Forbes INSIGHTS

ENTERPRISES RE-ENGINEER SECURITY IN THE AGE OF DIGITAL TRANSFORMATION

CIOs AND CISOs NEED A NEW SECURITY MODEL TO CLOSE TODAY'S SECURITY GAPS AND EFFECTIVELY WAGE CYBER WARFARE

IN ASSOCIATION WITH: bmc

Forbes INSIGHTS

CONTENTS

INTRODUCTION

It's no secret that CEOs across North America and Europe have been marshaling forces for digital transformation in a high-stakes battle to ward off ambitious insurgents, maintain market share and address the changing demands of today's customers. This is a once-in-a-generation challenge for any business leader, but it's not the whole story. Behind the scenes, a fourth imperative is being added to the list of transformation considerations—combating modern cybercriminals.

Security managers are seeing upheaval within their own organizations as they adopt new security policies and technologies designed to keep pace with the changes happening within business units. The extent of this disruption is undeniable—69% of senior executives recently surveyed by Forbes Insights and BMC believe that digital transformation is forcing them to rethink their cybersecurity strategies.

This survey also found that security transformation doesn't affect only the technology choices enterprises make to ward off cyber-thieves. The aftershocks are rippling throughout large companies and causing them to rethink how they organize internal stakeholders, assess risk and prioritize future investments. In short, many firms are rewriting their cybersecurity playbooks.

"We're taking a new look at cybersecurity from a variety of facets—from within the enterprise and user end-points to our broader ecosystem of partners and digital channels," says Michael Mathews, CIO of Deluxe Corp. A century ago, Deluxe Corp. began its check-manufacturing business and steadily rose to a leading position within the market. But after senior leaders recognized that credit cards, digital wallets and Bitcoin threatened their established business model, the company made an aggressive move—and found a new model for success—by providing marketing solutions and other services to financial institutions and small businesses.

Deluxe isn't alone in realizing that with new business models comes the need to rethink security. In this report, we highlight key findings from a recent survey of more than 300 CIOs and CISOs, and outline how executives are actively revising security models to create a culture of cybersecurity and safeguard their organizations in today's continually changing business environment.

KEY TAKEAWAYS

69% of senior executives say digital transformation is forcing fundamental changes to security strategies

64% will boost spending to protect against known security threats

43% will make timely patching and remediation a higher priority in 2017

68% plan to enhance incident response capabilities in the next 12 months

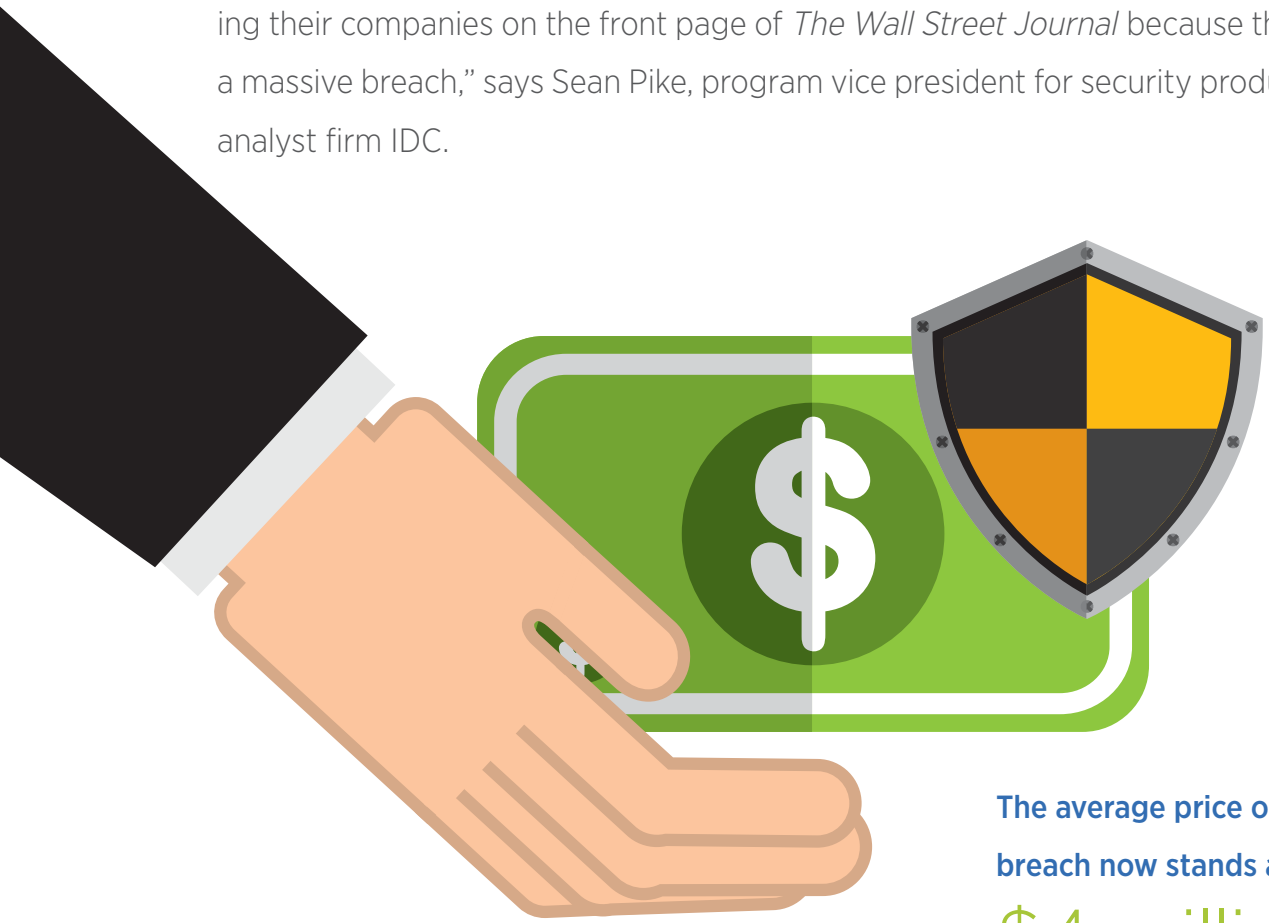
Operations teams are seeing heightened accountability for security breaches

72% believe line-of-business managers must take a greater role in developing security strategies

Nearly half of enterprises will combine security and operations personnel into teams for fortifying mission-critical applications

THE NEW REALITY— WHAT'S AT STAKE

When hackers breach cybersecurity defenses, the risks to enterprises are enormous, ranging from financial losses and damage to corporate reputations to exposure of intellectual property and the release of sensitive customer information. One worry encapsulates all these perils. "The biggest fear of the CIOs and CISOs I speak to is seeing their companies on the front page of *The Wall Street Journal* because they've had a massive breach," says Sean Pike, program vice president for security products at the analyst firm IDC.



The average price of a data breach now stands at about

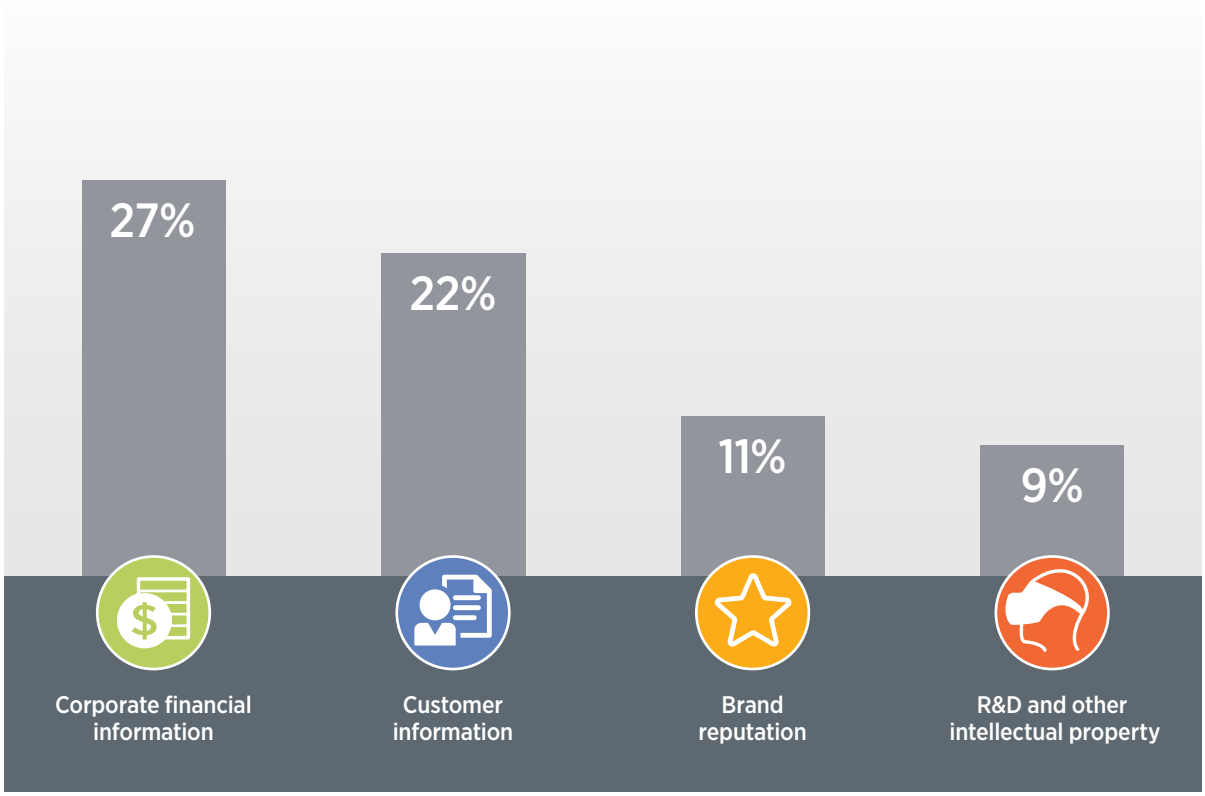
$4 million

This concern is well-founded. Headline-grabbing breaches have become routine in recent months, and corporations are paying the price. The average price of a data breach now stands at about $4 million, according to the Ponemon Institute.[1] But the financial damage from a massive breach can be much higher. The fallout for one large retailer is estimated at $252 million.[2]

While financial concerns are real, the Forbes Insights/BMC survey finds that two dangers in particular are causing executives on both sides of the Atlantic to lose sleep: the theft of corporate financial data and the theft of customer information. Both are described as the most important assets to protect against a security breach, more so than other important areas like intellectual property and employee information.

Unfortunately, the risks to these and other corporate assets will likely grow in the months ahead. CIOs and CISOs must not only address a sophisticated army of global cyber-thieves—many of whom are backed by national governments—but simultaneously close the new security gaps that arise as their organizations embrace digital transformation.

FIGURE 1. Most Important Assets to Protect Against a Security Breach



[1]http://businessinsights.bitdefender.com/security-breaches-becoming-more-costly

[2]https://www.rsaconference.com/blogs/do-data-breaches-affect-company-value

NEW TECHNOLOGY = NEW CHALLENGES

New business priorities and the technology arriving to support them are creating new challenges for IT and security staffs. The top three technologies cited in the Forbes Insights/BMC survey as having the biggest security implications are public clouds, big data and mobile applications, each of which have seen high adoption rates in recent years.

Cloud and mobile technology create security threats because they send data flowing into, or out of, well-controlled internal networks. Big data is a concern because to manage and analyze it, enterprises must consolidate information within central storehouses, which, if breached, give thieves one-stop shopping for a trove of valuable corporate data.

In addition to the individual security implications of each technology, their collective impact is reshaping corporate strategies. "Organic and inorganic business growth changes the attack surface and risk profile for an organization," says Cameron Brown, a cyber-defense advisor and cybersecurity strategist based in Frankfurt, Germany, and a former digital forensics specialist for the United Nations. "As information systems converge and disparate networks are linked together, new security vulnerabilities emerge.

The specific types of security challenges that new technology creates is one area of widespread agreement among enterprise executives, no matter what their job title or location.

"Architects of secure environments carefully tailor their systems to meet challenges within a specific context. When the context shifts, so too do the stressors that impact these systems. For continuous security improvement to occur, change management must be a key part of enterprise growth and contraction."

The specific types of security challenges that new technology creates is one area of widespread agreement among enterprise executives, no matter what their job title or location. Across the board, the primary security challenges arising from new business and technology trends are end-user authentication, keeping the organization up to date on the latest exploits and improving security training for end-users.

The need to address these priorities, while maintaining traditional defenses, is convincing IT and security managers to reevaluate and update their security strategies.

FIGURE 2. Technologies With the Biggest Security Implications

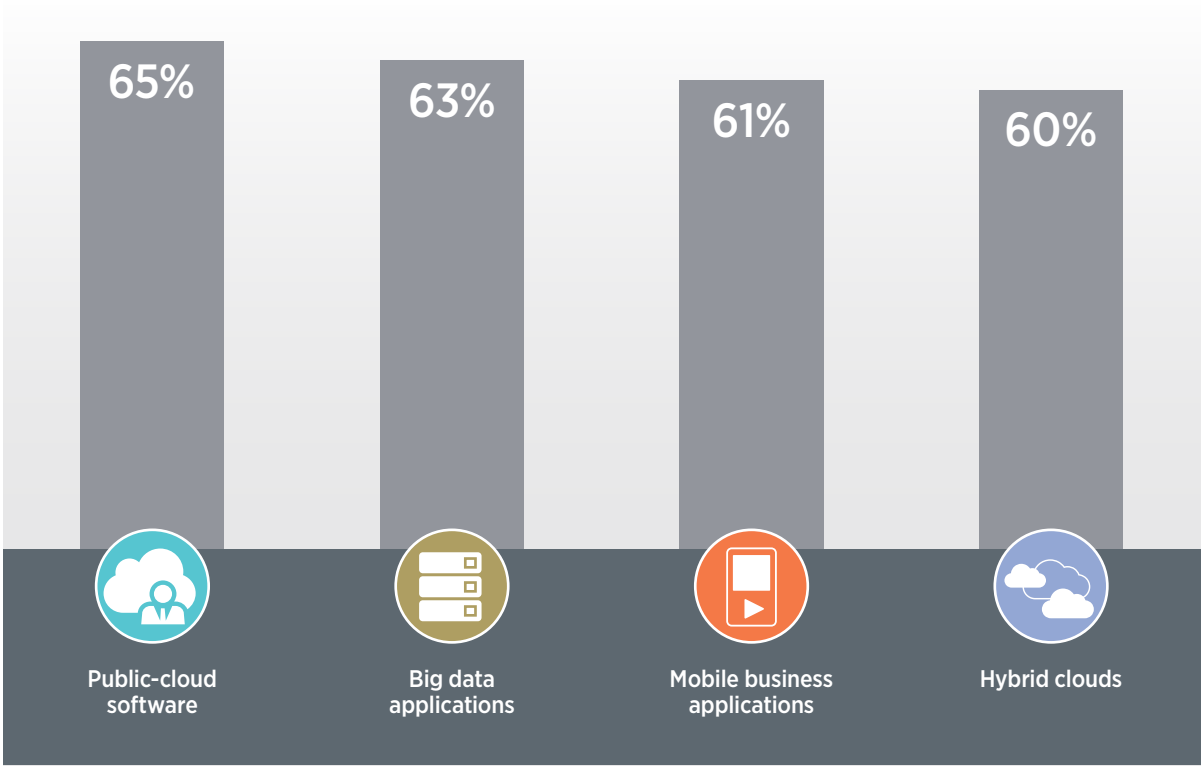
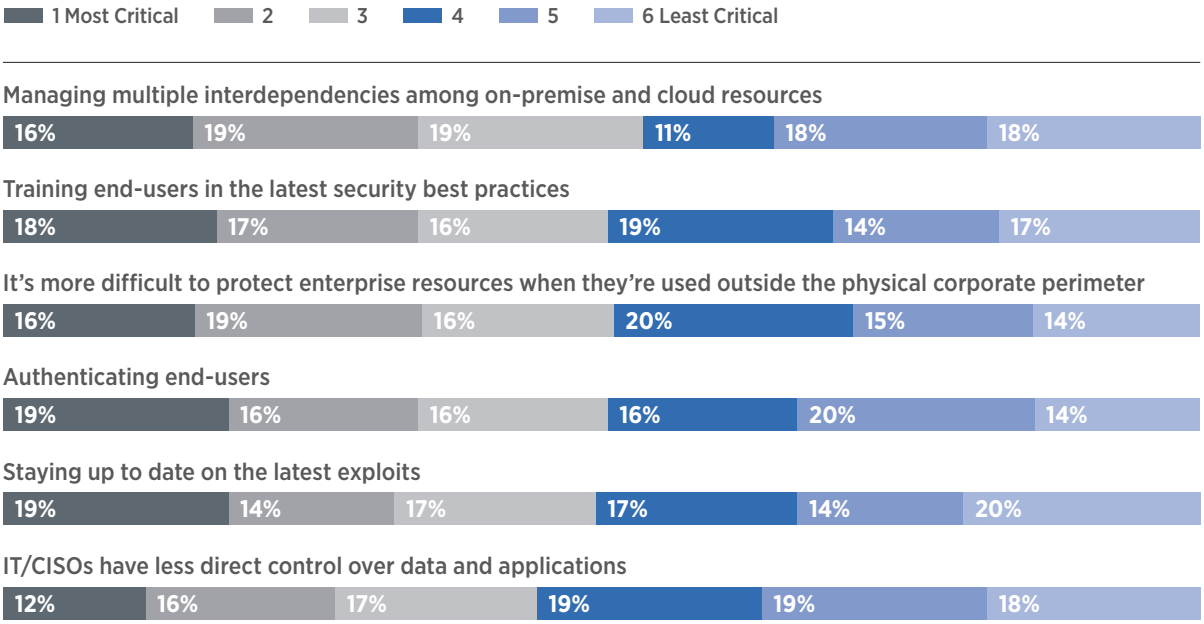


FIGURE 3. Ranking of the Security Challenges Arising From New Business and Technology Trends



FUNDING PRIORITIES:
INNOVATION VS. SECURITY

As digital transformation pushes IT and security leaders to reevaluate and rethink their cybersecurity strategies, it's also impacting enterprise priorities. A solid majority—74%—of CIOs and CISOs say security was a higher priority in 2016 than in the previous year, and a decisive 82% of executives in Europe and North America say security investments will rise again in 2017.

But these executives also acknowledge that when lobbying for additional security funding, technology leaders are competing with business peers, all of whom are trying to convince the board where it should allocate money. Most respondents say their C-suite and board will earmark significant percentages of new funding for business innovation and IT modernization. "Line-of-business people want new, next-generation technology, so the big question for boards is, 'Where should we focus our funding efforts?'" says Scott Crowder, CIO at BMC, a vendor of enterprise management software. "Do you devote money to maintaining the old environment and preventing security problems that might happen, or do you invest in technology that could be a game changer for the business unit?"

THE ANSWER: Boards are willing to increase investments in security if proposals come with solid business models.

A decisive 82% of executives in Europe and North America say security investments will rise again in 2017.

WAGING CYBER WARFARE

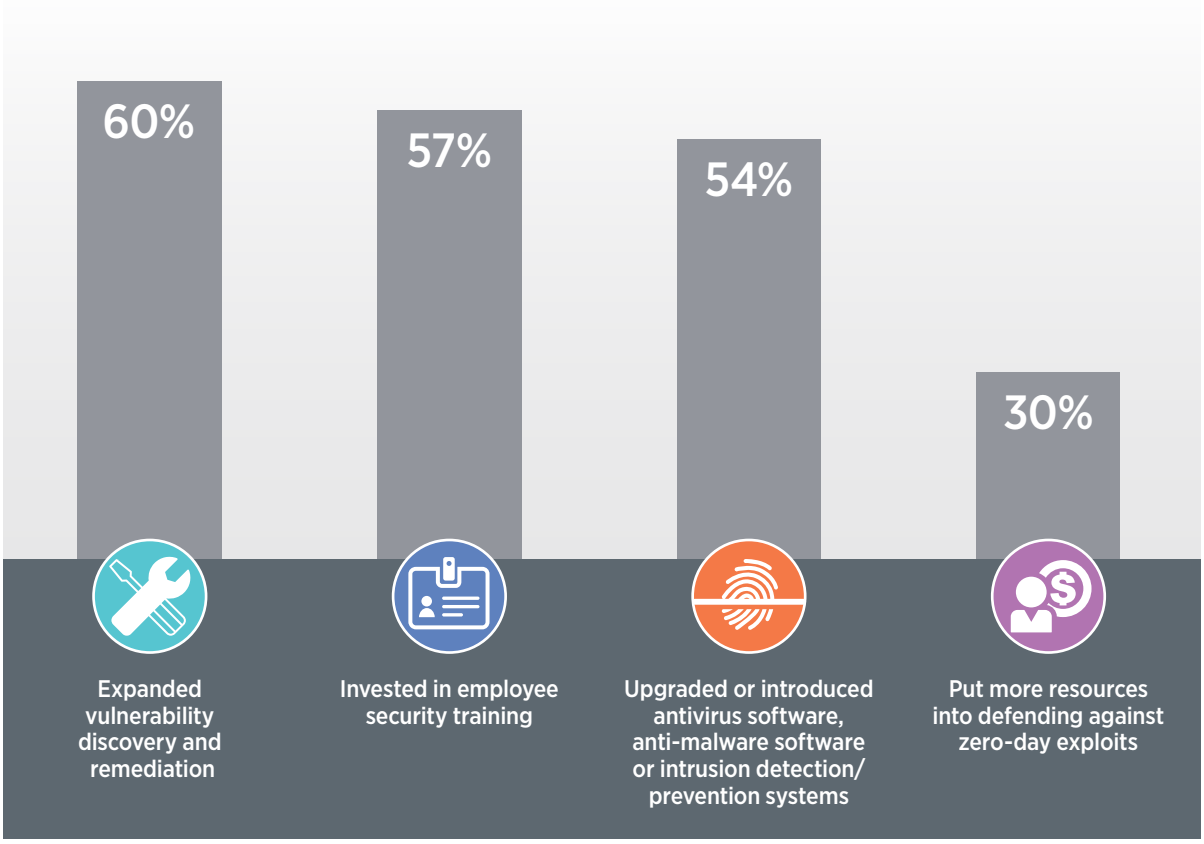
According to the Forbes Insights/BMC survey, change to enterprise security profiles was under way in 2016, and CIOs and CISOs have clear plans for the new, or ongoing, changes they'll need to make in the coming year.

In 2016, enterprises placed greater emphasis on two initiatives to make themselves less attractive to hackers: vulnerability discovery and breach remediation. Going hand in hand with these efforts are strategies that emphasize proactive measures. "In the past, security teams in many organizations have been reactive," says Betty Elliott, head of information security and CISO at MoneyGram International. "Now the focus is on what we can do to gain greater visibility into attacks and attempted breaches so we can act more quickly. That shift from reactive to proactive is something that we've been more focused on, and it's making a significant difference in how quickly we can defect and mitigate threats."

Another area drawing greater attention in recent months is employee training, presumably to keep people informed about the latest exploits and, in turn, make them less vulnerable to targeted social engineering and phishing attacks.

To make way for this new focus, enterprises have made upgrades to tried-and-true antivirus software, anti-malware software and intrusion-detection systems less of a priority. Looking ahead, the biggest priorities for IT and security executives include addressing a venerable problem—protecting against and responding to known security threats.

FIGURE 4. Primary Initiatives Undertaken in the Past Year to Make My Organization Less Attractive to Hackers

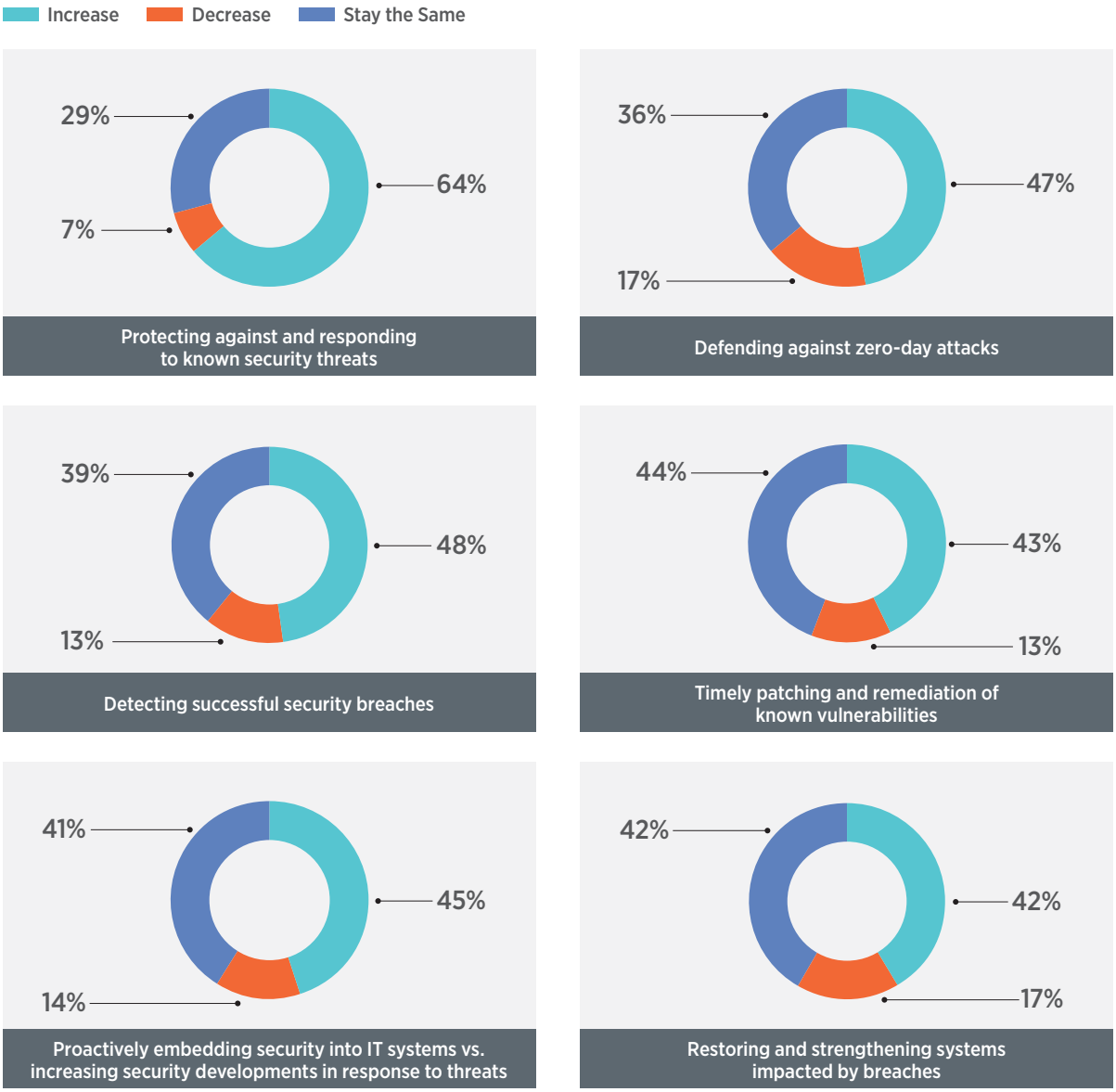


In 2016, enterprises placed greater emphasis on two initiatives to make themselves less attractive to hackers: vulnerability discovery and breach remediation.

It's no wonder that protecting against known threats is poised to see the biggest change. For years, enterprises have grappled with the challenge of quickly updating security patches and other remediation because of scheduling and logistical issues that left organizations unnecessarily vulnerable. Not closing the door on an imminent danger can be a business disaster for companies and a career killer for security professionals.

Also high on the list of priorities are two activities that round out known-threat strategies: defending against zero-day attacks (the second in the sequence of one/two defensive punches) and timely patching and remediation of known

FIGURE 5. How Security Priorities Will Change in Priority Over the Next 12 Months



Note: May not add to 100% due to rounding.

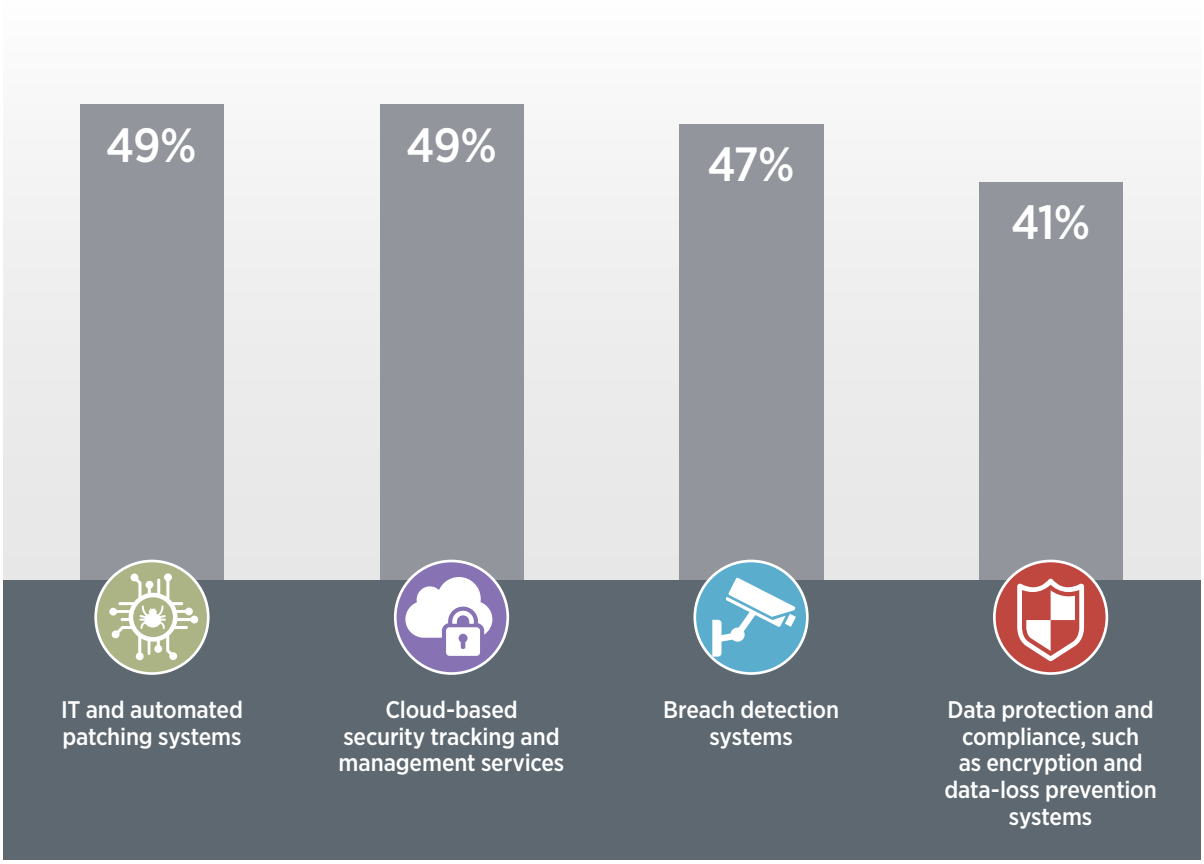
The appeal of patching systems is a combination of its effectiveness and the fact that it's a good investment.

vulnerabilities. The latter is accomplished through technologies that automate patching and closer coordination between IT and operations staff. It's noteworthy that the appeal of patching systems is a combination of its effectiveness and the fact that it's a good investment. A majority of executives named investments in IT and patch-automation systems as the ones that delivered the best returns on their security investments in the past year.

Investment plans for the next 12 months seem to be in sync with priorities. Further demonstrating the diminished role of anti-malware solutions in modern security efforts, advanced antivirus solutions rank lowest in funding plans. By contrast, patch-automation systems top the list of areas set to receive the highest funding. It's tied with cloud-based security tracking and management services, and followed closely by breach detection systems and data protection and compliance tools, such as encryption and data-loss prevention systems.

At the same time, more than two-thirds of CIOs and CISOs say their enterprises will give incident response a higher priority in the next year. They'll do that primarily by making better use of existing tools and by evaluating and adopting cloud-based incident-management solutions.

FIGURE 6. Areas That Will See the Highest Investment in the Coming Year

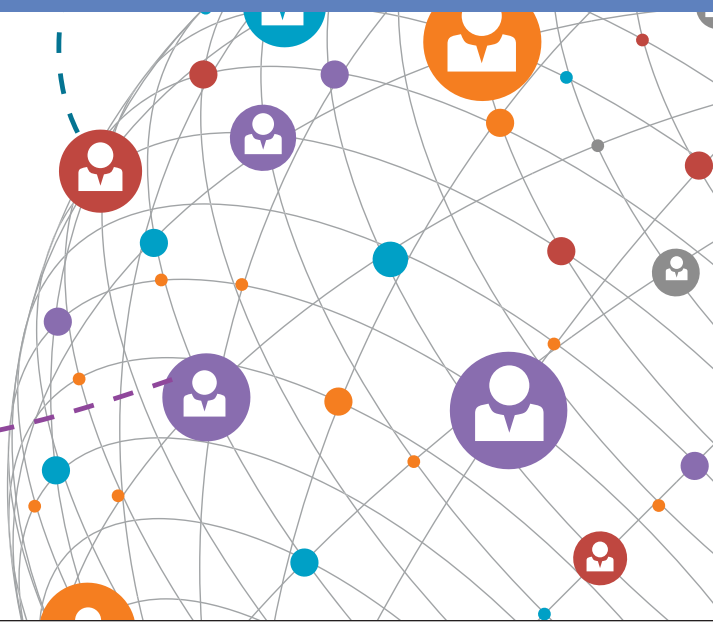


THE PEOPLE IMPERATIVE

Addressing the technology changes associated with digital transformation and resetting investment priorities will be important for modern security strategies, but they're not the only considerations. For many organizations, addressing modern cybersecurity challenges has as much to do with culture and organizational structures as with technology. Unfortunately, in an era of technology innovation and upheaval, many roadblocks still keep enterprises from successfully creating a culture of cybersecurity for all stakeholders.

52%

of executives say accountability for security breaches has increased for the operations group.



"Misaligned reporting and governance structures can quickly lead to dangerous blind spots," Brown says. "Many organizations lack clarity around security roles and accountabilities because some still see security as an IT issue rather than a business asset. Where silos exist and there is a disconnect between operational teams and middle management, an impasse occurs. Critically, the C-suite needs to be aware of where valuable information is disbursed across their enterprise and how a compromise of that information will impact profitability, branding and reputation."

The Forbes Insights/BMC survey finds signs of problems in traditional reporting structures. While CISOs continue to report directly to CIOs at 43% of the companies surveyed, more than a quarter of respondents say this structure is only moderately effective, or not effective.

What's the underlying cause of this discontent? One reason is that the two groups aren't always on the same page about the degree of cyber-threats. For example, 33% of CIOs see public clouds as having an extreme impact on security, and while CISOs also rank cloud as their biggest concern, a much smaller group of them—21%—see it as such an extreme threat.

"In general, CIOs are more focused on technology innovation than security. By making the CISO a true executive, the corporation gains greater transparency over security operations by giving security people a direct reporting structure to the board of directors."

—Sean Pike,
Program Vice President,
Security Products, IDC

A dichotomy exists for big data applications as well. Nearly a third of CIOs see this area having an extreme impact, which is a level of intensity shared by only 18% of CISOs. Mobile technology follows suit, with a 12-percentage-point difference between CIOs and CISOs who believe untethered devices and apps raise the loudest alarms.

There are other underlying frustrations when CISOs report to CIOs. "When that's the organizational structure, CISOs are chief executives in name only," Pike says. "In reality, they're more of a senior vice president, because that's the level of power they actually have."

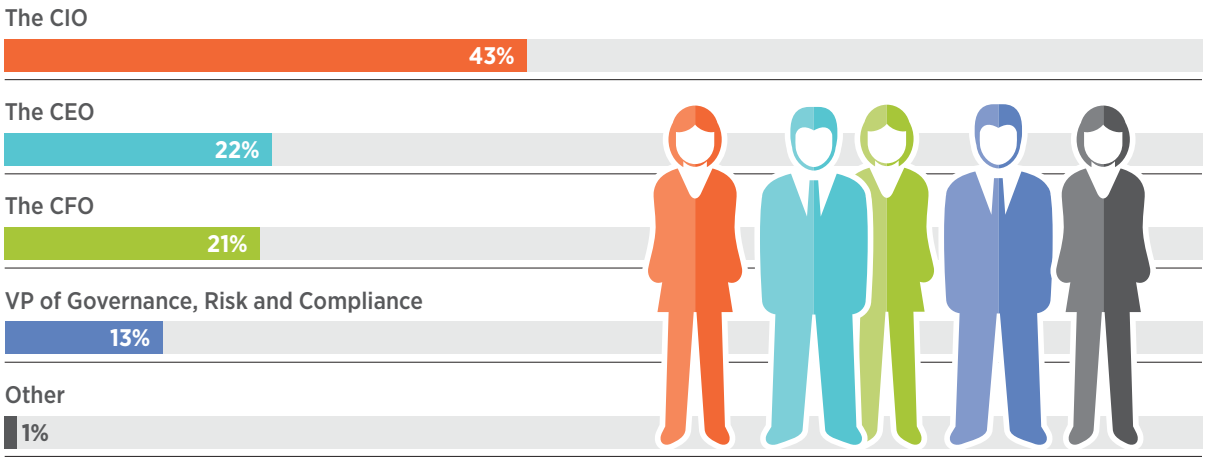
Pike also believes that moving CISOs from under the CIO's direct control is a better division of responsibilities. "In general, CIOs are more focused on technology innovation than security. By making the CISO a true executive, the corporation gains greater transparency over security operations by giving security people a direct reporting structure to the board of directors."

What other organizational changes would improve security? A large majority—65%—of CIOs and CISOs believe security would improve if the security staff collaborated more closely with operations teams. This is a sign of the operations staff's heightened responsibility for security breaches. More than half—52%—of executives say accountability for security breaches has increased for the operations group.

Specifically, the operations team is seeing increased responsibility for ensuring that known remediation, such as patches for previously identified malware, is applied within established service level agreements.

The operations department isn't the only area where closer coordination over security would have a positive impact. The security role of line-of-business managers is also evolving in today's era of transformation. Forty-one percent of North American executives say better collaboration between security and LOB managers is important, and nearly three-quarters of executives in Europe and North America believe LOB managers must take a greater role in better prioritizing security investments.

FIGURE 7. Whom Does the CISO Directly Report to in Your Enterprise?

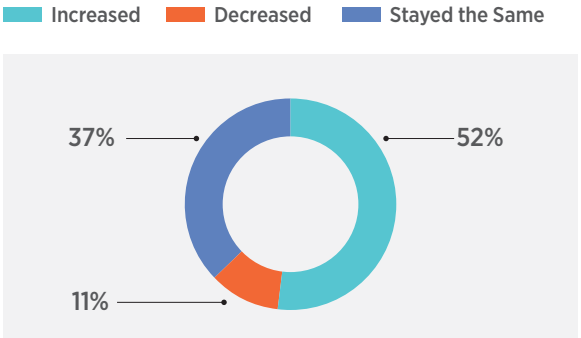


"The reality is that the line of business has a much better appreciation for the relative importance of individual data assets, down to each client, product and transaction, and whether each should be considered confidential, secret, top secret or public," says Paul Lewis, chief technology officer for Hitachi Data Systems.

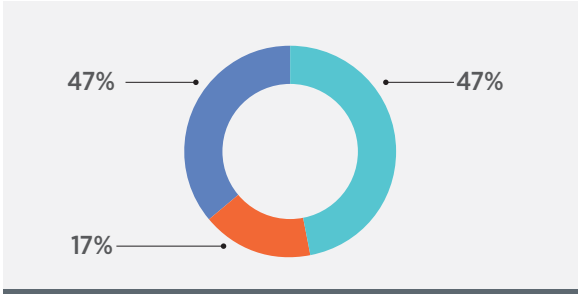
Given finite resources, the security staff needs these insights to prioritize its efforts and ensure the most valuable assets receive the right resources. Fortunately, mutual goals are helping to tighten the bonds between security teams and business people. "Security professionals must rely on the line of business to tell them what applications they're using, otherwise companies run the risk of shadow IT," Pike says. "At the same time, the line of business wants to know how to protect customer and financial data, and they view security folks as the experts for doing that. So business people are increasingly reaching across the aisle."

However, to fully promote greater collaboration, the security and business groups must work through any longstanding friction. For example, some business owners resist seeing their most critical systems patched regularly, fearing that the change process will increase downtime and lead to lost productivity. A close partnership for ironing out when best to schedule updates, along with extensive testing of patches, will help alleviate these concerns.

FIGURE 8. How Has the Role of the Operations Team Changed With Respect to the Following?



Accountability for security breaches



Ensuring that known remediation is applied within established service level agreements

A NEW SECURITY MODEL

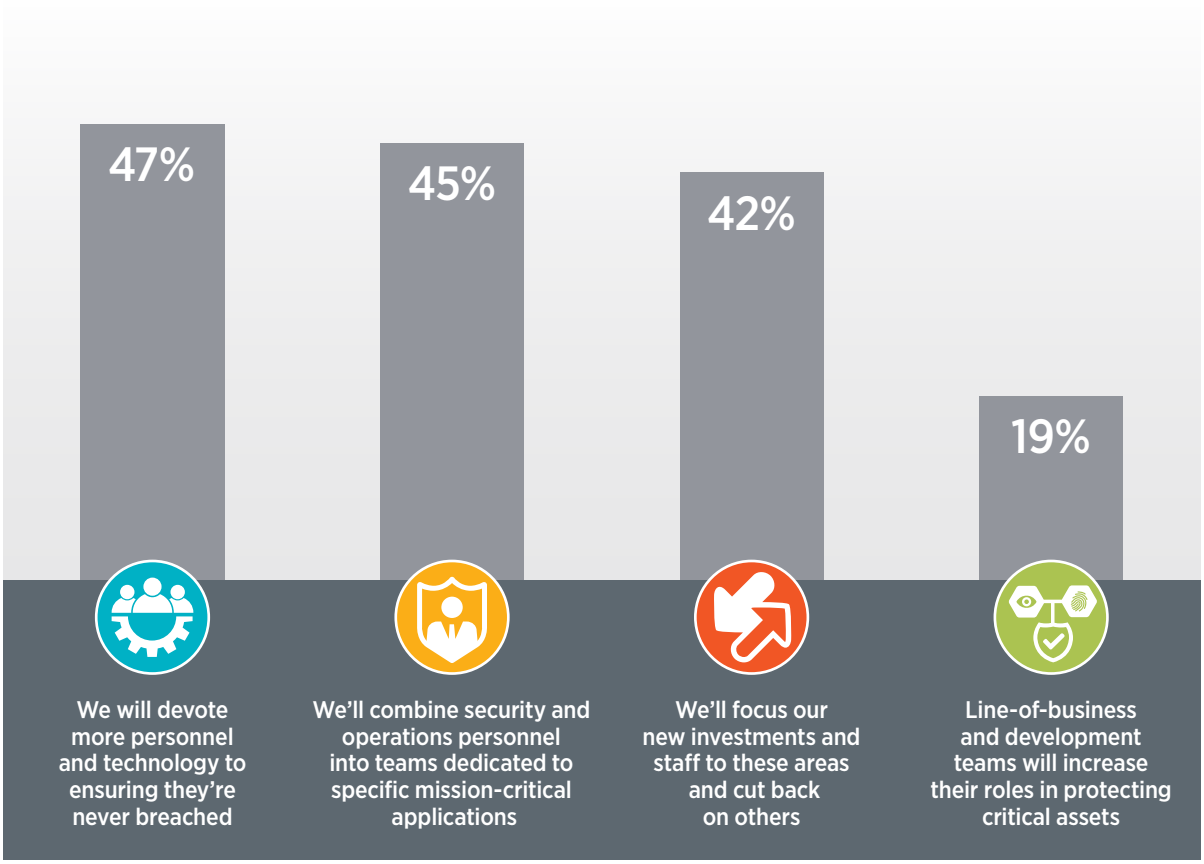
Security veterans acknowledge that fewer C-suites and boards today need to be schooled on how security is a strategic asset to businesses. No longer is security viewed as a costly necessity with an unknown ROI. Business executives now generally understand that customers gravitate to companies with the highest reputations for security, or conversely avoid those that have been victims of high-level breaches. Nevertheless, CIOs and CISOs won't have an open checkbook for every new funding request, as modernization continues to take precedence in the years ahead.

What will be the key to building an effective business case for security in the future? Justifications should focus on two essential areas. First, when it comes to new products and services, IT and security executives must demonstrate that proposed investments are where the organization will see the highest value for its security dollars. Second, as noted earlier, CIOs and CISOs must continue to look beyond technology by addressing organizational and personnel issues.

One of the best ways to maximize the impact of new investments is to direct them to mission-critical assets. This aligns with the longstanding industry truism: if everything is protected equally, then nothing is adequately safeguarded. Many executives agree that targeting available resources to mission-critical applications is one way to get the biggest impact from their investments. In fact, 47% say their companies will devote more personnel and technology to ensuring they're never breached. A greater emphasis on critical assets will also help alleviate the concerns cited earlier among

Many executives agree that targeting available resources to mission-critical applications is one way to get the biggest impact from their investments.

FIGURE 9. How Are You Planning to Protect Mission-Critical Resources in the Next Year?



"They're not looking for configuration files on your operating systems; they're looking for credit card information, for customer data, transaction histories and proprietary documents."

—Paul Lewis, CTO, Hitachi Data Systems

business managers who fear a loss of productivity as a result of the poorly coordinated patching of essential resources.

IT and security leaders are planning other related steps as well. A similar percentage—45%—expect to combine security and operations personnel into teams dedicated to specific mission-critical applications, presumably to create quasi SWAT teams with combined skills to best safeguard individual assets. Demonstrating their commitment, executives say actions like these justify cutbacks in other areas, presumably for more traditional measures like updates to network firewalls and antivirus software.

Some CIOs are ahead of the curve in this area. For the past year, BMC has bolstered the security of its critical assets with an extensive network segmentation and segregation effort. The goal: if people without the proper authorization were ever to access its network, they would be walled off from the most valuable corporate resources. "More and more, we're compartmentalizing business applications into small segments of the network and creating entry points only where they're needed," says BMC's Crowder. "In this way, someone would need intimate knowledge of communications ports and other entry points from one segment to the next, rather than having a flat network they could traverse without any boundaries."

Another strategy for protecting the most valuable assets managed by enterprises is to shift thinking from safeguarding applications and systems to securing the data itself. "Here's the reality: your organization doesn't get bad press because you let bad guys into your network. It's because of what they stole once they broke in," says Hitachi Data Systems' Lewis. "They're not looking for configuration files on your operating systems; they're looking for credit card information, for customer data, transaction histories and proprietary documents. Data is the focal point, not the infrastructure and applications that are supporting it. Therefore, data becomes the asset that we need to secure most."

In response, Lewis's company created the position of chief data officer, with the responsibility of being the steward of corporate information—and advises all enterprises to do the same. "If you don't have someone like that in charge, then, arguably, nobody is responsible for protecting valuable information," he says. "Once you have a responsible party, you can implement data-centric capabilities, such as classification, stewardship, storage, auditing and compliance, and security."

IDC's Pike says the heightened emphasis on securing data versus systems recognizes the new realities of digital transformation. "The key word here is 'distributed.' We have distributed workloads, distributed office environments, employees who are distributed, devices that are distributed," Pike explains. "As a result, data is constantly flowing in and out of organizations, which in turn means enterprises must protect data wherever it is at any time."

To do this, corporate security arsenals must include tools that tell organizations exactly who is accessing individual files, whether these people are in fact who they say they are, and where they are physically located when they log on to networks. "We are seeing a huge uptick in identity and access management applications," Pike says.

Accurately identifying and authenticating the people trying to access sensitive data is aided by a category of sophisticated software dubbed user and entity behavior analytics, or UEBA. Essentially, these programs compare real-time activities with usual patterns of behavior and alert the security staff when anomalies occur. For example, alerts would sound if someone in the marketing department suddenly tried to download personnel files from HR. Similarly, security personnel would be

notified if someone who logs in from a U.S. location one minute, then tries to gain network access from China a short time later. "These types of resources ensure we have as many eyes as possible looking at our crown jewels," Crowder says.

Lewis also notes organizations' increased interest in analytics. "I see enterprises spending a lot more money on this area than they have in the past," he says. "It's part of an effort to have detailed insights into security activities so they can better manage incidents and make sure their data isn't corrupted in any way."

Some global enterprises are already seeing a payoff from their investments in analytics. MoneyGram International, for example, uses an advanced analytics tool that enables early detection of potential problems across the more than 200 countries where it conducts business. The security department also employs a team of statisticians who watch for anomalous behavior. Although the company saw a significant increase in the number of situations that required attention in 2016, MoneyGram International saw a substantial reduction in losses that same year. "It's all about using the information that we have and fully leveraging it to detect events and prevent incidents from occurring," Elliott says.

"In the past, we protected the castle. But because the castle is now all over the world, these global, cloud-based security tracking mechanisms become more valuable."

—Scott Crowder, CIO, BMC

As enterprises enhance their security-analytics capabilities, they're looking beyond traditional onsite options to security being handled in conjunction with cloud services. Security organizations are undergoing similar transformation as business units, and that's fueling greater reliance on SaaS-based security services. Nearly half of the executives surveyed say cloud-based security tracking and management services will see the highest levels of IT security investments in the coming year.

A big incentive for using the cloud relates to skilled talent. "Many organizations are finding it difficult to hire the level of talent that they need for security today," Pike says. "Not only can they not hire enough people to manage security inside their organizations; they also don't have the talent available to take care of a breach if it occurs."

Contracting out for more experienced service providers is one way to get a bigger bang for security bucks. "You're essentially swapping out one full-time employee for the resources of a number of folks with a range of different talents," adds Pike.

Crowder says his company will make significant investments in SaaS services for response remediation platforms and security tracking. "In the past, we protected the castle," he says. "But because the castle is now all over the world, these global, cloud-based security tracking mechanisms become more valuable."

CREATE A CULTURE OF SECURITY

Modern security strategies must also focus on personnel, given the frictions that arise from misaligned organizational structures and breakdowns in interdisciplinary collaboration. The overarching way to do this is by cultivating a corporate culture that makes everyone responsible for cybersecurity. The leading companies in the Forbes Insights/BMC survey understand the importance of this goal. More than half—54%—say this will be a key step they'll take over the next year to address the security risks resulting from new business and technology trends.

Expanded and continuous training is one of the best ways to develop this culture of security. Enterprises should first evaluate the skills of IT and security staffs to identify gaps and then make necessary adjustments through training, new hires or via third-party services. Next, they should focus on peers in all other business units and update training relevant to their particular responsibilities.

Deluxe Corp. is ahead of the curve in this area. "Because cybersecurity is front and center in our organization, we're making ongoing security training and communications available to our entire enterprise," Mathews says. "Security must be something that everybody within the company feels, owns and is accountable for."

European security experts also see enterprise-wide commitment to security as essential for the future. "Be realistic—at some point, you will have an incident, so the key is being prepared for it," says Steve Clement, a security analyst with the Computer Incident Response Center in Luxembourg. "If you're not ready, you'll panic, and that can be disastrous. Do everything you can to avoid that panic moment, and the best way to do that is by playing through various scenarios."

Examples include simulations and tabletop exercises scheduled several times a year that simulate cybersecurity events that are happening or may potentially happen. The goal of these exercises is to create the muscle memory so people know how to behave and react if they actually encounter a threat. These exercises also show organizations' security gaps and where they need to improve internal operations to be better prepared.

"In the recent past, security was something that you addressed after the fact. In the new world of today, security is something we have to build in from the start. It becomes the fabric of what we do, not an isolated activity."

—Michael Mathews, CIO, Deluxe Corp.

The simulations should be played out in the technology department, but also in other corporate entities, including operations, human relations, call centers, legal, marketing, communications and fulfillment. Sometimes lasting multiple days, the run-throughs simulate internal analysis and remediation efforts, communications with customers and outreach to external partners.

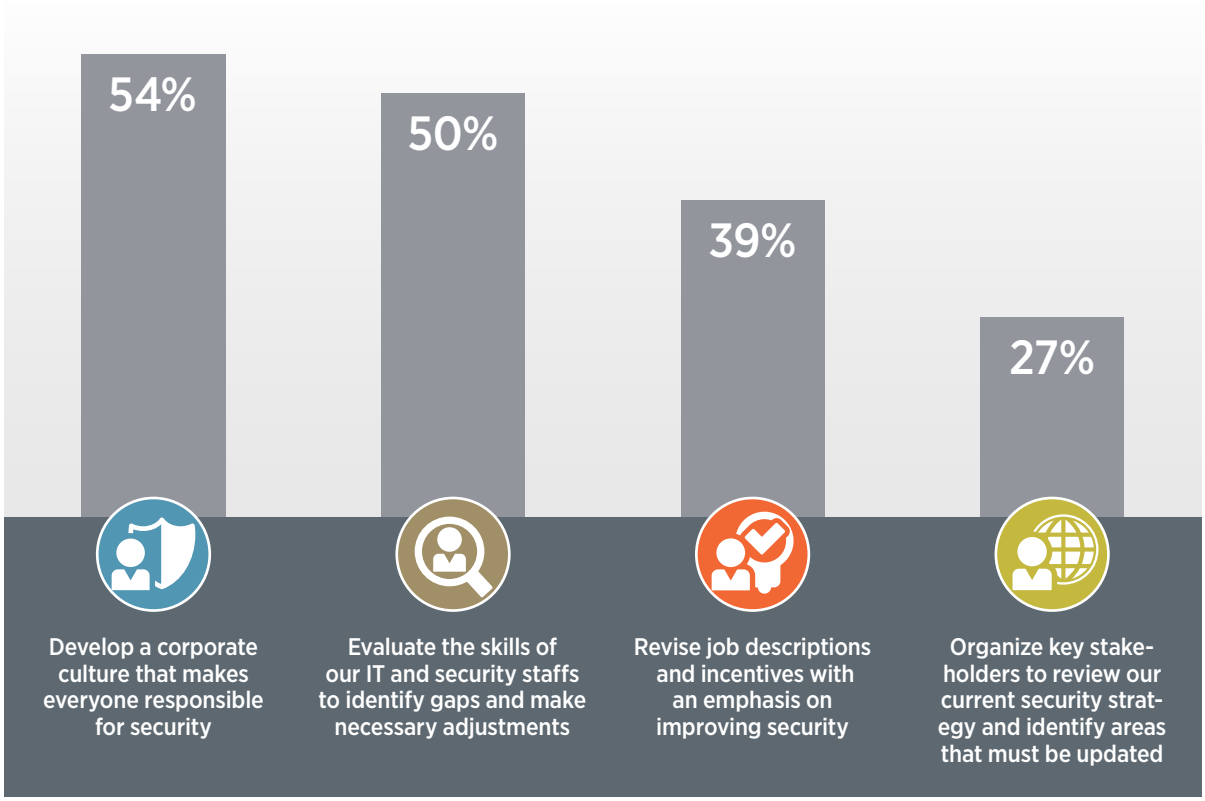
Corporate cultures must also infuse security as an essential component into all activities. It's an idea that's catching on. A high priority in the months ahead will be efforts to proactively embed security into IT systems, the international group of executives said.

"In the recent past, security was something that you addressed after the fact," Mathews notes. "If you built a product, you wrapped it with security by putting a wall around it and locking it up somehow. In the new world of today, we don't think about security as an aftereffect. It's something we have to build in from the start, which means we weave in security from the point of conception and design through the execution and building and deployment. It becomes the fabric of what we do, not an isolated activity."

To further this goal, Deluxe Corp. formed an Enterprise Risk Council (ERC) composed of senior leaders from a cross-section of departments ranging from IT and operations to business units, finance, and manufacturing. While this team and process are still maturing, the ERC meets regularly to review the latest security risks and other top agenda items. The group reviews the biggest concerns, offers recommendations about how to address them, and submits its findings to the appropriate organizational leaders.

"This is helping to advance a culture around the idea that risk and security are an enterprise-wide responsibility, and everybody needs to own a piece of it," Mathews says. "Everybody understands that they're intimately involved in the security of the entire company."

FIGURE 10. Steps My Organization Will Take Over the Next 12 Months to Address the Security Risks Resulting From New Business and Technology Trends



GUIDEPOSTS FOR A NEW AGE

1. **Create a modern cybersecurity strategy backed by a solid business model**
2. **Redouble efforts to secure mission-critical assets**
3. **Improve organizational effectiveness by investigating new reporting structures**
4. **Develop an enterprise-wide culture of security.**
5. **Shift thinking from safeguarding applications to securing the data itself**

Like a CEO racing to update an established business model to block an aggressive market insurgent, CIOs and CISOs are rushing to keep cybersecurity strategies viable in a fast-changing world. Enterprises that stumble at achieving security in the modern age may find themselves the subject of negative headlines, spurned by customers and perhaps burdened by lawsuits and regulatory fines. But organizations that successfully stay ahead of new security challenges will not only safeguard their reputations, they'll also attract digitally savvy customers who value secure environments for doing business.

Turning security into a strategic asset requires a fresh look at an area that enterprises have been investing in for years. New research and insights from leading executives show that focusing attention in the following areas is critical:

1. Create a modern cybersecurity strategy backed by a solid business model.
For many CIOs and CISOs, this means developing spending proposals that target security spending where it will have the biggest impact. For example, analyze increased investments for technology that protects against known security threats, such as patch-automation systems, and enhanced capabilities for incident-response applications.

2. Redouble efforts to secure mission-critical assets.
Decide which assets cannot be breached and dedicate more resources there; let automation and policy handle the rest. Also, combine security and operations personnel into teams dedicated to specific mission-critical applications. At the same time, identify security areas where spending can be safely reduced to help pay for additional investments for mission-critical resources.

3. Improve organizational effectiveness by investigating new reporting structures.
Consider having CISOs report directly to the C-suite to raise the profile of security and give CISOs a more direct role in recommending and justifying spending proposals. Also, find ways to enhance the security role of business managers for identifying the most-critical assets to secure. Finally, promote greater collaboration between security and operations teams to overcome breakdowns stemming from conflicting priorities.

4. Develop an enterprise-wide culture of security.
Employ updated training, simulations and tabletop exercises that involve everyone from the IT, security and operations staffs to HR, call centers, legal, marketing, communications and fulfillment. The involvement of everyone will help reduce "weak link" security gaps and help ensure a coordinated response if a breach occurs.

5. Shift thinking from safeguarding applications to securing the data itself.
After all, the ultimate goal of cyber-thieves is to steal credit card numbers, customer information, intellectual property and other valuable corporate data. To oversee this emphasis on information over systems, consider hiring a chief data officer.

Cybersecurity strategies must continue to evolve in the age of digital transformation. With renewed attention to technology, people and investment priorities, enterprises can rewrite their security road maps and safeguard their businesses in the years ahead.

METHODOLOGY

The data in this report is derived from a survey of 308 executives from a range of industries in North America and Europe, conducted by Forbes Insights in the fall of 2016. Half were located in North America and half in Europe. Titles included CIO (32%), CTO (16%), CISO (14%), CSO (4%) and VP/SVP of technology or information security (34%). All respondents were from companies with at least $100 million in annual revenue; 26% were from companies with revenue between $1 billion and $5 billion; 24% had revenue of $5 billion or more.

ACKNOWLEDGMENTS

Forbes Insights and BMC would like to thank the following individuals for their time and expertise:

- **Cameron Brown,** Cyber-Defense Advisor and Security Strategist; former Forensic Specialist with the United Nations
- **Steve Clement,** Security Analyst, Computer Incident Response Center, Luxembourg
- **Scott Crowder,** CIO, BMC
- **Betty Elliott,** Head of Information Security and CISO, MoneyGram International
- **Paul Lewis,** CTO, Hitachi Data Systems
- **Michael Mathews,** CIO, Deluxe Corp.
- **Sean Pike,** Program Vice President, Security Products, IDC

Forbes
INSIGHTS

ABOUT FORBES INSIGHTS

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, a global media, branding and technology company whose combined platforms reach nearly 75 million business decision makers worldwide on a monthly basis. By leveraging proprietary databases of senior-level executives in the *Forbes* community, Forbes Insights conducts research on a wide range of topics to position brands as thought leaders and drive stakeholder engagement. Research findings are delivered through a variety of digital, print and live executions, and amplified across *Forbes'* social and media platforms.

FORBES INSIGHTS

Bruce Rogers, Chief Insights Officer
Erika Maguire, Director of Programs
Andrea Nishi, Project Manager

EDITORIAL

Kasia Wandycz Moreno, Director
Hugo S. Moreno, Director
Alan Joch, Report Author
Kari Pagnano, Designer

RESEARCH

Ross Gagnon, Director
Kimberly Kurata, Senior Analyst
Sara Chin, Research Analyst

SALES

North America
Brian McLeod, Commercial Director
bmcleod@forbes.com
Matthew Muszala, Manager
William Thompson, Manager

EMEA
Tibor Fuchsel, Manager

APAC
Serene Lee, Executive Director