servicenow

Point of View

The Global CISO Study

How Leading Organizations Respond to Security Threats and Keep Data Safe

servicenow

Table of Contents

T OF C

Executive Summary

Enterprises face a rising risk to their financial performance, operational continuity, and reputation from information security breaches. According to research from the Ponemon Institute, costs per breach have increased by 30% in the last three years, and companies face a 26% probability of a material data breach in the next two years.[1] At stake is the very survival of these enterprises, but most organizations are not prepared to deal with imminent threats.

Our survey of 300 chief information security officers (CISOs) investigates the state of security response in large organizations and their strategies for navigating this challenging environment.

The results show that enterprises are not responding effectively—and CISOs are worried about the growing list of ever-evolving threats.

81%

of CISOs are highly concerned that breaches are going unaddressed.

78%

of CISOs are worried about their ability to detect breaches in the first place.

Response matters: Just 19% of executives surveyed say their company is highly effective at preventing security breaches.

CISOs in this survey have identified three major enterprise vulnerabilities:

- 70% of organizations surveyed say it is difficult to prioritize security alerts based on the importance of the data under attack. This failure to prioritize can paralyze organizations that try to address all threats equally, given that they can be hit by thousands of cyberattacks daily.
- 28% of CISOs say manual processes are a barrier to effective security, and two-thirds of those surveyed say they plan to automate more in the next three years.
- 91% of CISOs say attracting and upskilling talent is critical to enterprise security. However, only 55% say their teams have developed skills to address future threats. Stronger security is built on improving processes and technology, but also makes better use of the scarce talent in the field.

CISOs know what it is going to take to better arm their organizations, and many are moving in that direction. A group we identified as “Security Response Leaders” have a more advanced approach than their peers. They rate themselves as highly effective at protecting against the most serious types of breaches.

Data breaches are all but inevitable. Looking ahead, CISOs who will lead in protecting the enterprise will focus on three areas: prioritizing and automating critical security tasks, integrating security objectives across business functions, and attracting and retaining the right talent.

Research Methodology

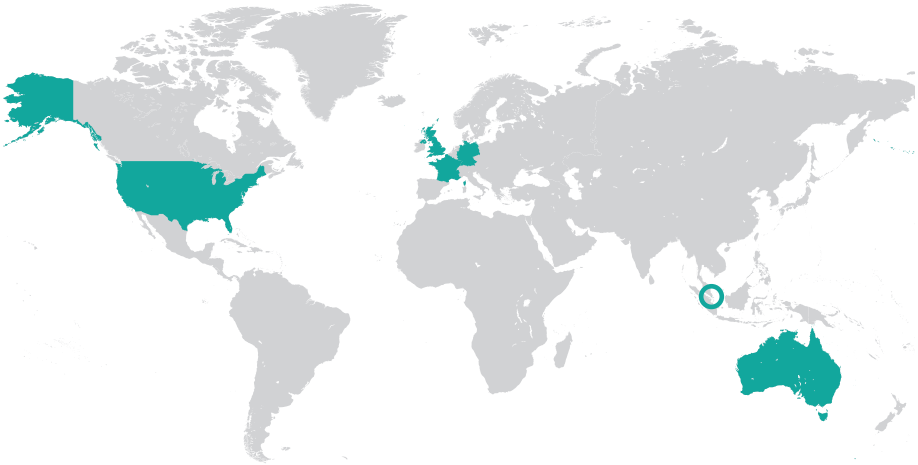
ServiceNow worked with Oxford Economics to field and analyze a survey of 300 CISOs about the state of the security function, with a focus on the automation of routine and more advanced security tasks.

We also conducted three qualitative interviews with executives:

- Daniel Conroy, chief information security officer, Synchrony Financial
- Carsten Scholz, chief information security officer, Allianz SE
- Dan Taylor, head of security, NHS Digital

Geographical Reach

Respondents come from six countries: Australia, France, Germany, Singapore, the United Kingdom, and the United States.



Company size	
$500 M–$749 M	16%
$750 M–$999 M	17%
$1 B–$4.9 B	33%
$5 B–$10 B	11%
$10 B+	23%

Industry breakdown	
Financial Services	22%
Technology	20%
Industrial Products	20%
Retail & Consumer Goods	8%
Media & Communications	8%
Energy & Mining	5%
Healthcare	5%
Government & Nonprofit	4%
Automotive	3%
Real Estate	3%
Education	2%

Introduction

CISOs must protect their organizations from an ever-evolving variety of threats, and adjust to a higher profile in the C-suite.

If it seems like security breaches are happening more often, that is because they are. These incidents are escalating in frequency and impact,[2] with significant increases in ransomware attacks (up 35% last year) and spear-phishing (up 55%).[3] A serious security breach might disrupt a company's day-to-day operations, or have disastrous consequences in terms of brand reputation and financial losses. The average total cost of a data breach has grown to $4 million.[4] The most-breached industries include Information and Communications, Government, Financial Services, Media and Entertainment, and Professional Services, but every sector faces security challenges.[5]

All of this makes the work of senior security executives increasingly important and complicated. They must protect their organizations from an ever-evolving variety of threats, and adjust to a higher profile in the C-suite—and to the board-level scrutiny of their effectiveness at the critical job of mitigating serious risks.

This report explores the progress CISOs have made and the goals they have yet to reach. Unlike many studies in the marketplace, it focuses on the specific steps organizations are taking to enhance security response. Developed from original research conducted in early 2017, it shows how executives are addressing security and operational issues through the use of technology and forward-thinking management.

A State of Insecurity

These are uneasy times for executives in charge of information security, and nothing worries them more than the things they do not know. CISOs fear that despite their best efforts, security breaches are going undetected, and are going unaddressed even when they have been discovered. Look no further than the long-overlooked—and massive—breaches at Yahoo! for an example of the reputational and financial hazards involved.

Why are CISOs struggling in these areas? Our study points to the fact that manual processes, data quality issues, and talent gaps hinder their ability to prioritize threats and respond to the most business-critical risks. This inability to prioritize according to organizational risk, combined with a significant talent shortage, has led to the perfect storm: undetected and unaddressed breaches.

Our survey results show these issues to be widespread among CISOs. Four out of five (81%) are highly concerned that detected breaches go unaddressed at their organizations, and 18% are somewhat concerned, leaving only 1% of respondents who say they are not concerned. More than three quarters (78%) of respondents are highly concerned that breaches are going undetected, with another 21% saying they are somewhat concerned, and just 2% claiming they are not concerned. More than two thirds (70%) say it is difficult to prioritize security incidents based on their highest business relevance, and large majorities rate staff skills as less than highly developed in areas ranging from business acumen to analytics. (For data on performance across specific countries and sectors, see our sidebar on geographic and industry variances.)

No wonder, then, that only 19% of CISOs say their organization is highly effective at preventing breaches. Just over one in ten respondents report experiencing a significant security breach causing reputational or financial damage in the past three years; given their lack of clarity into breach detection, the actual number of successful attacks may be higher.

70%

say it is difficult to prioritize security threats based on their highest business relevance.

Imagine one familiar scenario: Someone at your company uncovers a threat, and the security team scrambles to address it. Your CISO hears about it and wants to know if meaningful organizational risk is involved. The team races to assess systems and determine who needs to approve any emergency patching. Many processes are manual, so analysts struggle to quickly gather the information required to provide the CISO with an accurate assessment of the impact. Critical systems may be vulnerable, putting the business at risk of a serious data breach.

JUST

19%

are highly effective at preventing security breaches.

Looming threats, inadequate protection

Today, everyone from manufacturers to healthcare providers and financial services firms depends on data, so breaches can have serious consequences for companies and the people they serve. "The data that we hold is particularly valuable and sensitive, and therefore we have to keep the public trust in the way that we hold that data," says Dan Taylor, head of security at NHS Digital, which is responsible for delivering the National Health Service's IT infrastructure in the United Kingdom. "When you look at incidents where patient-facing appointments are canceled, it no longer becomes just a reputational risk, it also becomes a financial cost."

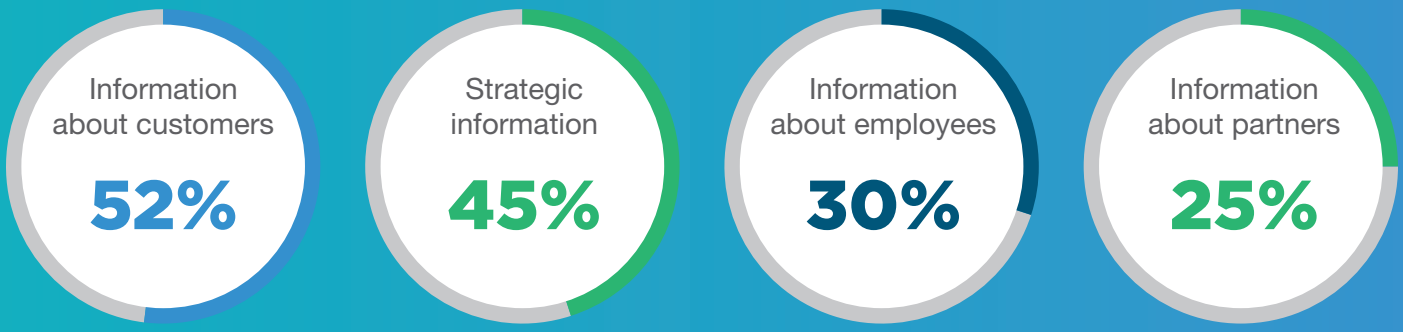
What are the threats that have security leaders so concerned? Respondents consider theft of personally identifiable information (PII) about customers and employees, Distributed Denial of Service (DDoS) attacks, and breaches of customer credit card or financial information to be the greatest dangers to their reputations and financial performance. Loss of customer data threatens the relationships that are essential to any organization's survival, while DDoS attacks—those massive floods of internet traffic directed against a particular website—can take an enterprise offline without warning, making commerce and even basic communication impossible.

Yet preparedness for these much-feared attacks does not match threat levels: Just 56% of respondents say they are highly effective at protecting against customer-information breaches, and just 51% are highly effective at preventing DDoS attacks from a variety of sources including criminals, governments, and online activists (aka "hactivists"). The numbers are no better when it comes to safeguarding particular types of data.

> "The data that we hold is particularly valuable and sensitive, and therefore we have to keep the public trust in the way that we hold that data."
>
> *– Dan Taylor, head of security, NHS Digital*

Threats outpace response capabilities

Q: How effective are you at protecting the following types of information?
"Highly effective" responses are shown



Outdated approaches and inadequate resources hinder security

The external risk factors that make security so difficult are widely understood, including organized criminal networks, state actors, political activists, and an increasingly sophisticated arsenal of tools to outmaneuver or overpower protective measures. In fact, the bad guys no longer need to be technologically adept to launch some dangerous attacks, says Carsten Scholz, chief information security officer for the German-based insurance company Allianz SE.

"Ransomware is not new, but what is new is that ransomware is very easy to use," he says. "You can find services for it on the 'darknet' side of the internet—you simply plug in your Bitcoin and get the software, and then you can go and shoot campaigns out. Of course, this is a criminal act, but it's easy for even non-IT-savvy people. They do not need to have any kind of IT knowledge. They do not even need to know where the potential victims are sitting."

Security responsiveness needs to keep getting better to stay ahead of such evolving threats, but too often, the security function lacks adequate resources and necessary organizational support.

Many organizations rely on manual, decentralized systems for tracking security incidents. In fact, 28% of CISOs say manual processes are a barrier to effective security. And the Enterprise Strategy Group, which surveyed lower-level security employees, found an even greater concern over manual processes, with over 90% of respondents saying their incident response effectiveness and efficiency are limited by the burden of manual processes.[6]

Compounding this issue is a lack of resources to carry out these manual processes; 30% of CISOs rate this as a barrier. Incident tracking often consists of little more than spreadsheets updated by individual analysts. Because these overworked analysts have varying levels of diligence and multiple focus areas, it is difficult to provide governance, properly track how incidents are being handled, and know whether the process is improving over time. Thus it is not surprising that there is a lack of confidence in the quality of the data. According to CISOs, insufficient quality and quantity of data are top barriers that interfere with the ability to protect against, detect, and respond to security issues.

In addition to the lack of resources, there is a critical need to upskill current talent. One-quarter of our respondents cite insufficient expertise as a barrier to security. Few companies have enough skilled security professionals who understand their company's strategic operations and the broader threat environment in a way that allows them to prioritize security threats—just 7% say this skill is highly developed. A large majority of CISOs (84%) say that prioritizing security alerts in the context of the larger business is critical to the success of their security function; clearly they are not getting the support they need.

"[Hackers] do not need to have any kind of IT knowledge. They do not even need to know where the potential victims are sitting."

—Carsten Scholz, chief information security officer, Allianz SE

47%

say insufficient data are a barrier to effective security.

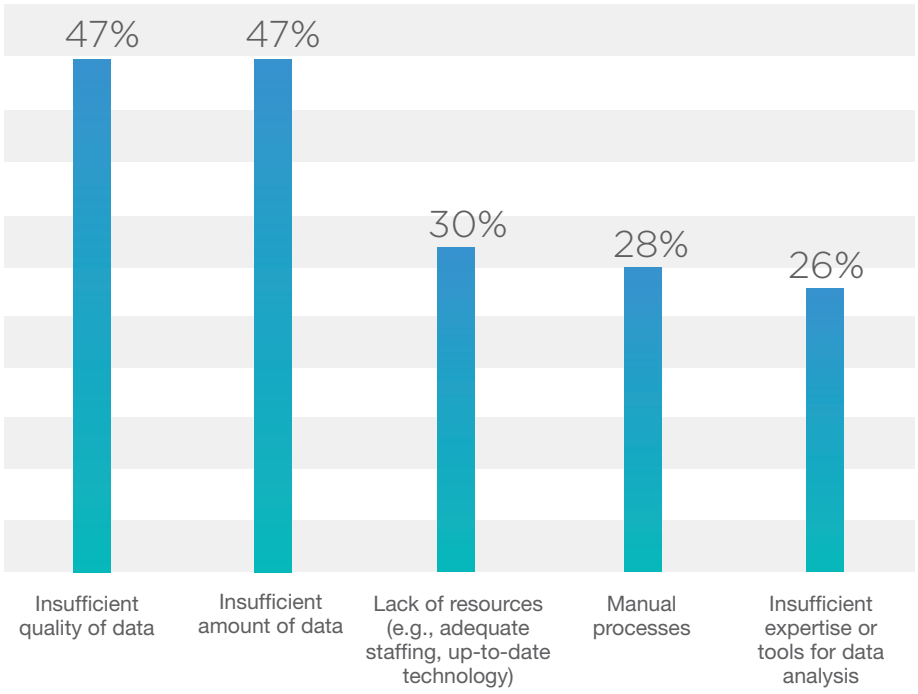
28%

say manual processes are a barrier to effective security.

Our survey makes it clear that many organizations lack a strategic, automated, and systematic process for prioritizing security alerts based on business context. As a result, hackers are able to exploit common vulnerabilities for which patches have been available for weeks or even months. To improve their ability to respond to threats in a timely manner, CISOs should work to orchestrate processes (e.g., human to human, machine to human, machine to machine) and automate response and remediation tasks.

Obstacles to information security

Q: To what extent do the following factors interfere with your security function's ability to protect against, detect, and respond to security issues? *"A substantial barrier" and "A complete roadblock" responses combined are shown.*



"We automate as much as possible. You have some threat vectors where you cannot survive if you are not automated. We want to have a viable environment consisting of real-time control and real-time reaction."

—Carsten Scholz, chief information security officer, Allianz SE

Security Response Success Hinges on Automation

Security threats are too numerous and fast-changing for humans to handle without some assistance. “We automate as much as possible,” says Mr. Scholz of Allianz. “You have some threat vectors where you cannot survive if you are not automated. We want to have a viable environment consisting of real-time control and real-time reaction.”

Automating security tasks—both routine and strategic—is a necessity. The volume of alerts, coupled with the manual processes most security organizations use to address these threats, undermines confidence that breaches are being addressed. Automation helps organizations prioritize and respond to threats in real time, effectively closing that confidence gap. Yet just 48% of those surveyed say they are automating prioritized alerts based on mission-relevant data, and only 40% are automating the aggregation of relevant information from business units.

By prioritizing threats through automation, CISOs can deploy their limited resources to make better decisions, respond more quickly to threats and breaches, and anticipate future dangers. It also helps mitigate shortages of skilled workers and frees security staffers to do higher-value work.

Executives in our survey see this as must-have technology, rating automation of routine processes as a top driver of their organization’s success in the next three years. Among the rewards of successful automation: streamlined workflows, the ability to prioritize threats based on business criticality, and reduced time to detect and respond to breaches.

CISOs are adopting automation technologies at an increasing pace. While just one-third of respondents automate more than 40% of their security processes today, two-thirds plan to automate that amount in three years. And the tasks being automated are increasingly sophisticated as well. Some organizations are further along than others: Most have done the basics—90% have automated alerts via email and phone—but the complexity of tasks automated is expected to see sharp increases in the near future.

JUST 48%

are automating prioritized alerts based on mission-relevant data.

JUST 40%

are automating the aggregation of relevant information from business units.

One-third automate 40% or more security tasks today.

Two-thirds will automate 40% or more security tasks in three years.

Automation on the rise

Q: Which tasks are you automating today? Which do you expect to automate in three years? *Select all that apply.*

Effective automation must address a growing variety of threat vectors (for example, third-party vendors with access to company systems). This kind of growth requires meaningful investment. Security spending is taking up a growing portion of IT budgets, and companies that automate more tasks are more likely to spend a greater percentage of technology dollars on security. Some of that money will flow to emerging technologies that should make automation more powerful and effective—particularly big data and analytics today, and, increasingly in the next three years, artificial intelligence and security platforms.

No matter how many tasks are done by machines, automation must be combined with process changes and effective talent strategies to deliver its full value. The quality and quantity of the data available is critical, too, and a lot of that data flows from IT; over 90% of respondents say this information is substantially or highly important to detecting and responding to breaches. Increasing automation from a common IT and security platform could improve the flow of data between functions and speed response times—as could improved relationships between security and other functions.

"We are feeding about three terabytes of logs today to our systems that we review, and a lot of those are automated systems that pop out things that are interesting to our analysts, and our analysts will then go and review those things and tune accordingly," says Daniel Conroy, chief information security officer at credit card giant Synchrony Financial. "So, yes, automation is a large component."

Meet the "Security Response Leaders"

We filtered the survey data to identify respondents who stand out for their security capabilities. The resulting leader group makes up 11% of the overall sample.

To qualify as Security Response Leaders, respondents must assess themselves as highly effective at protecting against the following types of attacks:

- Breach of personal information about customers (e.g., their preferences, passwords)
- Threats from insiders within the company
- Breach of personal information about employees
- Distributed Denial of Service (DDoS) attacks by criminals, governments, or "hacktivists"
- Breach of customer credit card or financial information
- Watch and wait attacks (monitoring of data and activity over time to identify vulnerabilities)

As we analyzed the performance of these Security Response Leaders, we found that they tend to demonstrate more maturity than other respondents across a variety of areas.

Security Response Leaders display certain characteristics that set them apart from other organizations. Among other things, they:

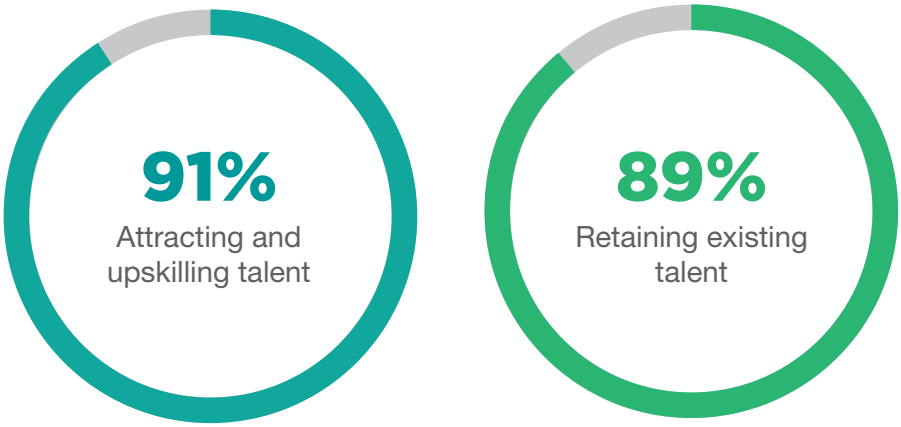
- Are more focused on increasing automation to make the security function successful, and are automating more strategic tasks.
- Report tight integration with other functions across the enterprise, especially IT.
- Say strong relationships between IT and security are important to the success of their security function.
- Rate the prioritization of security alerts in the larger context of the business as critical to the success of their security function.
- See security as a core strategic goal for their company.

People still matter to security response

The rise of machine-assisted information security does not minimize the role of humans. In fact, talent remains a critical issue for security executives, who recognize the monumental impact of automation but understand the ongoing importance of identifying and retaining people who can make the most of the opportunities automation brings. Our survey shows that executives rate talent as the most important element of success in detecting and responding to security threats.

Human factors in an automated age

Q: How critical are the following to the success of your security function in terms of detecting and responding to security threats? *"Important" and "highly important" responses combined*



Substantial skills-related barriers threaten the progress of the automation revolution. Just 9% of respondents say their company has highly-developed skills in automation. People need to understand how the larger business operates and be familiar with relevant security software to instruct, oversee, and extend the value of automated security systems. Combined with a lack of expertise in other technical areas and limited knowledge of the business, there are serious potential roadblocks to increasing automation.

"There is actually negative unemployment globally in information security, and it is very, very hard to get talent," says Mr. Conroy. And the needs go beyond technology prowess alone. "People coming from computer science or engineering are good, but we need someone with philosophy or psychology skills, too. We need to know why people would click on a link, or how people are thinking in order to change how we are operating." Synchrony is focused on innovative training approaches to help alleviate the talent crunch, including sponsorship of a research program at the University of Connecticut.

Ideally, automation will help security functions get more value from the talent and information they do have, allowing people to do higher-level work and removing some of the drudgery from their daily routines. Allowing security personnel to focus more on interesting things like threat hunting and remediation should make it easier to hang onto them.

> "I need someone with philosophy or psychology skills, too. I need to know why people would click on a link, or how people are thinking in order to change how we are operating."
>
> *—Daniel Conroy, chief information security officer, Synchrony Financial*

How the world views data security

Data security is a high-stakes issue everywhere, and our respondents from six countries (Australia, France, Germany, Singapore, United Kingdom, and United States) share the same concerns and are pursuing similar strategies to deal with them. But there are variations from one country to the next.

The global distribution of security response leaders is 21% in Australia, 21% in France, 9% in Germany, 15% in Singapore 18% in the United Kingdom, and 18% in the United States

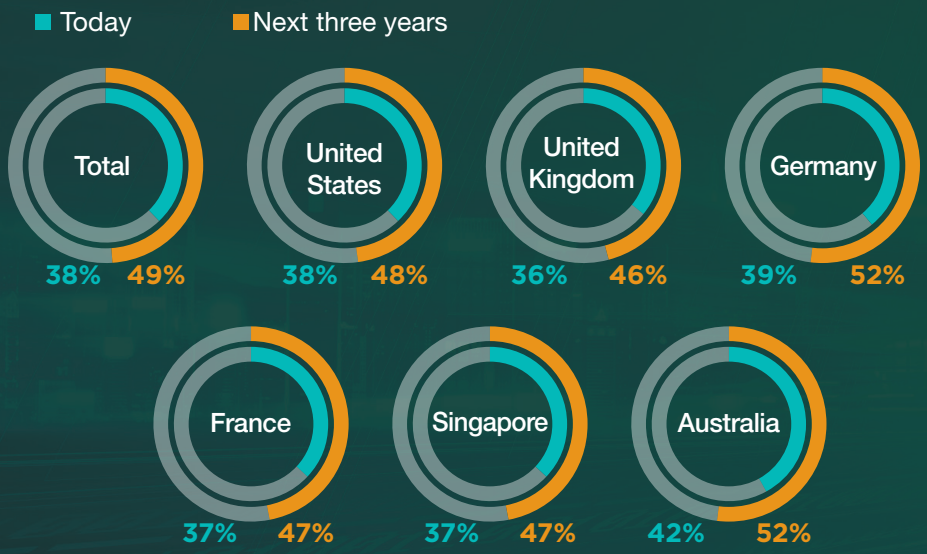
For example, when compared to global averages, respondents in Germany are somewhat less concerned that security breaches are going undetected (68%, versus 78% globally) while their neighbors in France are somewhat more concerned (86%); the same holds true for concerns that detected breaches are going unaddressed. Australian respondents are less likely to identify DDoS attacks as a primary threat (42% rank it as a top-two threat, versus 50% globally), while those in the UK worry more than others about attacks on the personal information of customers (58% versus 42%).

Respondents in Australia and France are more likely to say that over 40% of their security tasks are automated. Perhaps unsurprisingly, then, executives in these two countries are more likely to be Security Response Leaders.

When it comes to the barriers that prevent organizations from responding to security issues effectively, different countries emphasize different issues. Data quality is a big obstacle for UK respondents (56%, versus 47% globally), while those in Singapore are more likely to cite lack of resources (44%, versus 30% globally).

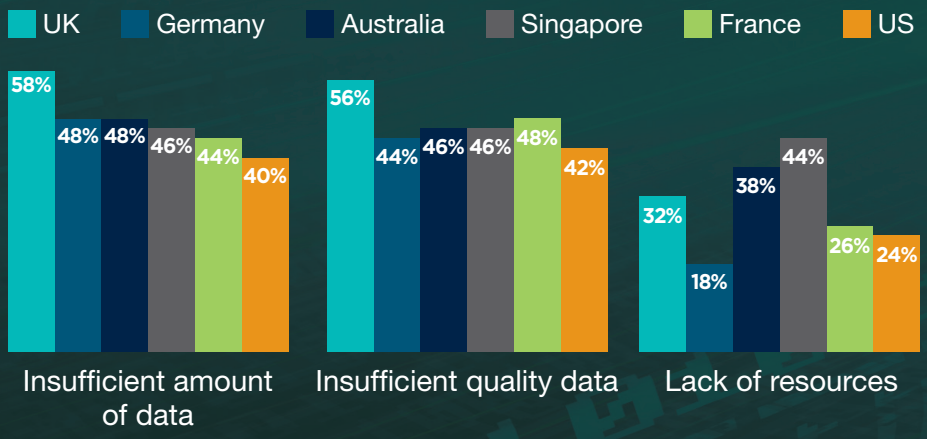
Automation on the rise

Q: What percentage of security tasks does your organization automate today? What percentage do you expect to automate in three years? *Mean scores are shown.*



Barriers to effective security

Q: To what extent do the following factors interfere with your security function's ability to protect against, detect, and respond to security threats? *"A substantial barrier" and "A complete roadblock" responses combined are shown.*



Security Response Leaders Get Better Results

The success of a company can be determined in large part by its security function. “Insurance companies build on the trust of our customers, so we invest a lot in protecting our customers’ data,” says Mr. Scholz. “Our reputation depends on the trust of our customers.”

Better security strategies and processes can mitigate operational, reputational, and financial risks by improving the speed and efficiency of detection and response. In fact, respondents are in widespread agreement that reducing time to detect and resolve breaches would improve overall financial performance; 88% say enhanced security would increase business continuity and the unbroken flow of operations.

What sets the most capable security organizations apart from their peers? Our top-tier respondents—those who assess themselves as highly effective at protecting against several different types of attacks, including the most serious threats—are automating a higher percentage of security tasks today than non-leaders, and they expect that gap to widen in three years (see sidebar, Meet the “Security Response Leaders,” page 14.). But there is more to the story than automation alone.

It starts with effective security prioritization strategies. Inability to prioritize security incidents based on the needs of the larger business is less of a roadblock for Security Response Leaders (only 3% say it is a barrier, versus 15% of others). They are more likely to say technology has allowed them to better prioritize security incidents based on the needs of the larger business (94% report substantial or transformative value, versus 76% of others).

Leaders also make security an organizational imperative. They are more likely to strongly agree that security is one of their organization’s core strategic initiatives (76%, versus 53% of non-leaders) and they have more buy-in from the top—all of our leaders agree or strongly agree that their CEO understands the business value of security, versus 89% of non-leaders.

Spotlight on Financial Services

Our survey sample included a significant number of respondents from the Financial Services industry. These firms are more likely than other industries to be Security Response Leaders, and show strength in numerous measures. Companies in this sector are:

- More focused than their peers on the impact of data and information security threats
- More likely to cite increasing quality of talent recruitment and retention and risk management as drivers of success
- More likely to say they are highly effective at preventing security breaches
- More likely to express concern over undetected and unaddressed breaches
- Automating a higher percentage of security tasks, now and in three years

“Our reputation depends on the trust of our customers.”

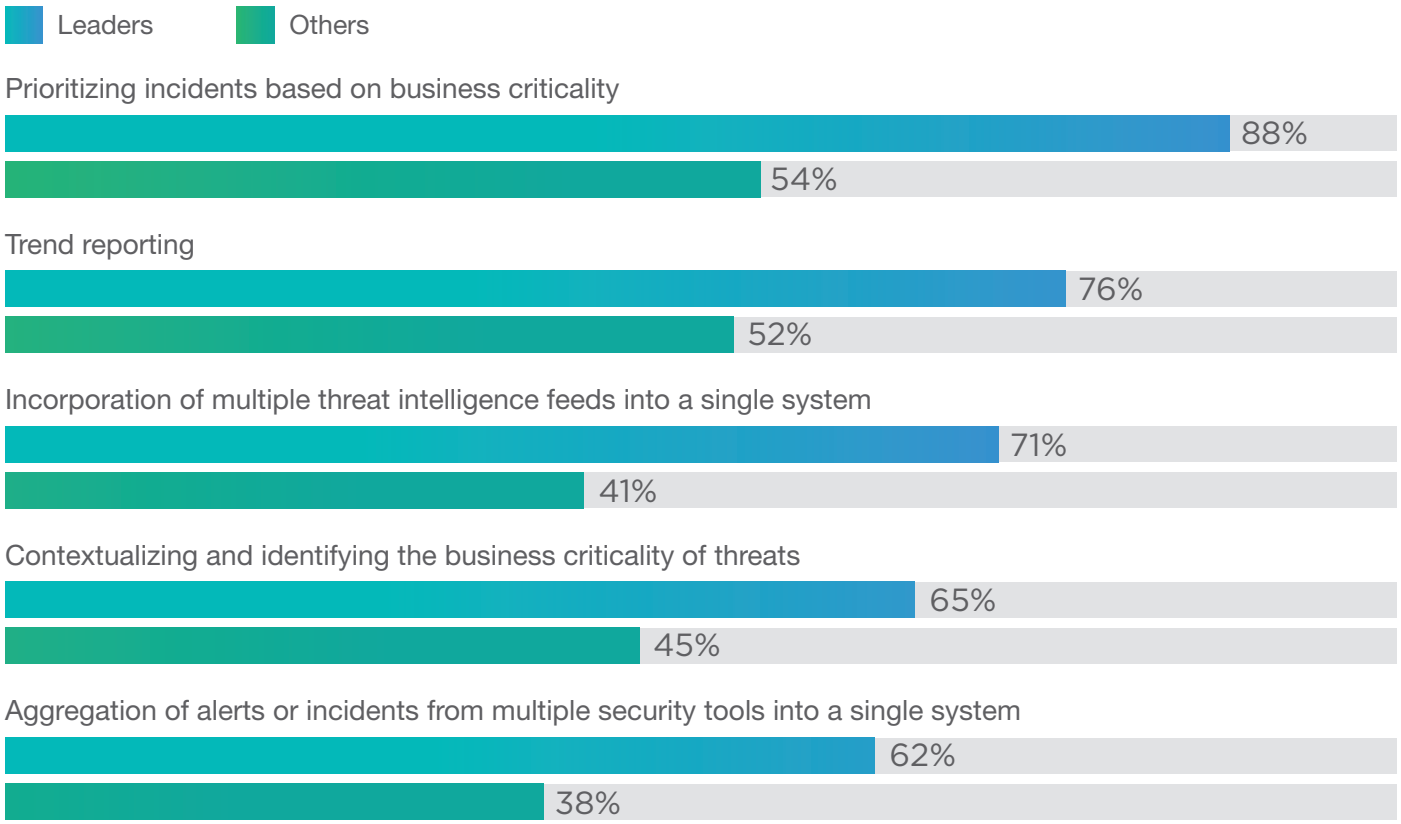
—Carsten Scholz, chief information security officer, Allianz, SE

These companies understand security as an issue affecting the entire business, and are effective at building strong connections across the organization. Strong relationships foster collaboration and help security personnel understand the business value of information and prioritize the right alerts. Nearly all leaders (97%) say their company sees internal collaboration as critical to security, versus 88% of others. They are more likely to say relationships between IT and security are very strong (91%, versus 79% of non-leaders), and to strongly agree that the CIO and senior-most security executives have strong working relationships (97%, compared with 88% of others). Leaders have greater confidence in the skills of security personnel, including their knowledge of the threat environment and weaknesses in security systems.

It is in this broader context that automation and technology provide the greatest value, and Security Response Leaders are ahead of their peers by several important measures. They are automating more sophisticated types of attacks, and are more tech-forward than other companies (50% are investing in artificial intelligence, versus 23% of others; 35% are investing in virtual or augmented reality, versus 13% of others).

Security Response Leaders have more advanced automation strategies

Q: Which tasks are you automating today? *Select all that apply.*



The Path Toward Security Response Leadership

Imagine the possibilities: Once someone uncovers a threat, the security response system is instantly mobilized.

First, data is automatically pulled into the security response system. Security analysts quickly ascertain that this malware is exploiting a severe vulnerability with a high probability of complete loss of data if unaddressed. Pertinent information to remedy the situation is immediately made available to the security team.

Then, hundreds of vulnerable items are correlated and prioritized based on business service impact, asset criticality, and the vulnerability score.

Built-in workflows take care of the next steps, ensuring analysts follow the security procedures. The system automatically triggers requests to approve emergency patches for critical vulnerable items.

Once the critical items have been patched, security and IT together create a plan to address the remaining vulnerable items on the security response platform. Automated workflows help security analysts route change requests to the right people within IT. The platform ensures they share information on a secure "need-to-know" basis, eliminating the need to memorize the organizational structure.

Now, the CISO receives an automatically generated post-incident report with accurate metrics. The CISO is happy, and the organization is secure.

Our research shows how security executives can tackle some of the most pressing issues faced by their organizations. To bolster enterprise defenses and to ensure reputations, we recommend a number of approaches to align business outcomes with information security success.

CISOs are faced with an overwhelming scale of security alerts and potential breaches. The best way to handle an overload of alerts is to automatically prioritize them based on their potential impact to your organization. Analysts need to know exactly which systems are affected and any subsequent consequences for related systems. Through workflows, automation, and orchestration, security organizations can increase their response speed and prioritize risks based on business criticality.

Many CISOs also cited the lack of communication and cooperation between functions across the business as a barrier to security success. It is critical to build relationships between security and other functions, not just at the C-level but well beyond into the trenches of those who fight security warfare every day. In order to best facilitate this, organizations should build a security response program that allows for communication across the business and allows security and IT teams to better coordinate responses.

Scarcity of resources and skilled talent was of highest concern for CISOs. Automation can increase worker satisfaction by moving people into higher-value work. For example, workflows are critical for ensuring adherence to your security procedures. Pre-defined processes enable lower-level personnel to perform actual security work, while more experienced security professionals focus on hunting down complex threats.

These are challenging times, but organizations that plan and execute effective security response programs can reduce risk to operational continuity, reputation, and financial performance.

Footnotes

1. 2016 Ponemon Cost of Data Breach Study, Ponemon Institute, June 2016.
2. State of Cybersecurity: Implications for 2016, ISACA and RSA Conference, 2016.
3. 2016 Internet Security Threat Report, Symantec, 2016.
4. 2016 Ponemon Cost of Data Breach Study, Ponemon Institute, June 2016.
5. These Industries Suffer the Largest Number of Cyberattacks, Inc. 5000, April 2015.
6. Status Quo Creates Security Risk: The State of Incident Response, Enterprise Strategy Group, February 2016.

Contributors

Amita Abraham	Claire Darling	Dan Huberty	Myke Lyons	Chris Peake
Yuval Cohen	Piero DePaoli	Michael Jones	Kathy O'Connell	Bryce Schroeder
Sean Convery	Riva Froymovich	Tim Kain	Paul Peterson	John Swick