Point of View

The Global CISO Study

How Leading Organizations Respond to Security Threats and Keep Data Safe in Europe

Global Issues, Regional Focus

In Europe, privacy is viewed as a human right, and it is the job of chief information security officers to ensure that their companies do not tread upon that right.

The European Union has some of the most robust data privacy laws in the world, putting the pressure on businesses to forge appropriate protections that secure customer information and notify authorities when major breaches occur. In addition, each EU member, including the exiting UK, has its own courts and set of codes when it comes to data security. For example, France recently strengthened the rights of individuals to control personal data,[1] and Germany has special requirements for critical infrastructure providers.[2]

While the combination of these factors leads CISOs in Europe to be slightly more concerned about how effective they are at securing customer information and responding to security threats, it also may push many of these CISOs to outperform their global peers.

> “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*

Our survey shows that respondents in Europe, like their peers around the world, are worried about their ability to protect data, and must do more to improve organizational skills and increase their automation of security tasks. Among our key findings for the region:

- 83% of CISOs in Europe are highly concerned that breaches are going unaddressed, with executives in France most concerned (90%, vs. 88% in the UK and 72% in Germany). And 81% of European CISOs are worried about their ability to detect breaches in the first place (88% in the UK; 86% in France; 68% in Germany). Just under one-fifth of European executives say their company is highly effective at preventing security breaches.
- Most security organizations in Europe fail to prioritize alerts based on the threatened data's importance—68% of respondents in Europe (72% in Germany; 68% in France; 64% in the UK) say they have difficulty doing so, vs. 70% globally.
- CISOs in Europe are betting on automation, and the pace of automation is quickening: Just under one-third of respondents in Europe (31%) automate more than 40% of their security processes today, while more than two-thirds (72%) plan to automate that amount in three years—numbers roughly on par with global averages. Germany is ahead on the number of security tasks automated, today and in three years.

83%

of CISOs in Europe are highly concerned that security breaches are going unaddressed.

68%

of CISOs in Europe say it is difficult to prioritize alerts based on business criticality.

The Automation Advantage

Advances in automation hold great promise—but organizations in the region have much work left to do. Just 51% say they have automated the prioritization of alerts based on mission-relevant data today (60% in Germany, 54% in France; 60% in Germany; 48% globally), and only 37% are automating the aggregation of relevant information from business units (42% in France; 38% in Germany; 30% in the UK; 40% globally).

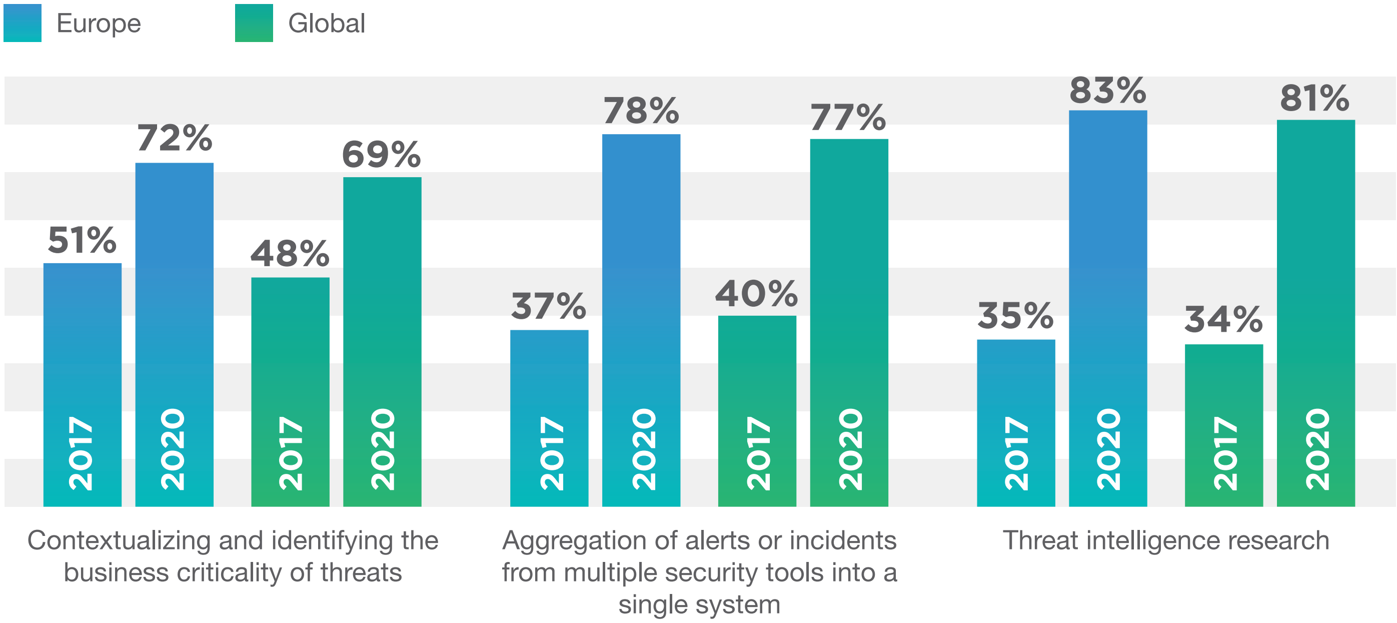
Over the next three years, security functions will begin automating more strategic tasks. Threat intelligence research, aggregation of alerts from multiple security tools, and contextualizing alerts based on business criticality will see the fastest growth.

"We automate as much as possible," says Carsten Scholz, chief information security officer of Allianz SE, a Munich-based financial services company. "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."

> "We automate as much as possible. You have some threat vectors where you cannot survive if you are not automated."
>
> *—Carsten Scholz, chief information security officer, Allianz SE*

Automated tasks are growing more sophisticated

Q: Which tasks are you automating today? Which do you plan to automate by 2020?



People still matter in the age of automation. Attracting skilled talent and upskilling and retaining existing talent, are rated as the most important elements to the success of security functions, with France and Germany even more focused than the UK on attracting skilled talent (96% in both Germany and France, vs. 90% in the UK) and retaining existing talent (96% France and 94% in Germany, vs. 88% in the UK).

Meet the “Security Response Leaders”

We filtered the survey data to identify respondents who stand out for their security capabilities and named them “Security Response Leaders.” This group makes up 11% of the overall sample.

Of all the CISOs polled in each country, 14% of respondents in France qualified themselves as leaders (equaling Australia for the highest proportion of leaders in any country), compared with 12% in the UK and 6% in Germany.

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) 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, globally, they tend to demonstrate more maturity than other respondents across a variety of areas. At the country level, however, confidence not always match up with more quantifiable metrics of performance; Germany, for example, is ahead of France and the UK on automation, yet its CISOs are less likely to claim effectiveness at protecting against security threats.

Globally, 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.
- 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.

Conclusion

Keeping data safe is a global challenge. Organizations in France, Germany, and the UK must address the same security risks facing their peers in other countries, while navigating the strict requirements of the EU as well as their own unique cultural and business landscapes. CISOs across the region must focus on automation and use technology to maximize the value of human capital in order to protect their organizations from the growing threat of security breaches.

About the research

We surveyed 300 chief information security officers (CISOs) about their strategies for navigating this challenging environment. This report covers the findings from our analysis of survey results from France, Germany, and the United Kingdom, from which we collected 50 responses each; numbers for Europe represent the average results from these three countries. See our full report (www.servicenow.com/c-suite/ciso.html) for in-depth, global analysis from our survey.

Footnotes

1. What the EU’s new data protection laws mean for UK industry, ComputerWeekly.com, May 2016. http://www.computerweekly.com/feature/What-the-EUs-new-data-protection-laws-mean-for-UK-industry

2. Germany passes strict cyber-security law to protect ‘critical infrastructure’, Reuters, July 2015. https://www.rt.com/news/273058-german-cyber-security-law/