Harvard Business Review
ANALYTIC SERVICES

Pulse Survey

IT SECURITY

New Analytics-Driven Model

Sponsored by

splunk>

HAIYAN SONG

SENIOR VICE PRESIDENT AND GENERAL MANAGER, SECURITY MARKETS

SPLUNK

Digitization means greater efficiencies and boundless opportunities for organizations of all sizes. But despite the benefits of living in an interconnected world, digital transformation does not come without significant challenges. New security vulnerabilities can be exploited, and businesses face the challenge of embracing new technologies while building a security portfolio that can stay ahead of threats at machine speed.

It has become increasingly important for enterprises to protect their data, including data shared via users, customers, or any other stakeholders. A lapse in security could otherwise mean a disruption in services, considerable financial loss, and a tarnished reputation.

To prevent this, organizations need a flexible, customizable security solution that combines the power of an analytics-driven platform with the benefits of machine learning (ML). The power of ML is twofold—it uncovers behavior and scenarios that are unknown and unforeseen, and it helps organizations predict risk before it can happen.

So how are organizations planning to protect their networks, customers, and employees from cyber threats? The enclosed survey found that 40% of 223 global executives believe the answer to this challenge is hidden in machine data.

In fact, they plan to implement new technology that can collect machine data from all of their existing IT systems, as well as rapidly identify and respond to potential security threats. Solutions like Splunk effectively gather and query data from disparate sources—from apps to CPUs to firewalls to IoT devices and beyond—and help turn chaotic data into meaningful security answers.

Aflac is an example of an organization unlocking the benefits of a machine data platform with ML capabilities to stay ahead of the cybersecurity arms race.

“Splunk has made it very easy to ingest data from different sources and then present them in a way that is meaningful to stakeholders, such as our board or other leadership,” said DJ Goldsworthy, director of security operations and threat management for Aflac. “We implemented Splunk first for threat intelligence and then security operations, and realizing how versatile the solution is, we determined that the logical next step for us was to apply that to fraud.”

While security will always be driven by human-centric data analysis, ML augments that analysis to better predict patterns, sequences, trends, and threats from data. Machine data contains a definitive record of the activity and behavior of your customers, users, transactions, applications, servers, networks, and mobile devices, so that you can better detect and respond to bad behavior. By applying ML to this data, you can tackle your greatest security challenges, and uncover additional insights on questions you didn’t even know you should be asking—ultimately providing the ability to act on any incidents that might arise.

IT SECURITY

A New Analytics-Driven Model

EXECUTIVE SUMMARY

The relentless digitalization of the world around us has created new opportunities for businesses and other large organizations, but also introduced new risks. While increasingly complex and highly extended computing environments enable more efficient and collaborative ways of doing business, they also open new paths to exploitation by bad actors. Enterprises today must protect not only their own data, systems, and intellectual property, but also content shared by customers, vendors, distributors, and other stakeholders. Lapses can disrupt an organization's operations, tarnish its reputation, and invite material financial penalties from government regulators. The ever-growing volume and variety of data and content to be managed, and the ongoing evolution of technology, add to the challenges of managing all these risks.

In this environment, enterprises need security and fraud-protection capabilities as agile and expansive as the challenges they face—capabilities that leverage automation, machine learning (ML), and other artificial intelligence (AI) techniques to work at the scale and speed necessary to truly protect. For many organizations, the goal is a cutting-edge cyber defense and fraud-detection program within a dedicated security operations center.

To find out where organizations are on this journey—and what leading companies are doing to build the best digital defenses possible—Harvard Business Review Analytic Services recently surveyed more than 200 executives around the globe about their organizations' cybersecurity practices. Among the key findings:

- **Cybersecurity is a high-priority issue nearly everywhere.** Ninety-three percent of survey respondents say their organizations have made cybersecurity a higher priority over the past two years, and nearly as many—86%—say it will become an even higher priority over the next two years.

HIGHLIGHTS

70%
OF RESPONDENTS SAY THEIR ORGANIZATIONS EXPERIENCED SECURITY BREACHES OR CYBER FRAUD OVER THE PAST TWO YEARS

66%
SAY THEIR ORGANIZATIONS HAVE UPGRADED THEIR NETWORK SECURITY MONITORING SYSTEMS OVER THE PAST TWO YEARS

86%
SAY THEIR ORGANIZATIONS WILL MAKE CYBERSECURITY A HIGHER PRIORITY OVER THE NEXT TWO YEARS

39%
SAY THEIR ORGANIZATIONS WILL INTRODUCE SECURITY SOLUTIONS RELYING ON ADVANCED TECHNOLOGIES SUCH AS ML OR OTHER FORMS OF AI

Ninety-three percent of respondents say their organizations have made **data and systems security, including fraud protection, a higher priority** over the past two years.

- **Organizations are putting their money where their mouths are.** More than eight in 10 survey respondents say their organizations boosted spending on cybersecurity over the past two years and will continue to do so over the next two.
- **Network safeguarding, regulatory compliance, internal security defense, and faster investigations and responses are key security priorities.** Nearly two-thirds of survey respondents say their organizations have updated their network security monitoring systems in the past two years, with 57% introducing systems or processes specifically aimed at ensuring compliance with regulations. Meanwhile, nearly half have introduced systems or processes aimed at detecting internal (insider) security threats, and a like percentage have done the same to execute faster security investigations and quicker incident response.
- **Leading organizations are looking to advanced technologies to improve cybersecurity.** Nearly four in 10 survey respondents say their organizations will introduce security solutions relying on advanced technologies such as ML or other forms of AI. And 40% say they'll implement new technology that can collect machine data from all of their existing IT systems and rapidly identify potential security threats.
- **Phishing is the top cybersecurity worry today, cited by 81% of respondents as a significant concern.** Other top fears are malware, viruses, and unpatched software vulnerabilities, each of which are cited by 76% of survey respondents.
- **Concern about top security issues exceeds confidence in managing them.** Only about two-thirds of respondents say their organizations perform well today in addressing phishing, malware, and viruses, and fewer still—60%—say they do a good job addressing unpatched software vulnerabilities.

The Downside to Digital Transformation: Cyber Vulnerability

The cybersecurity arms race shows no signs of slowing. As technology becomes an increasingly powerful and pervasive component of the business and social landscape, the opportunities to steal intellectual property, disrupt business operations, or influence public attitudes about companies or their products are increasing exponentially.

Not surprisingly, companies are fighting back. In a survey of more than 200 business executives globally by Harvard Business Review Analytic Services, 93% of respondents say their organizations have made data and systems security, including fraud protection, a higher priority over the past two years. And 86% say that focus will only ratchet up over the next two years.

Cybersecurity experts say organizations really don't have much choice.

"Attackers and their attacks are growing more sophisticated," says Joseph Steinberg, a consultant to cybersecurity and emerging technology companies who cofounded cybersecurity firms SecureMySocial and Green Armor Solutions. "There are many more things to attack, and more people out there capable of doing the attacking."

Steinberg notes that a decade ago no one was talking about complicated ransomware and North Korea wasn't

involved in corporate hacking. Cryptocurrencies were in their infancy—the first Bitcoin was mined in early 2009—so there was obviously no cryptocurrency mining malware. And the internet of things (IoT) was just starting to evolve, so there weren't millions of refrigerators, doorbells, cameras, equipment sensors, and other household items connected to the internet and often improperly secured.

Eugene H. Spafford, professor of computer science at Purdue University and a frequent consultant to corporate clients, identifies two other trends complicating the cybersecurity challenge. One is the proliferation of personal computing devices that people carry into work environments where, knowingly or not, they can pair with local computer networks and serve as access points for malicious software.

Another is the broad expansion of supply chains. Where many organizations in the past may have digitally connected to a handful of trusted vendors, it's now common to have far-reaching supply chains connected by software systems whose security can't be taken for granted.

"Those systems open up lots of avenues for attack through software updates, or by tempting people to install things that are improperly vetted or that were built into the product or the hardware by another company or national agency interested in penetrating corporate boundaries," Spafford says. "This is particularly true in high-tech areas where the work being done has large economic or national interest. We're talking about both corporate and political espionage."

In fact, 70% of the survey respondents say their organizations experienced security breaches or instances of cyber fraud over the past two years, including 9% that say they experienced material breaches or frauds.

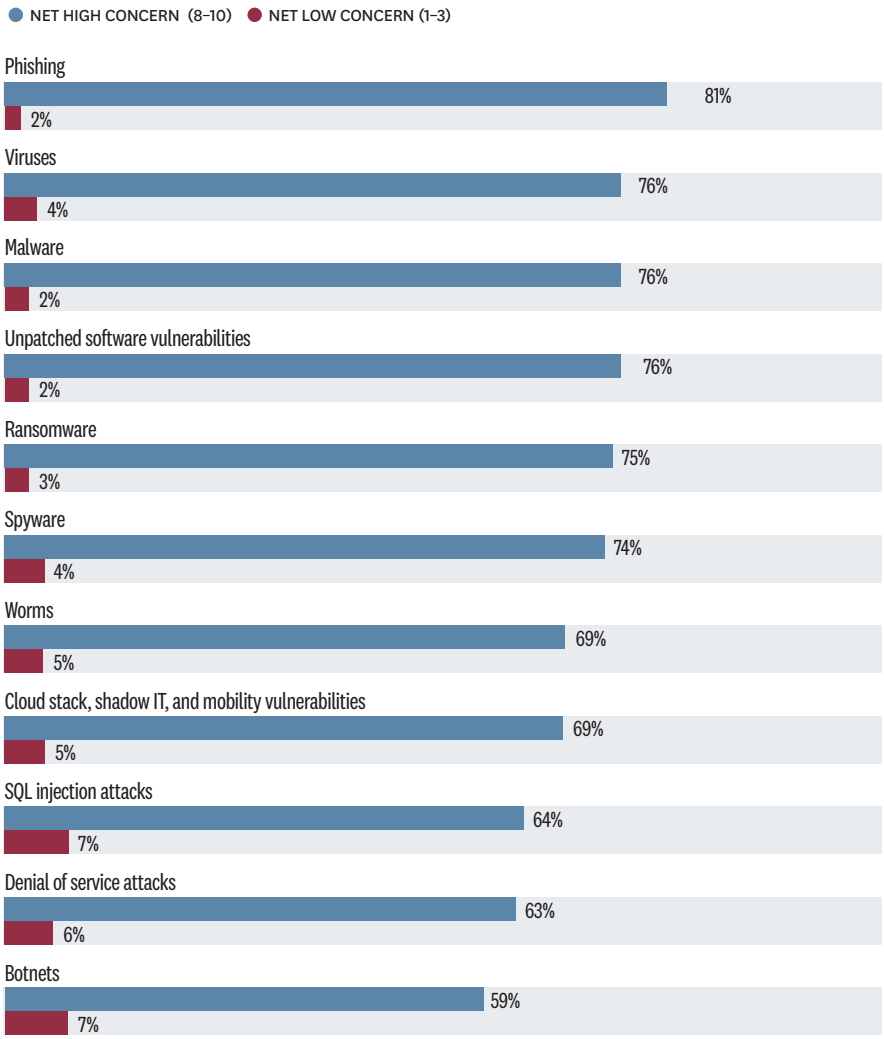
Topping their list of security concerns today is phishing, cited by 81% of respondents as a significant concern—and deservedly so. With the advent of social media, criminals are now able to mount phishing expeditions populated with personal data that can make their missives appear more real than ever. And with IT security tools and systems becoming more sophisticated, targeting computer networks through human vulnerability has become even more appealing to criminals.

Other top security concerns are malware, viruses, and unpatched software vulnerabilities, each of which are cited by 76% of survey respondents. FIGURE 1

FIGURE 1

PHISHING IS TOP CYBERSECURITY CONCERN

How much of a concern are these security issues for your organization?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2018

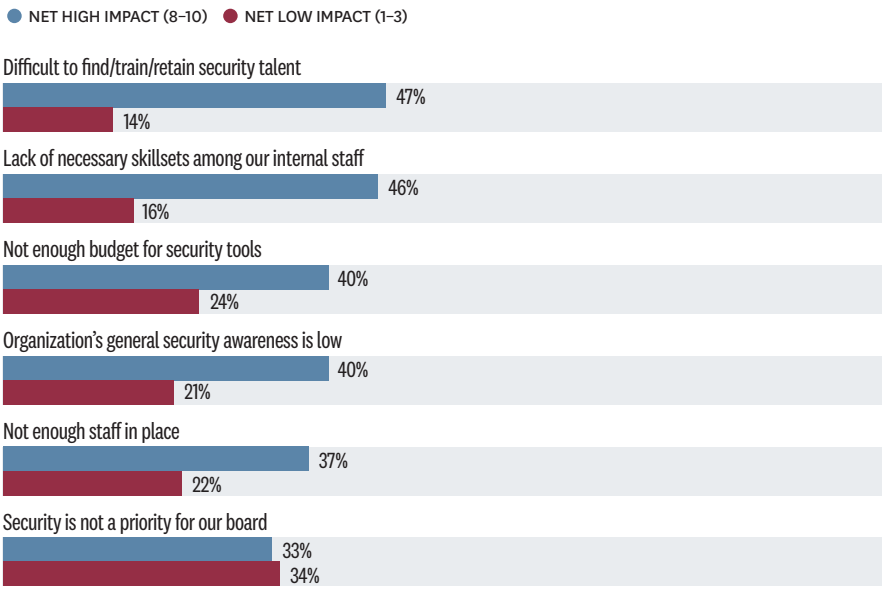
In all of these areas, concern about the specific security issues exceeds confidence in managing them. Only about two-thirds of respondents say their organizations perform well today in addressing the first three issues, and fewer still—60%—say they do a good job addressing unpatched software vulnerabilities.

Alex Maestretti, engineering manager on the Security Intelligence and Response Team for internet entertainment company Netflix, says that staying on top of cybersecurity ultimately boils down to maintaining customer trust, which is critical to long-term success. "We're humbled to have an opportunity to help reshape the media landscape, and one of the ways we could mess that up would be to lose the trust of our customers," he explains. "So we work hard on a lot of different fronts, including security, to maintain that trust, which requires that we act with integrity, and that we are proficient and capable at delivering what we promise. So protecting customer information, and making sure that customers are able to watch what they want to watch when they want to watch it, are top of the priority stack for us."

FIGURE 2

PEOPLE-RELATED ISSUES ARE BIGGEST CHALLENGES TO MAINTAINING CYBERSECURITY

To what extent do each of the following impact your organization's efforts to protect the security of its data and systems and to detect fraud?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2018

Cybersecurity Challenges Extend Beyond Fast-Changing Technology

Beyond trying to keep pace with an ever-expanding list of technological challenges, many organizations today, especially smaller ones, are struggling to protect legacy hardware systems with built-in vulnerabilities to both outside actors and corrupt or unwitting insiders—systems that can nonetheless be expensive to replace.

Money is, in fact, an issue in managing IT security. But it's not the biggest one. Four in 10 survey respondents say securing an adequate budget for cybersecurity tools is having a significant impact on their organization's ability to protect their data and information systems, and to detect fraud. But nearly half say bigger problems revolve around people. Forty-six percent cite a lack of the necessary skillsets among internal staff as a significant hindrance, and 47% cite difficulty in finding, training, and retaining security talent. FIGURE 2

"There's a massive shortage of good security people, and it's expensive to employ them—especially in competitive markets," confirms Steinberg, the consultant to cybersecurity and emerging technologies companies.

Outside the security function, people present yet another challenge to protecting data and systems security, simply because they are human and mistake-prone. "For years, we've trained people how not to get viruses on their computers," says Steinberg. "Don't click on that link sent to you in an email. Don't download software from questionable sources. But despite all of society's efforts, plenty of people still inadvertently infect their devices with malware. Nearly all security breaches begin with human mistakes, and criminals know that, which is why they increasingly target people."

Other challenges to security include failures of imagination. Too many organizations fail to give sufficient thought to what could happen to their data and systems, and so don't prepare for it, says Dan Geer, a computer security analyst and risk management specialist, and chief information security officer of not-for-profit In-Q-Tel.

Cybersecurity Has the Board's Attention—at Most Organizations

Executive and boardroom leaders are well aware of the digital challenges they face and the importance of managing them. Cybersecurity is now "a solidly board-level issue," says Geer. "The firm that does not know this does not have its eyes on the road."

Netflix's Maestretti has seen this first-hand. "Our C-suite is highly engaged in this effort and meets frequently with Jason Chan, our vice president, information security, to discuss in fairly great detail how we're approaching the issue," Maestretti says. "Our board has become more engaged on this topic, too, which is in line with what I'm hearing from my peers across the industry. Boards are just more aware of information security as a business risk."

That said, a third of survey respondents say a significant impediment to cybersecurity is the fact that their board does not make it a priority.

Where boards do make it a priority, at least five key developments appear to be factoring into their thinking. First, their businesses in many instances depend on keeping valuable data, including trade secrets and other intellectual property, secure. Second, and somewhat related, their stakeholders, whether customers or business partners, expect their shared data to be kept safe by the organizations they do business with. Third, regulators are putting teeth behind customer expectations; witness the adoption of the General Data Protection Regulation (GDPR) in the European Union, and the similar if less expansive California Privacy Act of 2018, which goes into effect in January 2020. Fourth, as Maestretti points out, customers expect the organizations they do business with to deliver the goods or services they've promised on time, without being compromised by cyber attacks.

Finally, C-suite executives and corporate board members know their personal liability may be at stake. Although most of the earliest cyber-related shareholder derivative lawsuits against officers and directors were dismissed by the courts, the coast is not incontrovertibly clear. In 2017, The Home Depot Inc. settled a shareholder derivative lawsuit for more than a million dollars in attorneys' fees, and several months later Yahoo settled a similar lawsuit for $80 million.[1]

While officers and directors didn't reach into their own pockets to settle those cases, attorneys at the New York law firm of Pillsbury Winthrop Shaw Pittman have written that corporate directors found to have breached their duty of loyalty—that is, to have been part of an "egregious failure of the board to direct and oversee the business and affairs of the corporation" if it "amounts to conscious disregard of their responsibilities"—could not be indemnified by the corporation they serve in the event of a judgment against them. Pillsbury attorneys also note that public companies may have cybersecurity obligations under Securities and Exchange Commission rules requiring that contingent liabilities be adequately disclosed and that accounting reserves be set up against them where appropriate.[2]

The importance placed on cybersecurity at leading organizations, Geer adds, is evidenced not only by a proliferation of internal controls around it, but also by a willingness among many organizations to buy cyber insurance "even when coverage is priced to market rather than priced to risk."

Basic Hygiene: Benchmarking

Because maintaining cybersecurity is so challenging and fast-moving, and because criminals who find vulnerabilities at one organization will often seek to exploit them at others, leading organizations have found that it makes sense to compare notes with their peers about how to safeguard their data and information systems. In many cases, they now choose to benchmark their cybersecurity systems against each other. For example, 120 firms participate in the Building Security In Maturity Model (BSIMM) study, which describes what those firms are doing on the cybersecurity front and allows participants to compare their work against others' work.[3]

Elsewhere, many organizations participate in an Information Sharing and Analysis Center (ISAC). There are 24 ISACs in operation, all part of a nonprofit, member-driven organization in which private sector entities collaborate with others in their industry and government to share information about protecting their facilities, personnel, and customers from cyber and other security threats.

Only 41% of respondents in the survey by Harvard Business Review Analytic Services say their organizations benchmark their security programs against those of others, although the actual number may be a bit higher. While 26% said their organizations do not benchmark, 34% said they did not know if benchmarking is taking place.

How Leading Organizations Are Responding to the Cybersecurity Threat: Technology

Organizations are backing up their commitment to cybersecurity with hard-dollar investments. Eighty-three percent of survey respondents say their organizations have boosted spending on data and systems security over the past two years, and 85% expect it to increase again over the next two. None say they plan to decrease spending.

Much of that money is going to investments in technology. Nearly two-thirds of survey respondents say their organizations have updated their network security monitoring systems in the past two years. Fifty-seven percent have introduced systems or processes specifically aimed at ensuring compliance with regulations. Nearly half have introduced systems or processes directed specifically at detecting internal (insider) security threats, and a like percentage have introduced systems or processes targeted at driving faster security investigations and faster incident response.

More investment is anticipated. Nearly half of survey respondents say their organizations will continue to invest in their network security monitoring systems over the next two years, and approximately four in 10 will also be investing in improving regulatory compliance, detecting internal threats, and driving faster security investigations and responses. FIGURE 3

Notably, 39% of survey respondents say their organizations will introduce security solutions relying on advanced technologies such as ML or other forms of AI. And 40% say they'll implement new technology that can collect machine data from all of their existing IT systems and rapidly identify potential security threats.

Cybersecurity experts say investments like those are almost inevitable.

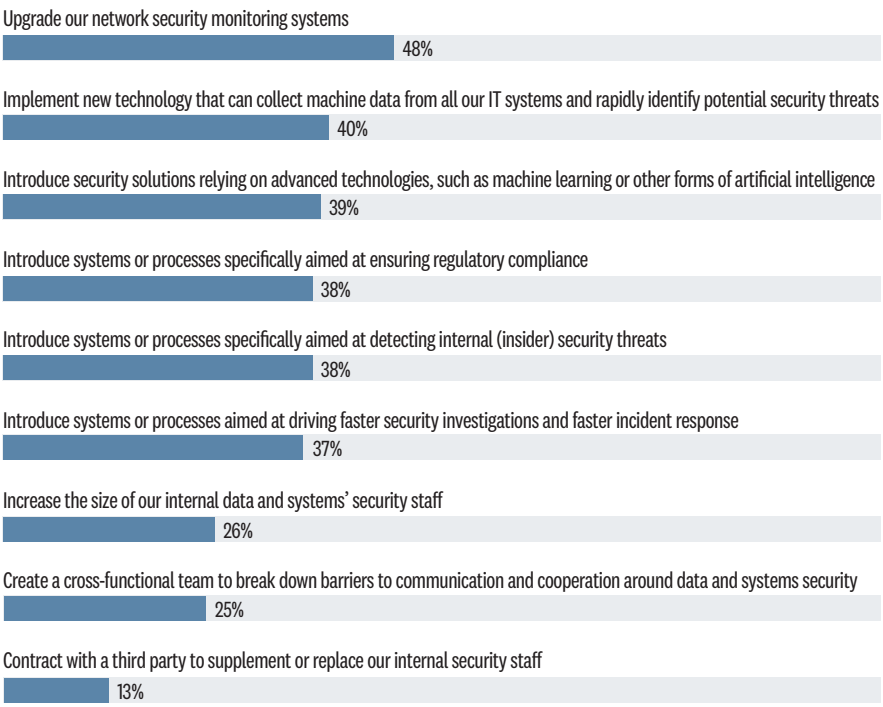
"There's too much data out there," says Steinberg. "The number of people you'd need on a security team to actually analyze the volume of records and alerts that security technology is generating is mind-boggling. That's one reason there is more and more work being done to leverage AI, including ML, to inspect security logs and the like, and to highlight what should be viewed as a high priority. Eventually, we will reach the point at which AI is fully and independently taking action, rather than just identifying action items."

In fact, Steinberg notes, criminals count on the notion that organizations are challenged to identify and investigate every possible security breach or fraud. "There's a hacker strategy that says let's overwhelm the security team by launching many different things at them at once, and even if they react to 99%-plus, they might miss that one that's actually going to make it through. Hackers regularly distract defenders from their real attacks with overwhelming

FIGURE 3

ORGANIZATIONS ARE LOOKING TO TECHNOLOGY TO BOOST CYBERSECURITY

What new initiatives does your organization plan to undertake over the next two years to improve data and systems security, including fraud detection?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2018

numbers of other attacks. Which also raises the issue of the asymmetrical nature of cyber war. The defender has to defend against 100% of attacks, and the attacker only has to get through once."

"We are at the stage," adds In-Q-Tel's Geer, "where firms that do not or cannot choose simplicity, but rather adopt complexity, will have only one path—to deploy algorithms to do what they themselves can no longer do—protect themselves from other algorithms."

Many survey respondents appear to grasp this point. When asked to what extent the use of several advanced technologies is having an impact on their efforts to optimize their security operations—or would have if deployed—two-thirds said advanced analytics, along with automation and orchestration technologies, were having or would have a significant impact. Sixty-two percent said the same about ML, as did 37% about blockchain.

The end goal for most is a highly automated security and fraud-detection program within a dedicated security operations center—one that protects against intrusion or fraud where possible, provides real-time alerts when defenses are penetrated, and, when that happens, enables a fast and effective response. Automation is critical because it augments and empowers security teams by eliminating the repetitive tasks of validating and manually responding to alerts. It allows a small team to do the work of a large one, its members focusing on the more critical tasks that require human assessment, from threat hunting to detection optimization to identifying and approving remediation tactics.

Four Big Cybersecurity Mistakes

Protecting data and information systems from cyber-attacks and fraud is a challenging undertaking that requires sophisticated knowledge and technology. But often, it's the basics that leave organizations vulnerable. Cybersecurity experts say there are four big or common mistakes organizations make.

- **Mistaking compliance for completeness.** "Organizations sometimes think that if they're compliant with whatever checklist or set of rules they adopt, they'll be okay," says Eugene Spafford, professor of computer science at Purdue University. "But when those checklists are put together, they're saying you should do at least this. The 'at least' is often overlooked, and 'the least' is not necessarily the best practice."
- **Not doing enough risk analysis.** Too often, Spafford says, organizations commission a risk analysis from experts, but then give it too little weight, investing in solutions or making economic decisions to achieve lower costs rather than the best result. Worse still, says cybersecurity expert Joseph Steinberg, are organizations that don't even bother to analyze their risks, making it impossible to know what type of security they need to put in place.
- **Not paying enough attention to humans.** "In the end, it is ultimately people who are the issue," says Steinberg. "It's people using technology, it's people making mistakes that lead to breaches, and it's people running cyber attacks, even if those attacks are automated."
- **Assuming there's a finish line.** Because technology is always changing, and because criminals are always looking for new ways to take advantage of it, cybersecurity will remain an ongoing battle. "The biggest mistake would be thinking you can at some point declare success," says computer security analyst and risk management specialist Dan Geer. "You can't."

How Leading Organizations Are Responding to the Cybersecurity Threat: People

In addition to investing in advanced new technologies, companies leading the way in developing proficient data and systems security programs are investing in people—both to access the IT security skills they need and to continue to educate employees on sound IT security practices.

"Leading organizations are hiring people and are willing to pay what doing so costs," says Steinberg. "That means budgeting sufficiently, which often translates to a much larger amount than one might have expected just a few years ago."

At Netflix, says Maestretti, investing in technology and people at comparable rates has been important keep pace with the demands on his organization, particularly as Netflix has seen its paid membership base soar to more than 130 million in over 190 countries.

"We've been very thoughtful in building out our technology and people at the same rate so that if we have technology that's generating alerts, we have people who are able to respond to them," he says. Since Maestretti joined Netflix in March 2016, the Security Intelligence and Response Team has roughly tripled in size. That expansion has not only allowed some team members to specialize, but also created more time for them to develop tools to automate processes and further improve their efficiency.

Where companies don't have sufficient internal expertise in cybersecurity—and can't afford to make the necessary hires—experts recommend they look not just to automation but also, in some cases, to third-party providers. "For small- and medium-size organizations, it may be better to outsource to a reliable firm," says Purdue's Spafford. "As we get into larger organizations, a hybrid model, where you have some people internally and some external resources, begins to make sense. And when you get to really

As technology advances and the human brain doesn't, **we become the weak link in the chain**, observes Steinberg.

large organizations that have special needs, they're able to staff a larger organization and enforce the policy that goes with it."

Leading organizations also prioritize mitigating human error related to IT security. "Technology advances rapidly, but the human brain takes many thousands of years to evolve. As such, humans increasingly become the weak link in the security chain," observes Steinberg. "Training people to recognize phishing attacks, and using test phishing emails to verify folks' relevant performance, as well as using social media security systems to make sure people do not overshare information on social media, are among the human-centric approaches advanced companies are utilizing. Such defenses can deliver a significant return on investment, because reducing your exposure to human mistakes can have dramatic, positive security implications."

Conclusion

Few if any organizations can afford to opt out of the cybersecurity war. The worst consequences of having data or information systems compromised are simply too great. They can include a loss of intellectual property, material disruptions to operations, a loss of customer trust and corporate reputation, and regulatory penalties.

Increasingly, fighting that war requires sophisticated cybersecurity technology, including a protection platform that can continually monitor information systems and kick out prioritized, real-time alerts to anomalies and threats.

So how do you build a strong cyber-security program? Cybersecurity experts offer these additional tips:

- Develop and maintain a cybersecurity threat model. For decades, smart organizations have been developing threat models in which they seek to identify and prioritize vulnerabilities in their data and information systems. Those that have not done so need to go through this exercise, and continually update their model.
- Quantify cybersecurity risks. Knowing what's at stake if cyber defenses are compromised can sharpen an organization's focus on where it should be directing its cybersecurity resources. "The traditional approach to risk has involved ranking risks on a scale—high, medium low," says Maestretti. "We need to be able to talk about risk in dollar terms."
- Uniformly enforce rules for protecting data and network integrity. All employees, from frontline workers to the occupants of the C-suite, should have access only to what they need—minimizing the potential for internal attacks or mistakes.
- Invest in ongoing training and education around cybersecurity. This includes training and education not only for IT staff, but for the entire employee population.
- Look for opportunities to re-architect information systems. Rather than making incremental upgrades when some part of the technology infrastructure has to be replaced or patched, look for opportunities to overhaul the infrastructure in ways that fundamentally improve security, placing special emphasis on those areas where security is most important.
- Stay on top of emerging security technologies. The newest technologies can provide new solutions to growing security challenges, such as resource management, an ever-expanding attack surface, and the constantly evolving tactics of intruders.
- Test and benchmark your defenses. Geer advises organizations to hire consultants to do "brutal testing" of their information networks, identify the level of effort needed to penetrate or compromise their defenses, and assess whether or not those defenses are sufficiently robust given what they know or can imagine an intruder might try to do. Then, he says, organizations should hire a different consultancy to repeat the exercise. He also urges organizations to join the Information Sharing and Analysis Center relevant to their industry to further benchmark themselves against their peers.

Ultimately, no organization can ensure that it will never be compromised by a cyber attack. But all organizations can make it dramatically harder to penetrate their cyber defenses. With the right systems in place, they also can ensure that they are able to spot unwanted cyber activity and quickly contain it.

METHODOLOGY AND PARTICIPANT PROFILE

A total of 222 respondents drawn from the HBR audience of readers (magazine/newsletter readers, customers, HBR.org users) completed the survey.

SIZE OF ORGANIZATION

47% 10,000 OR MORE EMPLOYEES

37% 1,000-9,999 EMPLOYEES

16% 500-999 EMPLOYEES

0% 499 AND FEWER EMPLOYEES

SENIORITY

9% EXECUTIVE MANAGEMENT/ BOARD MEMBERS

50% SENIOR MANAGEMENT

32% MIDDLE MANAGERS

7% OTHER GRADES

KEY INDUSTRY SECTORS

14% FINANCIAL SERVICES

12% TECHNOLOGY

10% HEALTH CARE

9% MANUFACTURING

8% OR LESS OTHER SECTORS

JOB FUNCTION

21% IT/SECURITY

18% GENERAL/EXECUTIVE MANAGEMENT

10% CONSULTING

8% OR LESS OTHER FUNCTIONS

REGIONS

37% NORTH AMERICA

31% EUROPE

18% ASIA/PACIFIC

8% MIDDLE EAST/ AFRICA

5% LATIN AMERICA

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

ENDNOTES

1 "D&O Insurance, Cyber Liability, and a (Big) Crack in the Board's Armor," Anderson Kill P.C., April 24, 2018

2 "What Corporate Directors Need to Know about Cybersecurity," by David M. Furbush and David M. Lisi, Pillsbury Winthrop Shaw Pittman LLP, November 14, 2017

3 BSIMM, www.bsiimm.com, viewed November 12, 2018

Harvard Business Review
ANALYTIC SERVICES

hbr.org/hbr-analytic-services

CONTACT US

hbranalyticservices@hbr.org