Publication date: October 2023
Authors:
Andrew Braunberg
Philip Benton

State of Security for Financial Services

Evaluating financial institutions' ability to tackle emerging cybersecurity threats

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Swimlane

Contents

Executive Summary

The current cybersecurity threat landscape remains dynamic and challenging. New threats continue to emerge as adversaries leverage new technologies, such as generative AI, to create new methods of attack. Traditional attack vectors, such as phishing, continue to confound even savvy end users, while traditional criminal business models, such as ransomware, continue to mature and evolve.

Financial services organizations face all the cyber security concerns experienced by other verticals, whilst also operating under unique constraints and with the additional challenges associated with financial fraud. And if there is an environment as dynamic and challenging as cyber security, it is financial fraud.

As a result, financial services organizations have invested heavily in cyber security and anti-fraud solutions. It is not unusual for the average financial firm to juggle dozens of security controls and our research shows that a significant proportion of organizations surveyed have deployed multiple, separate security solutions. Such complexity raises its own concerns, particularly around personnel training and retention. Considering the global shortage of security expertise, this is a concern that needs to be addressed.

Financial institutions also face mounting pressure to tackle fraud from regulators, customers, and shareholders and are required to balance product and service innovation and investment in technology with the evolving risk of fraud. Historically, fraud has been addressed with a dedicated, and siloed, team. However, as more financial fraud moves to digital channels the benefits of collaboration between security and fraud teams have become more apparent. Given that financial organizations are built on customer trust, cyber security breaches and fraud can have impacts well beyond their hard costs.

Unfortunately, the size and scope of these problems has left both security and fraud teams struggling to keep up. Security automation can help. Security Orchestration, Automation, and Response (SOAR) solutions are designed to automate and orchestrate time consuming manual tasks for security and other operational teams, delivering productivity benefits and improving accuracy of response.

These solutions are broadly seen as improving analyst accuracy, enabling better insights, and improving productivity. Financial services organizations of all types should investigate the benefits that security automation can bring to easing the burden on both security and fraud teams.

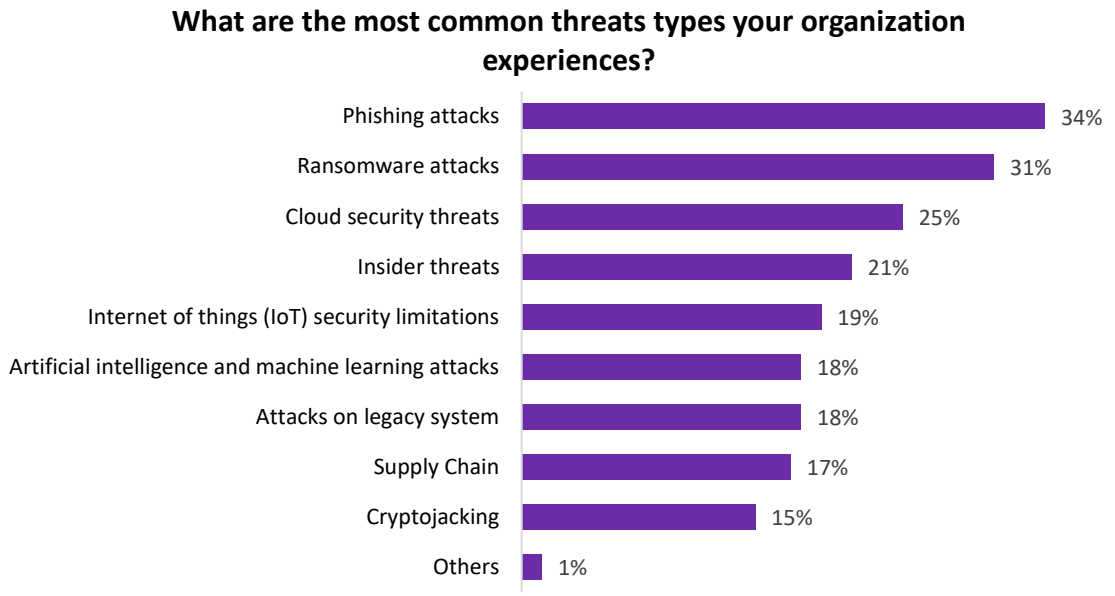
Financial Services Threat Landscape

Globally, financial services organizations face a host of cyber security threats. Some threats are industry agnostic, so organizations may deploy many of the same security controls seen in other large organizations. But financial services organizations also need to protect against targeted and sophisticated forms of fraud, much of it utilizing digital infrastructure. These organizations have therefore also invested heavily in anti-fraud solutions.

Common Cyber Attack Vectors

Phishing and ransomware are widely used attacks because they remain effective, and lucrative. (Phishing, of course, can be a step in a broader ransomware attack.) Financial services organizations of all sizes report that these two types of attacks are among the most common they encounter (see **Figure 1**). As these organizations continue their digital transformations, threats targeting cloud assets, as well as internet of things (IoT) assets have also become more common. Perhaps demonstrating that no infrastructure is safe from attack, financial organizations with revenue between $5 billion and $10 billion, report almost as many attacks against legacy infrastructure (27%) as cloud assets (31%).

Figure 1: Most common threats targeting financial services organizations



Source: Omdia

Unique challenges and concerns in financial services

Financial organizations recognize that they operate under unique constraints, which contribute to industry specific challenges (see **Figure 2**).

Figure 2: Unique security challenges in financial services

Source: Omdia

For example, financial organizations of all types retain very sensitive information on their customers. This contributes to the related business constraint that financial services are also highly regulated.

Financial services organizations find themselves between a rock and a hard place. Customer and market demands have accelerated the speed and scale of their digital transformations. But all this must be done within the constraints of regulatory requirements and with the safety of customer data kept top of mind. Which brings up the problem of financial fraud. While not all these security concerns are unique to financial services, the combination of concerns is itself a unique challenge. It reminds us of the old joke about the dance partners Fred Astaire and Ginger Rogers. Yes, they performed the same routine, but Rogers had to do it backwards and in high heels.

While the sensitivity of stored customer data is broadly recognized as the top challenge for financial organizations, Omdia research found that the priority of additional concerns diverges depending on what chair a respondent sits in.

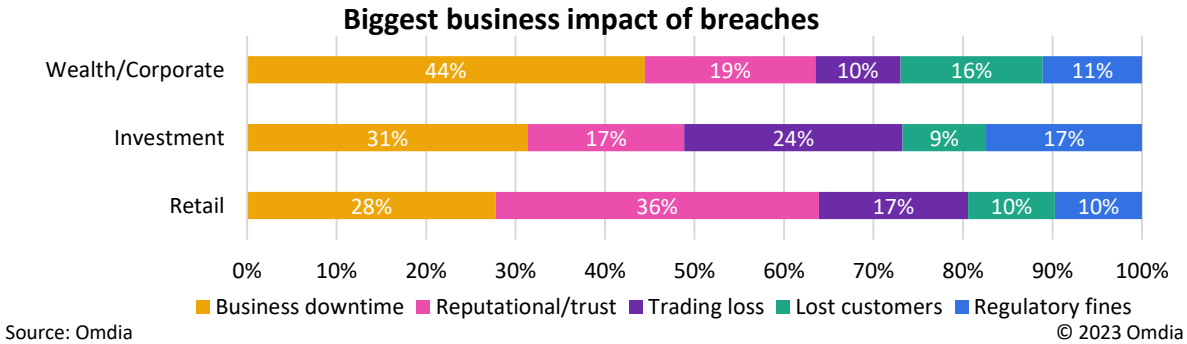
Omdia found that different departments tend to have different security concerns. Compliance and treasury employees tend to be more concerned with the scale of digital transformation, IT Ops are more concerned about compliance requirements and security personnel are more concerned with fraud.

Financial services are a 24/7 industry with very high customer service expectations. It is not surprising; therefore, that business downtime is broadly considered the most troublesome consequence of cyber breaches. Ongoing “digital first” strategies have exacerbated this requirement as organizations have shifted from “planned downtime” to an “always on” orientation.

That said, the impact of successful cyber-attacks is assessed differently depending on the type of financial institution. Wealth management and investments banks rate downtime as the largest concern associated with cyber breaches (see **Figure 3**), but retail banks (whose customers can more easily change service providers) are more concerned with loss of reputation and customer trust.

> Retail banks (whose customers can more easily change service providers) are more concerned with loss of reputation and customer trust.

Figure 3: Breach impacts by type of financial organization

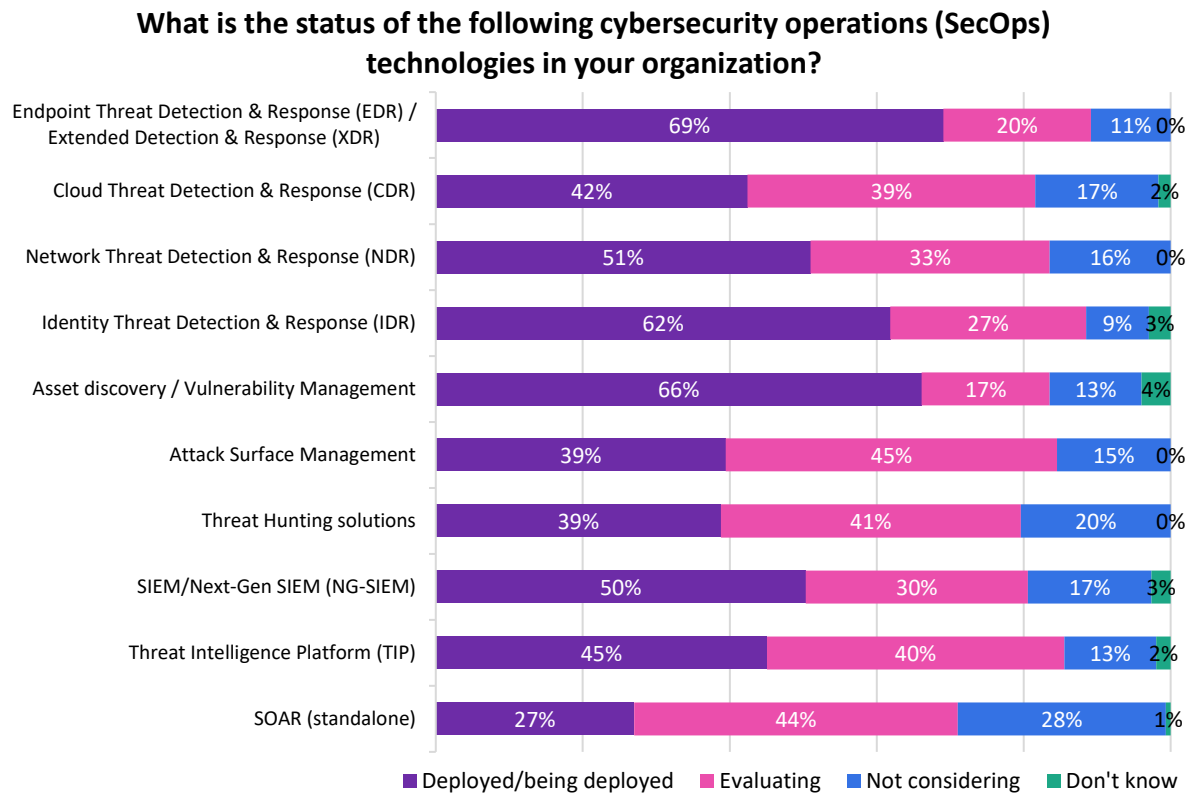


Source: Omdia

Security investments and trends

Large financial institutions have long been seen as early adopters of new security controls, and many of these firms were early innovators in creating security operations centers (SOC). Detection and response tools are the most broadly deployed products, along with asset discovery and vulnerability management solutions and the industry continues to invest in building out additional SOC functionality (see **Figure 4**).

Figure 4: Prevalence of security controls in security operations centers



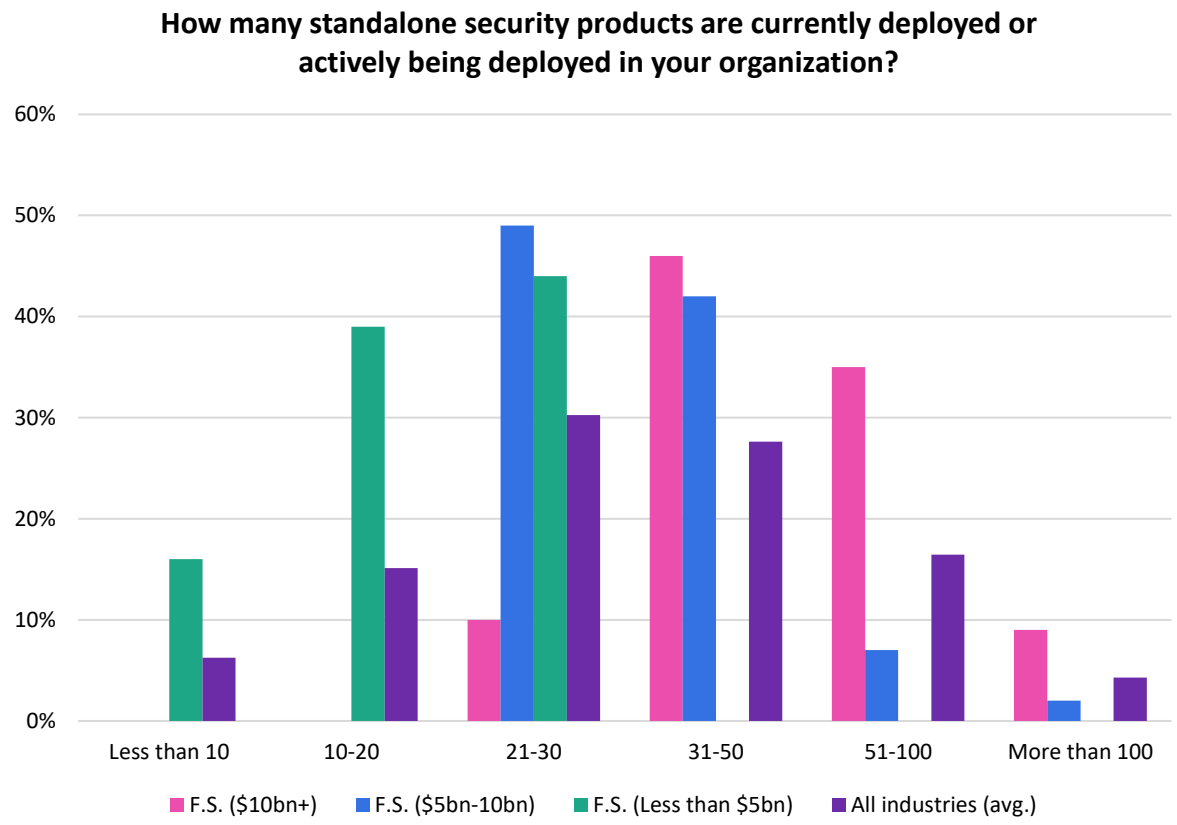
Source: Omdia

Newer tools in the SOC arsenal, such as Attack Surface Management (ASM) and SOAR, are being evaluated at the highest rate of any SOC tool.

Almost half of all respondents have 31 or more separate security controls in place, but the average number of controls varies significantly by company size. For example, 9% of the largest organizations had more than 100 security controls. To appreciate the level of investment, figure 5 includes the average number of security controls in place across all industries according to Omdia's 2023 Decision Maker survey. As can be seen, larger financial institutions have many more security controls than businesses generally, while smaller financial institutions tend to have less.

There is also significant variation by type of organization. 31% of wealth/corporate institutions have 50 or more standalone security products deployed (inclusive of 6% who have over 100), while just 8% of investment firms have more than 50 standalone security products (see **Figure 5**).

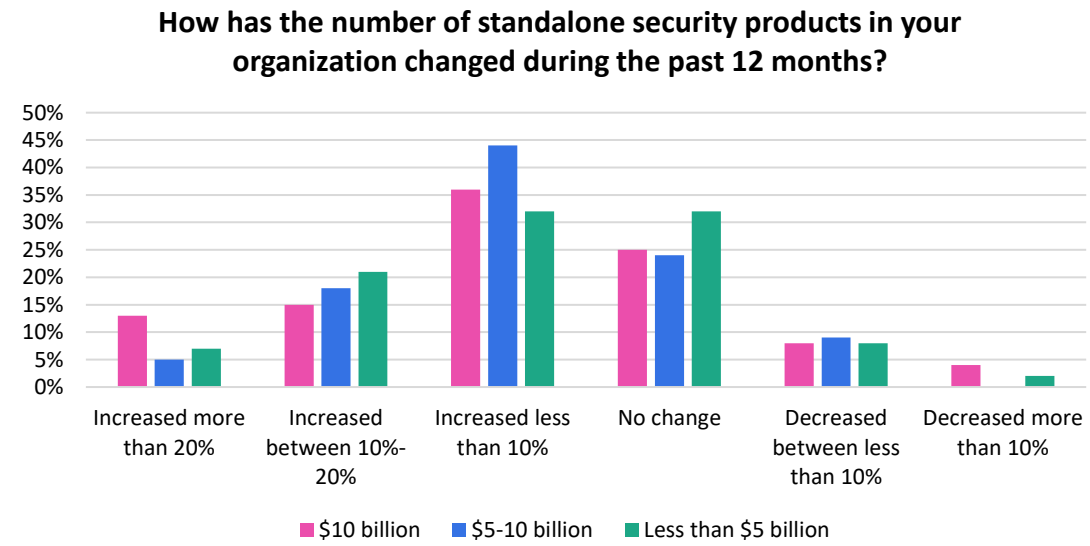
Figure 5: Total number of security products deployed, by size of financial organization



The need (and desire) to consolidate security products and security vendors is often discussed by security practitioners, but Omdia research shows that it seldom is achieved. Most financial organizations of all sizes plan to increase the number of deployed security products over the next 12 months (see **Figure 6**).

> Most financial organizations plan to increase the number of deployed security products over the next 12 months.

Figure 6: Planned change in number of security products, by size of financial organization

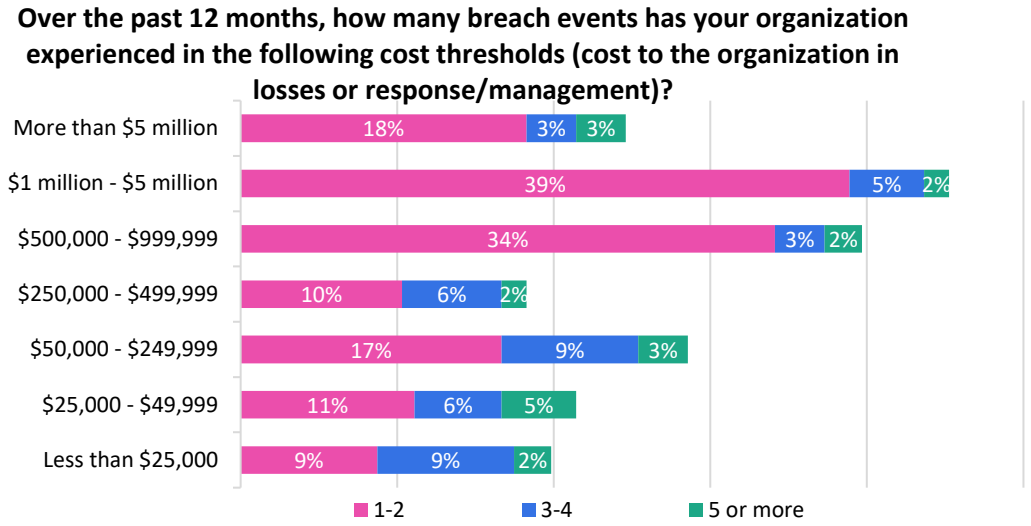


Source: Omdia

Despite the depth and breadth of these security architectures, financial organizations continue to be the victims of frequent and costly breaches. 20% of respondents have had at least one breach with a total cost of $5 million in the last 12 months. And 42% of respondents have had at least one breach with a total cost of $1 million in the last 12 months (see **Figure 7**).

> Financial organizations continue to be the victims of frequent and costly breaches.

Figure 7: Frequency of breaches, by cost



Source: Omdia

There is some variability in the numbers. For example, organizations with more than $5 billion in annual revenue are significantly more likely than smaller organizations to be the victim of breaches with total costs of more than $1 million. And North American-based organizations were significantly more likely than UK-based organizations to be the victims of breaches with total costs of more than $1 million.

Cyber-attacks can have different motives, goals, and impacts. With respect to their impact on customers, they can limit access to assets (due to infrastructure downtime) or result in the loss of personal data, which can enable fraud.

Threat of Fraud©

With new fraud tactics constantly emerging, business agility and investment in the latest technologies that better evaluate existing and quickly emerging threats have never been more critical. Institutions are also under increasing pressure to provide a strong user experience that consumers expect to remain competitive. However, many existing fraud solutions currently utilized by banks are poorly integrated with the organization's broader objectives, which is detrimental to customer satisfaction and the bank itself.

Financial institutions face mounting pressure to tackle fraud from regulators, customers, and shareholders and are required to balance product and service innovation and investment in technology with the evolving risk of fraud. They are expanding the use of artificial intelligence (AI) and machine learning (ML), behavioral analysis, and biometrics to both address a wider field of threats and automate as much of the process as possible to bring efficiencies. These tools can also aid regulatory compliance and help achieve growth by driving consumer trust and loyalty with the brand. However, organizations need an approach that not only enables the use of latest technologies and techniques and detects fraud in real time but allows for real-time fraud attack information to be shared across business functions and with stakeholders across the organization.

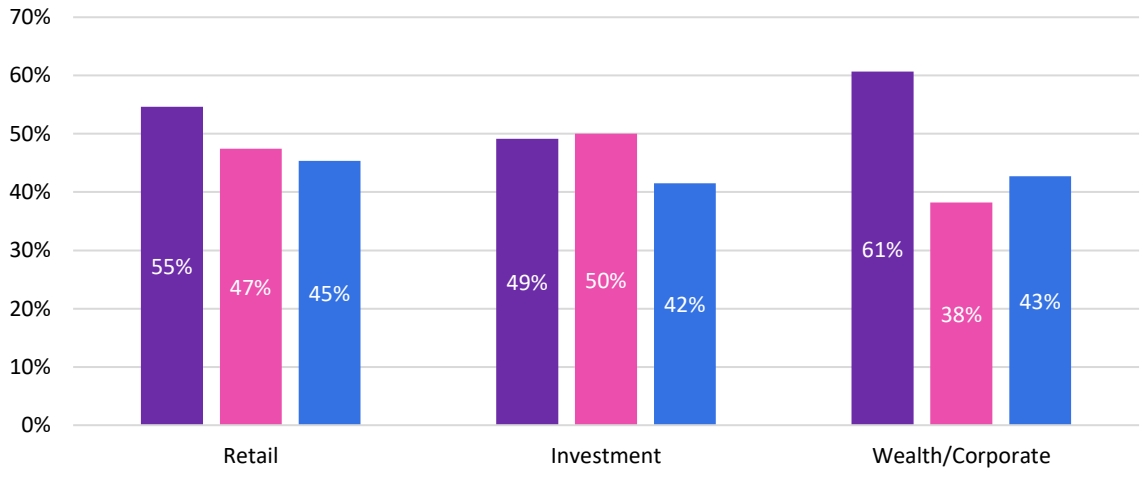
> The threat of fraud is a significant cybersecurity challenge, yet fraud and security teams struggle to collaborate

Fraud prevention, unique to financial services, is a top cyber security challenge

Although financial services (FS) as an industry face many similar challenges to other verticals in dealing with cybersecurity whether its budget constraint, a growing threat landscape, siloed processes or visibility into user data/devices, fraud remains unique to the FS sector along with sensitivity of data and its compliance/regulatory requirements (see **Figure 8**). Regulated financial institutions are obliged to report to authorities on a regular basis with fraud and financial crime a key component that regulatory bodies will scrutinize. Although fraud is evolving, and new types are emerging constantly, it is generally classified into four common areas:

- **Card fraud** (card not present, counterfeit, lost/stolen, ID theft etc.)
- **Remote banking fraud** (internet banking, telephone banking, and mobile banking)
- **Authorized push payment fraud** (through deception and impersonation)
- **Scams** (purchase, investment, romance etc.)

Figure 8: Cyber security challenges unique to FS

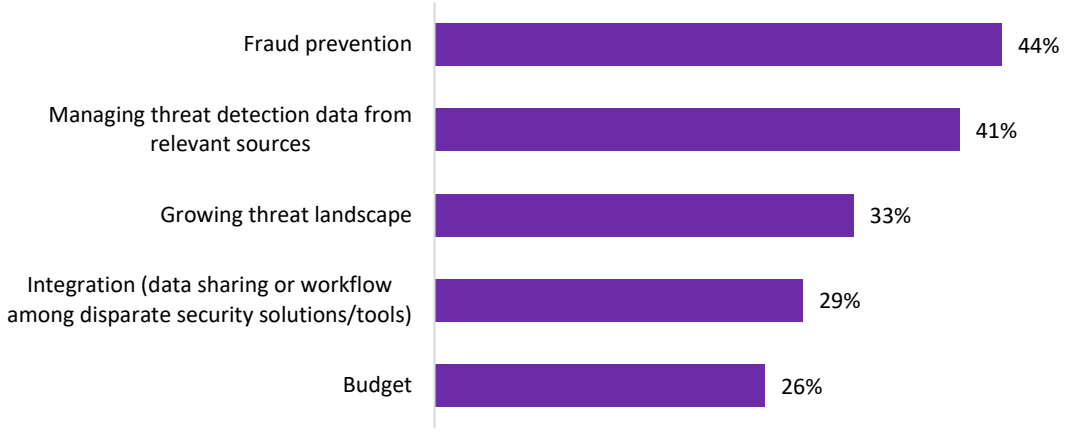


Source: Omdia

Fraud is consistently a challenge for all types of financial institutions. It is closely linked with the other key unique sector challenges as it relates to the sensitivity of the data that banks hold on customers and have stringent compliance and regulatory requirements, which mean they must report on fraud whenever it occurs.

Preventing fraud is therefore, unsurprisingly, the top cybersecurity sector challenge (**Figure 9)** with 44% of respondents indicating it is their number one priority. However, there are slight variations in terms of how segments of financial services view the challenge with it being overwhelmingly the main concern for wealth/corporate firms (53%) but second choice for retail (46%) and investment (36%), behind managing threat detection data (53%) and budget (40%) respectively.

Figure 9: Fraud prevention the top cybersecurity challenge for almost half of respondents



Source: Omdia

> Preventing fraud is therefore, unsurprisingly, the top cybersecurity sector challenge

In fighting transactional fraud and financial crime, financial institutions face ongoing challenges. Firstly, there is the need to keep pace with new types of fraud as well as new patterns of fraudulent activity. Secondly, fraud prevention systems need to be accurate as poor fraud controls can lead to high levels of false positives to the detriment of customer satisfaction.

A sudden shift to increased online payments (as exemplified during the COVID-19 pandemic) has resulted in detection systems recognizing behavioral changes forced onto the consumer by circumstances as fraudulent; leaving banks to deal with large volumes of false positive alerts, and to then adapt their systems and processes accordingly. Not only has the sudden shift to online payments made fraud detection harder but the adoption of digital wallets, such as Apple/Google Pay, where virtual cards are more prevalent, have created more potential loopholes for fraudsters to

exploit. As new payment methods continue to emerge (open banking, crypto, BNPL), scenarios for fraud to occur continue to multiply requiring additional resource from financial institutions to monitor and prevent attacks.

According to *Omdia's Retail Banking Technology Spending Spending Forecast,* IT spending on antifraud systems for monitoring, fraud analytics, case management, and the aggregation of fraud-related data services by retail banks will reach $4.5 billion globally by end-2024, which will be an increase of 5.7% on the previous year. Use cases for addressing financial fraud are centered around automation and include transaction monitoring and response, credit line monitoring, case management for declined credit cards and third-party risk and continual vendor verification.

Combining security and fraud teams is essential to combat evolving threat, but still a distant goal for financial institutions

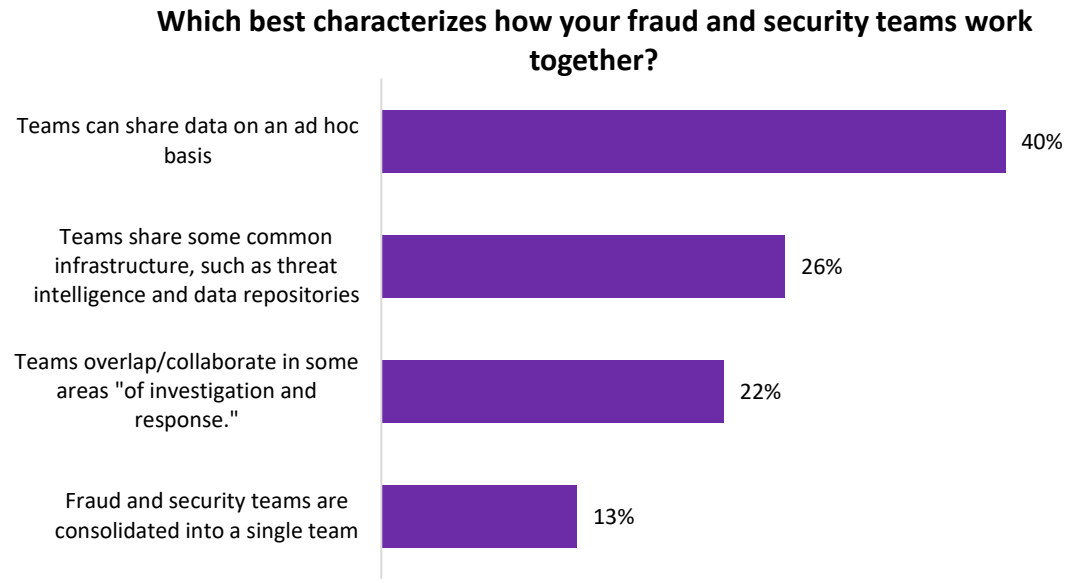
Traditionally, financial institutions operated in silos and interactions with customers and subsequent data maintained with the walled gardens of the specific department. As the financial services sector has increasingly digitalized, the need to share and collaborate across silos has become paramount as much as from a cross-selling and strong user experience perspective as for fighting cybersecurity and preventing fraud.

Financial institutions need to balance innovation and technological investment with the requirements of stability, security, and operating at scale. Fraud management solutions have traditionally been maintained in-house, but such is the velocity and variety of emerging fraud types that increasingly financial institutions are turning to external vendors to support their fraud and security functions. While they have traditionally wanted to keep fraud management practices in house, they should be aware that they might not be able to optimize the benefits of technology in the same way if they chose to have access to solutions provided by specialist vendors. The pace of change in advancement in technology means that some institutions struggle to enable their existing platforms to support newer approaches, which should force banks to increasingly outsource the techniques that they are currently using.

One of the key elements of deploying new technologies without negatively impacting customer experience is to ensure that solutions are well integrated rather than additive with appropriate risk tolerance to minimize friction. Banks need to increasingly put modern technology and solutions into practice, while driving best practice and real-time fraud attack data sharing with key stakeholders to achieve success. Banks cannot do it on their own, regulators need to provide the legislative framework to mandate the horizontal data sharing—because it is too complicated and it is unclear under whose authority that would happen if not the government—but it can be an instrumental tactic that they should consider to make it much harder, now and in the future, for criminals to have a sustainable attack on banks and their customers.

Given the amount of fraud initiated or executed through digital channels, it seems natural that cybersecurity and fraud teams at financial services companies would look to collaborate on investigations. Both fraud and security teams need tools that can speed up and improve remediation efforts. Yet only 13% of respondents indicated that their fraud and security teams were consolidated into a single team with the majority (40% of respondents) stating that their teams only share data on an hoc basis (see **Figure 10**).

Figure 10: Fraud and security teams typically only share data on an ad hoc basis



Source: Omdia

© 2023 Omdia

Interestingly, firms with between $5 billion and $10 billion in annual revenue were much more likely (33%) to have achieved this consolidation. Only 14% of larger organizations (perhaps because of more difficult internal politics) have consolidated these teams, compared to only 6% of organizations with less than $5 billion in annual revenue.

Over the next 12 months, however, more than half of all respondents plan to integrate their fraud and security teams. This is true regardless of company size or geography, but investment firms are more bullish (58%) on integration while wealth management firms were less likely (45%) to plan consolidation this quickly. Less formal or comprehensive collaboration is more frequent today, with 40% of respondents (see **Figure 10**) supporting ad hoc data sharing between fraud and security teams and 26% sharing some infrastructure, such as data repositories and threat intelligence.

Lack of automation and collaboration between systems is preventing a joined-up approach to security and fraud

According to Omdia's *Retail Banking Technology Spending Forecast*, flexibility of technology systems (45%), speed to change technology systems (43%), and cost of technology systems (41%) are the top three priorities for banks when it comes to technology-related challenges for anti-financial crime. Flexibility of technology systems is top challenge for banks for anti-financial crime and is problematic for both combating transactional fraud and meeting anti-money laundering (AML) compliance. As the payments landscape continues to evolve—playing a key role in the digitalization of financial services and the adoption of new products—fraud prevention techniques need to keep pace and adapt rapidly to emerging threats. Indeed, while banks have invested significantly over the last several years, this investment has limited value if systems are unable to adopt to emerging threats as players roll out new services.

According to the *State of the Security in Financial Services* survey, existing internal processes are generally seen as more of an inhibitor than technology. That said, security and fraud teams have historically operated in technology silos that also complicate potential cooperation between these teams. This is particularly true of investment firms where fragmented technology systems (40%) came slightly ahead of inflexible operational processes (37%).

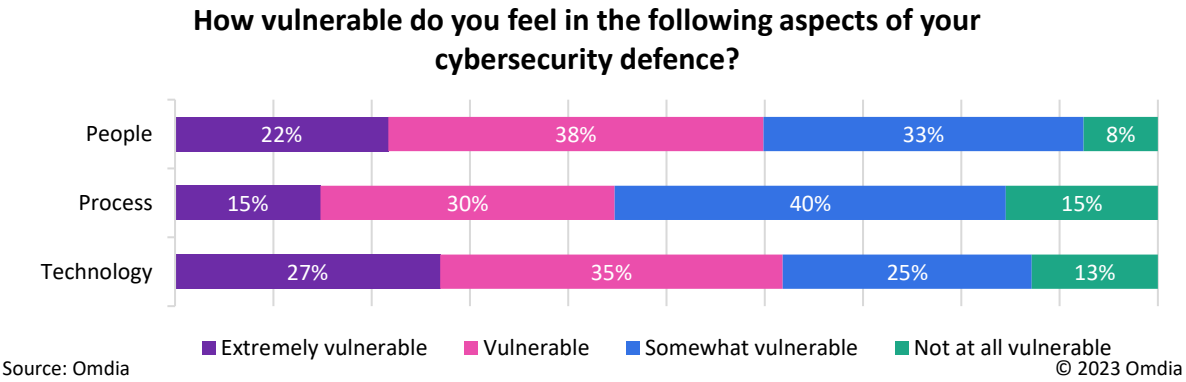
However, security automation can be a key enabler to ensure flexibility of operational processes and help avoid silos. If data sharing can be automated, for example, it will increase transparency and visibility amongst security and fraud teams and increase efficiency and effectiveness of existing systems.

Clearly there is a need to upgrade systems that are poorly integrated or incompatible resulting in friction with consumers and inhibiting bank's ability to meet their wider business objectives. The problem with legacy systems is that they are expensive to run, requiring switching between systems, which is inefficient and prohibitive of systems being able to adapt rapidly to emerging threats.

> Security automation can be a key enabler to ensure flexibility of operational processes and help avoid silos.

Despite inflexible operational systems seen as a barrier to improving collaboration between fraud and security teams, it is perhaps surprising that only 15% of respondents felt extremely vulnerable to attacks on their defense in relation to processes compared to 22% for people and 27% for technology **(see Figure 12).**

Figure 12: People and technology are most vulnerable to breaching cybersecurity defense

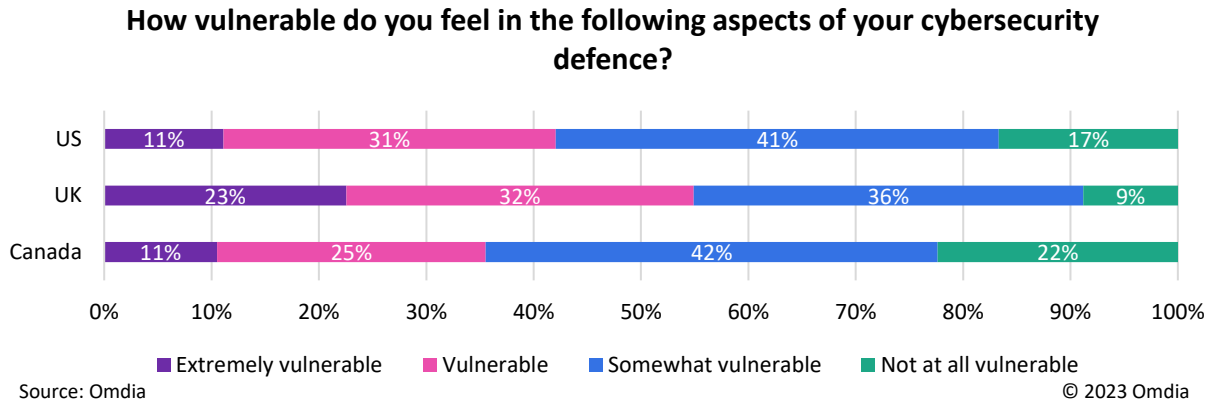


Source: Omdia

From a regional perspective, there is a stark contrast between how vulnerable respondents felt in terms of their people, processes, and technology with the UK far more concerned about its vulnerabilities compared to the US and Canada. There may be some cultural factors at play in terms of UK respondents being more conservative in their confidence of their cybersecurity defense.

Although it is still significant that 23% of UK respondents stated that their processes were extremely vulnerable versus the combined 22% of US/Canada respondents (see **Figure 13**). Canadian respondents are very confident in their process cybersecurity defense by comparison with 22% stating it is not vulnerable as compared with 9% of UK respondents.

Figure 13: UK respondents far more concerned with cybersecurity defense versus US and Canada



Source: Omdia

Security Automation

As the name implies, SOAR solutions are designed to automate and orchestrate time consuming manual tasks for security and other operational teams. SOAR solutions typically support data gathering, case management, workflow, and reporting. Leading SOAR solutions are expected to support the following functionality:

- Aggregate alert data and store them in a unique location for further investigation.
- Allow users to manage research and investigations with built-in case management capabilities.
- Support complex workflows to enable automated incident response through integration with 3rd party tools, systems, and applications.
- Address specific threats with pre-built playbooks that allow automated or guided response.

The term SOAR was coined in 2017 but the need to simplify and automate many security tasks (particularly in the SOC) had been apparent for some time and, in fact, several “SOAR” startups had already been founded by this time.

It immediately became apparent that a primary use case for SOAR would be augmenting traditional SIEM tools to alleviate many of the short comings in those products. This led to a rash of acquisition in the space even before the segment had a proper name (e.g., IBM’s acquisition of Resilient Systems in 2016).

It is clear today, however, that SOAR has numerous use cases outside of the SOC and the evolution of the standalone SOAR market in many ways is tailored to make these security automation products more user friendly for teams outside the SOC. These improvements include much richer case management features, and the introduction of low code, and no code capabilities.

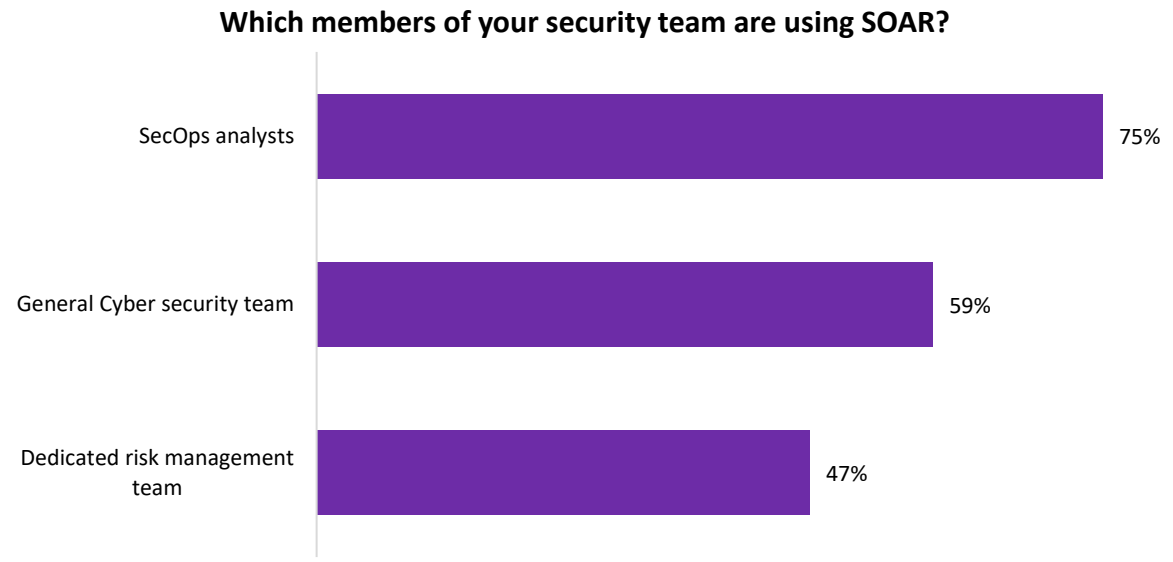
Users and Use Cases

SOAR really made a name for itself in security operation centers and SOCs remains a stronghold for the products. Traditional SOC use cases include:

- Unified alert management
- Automated phishing investigation
- Threat hunting

Not surprisingly, security operations analysts are often the primary users of SOAR solutions among security personnel, and this holds for financial services organizations as well (see **Figure 14**). But SOAR tools are increasingly finding a home with dedicated risk management teams as well. Omdia views proactive, risk-based remediation of exposures across an organization's entire attack surface as an emerging best practice, and one that increasingly will be managed by dedicated risk management teams, particularly with large enterprises. SOAR capabilities are an important enabler of proactive strategies.

Figure 14: Users of SOAR products in security teams



Source: Omdia

But SOAR products are increasingly being used outside the SOC, and even beyond security use cases. For example, emerging SOAR use cases outside of the SOC include:

- Automated compliance
- Automated invoicing
- Legal case management
- Identity provisioning
- Merchant onboarding

As the number of use cases for SOAR solutions expands, it is important to consider the amount of coding required to implement each additional use case. Modern SOAR products typically support low code, or no code development tools for the creation of workflows and playbooks. End users need to balance the need to reduce the amount of custom coding required with the flexibility supported for custom use case development. Tools should be flexible enough to support use cases beyond the SOC.

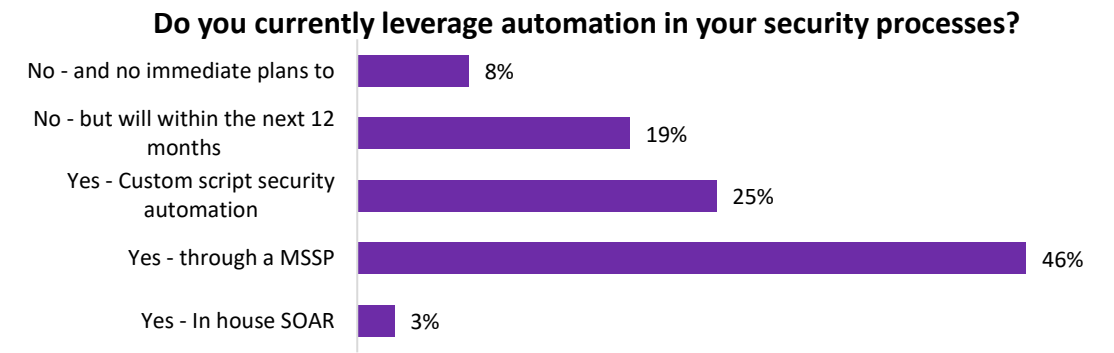
Benefits and Challenges

Among financial services organizations, SOAR capabilities are already broadly utilized. Only 3% of respondents reported they have no plans to adopt SOAR capabilities. There is considerable variation in how security automation is currently deployed at financial institutions.

The popularity of using MSSPs for SOAR is not surprising given that a primary driver in adopting SOAR is easing the workload of security analysts. Omdia believes, however, that the increased usability of modern SOAR, low code security automation solutions, combined with the flexibility of an in-house approach will drive stronger adoption of SOAR products.

Omdia also expects the use of custom scripting to drop as enterprise moves to either low code solutions or MSSPs (see **Figure 15**).

Figure 15: Security automation deployment models

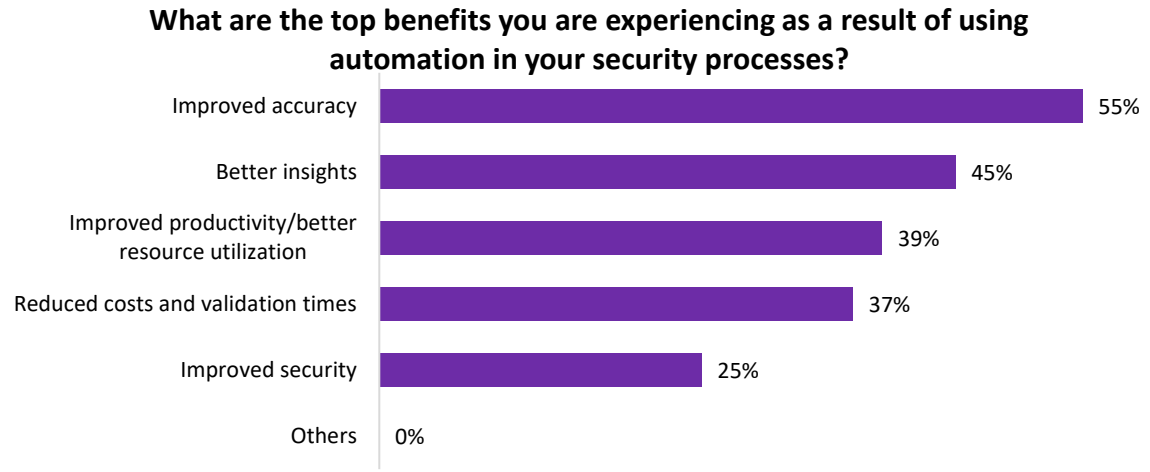


Source: Omdia

© 2023 Omdia

Benefits

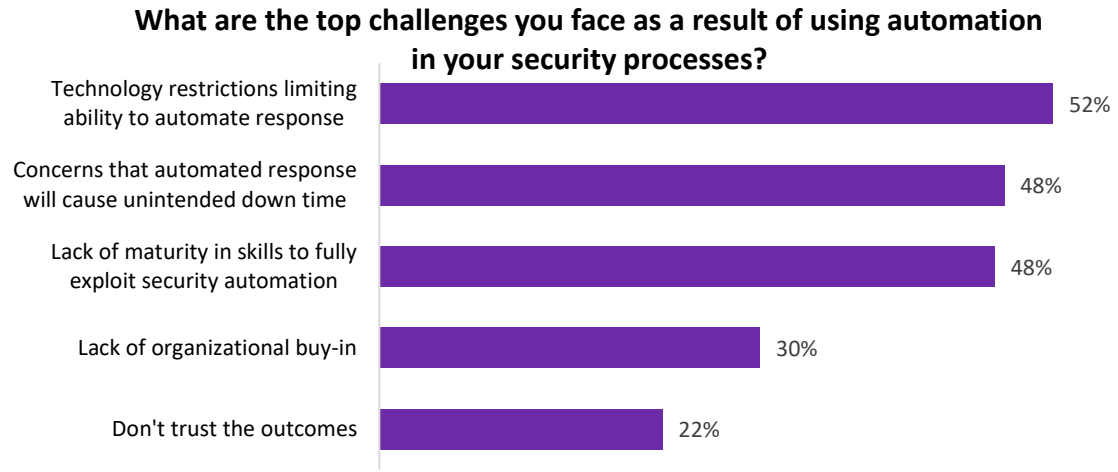
Figure 16: Top benefits of security automation



Source: Omdia

Challenges

Figure 17: Top challenges of deploying security automation



Source: Omdia

Conclusions

Financial services organizations have been on the leading edge of adoption of new security controls for decades. Unfortunately, old threats rarely disappear, and many organizations are now left managing dozens (if not more) security controls. And despite a widespread goal of wanting to consolidate the number of tools and vendors these companies work with; the total numbers continue to grow.

On top of being an attractive target for a broad set of cyber threat actors, financial organizations are also targets for very specific types of fraud. Much of this fraud utilizes digital channels, adding to the total number of deployed detection and investigation products and services. Given that financial organizations are built on customer trust, cyber security breaches and fraud can have impacts well beyond their hard costs. Unfortunately, the size and scope of these problems has left both security and fraud teams struggling to keep up.

Security automation can help. Financial organizations can start small but should have a clear view of the optimal end state, which is an integrated fraud and security infrastructure. Technology alone is not going to bring those teams together, but security automation can act as a particularly effective glue for enabling better cooperation, while improving analyst accuracy, enabling better insights, and improving productivity.

Only about a quarter of financial organizations currently support the sharing of common infrastructure, such as threat intelligence and data repositories between these teams and less, about a fifth, have any overlap in investigation and response activities. These are important first steps that financial organizations should take to build trust between these teams and enable further cooperation and consolidation.

The usability of modern SOAR products has significantly expanded application well beyond the SOC. Financial services organizations of all types should investigate the benefits that security automation can bring to ease the operational burden on both security and fraud teams.

Appendix

Methodology

The primary study consisted of 304 interviews with financial institutions senior executives across group's functions responsible for cybersecurity conducted online in August 2023. The survey respondents were screened to ensure that participants were directly involved in supporting or managing the security investment decisions. Respondents were also screened to ensure their institution was either retail, wealth management/corporate or investment related, with insurers exclude from this study. Markets covered include Canada, the UK and the US.

Fraud management spending data includes project, delivery, operations, and maintenance costs of supporting fraud management functions (across prevention, detection, and investigation). This includes anti-fraud systems across all fraud types and product lines, such as CNP, lost/stolen, account takeover, application fraud, insider fraud, counterfeit, phishing, online fraud, and so on but excludes financial crime related to AML and CTF. Systems include monitoring, fraud analytics, case management, and the aggregation of fraud-related data services, but would exclude the cost of fraud data information services themselves (e.g., watch list screening). Channel-specific measures to prevent fraud (e.g., multifactor authentication) are also excluded.

Author

Andrew Braunberg
Principal Analyst, Security Operations
customersuccess@omdia.com

Philip Benton
Principal Analyst, Financial Services
customersuccess@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer