes to improve security. For instance, auto-classification of data lets companies use automation, instead of people, to identify documents like contracts and marketing strategies, classify them as such, and then apply relevant data security policies.

Some organizations have had to make tough, if temporary, business process decisions during Covid-19. For instance, many companies with customer or product support staff working from home chose to stop taking credit card information and changes to payment methods from customers over the phone, Hanspal says, and steered them to more secure channels.

Using and Securing Artificial Intelligence

Inside IT security departments, advanced technologies like AI, ML, and automation are becoming increasingly important. They can make sense of rivers of sensor and event data so companies can more quickly identify security breaches and improve security decision making, assuming their massive data stores are well managed and analytics tools are powerful enough.

However, these technologies are not yet integral to business operations or security operations at many companies, according to the survey. Although most executives say data analytics (72%) are very important to their organizations' business operations, fewer (61%) say they are very important to their security operations. About half consider automation very important to their business operations (53%) and their security operations (52%). But less than a third of respondents consider AI/ML to be very important, whether to their business operations (28%) or to their security operations (34%). **FIGURE 4**

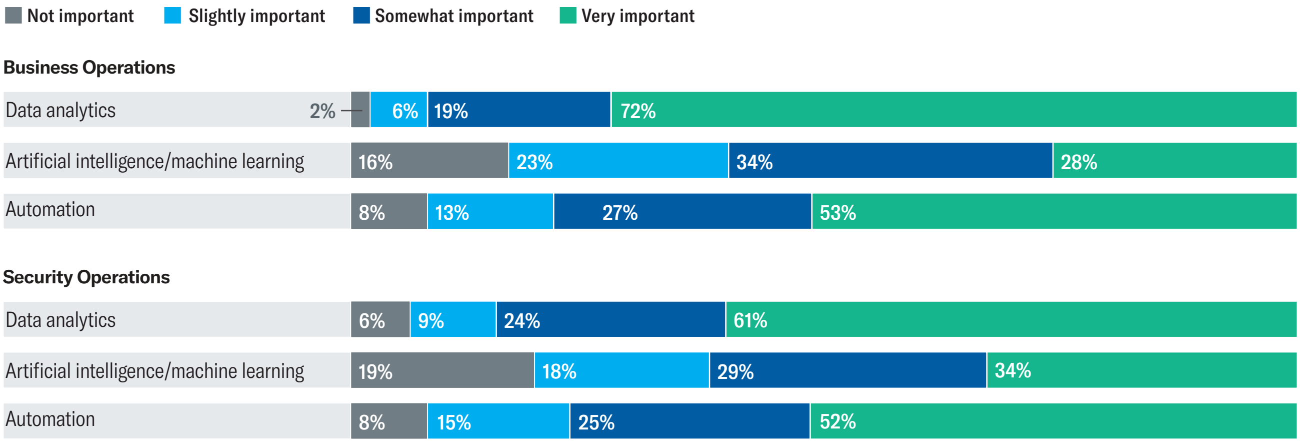
Tepid adoption in large part reflects technology immaturity. "I'm a great believer in machine learning," particularly to look for intrusions and attacks, Ulliott says. "It's a really great

FIGURE 4

The Machines Aren't in Control ... Yet

Advanced technologies are not yet integral to organizations' security operations

How important are the following technologies to your organization's business/security operations today?



Source: Harvard Business Review Analytic Services survey, March 2021

way of taking a mass of information to give to the analyst the really prudent things they need to make a decision. But we wouldn't necessarily use machine learning to do enforcement today, because I don't think the technology is that mature," he says. "I look forward to seeing what the future brings."

Though imperfect, ML and AI have improved significantly, Hanspal says. These advanced technologies can help security professionals find ways to block barrages of attacks and detect unusual behaviors that indicate stealthy novel attacks, both of which are hard for humans to do on their own.

There are a number of other challenges to more widespread use of AI, ML, and automation. Talent is one. AI and ML require specialized skills that companies need to invest in acquiring. "Having skills but not the tools, and having tools but not the skills, is not going to work," Hanspal says. Organizations are also still working on the quality and reliability of the data that these advanced tools use, she adds. "If data is driving AI/ML decision making, we also have to ask, 'Is that data trustworthy?'"

Ulliott is concerned about system integrity and the ethics of machine learning. It is vital to understand how ML models are created and ensure they don't perpetuate biases, he says. "There's an AI and machine learning ethics piece that the industry is only just touching the surface of at the moment, and we've got to be very aware of that."

And then there are the security worries: Increased use of AI and ML could lead to more malicious attacks on those systems. "We are at risk, if we're not careful, of an arms race of using machine learning for good versus abusing it for bad," Ulliott says. "We just need to be very wary where we use some of these models, because they can be and will be attacked in the future."

Some experts say the arms race is already underway. Outside regulated industries like financial services, most companies don't know when they're being attacked because "they're not looking for it," says Gartner's Litan, whose research is focused on AI trust and risk. "If you believe China is stealing all our intellectual property, what better thing to steal than our AI models?"

For now, executives are more concerned about liability and social risks, Litan says. "The threat they worry about most is that they don't know what's going on within their AI systems." A utility plant's system could make a wrong decision that leads to a polluted waterway. AI in a tech company's human resources system could screen out women or minorities, leading to discriminatory hiring and bias claims. "Whether they built [the AI] or they bought it, it's a black box for them, so they won't know if it's getting out of control, if it's doing what it's supposed to do."

AI trust and risk is "one of these areas that's very important to CIOs and executives," Litan says. "In fact, it's the biggest

“There’s an AI and machine learning ethics piece that the industry is only just touching the surface of at the moment, and we’ve got to be very aware of that.”

Chris Ulliott, chief information security officer, NatWest Group

> "It goes back to the eons-old adage: people, process, technology. That has not changed," says Lakshmi Hanspal, global chief security officer at Box Inc.

reason why AI doesn't go into production. It's because they're afraid of the security and privacy problems."

Companies are struggling to manage these risks, in part, because so many facets of the organization are involved—legal, compliance, privacy, security, third-party risk, cloud. "It involves everybody, so nothing really gets done," Litan says. The French bank BNP Paribas offers a model, she says. It has a dedicated AI risk manager with a full program who reports to the global head of risk management and has dotted-line reporting relationships across eight groups. "That's best practice, but you don't see that very often," she says.

Conclusion

The ever-expanding attack surface is requiring companies to take fresh looks at the security technologies, policies, procedures, and education programs they have in place. In this era of pervasive remote work and relentless attacks, companies must focus controls on the data they are protecting and use technologies like AI, ML, and automation to work faster, harder, and smarter.

"AI and ML have been the heart of automation, and automation has been the best friend for many practitioners within the last year to sustain volume and velocity of attacks," Hanspal says. These technologies are security-staff force multipliers that more organizations need in order to achieve security excellence in today's world.

Most organizations are able to "obtain, maintain, and sustain" solid security operations, she says. But far fewer reach the "thrive" phase that can come with automation. "Sustain would be doing manual response," Hanspal asserts. "Thriving is you're detecting it; you're preventing that from happening."

To thrive, companies must first ask themselves what thriving looks like in their environment. When they have a vision, they can establish metrics and goals—for example, on speed of detection and response—that are appropriate for them, she explains. Then they can add automation that levels up their security operations and gets them into thriving mode.

"It goes back to the eons-old adage: people, process, technology. That has not changed," Hanspal adds. It is not until these areas are addressed that business leaders can say with justified confidence that their organization is well protected.

METHODOLOGY AND PARTICIPANT PROFILE

A total of 332 respondents drawn from the HBR audience of readers (magazine/enewsletter readers, customers, HBR.org users) completed the survey.

Size of Organization

22%
10,000 or more employees

9%
5,000–9,999 employees

18%
1,000–4,999 employees

11%
500–999 employees

13%
100–499 employees

28%
Fewer than 100 employees

Seniority

35%
Executive management/board members

32%
Senior management

28%
Middle management

4%
Other grades

Key Industry Sectors

13%
Financial services

12%
Technology

12%
Business/professional services

8%
Manufacturing

8%
Government/not-for-profit

8%
Education

All other sectors less than 8% each

Job Function

24%
General/executive management

12%
HR/training

9%
Administration

8%
Sales/business development/customer service

All other functions less than 8% each

Regions

49%
North America

19%
Europe

17%
Asia/Pacific/Oceania

7%
Latin America

8%
Middle East/Africa

Figures may not add up to 100% due to rounding.

Harvard Business Review
ANALYTIC SERVICES

ABOUT US

Harvard Business Review Analytic Services is an independent commercial research unit within Harvard Business Review Group, conducting research and comparative analysis on important management challenges and emerging business opportunities. Seeking to provide business intelligence and peer-group insight, each report is published based on the findings of original quantitative and/or qualitative research and analysis. Quantitative surveys are conducted with the HBR Advisory Council, HBR's global research panel, and qualitative research is conducted with senior business executives and subject matter experts from within and beyond the *Harvard Business Review* author community. Email us at hbranalyticservices@hbr.org.

hbr.org/hbr-analytic-services