Forbes insights

MAKING TOUGH CHOICES

How CISOs Manage Escalating Threats And Limited Resources

IN ASSOCIATION WITH

FORTINET

Table Of Contents

Introduction

Life for chief information security officers boils down to this: How do they allocate limited resources to meet a growing range of cyber threats?

At stake are the most vital assets—sensitive and proprietary data at the heart of their business and brand.

Chief information security officers (CISOs) are engaged in an arms race between the capabilities of attackers and their own defense postures. Many organizations were once resolutely focused on "the perimeter defense"—keeping anything from getting into the network in the first place. However, there is a growing realization that breaches are inevitable, and that strong detection and response practices are a greater priority. This is reflected in the research conducted by Forbes Insights for this report.

Real-world cybersecurity demands that CISOs make hard choices. They must allocate limited funding to the highest-return projects. They must direct their overburdened teams to the most serious breaches. Above all, they must rebalance their own time and resources, pivoting from dealing with tactical issues to strategic leadership.

To gain insight into the strategic decisions being made among leaders on the front lines of security, Forbes Insights surveyed more than 200 CISOs about the cyberscape before them—and how they maximize their company's security with finite resources.

Our report is for CISOs, by CISOs—and it's ultimately about the confidence that comes from building and executing a strategy that effectively prioritizes resources against threats. We directed the questions and interviews exclusively at C-level security leaders to get a senior perspective on the lessons learned and the practices in place to build holistic and effective cyber-defense programs. What are they doing to sleep well at night?

Key Findings

CISOs believe that the risk of cyberattacks will increase in the future—and almost a quarter of them question whether their organization will be able to defend against them

- Eighty-four percent of security executives believe the risk of cyberattacks will increase
- Almost a quarter (21%) believe the capabilities of attackers are outpacing their ability to defend their organization

A priority for CISOs is defending the brand and reputation of their firm—and protecting their intellectual property

- Safeguarding the customer data and protecting the brand of the firm, combined at 36% of respondents, was the number one priority for cyber defense
- A fifth reported that intellectual property is a top priority

Leaders are facing a number of constraints—primarily the lack of an adequate budget and a central cybersecurity strategy

- More than a third (36%) cite the lack of an adequate budget as having a significant impact on their cybersecurity programs, and 18% cite it as their greatest constraint
- About the same percentage cite a lack of a central cybersecurity strategy (35%) and lack of support from senior management (35%)

Top goals among CISOs are about integration and analysis

- The traditional mindset geared toward best-of-breed solutions is still present—and 44% say they'll shift their technology strategy toward picking individual products
- But the focus among half (48%) is integrating security seamlessly into their network operations and having the analytics (45%) to gain visibility into their environments

In an ideal world, CISOs would devote more resources to response categories, shifting away from prevention

- Security leaders currently focus an average of 36% of their security budget on response. Given the chance, they would shift resources from prevention to bolster detection and response (increasing response to 40% of their budget)

Threats And Capabilities

A CISO—perhaps more than any other senior executive—navigates uncharted ground. No other part of the business is changing this rapidly, and in no other part of the business are the stakes so high.

"There is no playbook for being a CISO," says Dawn Cappelli, VP, global security and chief information security officer at Rockwell Automation, a provider of industrial automation and information technology. She notes that the threat landscape has changed dramatically over the past few years. "Everyone realized that cyber threats like ransomware are out there and can hit anyone. Everyone realized that you don't have to be the target, and you don't have to have something specific that they're after. It's a dynamic environment."

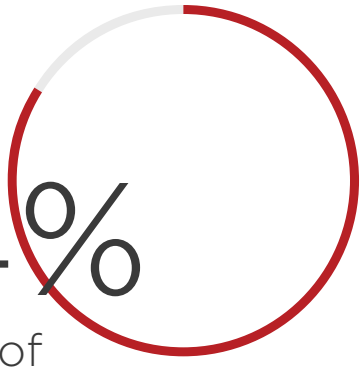
The Forbes Insights survey shows that CISOs by an overwhelming consensus feel that the risk of cyberattack is high and will inevitably get worse (Figure 1). More than eight in 10 executives expect the risk of cyberattacks to escalate into the foreseeable future, and 21% believe that the capabilities of bad actors—whether they're individual hackers, nation-states or careless employees—will grow faster than their ability to defend against them. They believe they face a serious situation, and it's remarkable that such a large segment of security professionals see themselves and their organizations falling behind in the race to keep up with threats.

What's at stake? It's no surprise to see the focus on defending the customer franchise of the firm, with over 36% of respondents selecting brand/customer data as the highest priority for protection.

Figure 1.

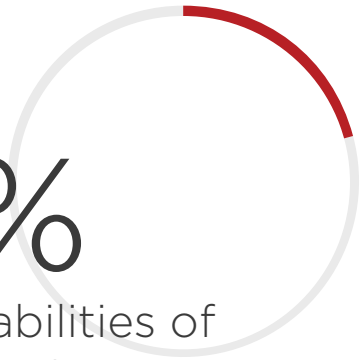
To what extent do you agree with the following statements?

(Percentage who answered 7 to 10 on a scale of 0 to 10, where 10 is strongly agree)



84%

The risk of cyberattacks will increase in the foreseeable future...



21%

The capabilities of cyberattackers are growing faster than my organization's ability to defend against them...

Figure 2.

Which of the following attack targets concerns you the most?

(Total does not add to 100% due to rounding)

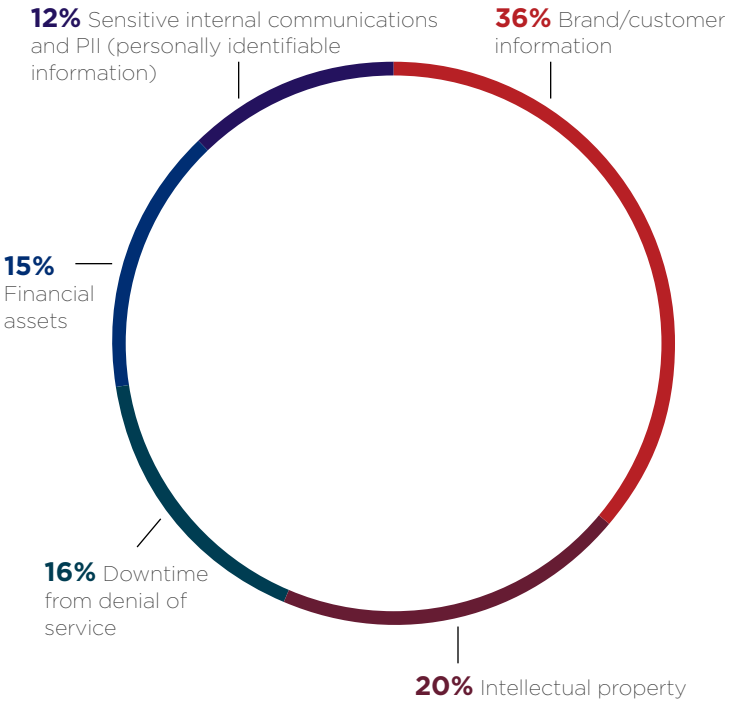
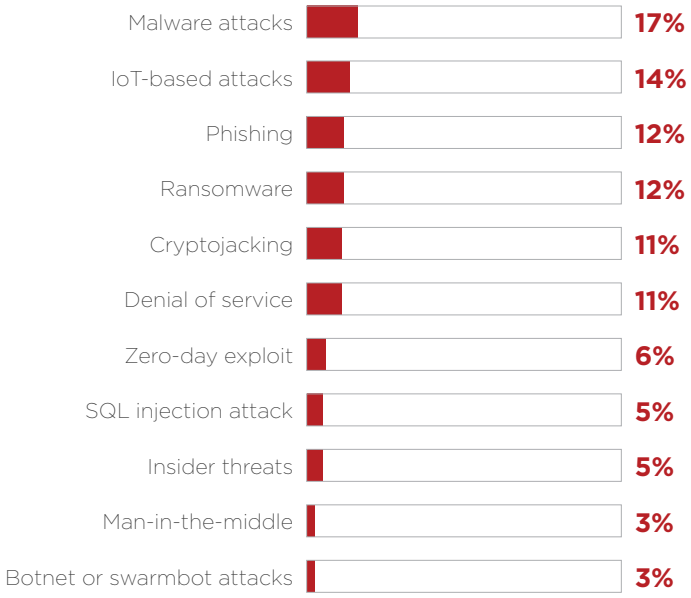


Figure 3.

Which of the following attack modes concerns you the most? *(Select one)*



The real takeaway, however, is the importance placed on intellectual property, which for many enterprises represents the keys to the kingdom and the essence of their competitive advantage. A brand image can be recovered; the heart of the business is another matter.

The survey also reveals the level of concern these leaders have about threats like malware, IoT-based attacks and brand-damaging ransomware (Figure 3).

The results imply that CISOs are busy fighting the common, known threats and are not able to anticipate or prepare for longer-term threats or new attack capabilities.

Threats appear as fast as vulnerabilities. IoT botnets, low on the list of concerns in Figure 3, can infect a whole range of devices, including key end points like medical devices in a hospital or switches in a power plant. One variant called VPNFilter can monitor protocols and steal website credentials—and it has a kill switch that can destroy a host device and also introduce a cyber weapon into the network. Zero-day exploits are targeted to previously unknown vulnerabilities, which makes detecting them in both hardware and software a critical—and exceedingly difficult—endeavor. SQL injection attacks can target applications, a new and evolving threat that is becoming an increasing concern.

Cappelli hears security leaders describe their role this way: I'm probably not going to drive customers to do business with our company, but I'm going to ensure that we don't lose any customers because of security. "I see it differently: Security is just becoming much more part of the strategy of the entire company," she says.

"The more the footprint of technology grows, the more the security risk grows," says Emily Heath, vice president and chief information security officer at United Airlines. "With the emergence of IoT and the OT world, pretty much everything is connected to Wi-Fi or Bluetooth. In an organization that's so highly distributed and moving, literally, that's always a challenge. You have to understand your business. For us, business operations are what defines the risk. We've got an organization of around 90,000 people. So how we communicate and embed security within the DNA of the organization is really important."

ACTION TO TAKE

Focus on protecting the brand and its reputation—and on intellectual property—the core targets of most malicious actors and the most important assets in the CISO's care.

Constraints: Budgets, Strategy And Skills

What's getting in the way of CISOs' ability to reach their cybersecurity goals? Three factors that are unavailable to many CISOs: an adequate budget, a clearly defined central strategy and the needed skills among internal staff.

Limited resources force leaders to make critical decisions or compromises (Figure 4a). Many also feel restrained by the lack of a central cybersecurity strategy that unites teams and experts across lines of business and network infrastructure (Figure 4b). This is significant, as the absence of this key component produces a cascade of problems across the security area of responsibility. What's more, many CISOs must cope with skill levels among their IT staff and across lines of business that fall short of needs in a complex and evolving threat landscape.

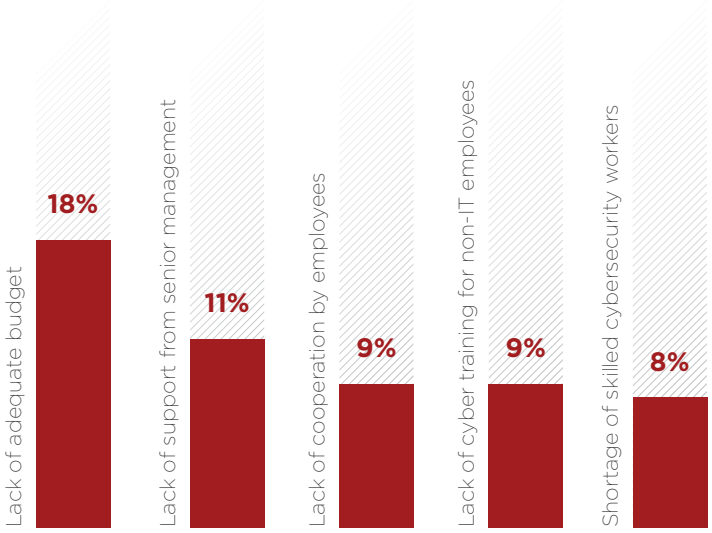
"There's no single good answer for where you should focus your budgets," Cappelli says. "I believe you should take a structured approach to look at the whole big picture and then prioritize based on risk. Some of those more mature companies in higher-risk sectors are looking at the leading edge; they're looking more at detection and response and recovery."

Figure 4.

Which of the following constraints has the greatest impact on your cybersecurity program?

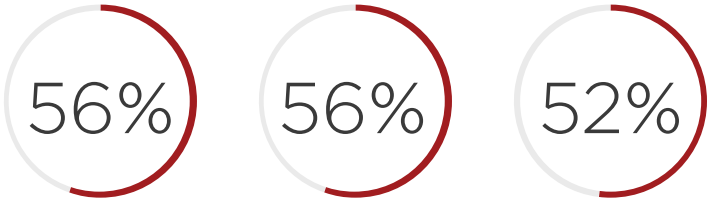
(Top 5 constraints shown)

A. Overall



B. Constraints with a big impact

(Percentages who answered 7 to 10 on a 0 to 10 scale of impact)



Forbes Insights dug deeper to get at the true impact felt at those organizations lacking a central cybersecurity strategy. Executives in the survey who said they are highly impacted by a lack of a central cybersecurity vision or strategy (a 9 or 10 on a scale of 0 to 10) were defined as strategy-constrained. We then looked at the effects of this weakness on various aspects of security.

CISOs who reported a lack of central cybersecurity vision or strategy...

are more concerned about cyberattackers' capabilities

38% agree that attackers' capabilities are outgrowing their own organization's, vs. 19% of all others

are less confident looking forward in their ability to respond to threats

23% are extremely confident in their response capability, vs. 49% of all others

believe talent challenges contribute more to their inability to execute strategic initiatives

27% say a shortage of qualified cybersecurity staff makes them unable to execute strategic cybersecurity initiatives, vs. 17% of all others

The lack of qualified staff is a continuing challenge for security leaders. When asked about the constraints lack of staff puts on resources, CISOs replied that it prevents them from being strategic, or prevents them from keeping up with new security challenges. This implies that the ongoing pressure of cybersecurity threats keeps them focused on the tactical, on the reactive, on the defensive. They cannot catch their breath to take a longer view, which is why they're focused on the known threats.

"The emergence of threats is continuous, and I just don't see it slowing down anytime soon," says Heath. "So we certainly don't just care about the known threats; we care very much about what we don't know. [Our cybersecurity staff] are six times the size we were a few years ago, and we continue to invest and grow in people, so we can evolve with technology and with the risk and the needs of the business."

Against the backdrop of United's expansion of its security organization is the shortage—one could call it a debilitating shortage—of talent. According to a recent survey of IT decision makers by the Center for Strategic & International Studies, 82% of employers say they're experiencing a shortage of cybersecurity skills—and "71% believe this talent gap causes direct and measurable damage to their organizations."[1] In fact, the National Initiative for Cybersecurity Education reported that, as of January 2019, the U.S. faces a shortfall of some 314,000 cybersecurity professionals.

"There are not enough security people available," Cappelli says. "**There is such a shortage of talent in the cybersecurity industry that you need advanced cybersecurity technology** to get the job done."

Health says United's efforts to hire a diverse, creative team is showing results in terms of retaining staff. "When you have true diversity, and a team of people who have a passion for what they each do, it's infectious. People don't want to leave when they are members of a team that operates with a creative mindset. It builds momentum and attracts other people to your organization."

1 "The Cybersecurity Workforce Gap," Center for Strategic & International Studies, 2019.

2 IBM, 2018 Cost of a Data Breach. https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#559c2a5f2f37

ACTION TO TAKE

Make the business case for the CISO's budget: Threats are only escalating, and resources must be maximized. Ask senior leadership to consider the cost in increased budget versus prospective loss. The average cost of breaches in the U.S. is $7.9 million.[2]

Protection: Strategy And Technology

The survey shows that more CISOs are repositioning their security strategy from prevention to more effective detection and remediation (Figure 5).

This is part of a growing consensus that organizations cannot fight off every attack and that breaches can be seen as inevitable. In that mindset, resources are better spent managing priorities and sharpening detection and response tactics—enabling a quick reaction. That comes down to strategy and technology adoption.

"AI is essential for us to be able to respond quickly enough to attacks," Cappelli says. "When you look at how quickly WannaCry and NotPetya spread across networks, it was incredible. There was no way a human could respond quickly enough to shut that down. It has to be technology—machine learning and AI technologies—that shuts the threat down."

Which security approaches are CISOs focused on? Above all, as seen in Figure 6, security leaders want to integrate security into network operations, and they want analytics to help give them the visibility into cross-network traffic, including insider activity, that can help them detect and investigate anomalous behavior. On the surface, the relatively low emphasis placed on automation (only 42% say they're planning to shift their technology strategy toward it) seems odd: In fact, it reflects the fact that most CISOs are already focused on automation. It's the new normal.

ACTION TO TAKE

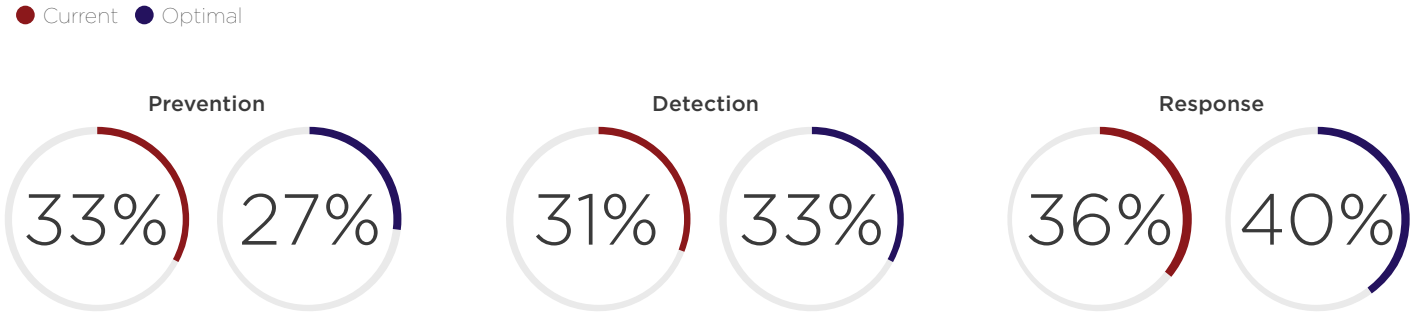
Automate your resources as much as possible.

Staff will continue to be constrained to tactical aspects unless automation takes on repetitive functions, enabling them to take a more strategic and effective security stance.

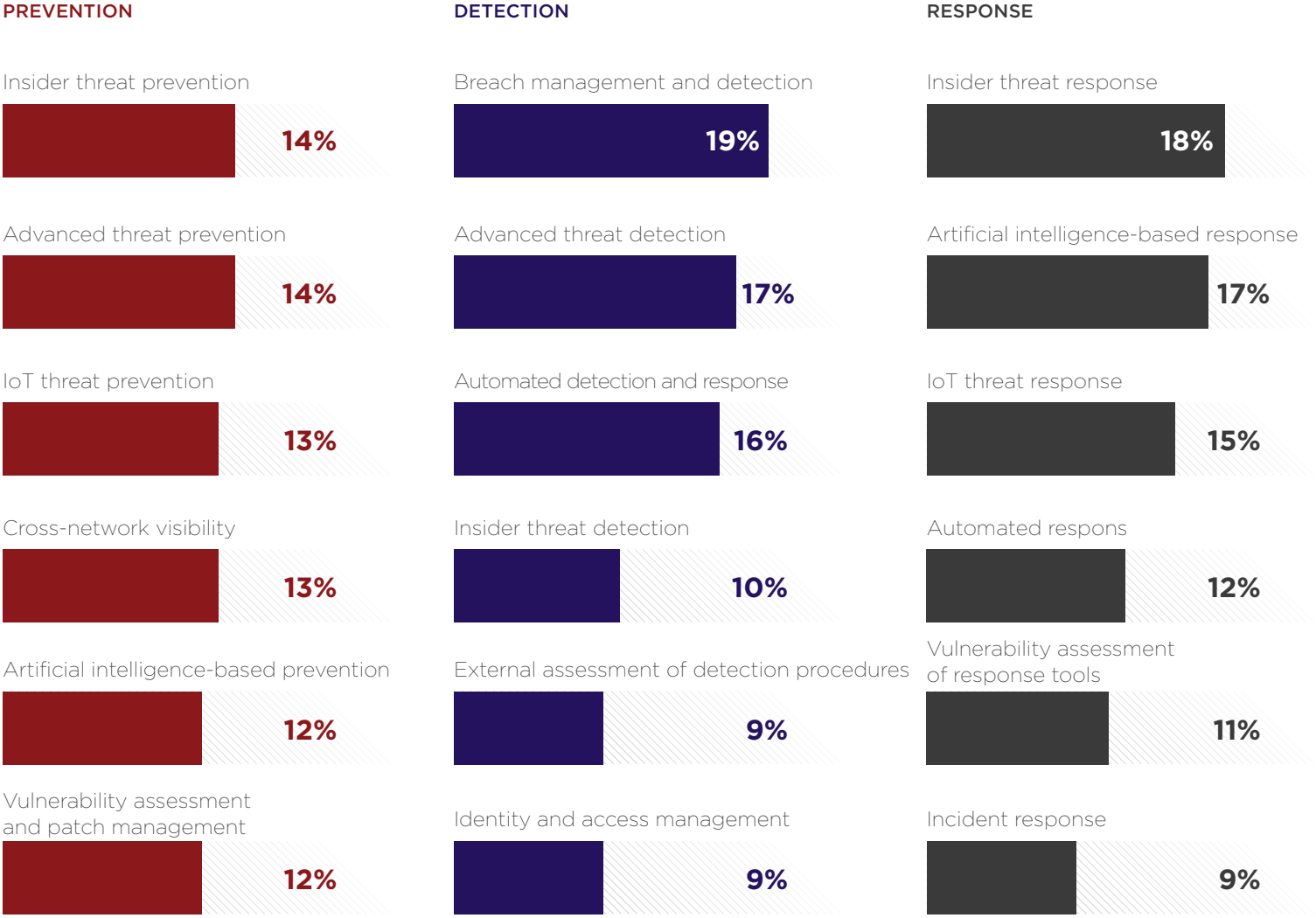
Figure 5.

The Shift to Detection and Response

A. What is your current allocation of your cybersecurity budget across the following three categories—and what would be your optimal allocation?



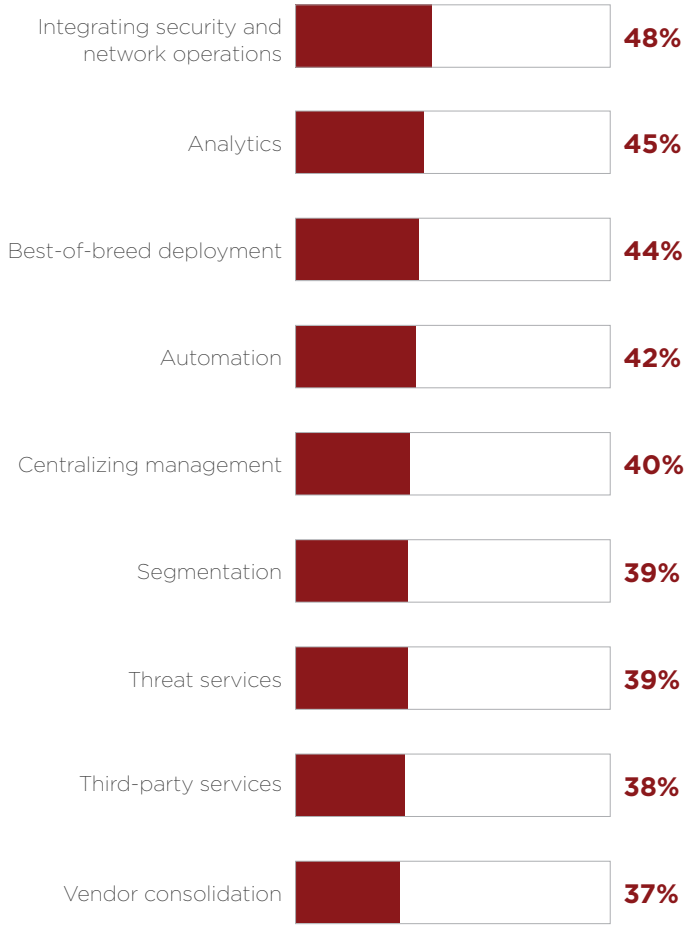
B. Which of the following practices have the highest priority across prevention, detection and response? *(Top 6 shown for each)*



"There's no way humans can do everything in cyber," Health says. "The sheer volume of data that is available these days from every sensor in every single piece of equipment make it an impossibility. The fundamental concept of security is understanding from a visibility angle. The other big part of it is understanding what normal looks like. And true machine learning helps you with this. Analytics 'listens' to an environment; it can understand what normal and abnormal looks like."

Figure 6.

Toward what approaches do you plan to shift or change your cybersecurity technology strategy? *(Select all that apply)*



Insider Threats: The Value Of Automation And Training

The Forbes Insights survey shows that, across prevention, detection and response, CISOs are concerned with insider threats, which reflects growing evidence of collusion between employees and hackers—and also the consequences of careless or poorly trained employees, or human error.

According to Verizon's 2018 Data Breach Investigations Report, 20% of incidents—and 15% of breaches—originate from people within the organization.

The significance of insider threats points to the value of technologies like machine learning—the foundation of tools that can monitor network behavior for anomalies and alert teams so they can act quickly—and in-house programs to train employees on best practices.

ACTION TO TAKE

Move more resources from prevention to detection/response. Don't just rely on defense, but also focus on deploying detection and response tactics and technologies.

Internal Actions: Talent And Teamwork

What steps can CISOs take within their organizations to respond to threats? Security leaders point to the need for an enterprise-wide, holistic approach to security and for the hiring of more cybersecurity staff.

A critical (and often overlooked) aspect of key internal actions is the training of employees to be more aware and knowledgeable about security, which can reduce the success of phishing and errors by employees that can expose the enterprise to cyberattacks (Figure 7).

"The ownership of security does not belong just to my organization," Heath says. "It belongs to everybody—developers, for example, or the infrastructure team. They often manage firewalls and build cloud environments. If we work alongside them and partner with them, it doesn't always have to be my team who take actions of security. It can be part of their jobs as well. It's about leveraging the rest of the organization."

It's critical for everyone across the enterprise to know and understand the threats. Security teams in different areas of the enterprise and lines of business—including a variety of subject matter experts within them—must be on point and united around cybersecurity best practices for initiatives to be as effective as possible. It takes true collaboration within an organization to establish roles and responsibilities—and to maintain clarity around operations that generally include detection and response practices.

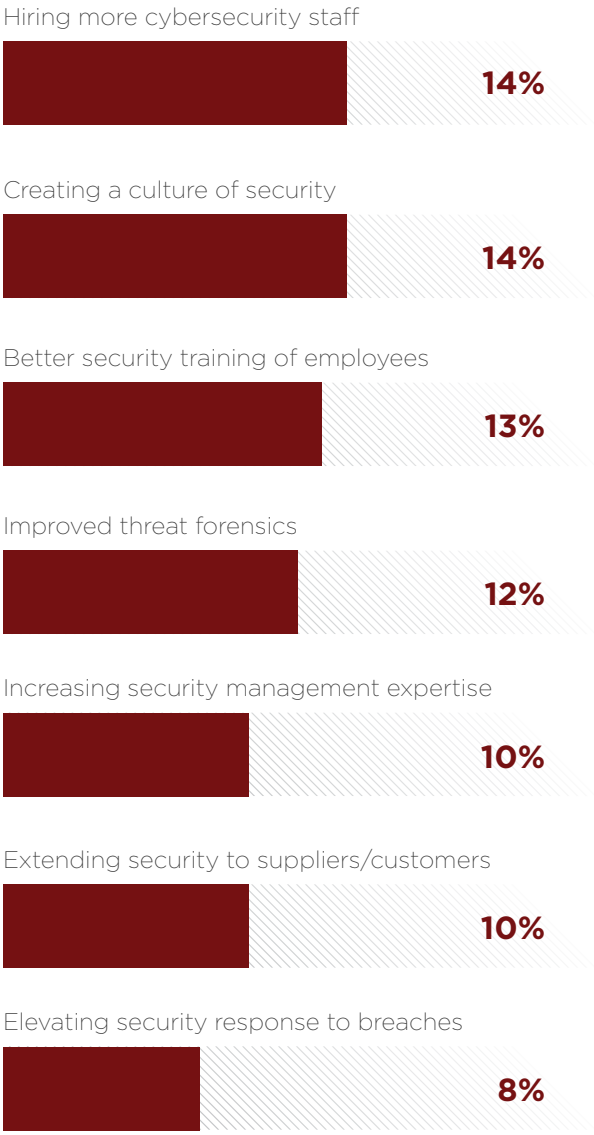
At Rockwell Automation, cybersecurity is ingrained into the fabric of the business, an effort it brings to its clients in the industrial production sector. **"We were all one big team," says Cappelli, "and we recognized that some people were subject-matter experts in one area, and some people were subject-matter experts in another. Seeing us all as one team was the best thing that we could have done, because if IT security tries to create a plan for securing a plant without working with the industrial automation engineers, it will be hard to get the buy-in that you need."**

"CISOs have to have influence, and they have to bring people together," says United's Heath. "It's a very unique job. You have to understand business. You have to understand technology. You have to also then understand security and how to apply it to that technology. Then you have to be an investigator, and you have to do it in the confines of the law. The broad range of the role means that the partnerships you have across your organization can literally make or break your program."

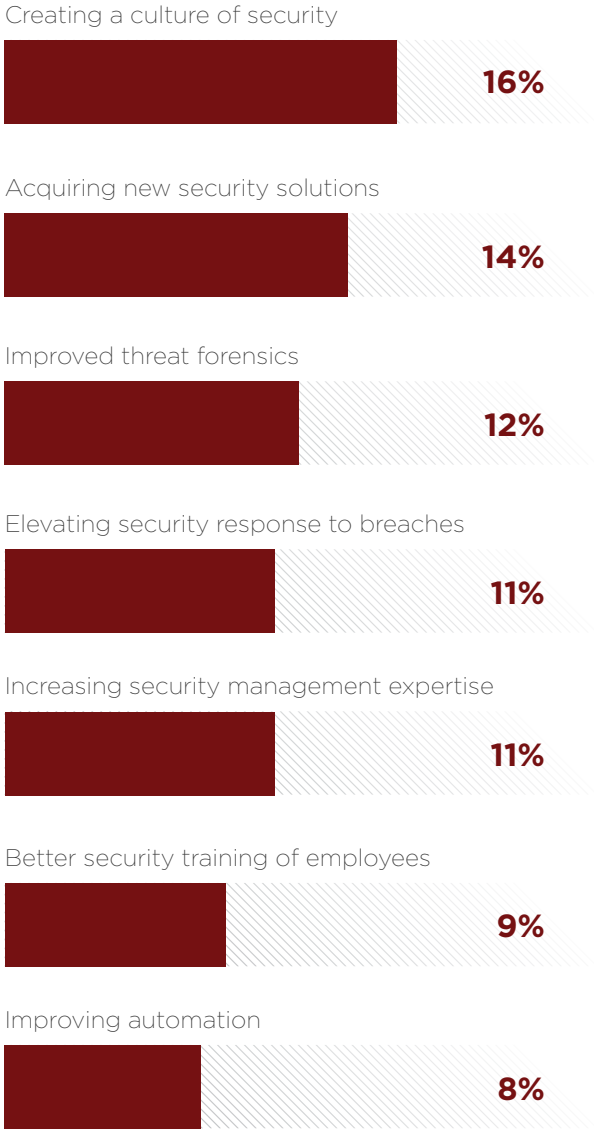
Figure 7.

Priorities: Security Initiatives

A. Which of the following security initiatives is your highest priority for funding in the coming year? *(Top 7 shown)*



B. ...in the next five years?



"It's a very unique job. You have to understand business. You have to understand technology. You have to also then understand security and how to apply it to that technology. Then you have to be an investigator, and you have to do it in the confines of the law..."

The impact of a talent and expertise shortage is profound, as seen in Figure 8. Our findings show that the shortage of talent prohibits security teams from pursuing strategic goals—such as executing strategic security initiatives or assessing new challenges—and keeps them stuck on tactical issues.

"At Rockwell Automation, we're creating a defined security career path so that our employees can see how they can evolve and what kind of experience or education they need to move to another position," Cappelli says. "All of our security leaders work together so that, when we have an opening, good in-house candidates are ready, even if they don't have exactly the experience. We train them for the new position rather than take a chance on their leaving the company. Retention is a very big thing—making your security people happy so that once you get them, you can keep them."

Cappelli points to new technologies that will help to create a baseline of all devices and network activity. Armed with this tool running in real time, security teams can segment parts of operations and detect anomalous activity quickly. But she adds that CISOs have key questions to consider around their talent and staffing: "Do you have the people to figure out what to do with that data? How do you integrate that data with all of your IT security data?"

The answers should be part of a CISO's playbook—and they should arrive fluidly from a commitment to security that results in automation technologies being deployed and teams being trained and ready to respond to incidents and breaches. And, given the insider threat factor, employees need to be trained properly to avoid careless behavior that can damage the business and the brand.

Figure 8.

What is the most serious challenge created by a shortage of qualified cybersecurity staff?

ACTION TO TAKE

Be sure you are focusing on your people, including employee training, education, understanding and the building of a culture of awareness.

The Road To Confidence: Actions To Take

All CISOs face the unknown every day and every week, but some are more confident about the future than others.

Given the coverage in this report about threats and constraints, and the perspectives from CISOs on the front lines, what are the top ingredients that form a strong security organization?

These core actions can help CISOs reach the highest level of readiness:

- ## Focus on protecting the brand.

  This is what many malicious actors are targeting. But it is also the most important asset in the CISO's care—the reputation of the company.

- ## Make the business case for the CISO's budget.

  Threats are escalating, and resources must be maximized for cost versus prospective loss. The average cost of breaches in the U.S. is $7.9 million.

- ## Automate your resources as much as possible.

  Staff will continue to be constrained to tactical aspects unless automation takes on repetitive functions, enabling them to take a more strategic and effective security stance.

- ## Move more resources from prevention to detection/response.

  Accept that you cannot defend everything by picking your battles and deploying detection and response tactics and technologies.

- ## Be sure you are focusing on your people's cybersecurity knowledge.

  This can be done with employee training, education, understanding and the building of a culture of awareness.

Conclusion

CISOs live in a world where cyber risk is almost certain to escalate. They also operate in an enterprise in which security resources are unlikely to keep up in this arms race.

As Johann Wolfgang von Goethe said, "things which matter most must never be at the mercy of things which matter least." In other words, pick your battles and stick to your priorities. This holds true for cybersecurity. Effective CISOs will maximize their resources—but will then marshal their people, budget and expertise to fight the battles that matter most. This kind of flexible, scalable defense will prove most effective in the counterattacks against cyber-breaches to come.

Methodology

Forbes Insights and Fortinet surveyed 209 chief security officers about their priorities during January and February 2019.

Some 39% of respondents were in North America, with 31% from EMEA and 30% from APAC. Seven in 10 come from organizations employing 10,000 or more workers, and all of the executives were from organizations with revenue in the most recent fiscal year of $1 billion or more—with 53% at $10 billion or more in revenue.

Acknowledgments

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

DAWN CAPPELLI

VP, Global Security and Chief Information Security Officer, Rockwell Automation

EMILY HEATH

Vice President, Chief Information Security Officer, United Airlines

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 94 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.

NICK LANSING

Report Author

499 Washington Blvd. Jersey City, NJ 07310 | 212.367.2662 | https://www.forbes.com/forbes-insights/