Point of View

The Global CISO Study

How Financial Services Companies Respond to Security Threats and Keep Data Safe

Financial services is an inviting target for cybercrime. These companies face substantial risks to their reputations and financial performance if they fail to keep their customers' information and funds safe, even as these same custumers demand new products and services that add complexity to security processes. Moreover, the sector must comply with daunting regulations, often across multiple jurisdictions. All of this is happening in a field where skilled talent is at a premium and difficult to find.

Chief information security officers (CISOs) at financial services companies have responded to these challenges by becoming the best in their field. They are ahead of CISOs in other industries in implementing new security technologies, automating more security response processes, and prioritizing which threats require immediate remediation. Perhaps unsurprisingly, then, they also are more confident in their company's ability to prevent data breaches than CISOs in other industries. Still, they know they cannot afford to relax in the face of an increasingly risky threat environment.

78%

of financial services CISOs surveyed cite data and information security threats as top-line business issues

Our analysis shows that financial services companies are:

- **Prioritizing security.** These companies are more focused on data and information security threats (78% versus 28% of others) as top-line business issues. They also are dedicating a higher percentage of their technology budgets to security (roughly 40% are dedicating more than 11% of their tech budgets, versus 25% of all others).
- **Focused on risk mitigation.** Brand reputation is critical to financial services firms, and they are twice as likely to say breaches of personal information about their customers pose a serious danger (98% versus 56%). They are much more likely than their peers from other sectors to cite risk management as a driver of success for their company over the next three years (58% versus 11%).
- **Ahead on automation and technology.** Financial services firms are automating a higher percentage of security processes today, and expect to keep their lead in three years. They are more focused than others on some critical emerging technologies including Big Data and Analytics (72% are investing heavily, versus 59% of all others), artificial intelligence (38% versus 23%), and augmented reality/virtual reality (30% versus 12%).
- **More confident in their ability to prevent breaches.** CISOs from financial services are more likely to say they are highly effective at preventing security breaches (32% versus 16% of others). They also report greater confidence in their function's ability to prevent specific types of attacks, including breaches of personal information about customers (86% say they are highly effective, versus 50% of all others) and customer credit-card or financial information (86% versus 28%).

versus 28%

of other CISOs.

The Automation Advantage

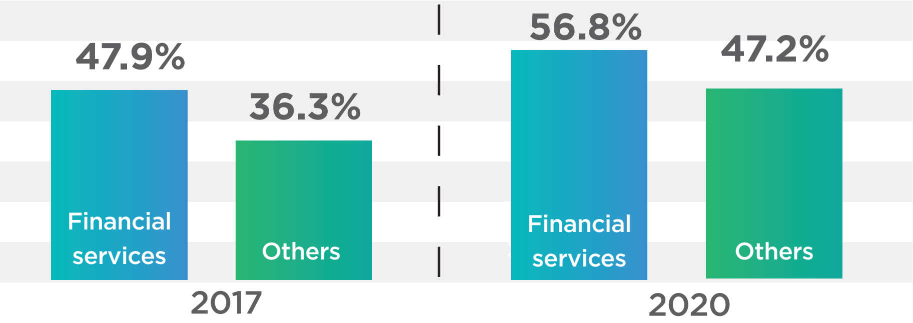
Advances in automation hold great promise—and financial services firms are making progress at a faster rate than firms in other sectors. They are more likely to say they are automating processes today (on average, they automate 48% of tasks today, while others automate 36% on average), and expect to keep their lead in three years (57% vs. 47%).

"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."

Financial services firms automate on average **48%** of security tasks.

Financial services firms are automating more security tasks

Q: Approximately what percent of security tasks have you automated? Approximately what percent do you expect to have automated in three years? *Mean responses shown*



Despite automating a higher percentage of security tasks, financial services firms are not ahead of other industries in terms of the sophistication of tasks automated. One reason may be poor data quality, which financial industry CISOs view as in worse condition than their peers. (64% of financial services CISOs cite data quality as a barrier to security effectiveness, versus 44% of others).

Another reason for lags in automation may be a lack of security expertise. As financial industry companies race ahead with automation, CISOs continue to focus on hiring skilled security professionals, retaining that talent, and upskilling. "There is actually negative unemployment globally in information security, and it is very, very hard to get talent," says Daniel Conroy, chief information security officer of Synchrony Financial.

Financial services firms are more focused on this challenge than peers in other industries, including attracting skilled talent (98% versus 91% of others) and retaining existing talent (94% versus 88% of others). Perhaps because of this focus, they also are more likely to rate the skills and expertise of their workers as well-developed in a range of areas, including routine threat detection (94% say these skills are well-developed, versus 63% of others), prioritizing threats based on their business impact (94% versus 67%), and predicting future threats (74% versus 51%).

> "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*

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.” 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) 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.

Across industries, Security Response Leaders display certain characteristics that set them apart from other organizations. Among other qualities, 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 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 challenge across industries, but as financial customers demand more mobile and responsive services and products, the risk of data breaches rises. CISOs in this industry are adopting new technologies to stay ahead of threats, and are doing so faster than peers in other industries. These CISOs must continue to focus on automation and maximize the value of human capital in order to build strong response strategies that protect against the consequences of information security threats.

About the research

ServiceNow and Oxford Economics surveyed 300 chief information security officers about their strategies for navigating in this challenging environment. This report covers the findings from our analysis of survey results from the financial services industry, from which we collected 50 responses. See our full report (https://www.servicenow.com/c-suite/ciso.html) for in-depth, global analysis from our survey, as well as real-world commentary from CISOs.