The State of the CISO

A study of CISOs by Optiv Security

OPTIV

Executive Summary

No "C-level" position has been under more pressure and undergone more change in recent years than the chief information security officer (CISO).

A relatively new role in the corporate executive hierarchy, CISOs have traditionally reported to the chief information officer (CIO), because the job has been considered a largely technical one focused on security IT systems. With the rise of the data breach epidemic, and the imposition of comprehensive privacy regulations like the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), cybersecurity has become a tier-1 business risk – and, as a result, the CISO's role has dramatically changed. Combined with CEOs being held accountable by boards for cybersecurity issues, this has helped to elevate some CISOs to a level commensurate with CIOs and other C-level executives.

Some organizations are farther along this evolutionary curve than others. There still are many that keep CISOs relegated to their traditional technical roles, but others view the CISO as an important part of next-generation digital transformation and other business initiatives, because they know that major security or compliance miscues can derail the business.

To understand the state of the CISO role, Optiv Security conducted a survey of 100 U.K. and 100 U.S. CISOs (or in companies without a CISO title, personnel with the equivalent job responsibility). The results of the survey illuminated how cybersecurity and CISOs are evolving, with data points outlined on the following page.

Key Findings: CISO Role Grows in Stature, but Challenges Remain

67% of respondents indicated that their organizations prioritize cybersecurity above all other business considerations. In other words, cybersecurity has become the key enabling function across business initiatives.

Consistent with this first finding, 96% of respondents either slightly or strongly agree that business executives have a better understanding of cybersecurity than they did five years ago.

As part of this "better understanding," many business executives no longer consider data breaches to be a "scarlet letter" for CISOs. In fact, 58% of CISOs now say that experiencing a data breach makes them more attractive to potential employers.

76% of respondents believe that managing cyber risk is becoming so important that we will see companies naming CISOs as CEOs.

When asked what they would focus on if they could stop business for six months, only 32% of CISOs said they would focus on catching up on basic functions like vulnerability scanning and patching, opting instead to focus on things such as employee education and new methodologies. This is concerning in light of the fact that, by some estimates, unpatched vulnerabilities account for more than half of all data breaches.

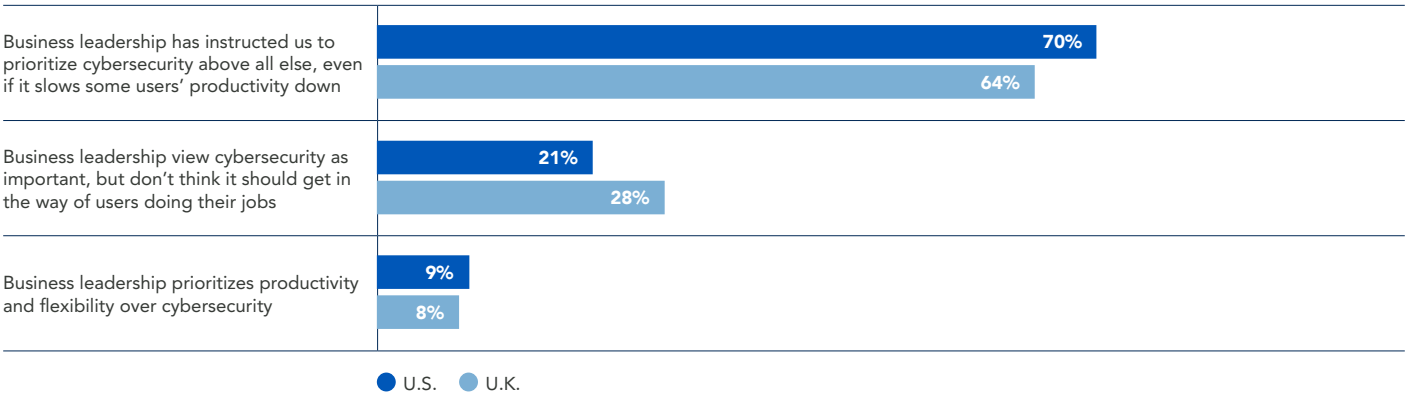
The following report goes into more detail on the State of the CISO study.

Cybersecurity Becomes a Business Priority

"Moving at the speed of business" has long been a sore point for cybersecurity professionals. Attend any major security conference, or read any top-tier security media outlet, and you will find stories about how security slows down business, which often results in business forging ahead with new initiatives before security has a chance to implement the appropriate controls.

According to respondents of the survey, this dynamic is changing. **A significant majority of both U.S. and U.K. respondents indicate that top business leadership has made cybersecurity a priority over "business speed."**

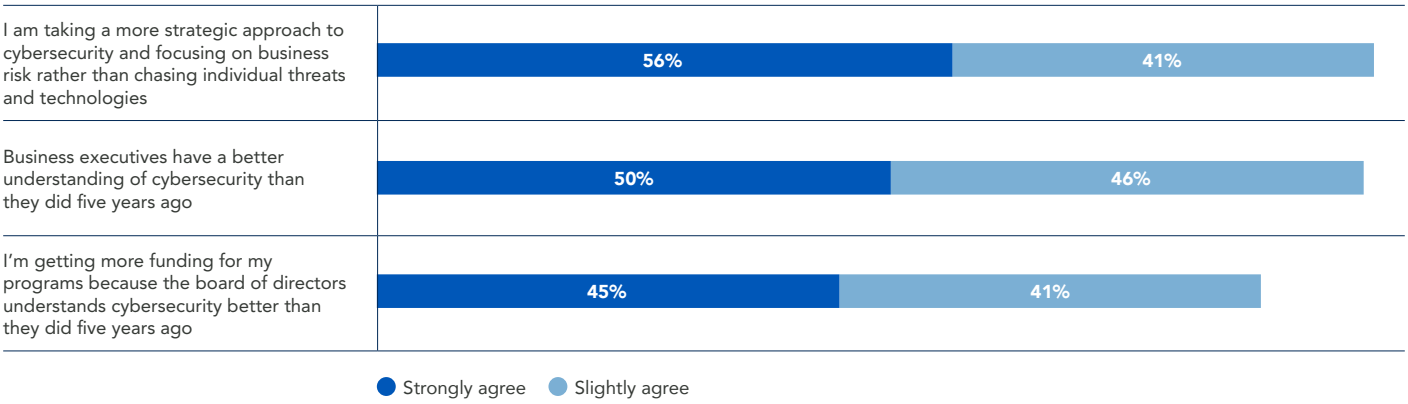
FIGURE 1: How does senior business management prioritize cybersecurity against general business objectives?



Cybersecurity Becomes a Business Priority (cont.)

Another point of conventional wisdom in the world of cybersecurity is that business executives and board members have a difficult time understanding cybersecurity, and CISOs have a difficult time communicating with them in meaningful business terms. According to the survey respondents, this dynamic has changed as well: **CISOs report greater alignment with business leaders.** As we see in Figure 2, a large majority of respondents indicate that they are able to take a more strategic approach to their roles, that business leaders have a better understanding of security than they used to, and that this alignment is translating into more funding for cybersecurity programs.

FIGURE 2: To what degree do you agree or disagree with the following statements?

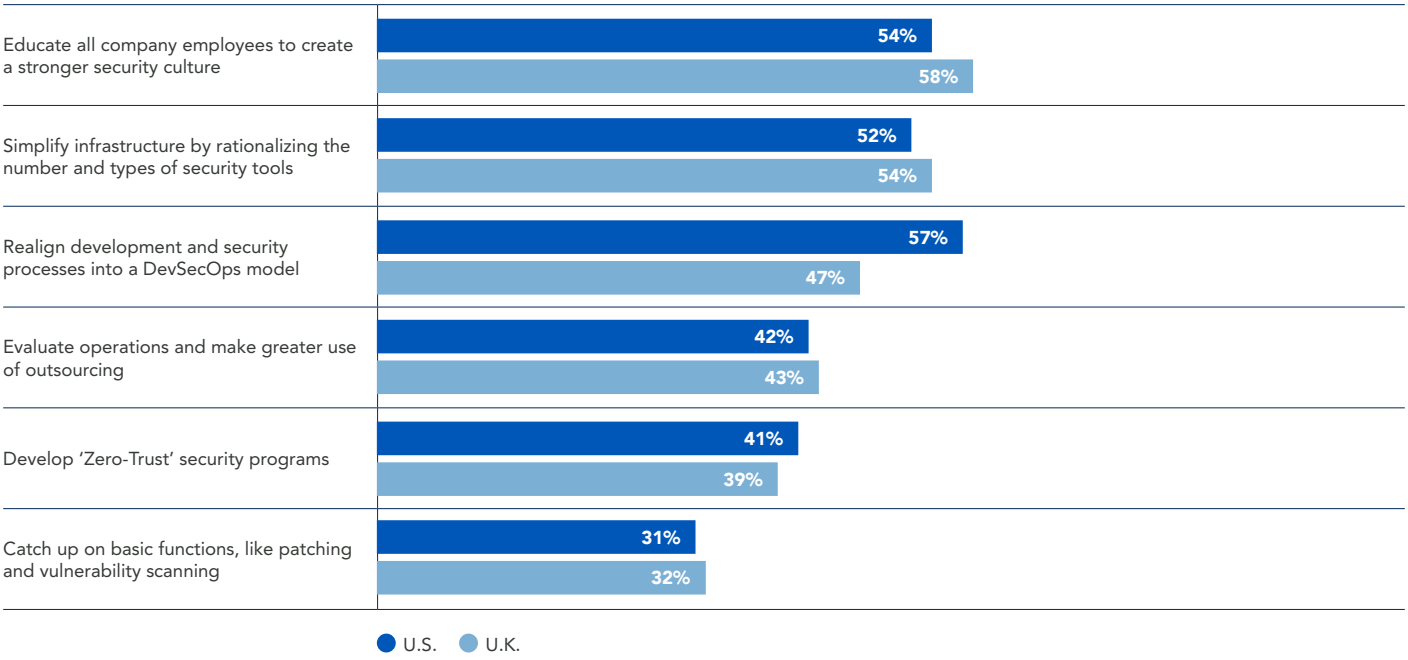


Most Important Security Activities

In an effort to understand CISO priorities, survey respondents were asked which activities they would undertake if they could stop the business for six months. The goal of this question was to identify how CISOs would prioritize security functions in the absence of day-in and day-out tactical demands from the business.

Basic functions like **vulnerability scanning and patching finished dead last,** as can be seen in Figure 3. This is surprising given that a recent study from the Ponemon Institute found 57% of data breaches stem from unpatched known vulnerabilities.[1] Educating employees, simplifying infrastructure and aligning security with development operations to create a DevSecOps model were indicated as the top priorities. In the U.S., DevSecOps was clearly the top priority, while in the U.K. employee education was deemed most important.

FIGURE 3: If you could stop the business for 6 months and have the luxury of time to execute any security priorities, which of the following areas would you choose to focus on?"



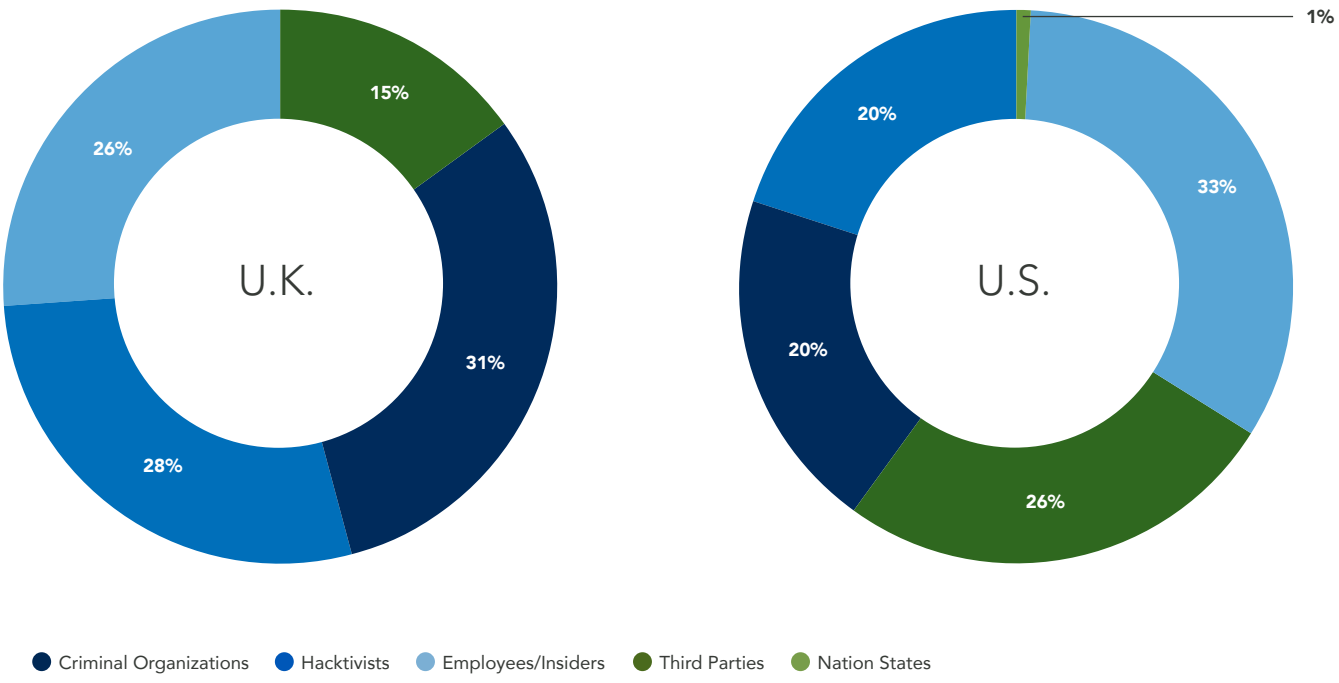
*Patch Work Demands Attention, Ponemon Institute and ServiceNow, 2018

Greatest Security Threats

There was a pronounced disparity between the U.K. and U.S. in terms of CISO opinions of security threats. As can be seen in Figure 4, criminal organizations were most commonly cited as the greatest security threat in the U.K., while in the U.S., employees and "insiders" were deemed the greatest threat by a significant margin.

Equally interesting, third parties (business partners, consultants, etc.) were deemed a much greater threat in the U.S. than in the U.K. **U.S. respondents indicated that third parties are the second greatest threat to security, and they were the most commonly cited among the "top three" security threats,** beating even insiders. In the U.K., third parties finished in last place among threat categories.

FIGURE 4: Which of the following are seen as the biggest cybersecurity threats to your organization?

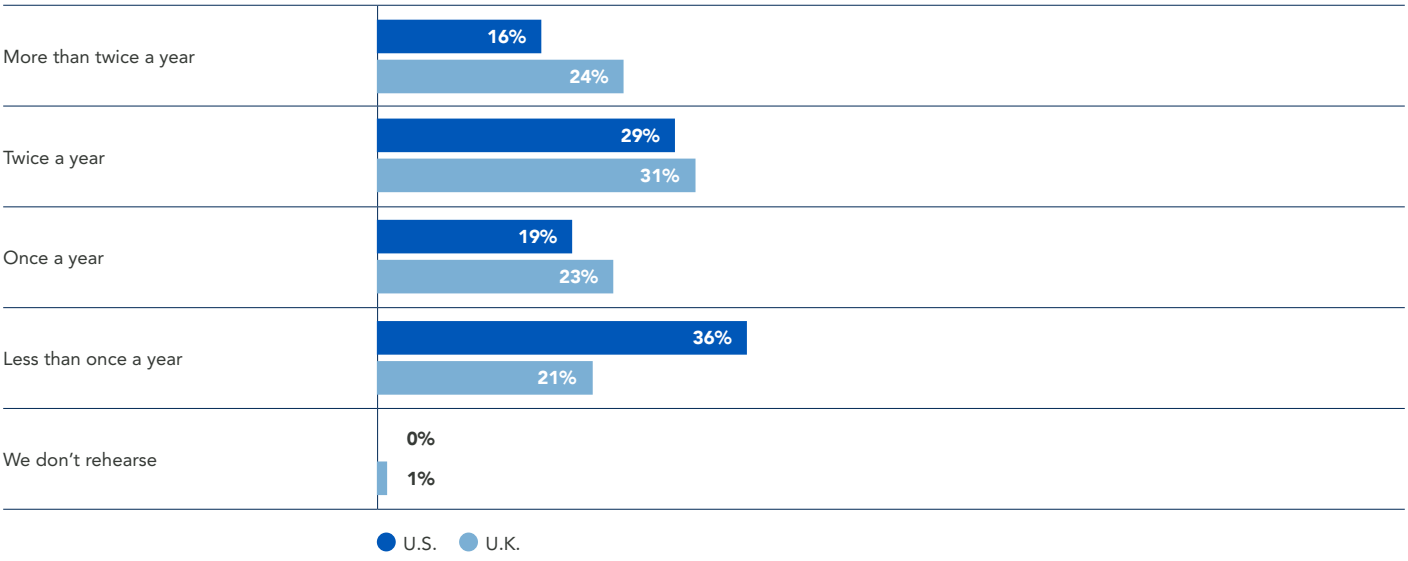


Incident Response Preparedness

Fully 92% of respondents across the U.K. and U.S. indicated they have a formal incident response plan in place. However, **the adoption of best practices relative to rehearsing incident response plans is lagging.**

In Figure 5 we see that in both the U.S. and the U.K., 45% of respondents indicated they rehearse their incident response plans at a frequency of once a year or less. These numbers compare unfavorably to the 45% of U.S. CISOs and 55% of U.K. CISOs indicating they rehearse their incident response plans at least twice per year, which is a frequency closer to industry best practices.

FIGURE 5: How often do you rehearse your incident response plan using 'table top exercises' or other forms of practice?

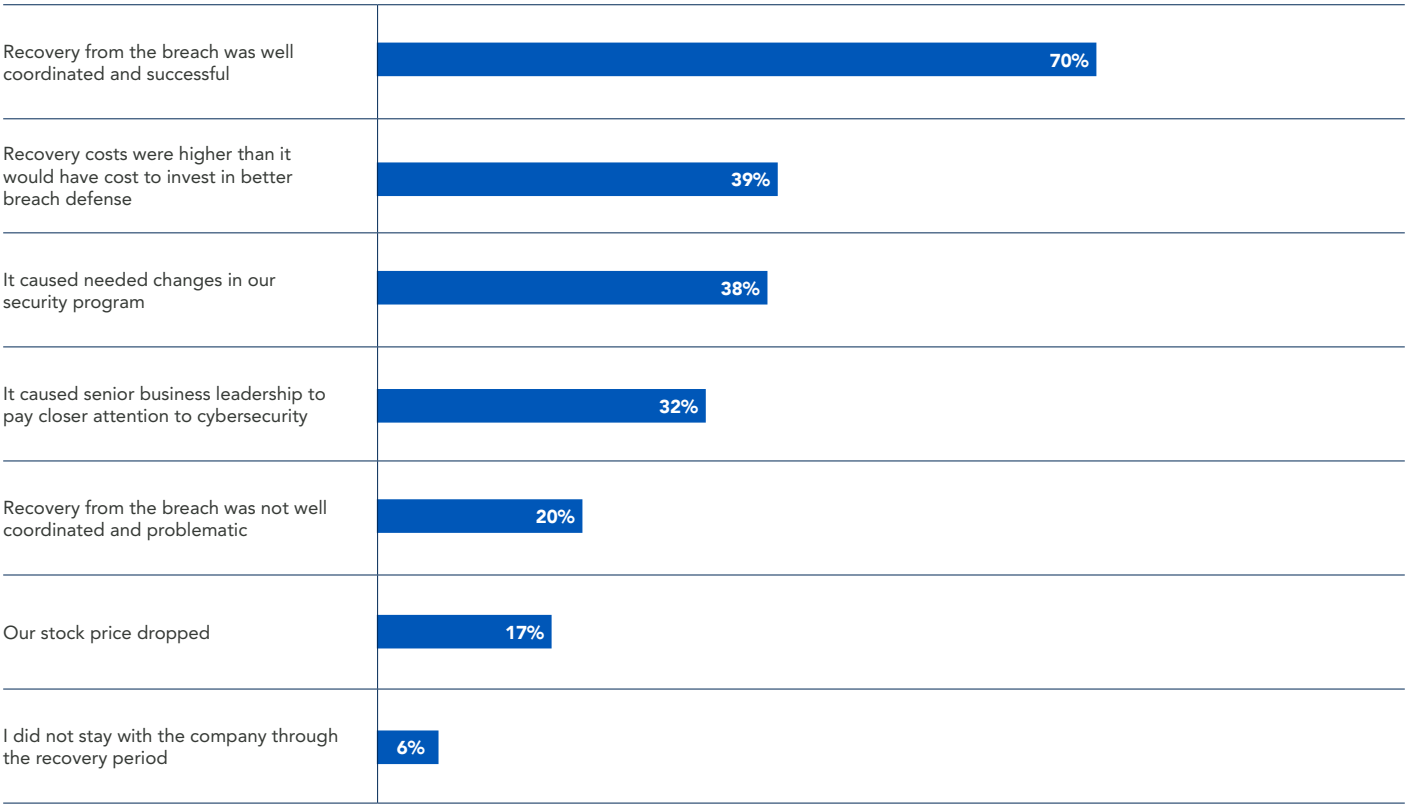


Breach Business Impact

Breaches still seem to serve as a "wake up call" for many organizations, where **needed changes and controls are only implemented after a breach has occurred.**

More than half (51%) of respondents had experience managing an organization through a data breach. Figure 6 shows that most respondents (70%) indicated that the recovery from the breach was well coordinated and successful. At the same time, 39% responded that recovery costs were more than it would have cost to implement a stronger breach defense. Almost the same number (38%) said that the breach caused needed changes in the security program, and 32% said the breach caused senior management to pay closer attention to cybersecurity. These responses would seem to indicate that it takes a breach for many organizations to apply the necessary focus on cybersecurity.

FIGURE 6: Thinking about the most recent breach you experienced, what was the outcome?

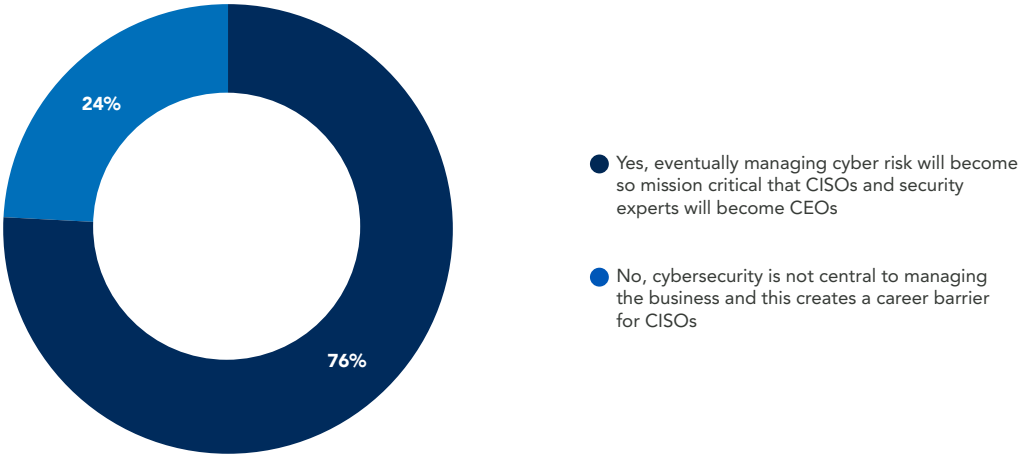


Breach Impact on CISO Careers

The CISO career track has changed significantly over the years. What was once a mostly technical job hidden in the bowels of the IT department (often without the CISO title), has now emerged as a true C-level business function.

In fact, Figure 7 shows that **76% of respondents believe that managing cyber risk is becoming so important that we will see companies naming CISOs as CEOs.**

FIGURE 7: A growing number of CIOs are being named CEOs at companies. Do you see a similar career path in the future for CISOs?

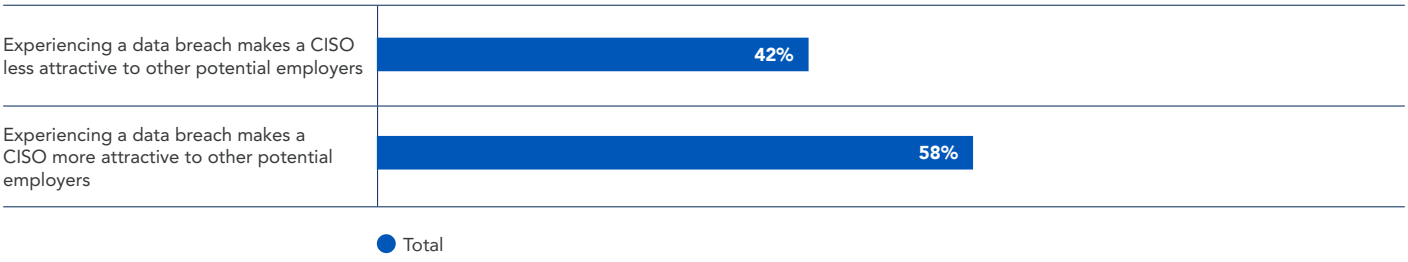


Breach Impact on CISO Careers (cont.)

And, where breaches once were the "kiss of death" for a CISO career, Figure 8 indicates that the experience of managing through a breach is increasingly valued both by CISOs and potential employers.

Of the 51% of respondents who had managed through a data breach, 95% also said that they are now better prepared to manage through the next breach. Remarkably, **58% of respondents said that breach experience makes them more attractive to prospective employers.** Only 42% believe managing through a breach makes them less attractive to employers.

FIGURE 8: Which of the following statements do you most agree with?

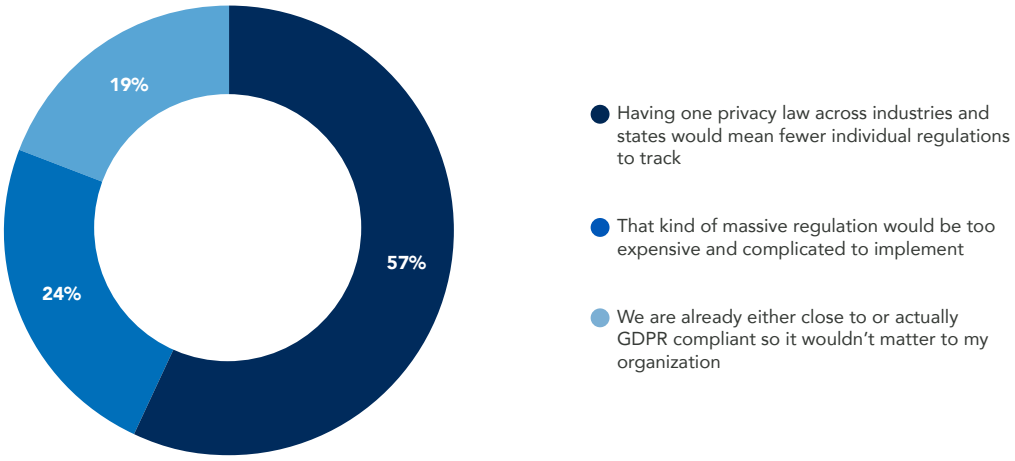


CISO Opinion: Regulatory Compliance

While stringent new privacy regulations such as the GDPR and CCPA have caused significant strain among organizations that need to comply with those regulations, **most U.S. respondents agree that having a single, comprehensive privacy regulation would be preferable to complying with multiple more targeted regulations.**

Figure 9 shows that more than half of U.S. respondents believe a single overarching privacy regulation would make compliance simpler, and nearly one in five of respondents indicated that they already comply with GDPR. Only 24% believed that a GDPR-like regulation would be too cumbersome to implement.

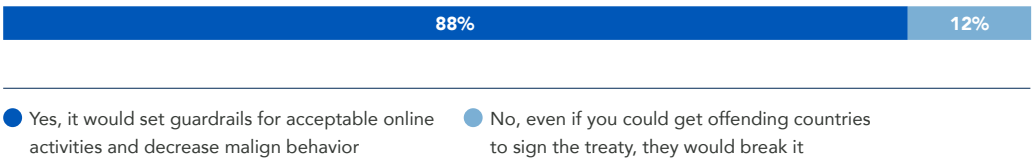
FIGURE 9: What impact would a GDPR-like regulation have on your business?



CISO Opinion: Regulatory Compliance (cont.)

To conclude the survey, U.S. CISOs were asked if they thought it would be worthwhile for there to be a global agreement on cybersecurity in place, similar to the Geneva Convention, where countries agree to a set of principles governing their conduct on the internet. **A whopping 88% of respondents agreed that such an agreement would establish guardrails that decrease malign behavior.**

FIGURE 10: Would it be worthwhile having a global agreement on cybersecurity, similar to the Geneva Convention, where countries agree to a set of principles governing their conduct on the internet?



Methodology

In June 2018, Optiv Security, working with market research firm Loudhouse, conducted structured telephone interviews with 200 CISOs, or IT employees with CISO duties in companies without a CISO title. The following tables provide information on survey respondents, along with geography and their organizations.

REGION	
Total	**200**
U.S.	100
U.K.	100

COMPANY SIZE	
500-999	43
1000-4999	100
5000+	57

JOB FUNCTION	
CISO/CSO	143
IT Director/VP/CIO	38
IT System Admin/Engineer/Architect	14
Operations/System Manager	4
Other	1

Want to learn more?
Contact Your Optiv Representative

Optiv Global Headquarters
1144 15th Street, Suite 2900
Denver, CO 80202

800.574.0896 | optiv.com

Who secures your insecurity?™

Optiv is a security solutions integrator – a global, "one-stop" trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.