The 2020 Faces of Fraud Survey

Enabling Digital Trust in a Connected Fraud Landscape

appgate

iSMG
INFORMATION SECURITY
MEDIA GROUP

Nick Holland
Director, Banking and Payments

The 2020 Faces of Fraud Survey

A quarter of financial institutions experienced at least one spear-phishing or business email compromise attack in 2019 where user credentials were compromised and/or fraud was committed. These attacks also often resulted in intellectual property and physical damage.

Yet, nearly half of institutions surveyed state that they have limited or no visibility in identifying the impact of such an attack.

These are among the results of the 2020 Faces of Fraud Survey sponsored by AppGate. Aimed at identifying whether financial institutions have the right technologies and procedures in place to mitigate fraud, the study draws upon responses from more than 100 participants to determine:

- The top forms of fraud affecting financial institutions in 2019;
- The biggest gaps in organizations' efforts to mitigate fraud;
- Where today's financial institutions are focusing their investments on fraud prevention technologies for the coming year.

Among some of the key findings:

Third-party risk is a significant concern: While the speed of evolution of fraud schemes is seen as the greatest vulnerability today (60 percent), the lack of awareness of socially engineered fraud schemes among customers and partners is a close second at 57 percent.

C-Level executives in financial services get that cybersecurity is critical: Nearly three quarters of survey respondents are confident or very confident that their C-suite understands the necessary investment needed to counter and mitigate growing fraud threats.

Mobile is plagued by the same fraud schemes as any other banking and finance channels: The top two fraud schemes via mobile devices in 2019 were fake accounts (22 percent) and account takeover (30 percent). The online channel, however, is still the fraudster's favorite, with over half of respondents stating that this is the source of a majority of fraud.

Read on for full survey results, as well as expert analysis of how to put this information to use to improve your organization's ability to detect and prevent financial fraud.

Best,

Nick Holland
Director, Banking and Payments
Information Security Media Group
nholland@ismg.io

This survey was conducted online in the fall of 2019; it generated over 100 responses from financial institutions primarily in the U.S. Forty-six percent of the respondent base was from financial institutions with $2 billion or more assets under management.

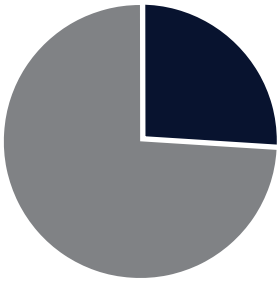
About Appgate:

Appgate brings together a set of differentiated cloud- and hybrid-ready security and analytics products and services. These include Appgate's SDP, the industry's leading Software-Defined Perimeter solution, and the Fraud Protection suite of risk-based authentication and Digital Threat Protection capabilities. Appgate also possesses a range of innovative threat management and analytics offerings, including the Brainspace digital investigations platform, and the company's Immunity range of offense-oriented software and adversary simulation services.

For more information about Appgate visit www.appgate.com

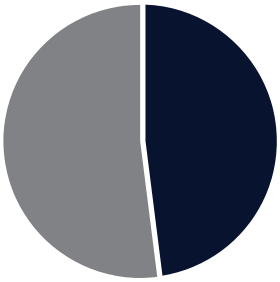
By the Numbers

Some statistics that jump out from this study:



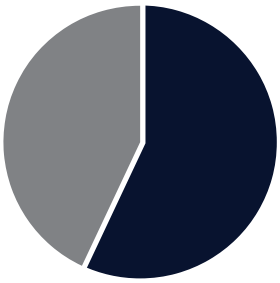
26%

of financial institutions experienced at least one spear-phishing or business email compromise attack in 2019 where user credentials were compromised and/or fraud was committed.



48%

of financial services organizations have limited or no visibility when it comes to identifying the impact of a phishing attack.



57%

say the lack of awareness of socially engineered fraud schemes among customers and partners is a serious concern.

Baseline Fraud Defense

This report begins by taking the pulse of respondents about their current anti-fraud defenses. Among the takeaways:

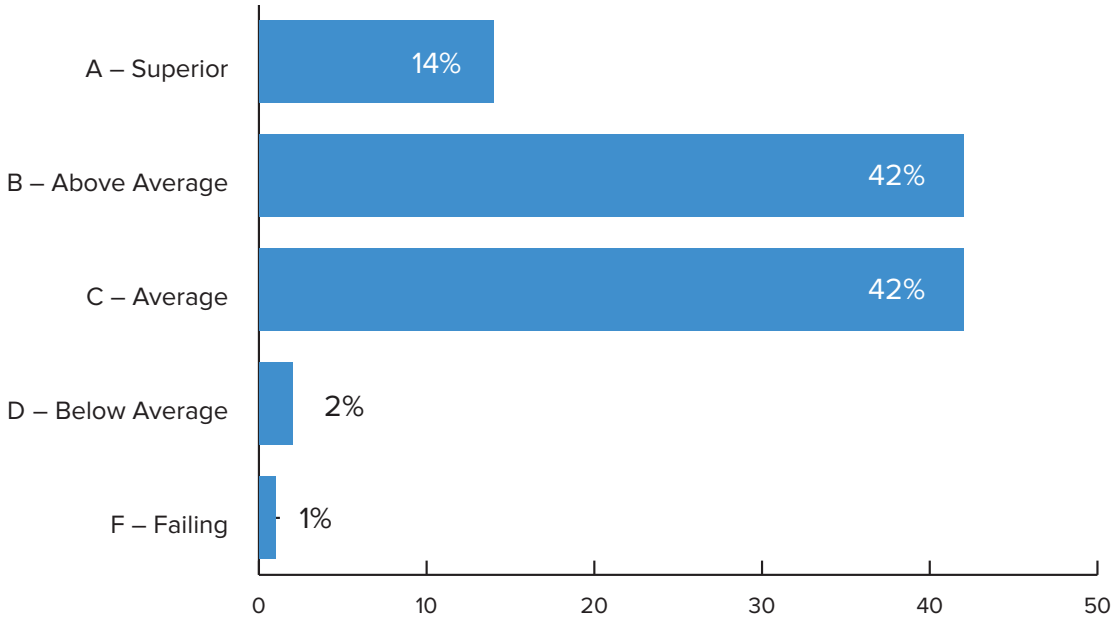
Nearly two-thirds of those surveyed are either confident or very confident about their employee education efforts and their employees' awareness of how to mitigate fraud.

Yet...

Nearly a third of survey participants think their employees lack sufficient awareness to protect themselves from socially engineered fraud schemes

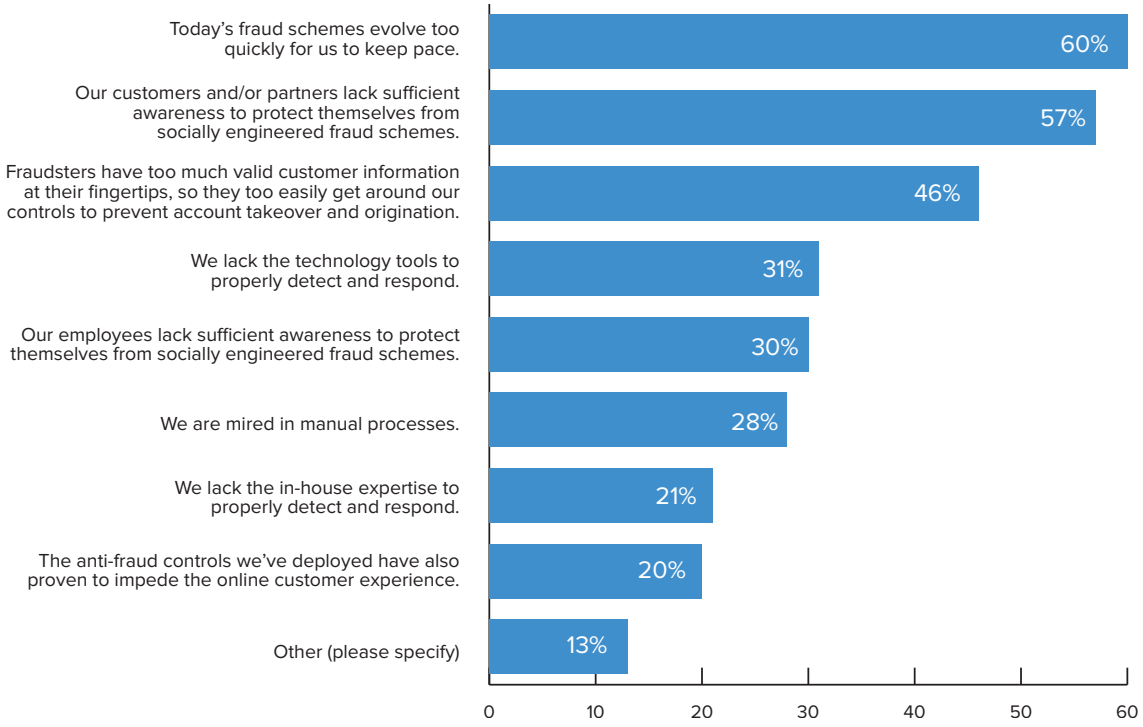
Complete results are below.

What grade would you give your organization's ability to identify and mitigate fraud?



The first question asked organizations to rate their ability to identify and mitigate fraud. Some 42 percent rate themselves as "above average" and the same percentage selecting "average."

What do you believe to be the top three greatest vulnerabilities in your fraud defenses?

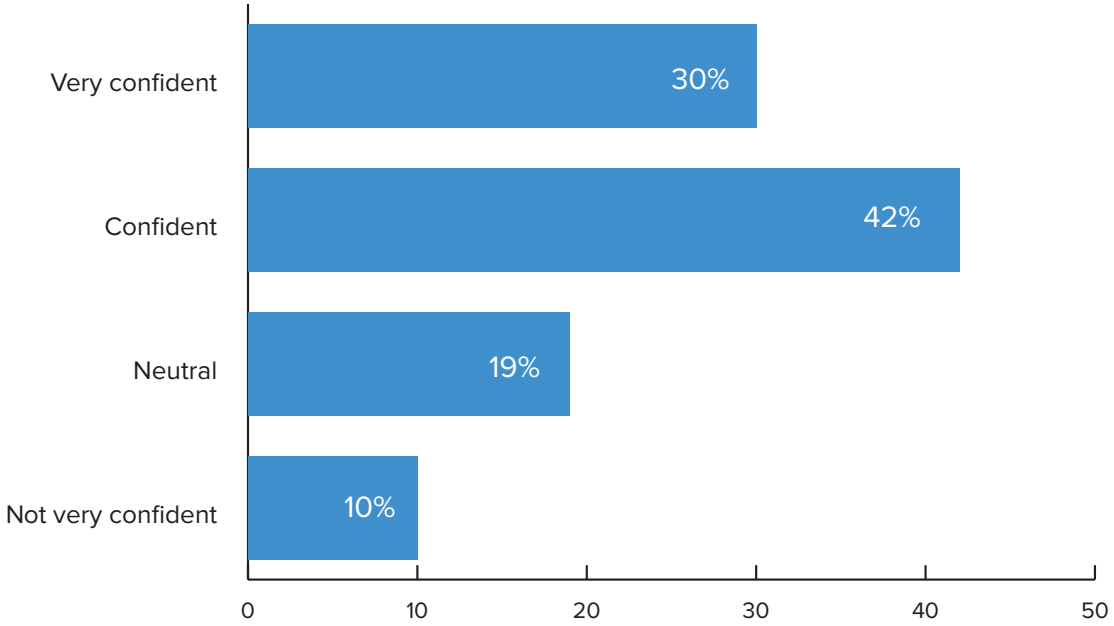


Security professionals working in financial services are most concerned about three areas of vulnerability, the survey shows:

- Fraud schemes are evolving too quickly to keep pace.
- Customers and partners lack sufficient awareness to protect themselves from socially engineered fraud schemes.
- Fraudsters have too much valid customer information at their fingertips, and therefore can too easily get around controls to prevent account takeover and origination.

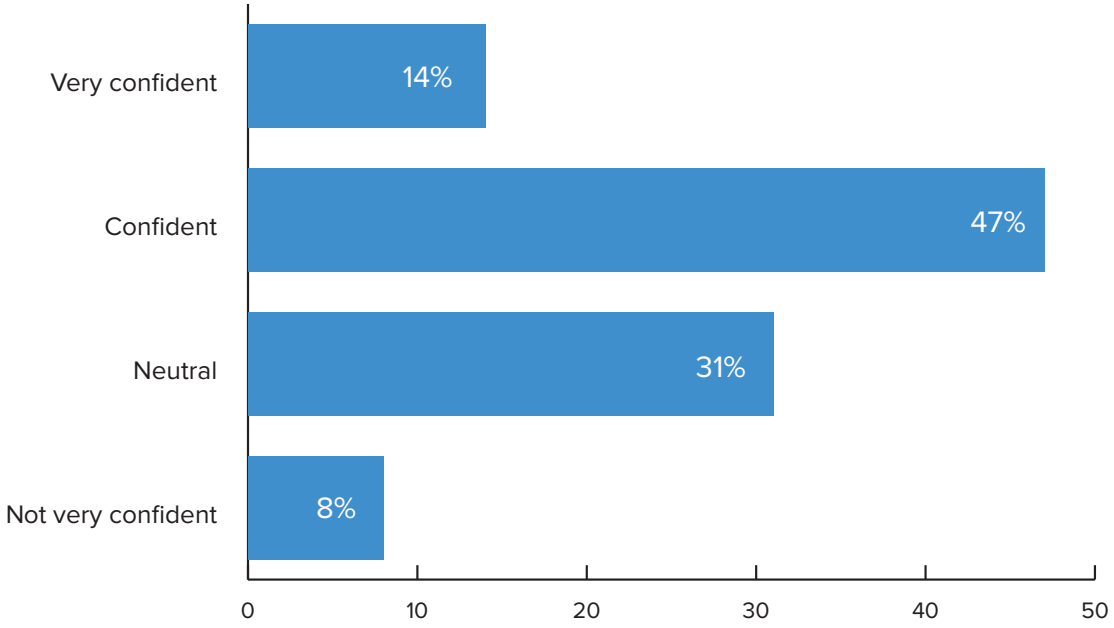
Some 60 percent are now concerned about fraud schemes evolving too quickly, up from 43 percent a year ago, while 57 percent are concerned about a lack of awareness of social engineering schemes, up from 42 percent. No area saw a decrease in concern in this survey compared with the previous survey.

What degree of confidence do you have that C-level executives in your institution understand the necessary investment in cybersecurity tools to deal with the evolving fraud threat?



Security professionals in financial services are confident that the C-suite understands the necessary investment in cybersecurity tools. Nearly three quarters of survey participants are confident or very confident that their C-level executives understand the requisite investment.

How would you rate employee education and awareness of how to mitigate fraud?

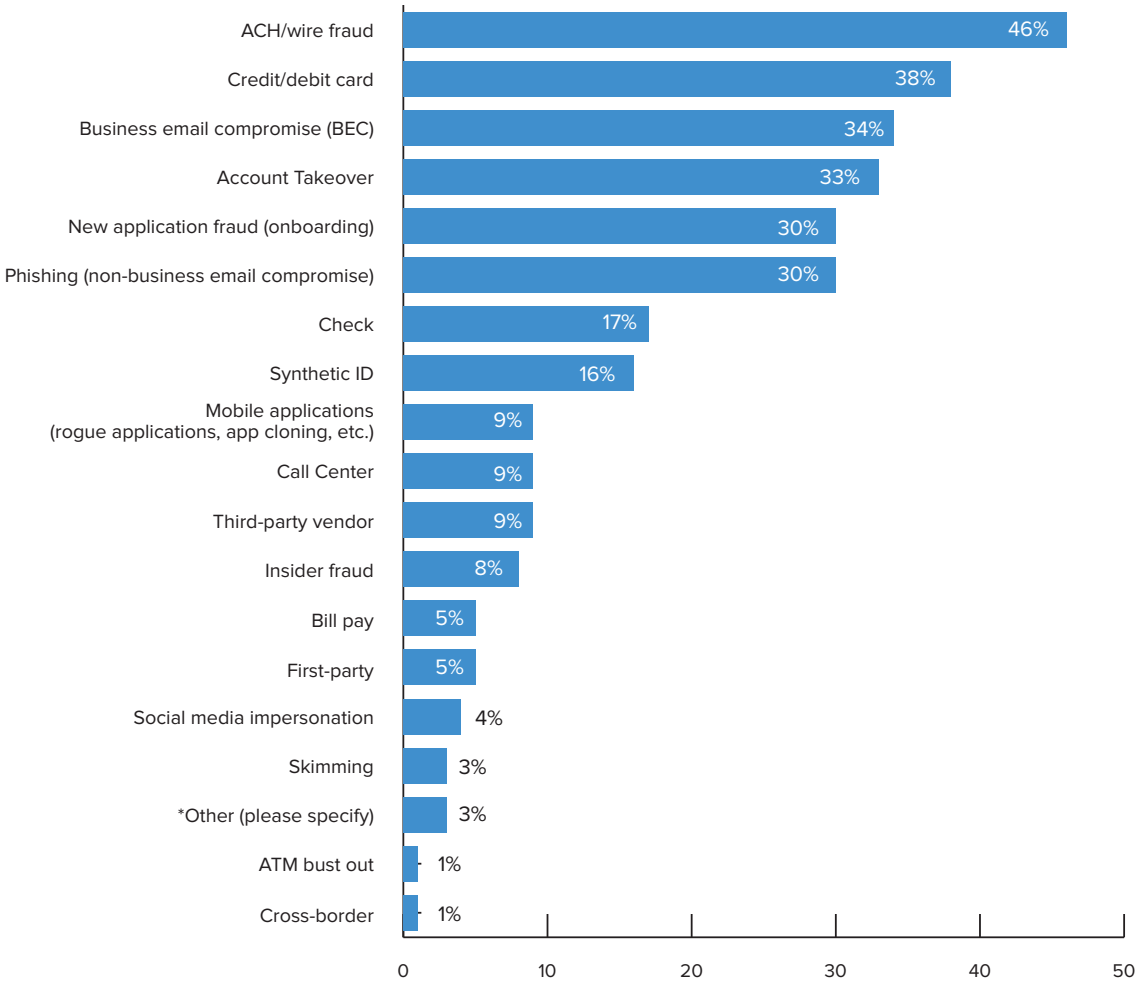


Nearly two-thirds of survey participants are either confident or very confident about their employee education efforts and awareness of how to mitigate fraud. But 31 percent are “neutral” on the subject, and 8 percent say they are “not very confident.”

Nearly two-thirds of survey participants are either confident or very confident about their employee education efforts and awareness of how to mitigate fraud.

2020 Faces of Fraud

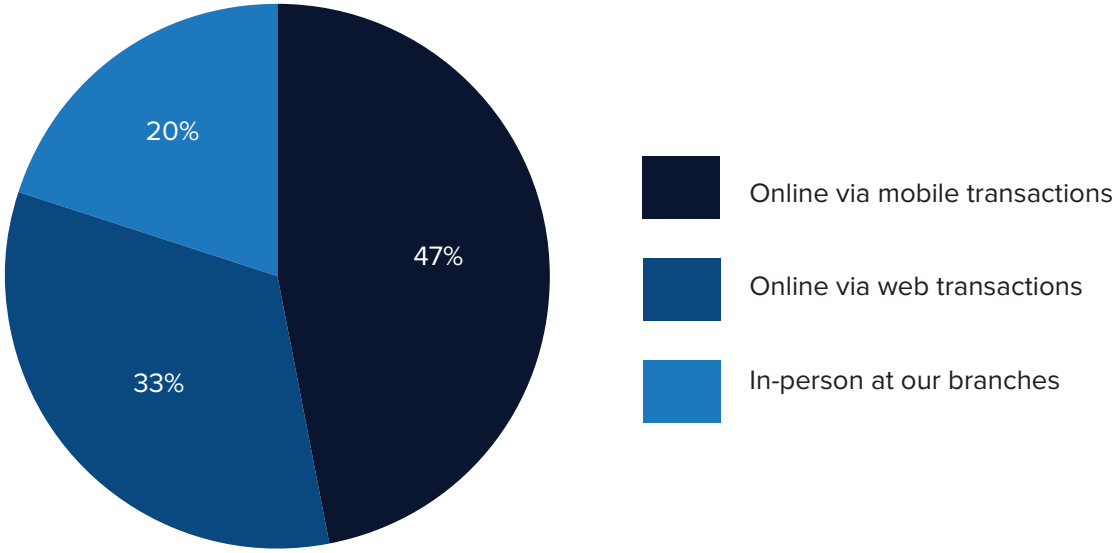
Please select the top three most concerning fraud schemes for your institution this upcoming year.



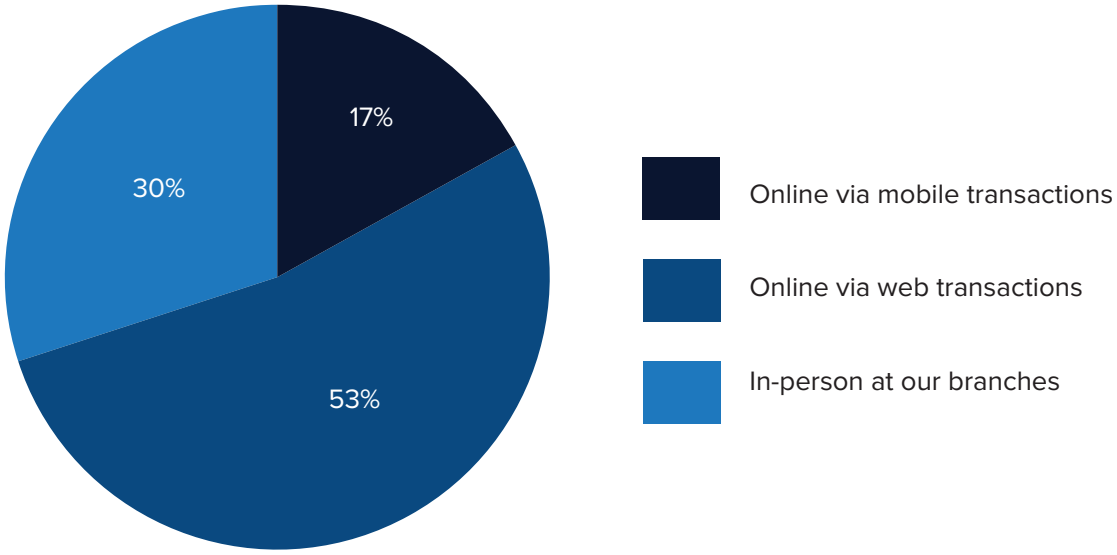
Some 46 percent of survey participants cited ACH/wire fraud as the greatest area of concern, presumably because of the potential transaction size and high degree of difficulty in orchestrating fund-reversal once the fraud has been perpetrated.

Another significant area of concern is credit/debit card fraud (38 percent). Further, business email compromise attacks are of slightly greater concern than phishing attacks.

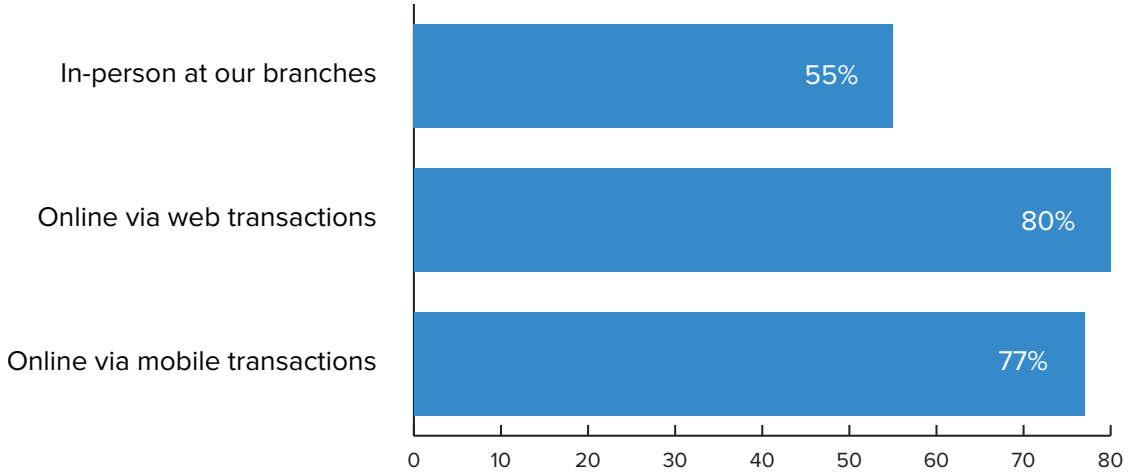
What is your customers' primary channel for conducting business with your institutions today?



Which channel has the highest incidence of fraud?



Which channels have a cybersecurity solution in place?

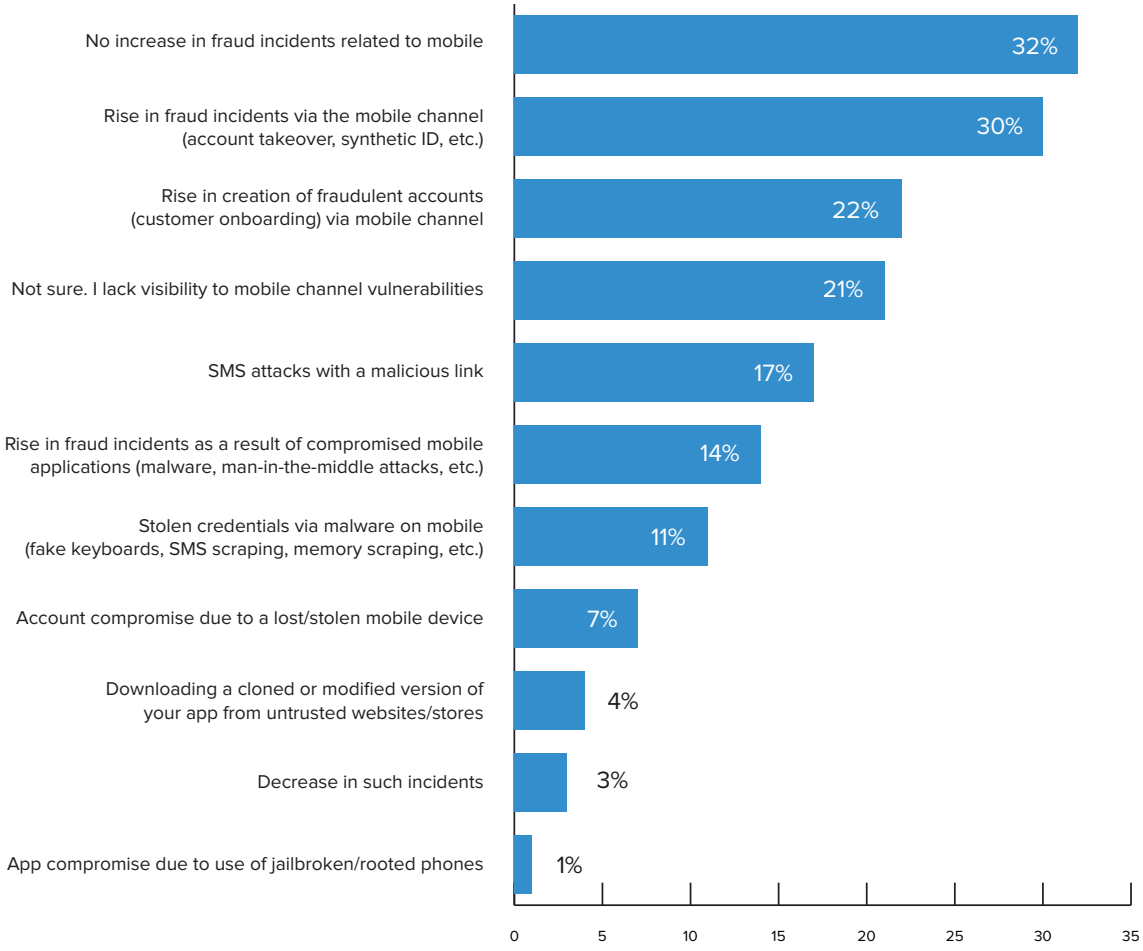


While online banking is still not perceived to be the primary channel for transacting, the highest degree of fraud occurs via this channel. Some 33 percent of business is conducted online, but 53 percent of banking security professionals say this is where the highest incidence of fraud occurs.

It's worth considering that mobile banking is probably not far behind online banking in terms of customer usage – and, correspondingly, increasing fraud risk.

While online banking is still not perceived to be the primary channel for transacting, the highest degree of fraud occurs via this channel.

In the past year, have you experienced any of the following fraud incidents specifically related to the mobile channel? (check all that apply)

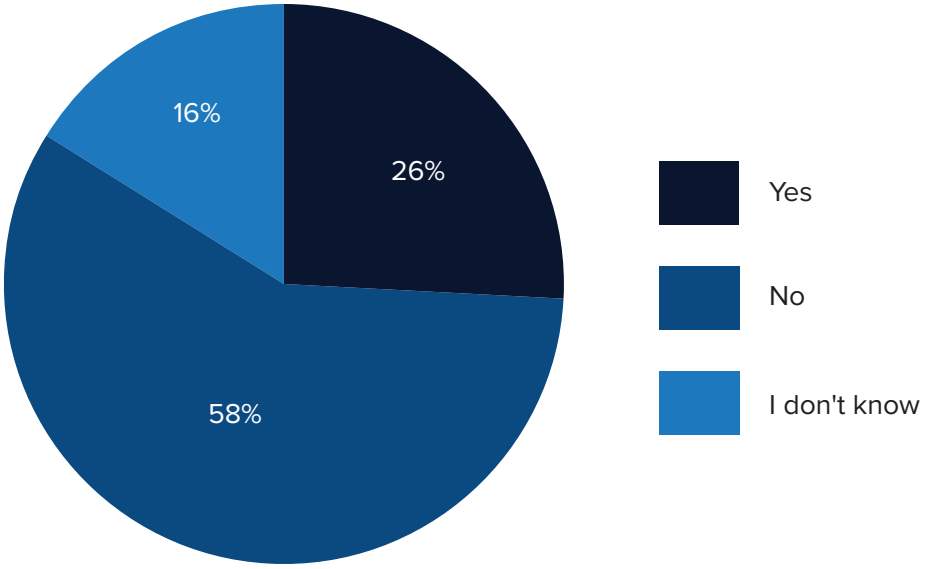


Drilling down into fraud occurring via the mobile channel, 30 percent of survey participants have seen an increase in fraud related to account takeover and synthetic ID in the past year. Plus, 22 percent have seen an increase in the creation of fraudulent accounts via the mobile channel.

It is also noteworthy that 32 percent of participants saw no increase in fraud incidents related to the mobile channel. Further, 21 percent of survey participants stated that they don't know about fraud activity because they lacked visibility into mobile channel vulnerabilities.

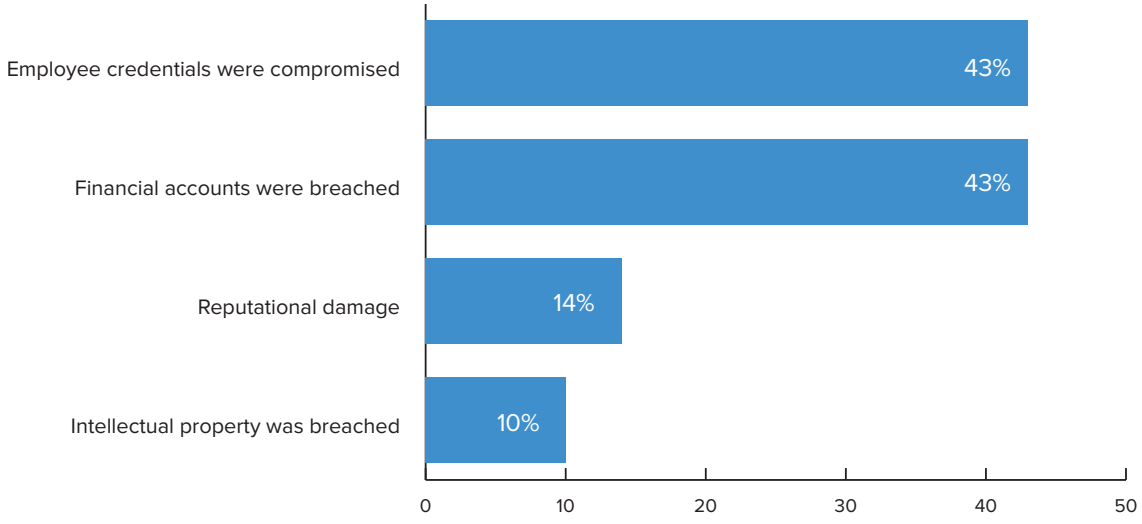
All areas of mobile fraud increased in this survey vs. the previous year, with the exception of SMiShing attacks, which may have given way to more prolific and lucrative attacks such as account takeover and synthetic identity. The level of visibility into mobile channel attacks has not improved, despite the relative maturity of mobile banking services.

Has your organization in the past year been the victim of at least one spear phishing attack / incident of Business Email Compromise, where user credentials were compromised and/or fraud was committed?



More than a quarter of survey participants report that their organization had been the victim of a spear phishing or business email compromise attack in the past year, in which user credentials had been compromised and/or fraud was committed, up five percentage points from last year's survey.

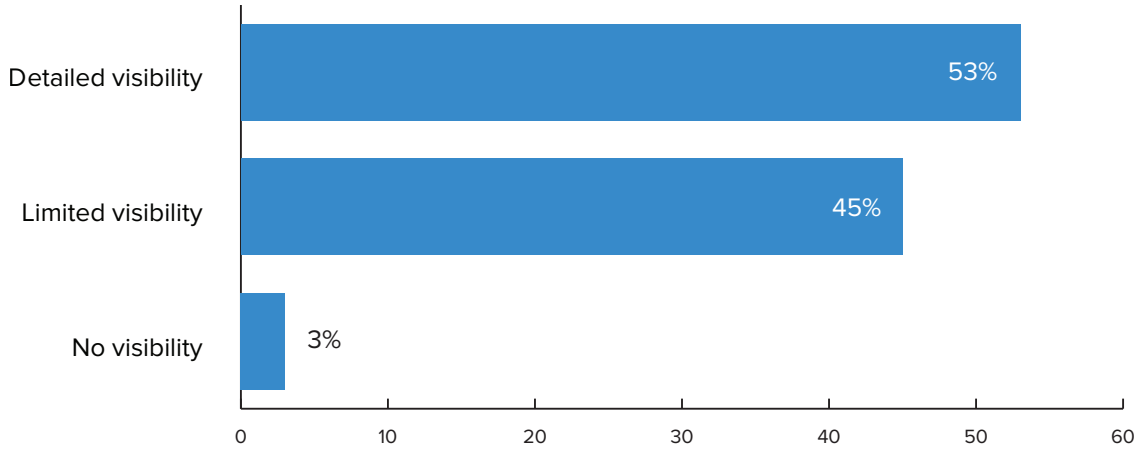
If you answered "yes" to the previous question, what business impacts did your organization experience as a result of the spear phishing attack(s) / Business Email Compromise? (check all that apply)



Of organizations that were victims of a spear-phishing or a BEC attack, the impact was seen across multiple areas of business. Some 43 percent of respondents state that employee credentials were compromised and financial accounts were breached, 14 percent saw reputational damage and 10 percent saw intellectual property breached. This is a more diverse spread of damage than in the previous year's survey, when these attacks were predominantly leading to breached employee credentials and attacks on financial accounts.

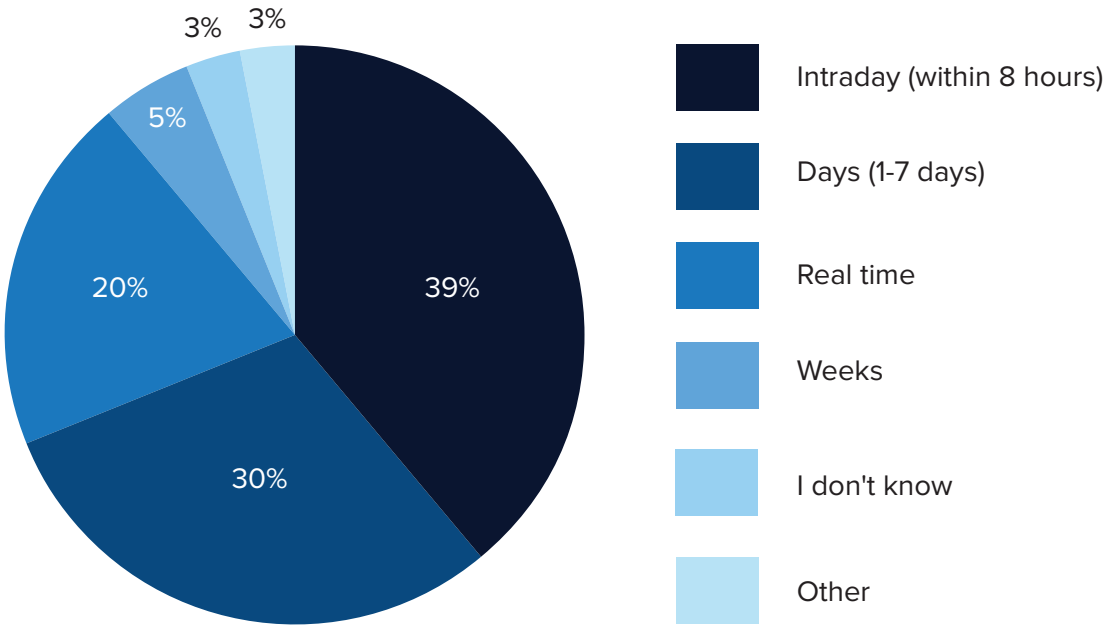
Fraud Prevention

How much visibility does your organization have when it comes to identifying the impact of a phishing attack?



While just over half of organizations have “detailed visibility” into the impact of a phishing attack, a concerning 45 percent have limited visibility and 3 percent have no visibility.

On average, how long do you estimate it takes your organization to uncover / mitigate a fraud incident once it occurs?

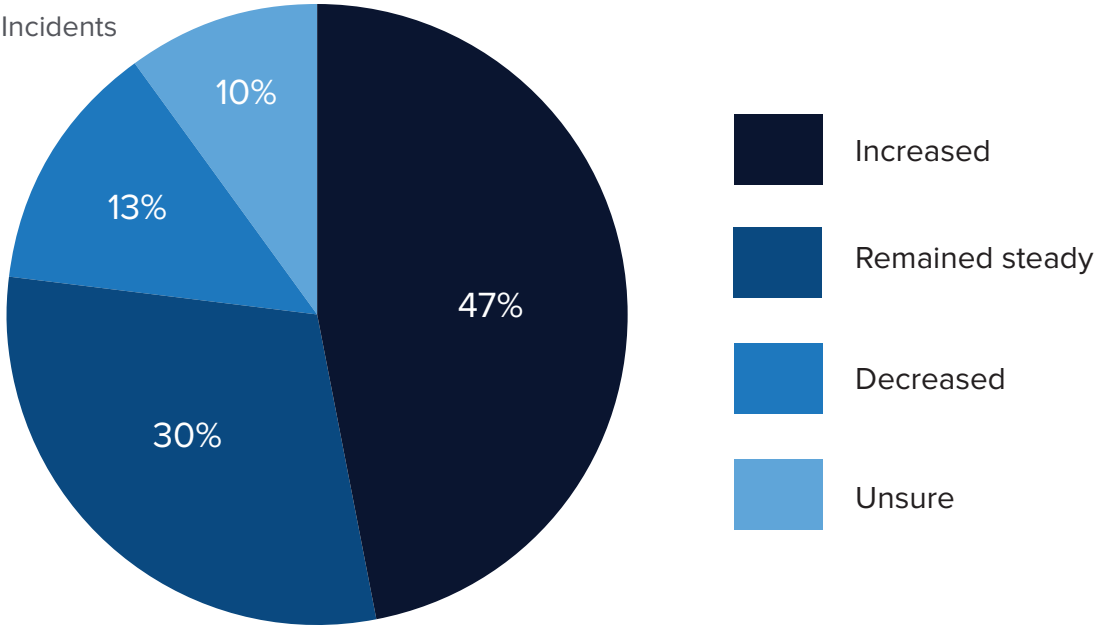


Most financial organizations can uncover a fraud incident the same day. Some 20 percent of survey participants state that they could uncover an incident in real time, up from 12 percent a year ago. Another 39 percent reported that that it would take 8 hours or less. Mitigation is typically within 7 days, although for 12 percent of organizations, mitigation takes weeks.

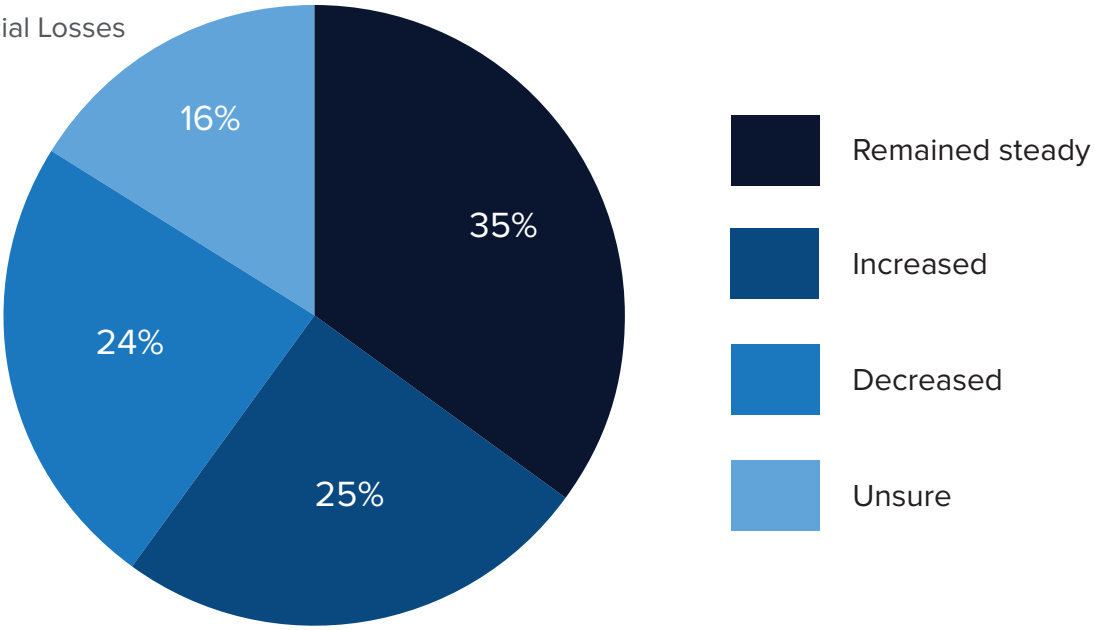
Unfortunately, mitigation of cyber events slowed down in the current survey vs. the previous year's survey. Real-time mitigation dropped from 17 percent to 13 percent and same-day mitigation dropped from 35 percent to 32 percent. Also, survey participants reported an increase in mitigation that took weeks, up from 5 percent in last year's survey to 12 percent in this year's survey.

Has the number of fraud incidents / financial losses involving your organization increased, decreased or stayed steady in the past year?

Fraud Incidents

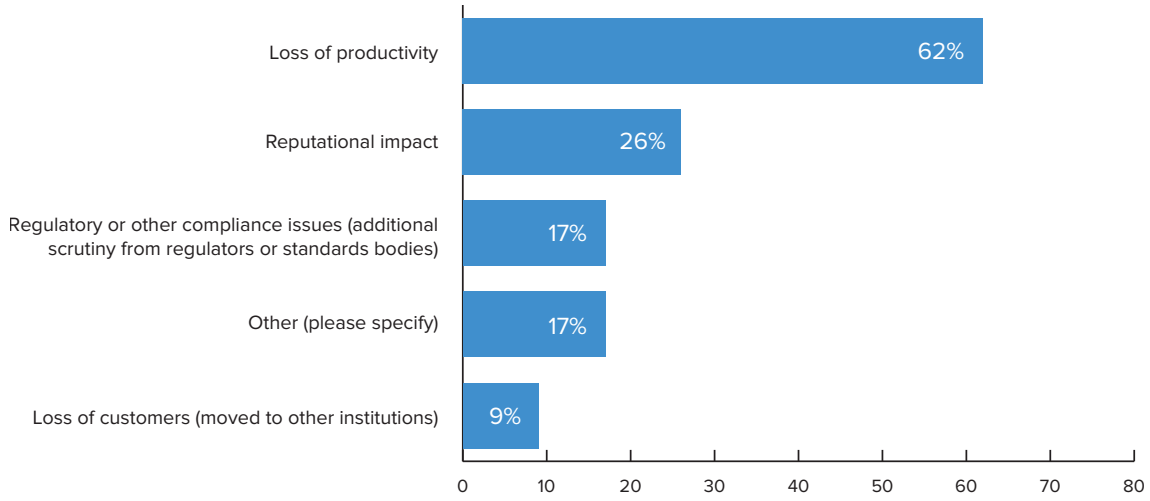


Financial Losses



While the number of fraud incidents increased in the past year, the cost of fraud has remained somewhat steady, according to this year's survey. Some 47 percent of survey participants indicate that fraud incidents had increased compared to the previous year, while 35 percent of participants state that financial losses had remained steady.

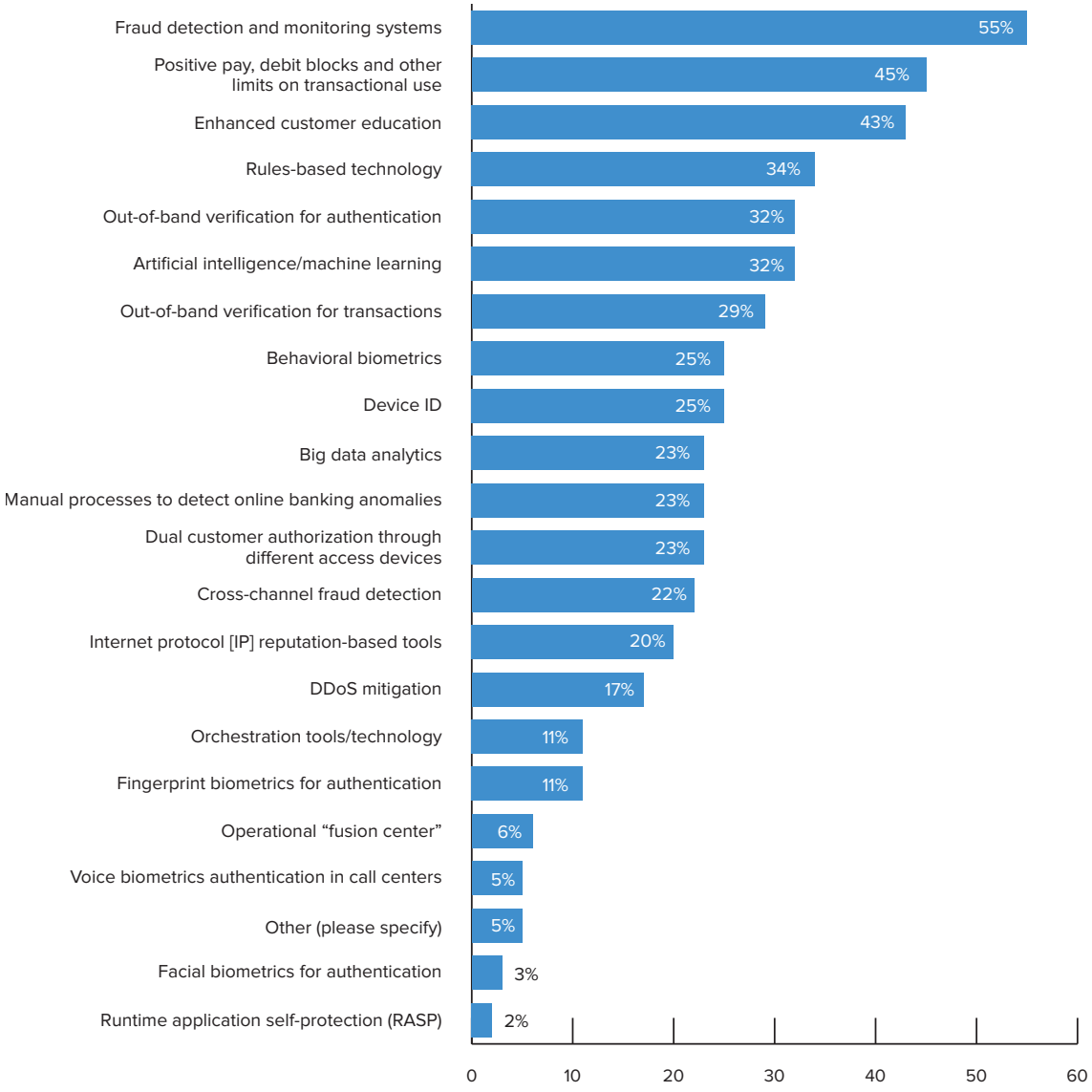
Beyond the financial toll from the fraud incidents, what non-financial losses did your organization suffer from? (check all that apply)



Beyond financial damage from fraud, the highest level of non-financial losses was in productivity, with 62 percent of survey participants stating they experienced productivity losses due to fraud. A quarter of respondents stated that they experienced reputational impact.

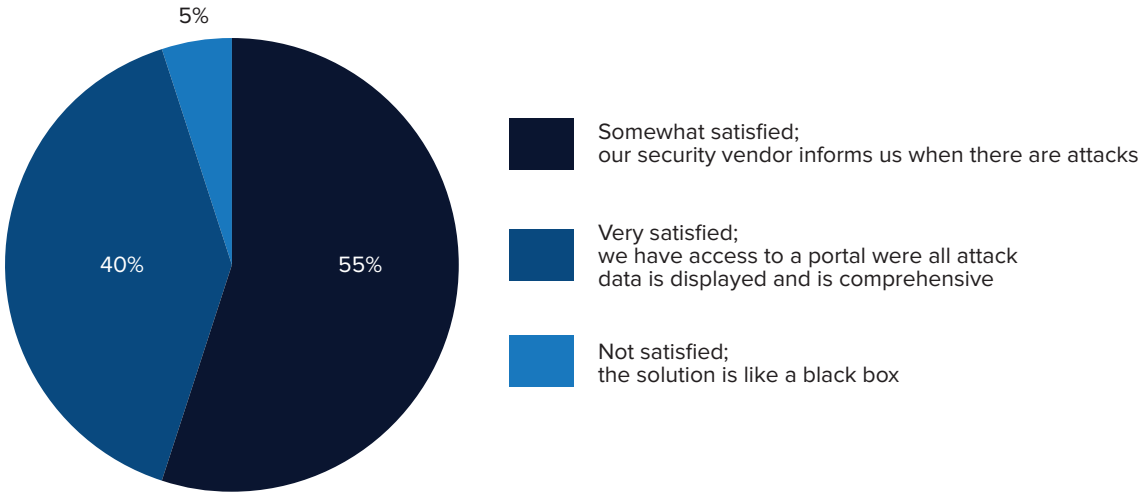
Comparing this year's and last year's survey results, we can see that financial institutions saw less customer attrition due to fraud incidents this year, but increases in loss of productivity, reputational impact and regulatory or compliance issues.

Which of these technologies has had the most significant impact on preventing fraud losses? (check all that apply)



Technologies that have had the greatest impact on preventing fraud losses include fraud detection and monitoring systems (55 percent); "positive pay" debit blocks and other limits on transactional use (45 percent); fraud detection and monitoring systems (55 percent); and enhanced customer education (43 percent). Biometric forms of authentication had a relatively low impact, as did running an operations “fusion center,” presumably due to the nascent nature of these technologies and the low level of adoption.

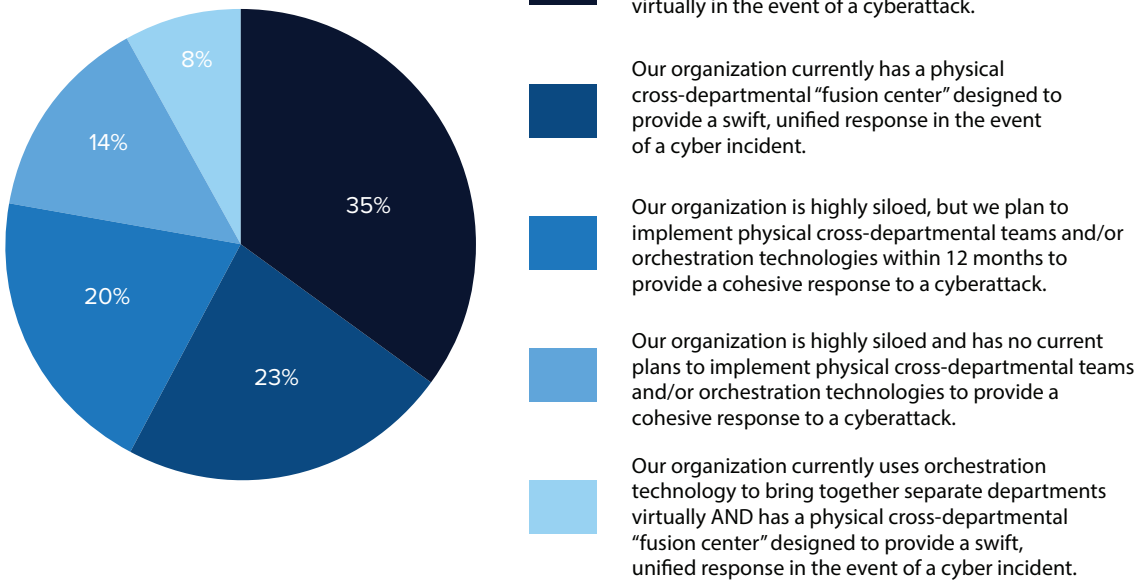
How satisfied are you with your cybersecurity solutions in terms of visibility of attacks against your organization?



Most financial institutions are satisfied with the visibility of attacks that they have with their cybersecurity solutions; 95 percent are satisfied or very satisfied with their existing capabilities, with just 5 percent concerned by the opacity of their solutions.

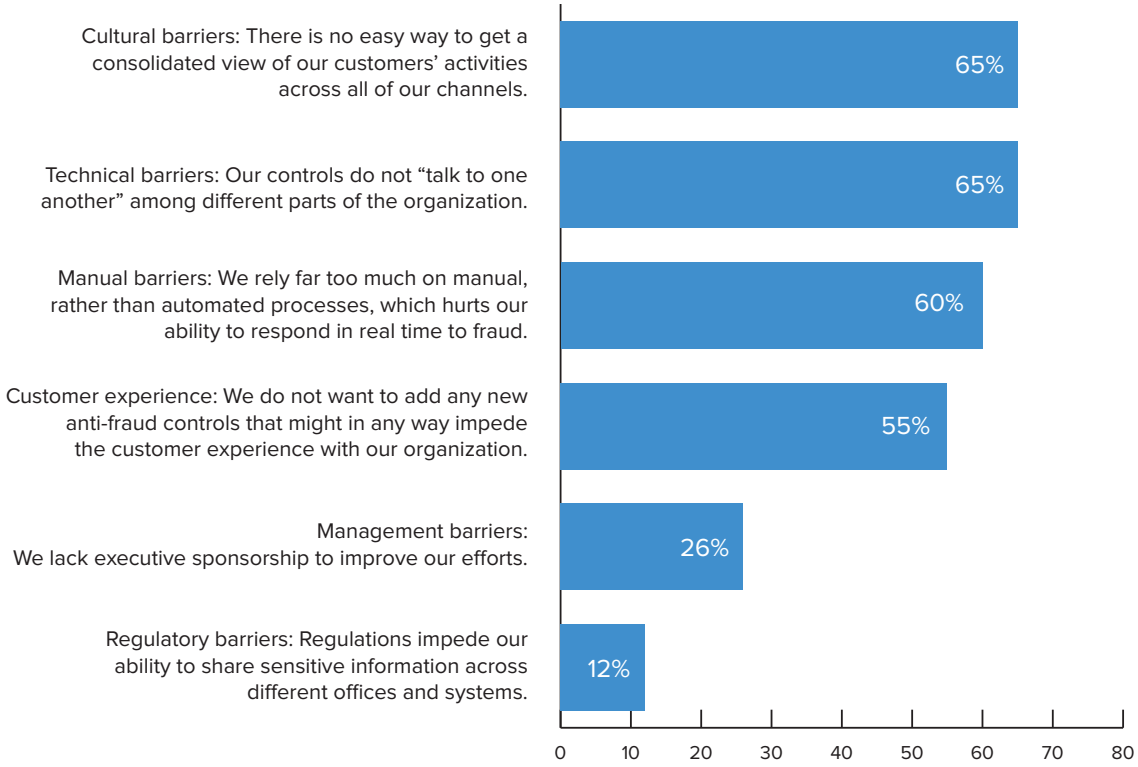
Most financial institutions are satisfied with the visibility of attacks that they have with their cybersecurity solutions.

How would you describe your institution's ability to work collectively across departments (security, legal, communications, product, operations) to share intelligence and provide a cohesive response to a cyberattack?



Some 14 percent of financial institutions have no current plans to implement physical cross departmental teams and/or orchestration technologies to provide a cohesive response to a cyberattack. Another 20 percent currently don't have these capabilities, but they plan to have them within 12 months. Those that have a solution in place for cross departmental collaboration are most commonly using orchestration technology to virtually bring teams together, rather than a physical "fusion center." Just 8 percent of organizations had both physical and virtual capabilities for collaboration of this nature.

Please select your organization's top three barriers to improving fraud prevention



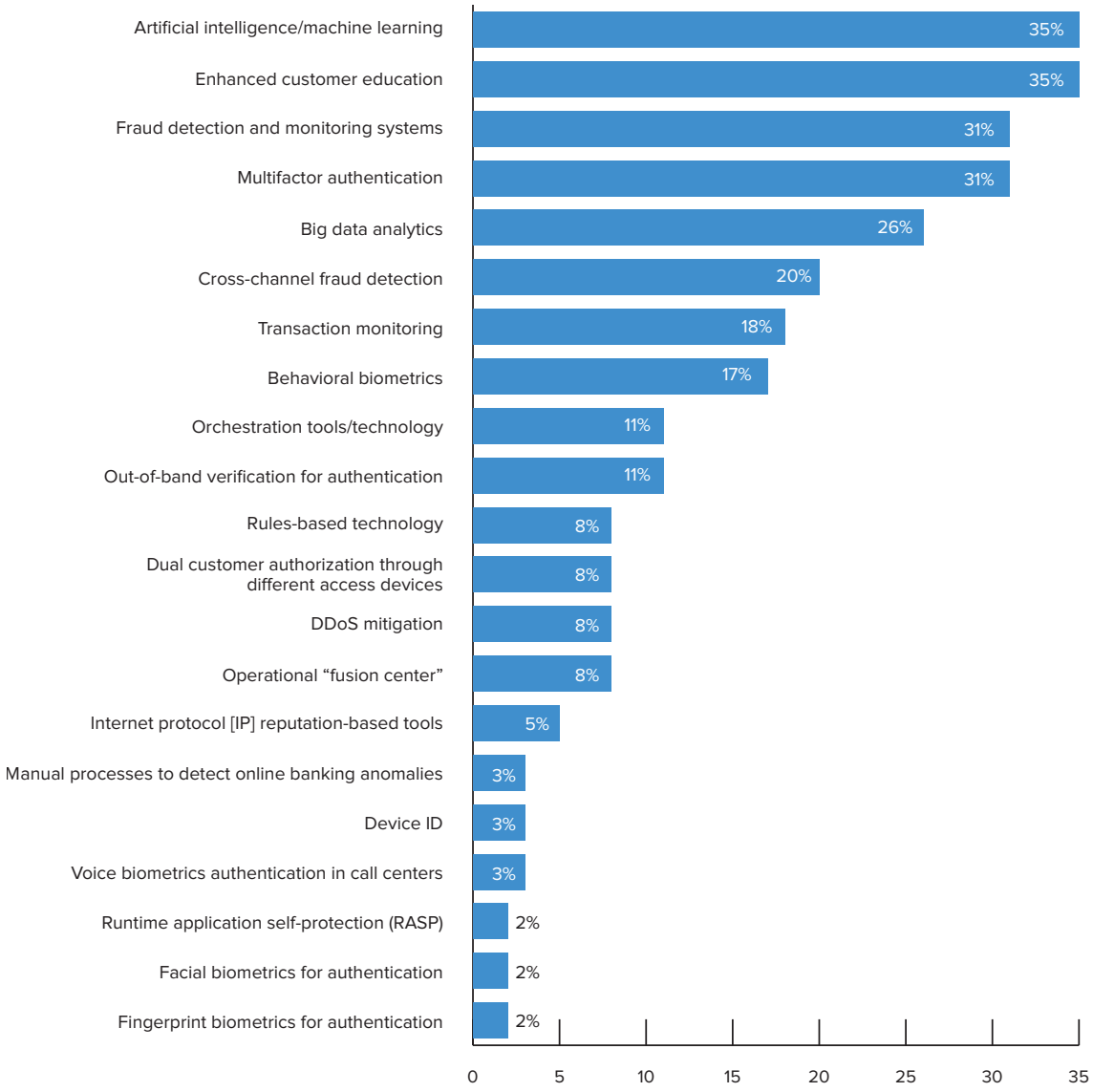
Handicaps to improving fraud prevention capabilities are primarily related to cultural, technical and user experience issues.

Banks are notoriously siloed; 65 percent of security professionals surveyed say cultural barriers are impeding the ability to get a consolidated view of activities across banking channels. The same percentage report that technical controls are not good at "talking to one another" across separate parts of the institution.

Financial institutions are also having to balance robust forms of consumer authentication with the desire for a streamlined user experience, such as strong authentication. Consequently, 55 percent of those surveyed state that a barrier to fraud prevention capabilities was not wanting to add any new anti-fraud controls that may impede the customer experience.

2020 Anti-Fraud Agenda

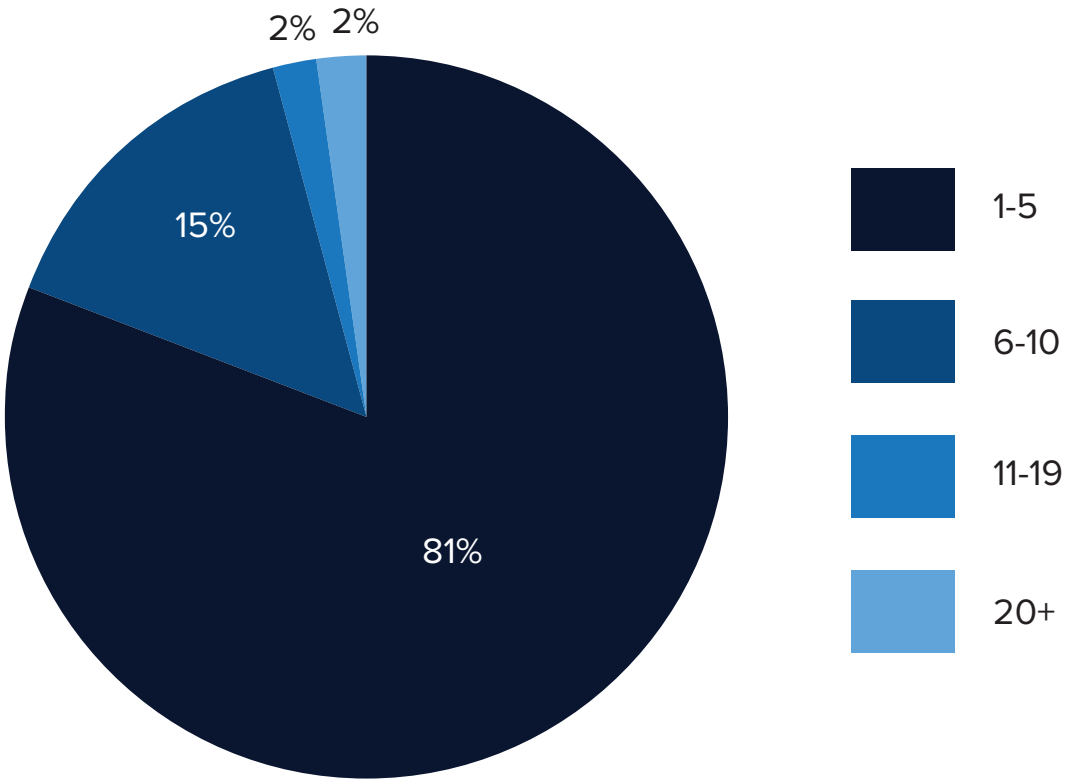
Which of the following technologies are you planning to invest in within the next 18 months? (check all that apply)



Fraud detection and prevention technologies that survey participants are most likely to invest in within the next 18 months include artificial intelligence/machine learning (35 percent), enhanced customer education (35 percent), multifactor authentication (31 percent), and big data analytics (26 percent). The least popular technologies included biometrics (excluding behavioral biometrics), runtime application self-protection (RASP) and device ID.

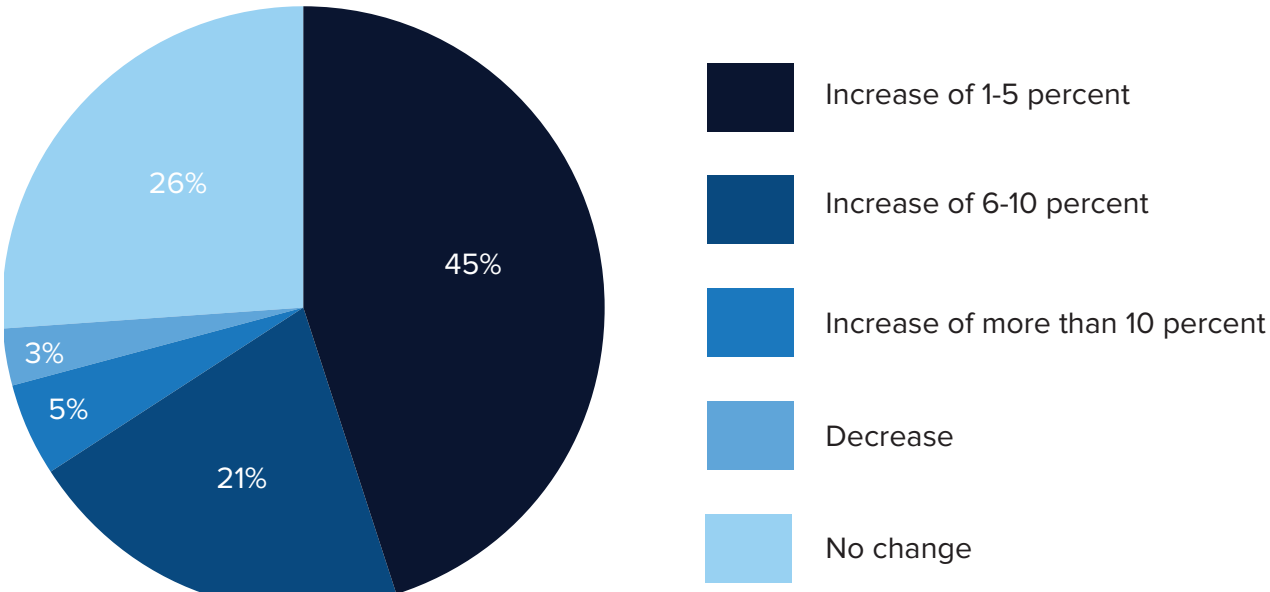
Fraud detection and prevention technologies that have gained in popularity in this year's survey, compared to last year's, include: artificial intelligence/machine learning (+13 percentage points), cross channel fraud protection (+14 percentage points), enhanced customer education (+7 percentage points) and out-of-band verification for authentication (+6 percentage points).

How many separate providers do you purchase from to achieve your anti-fraud needs?



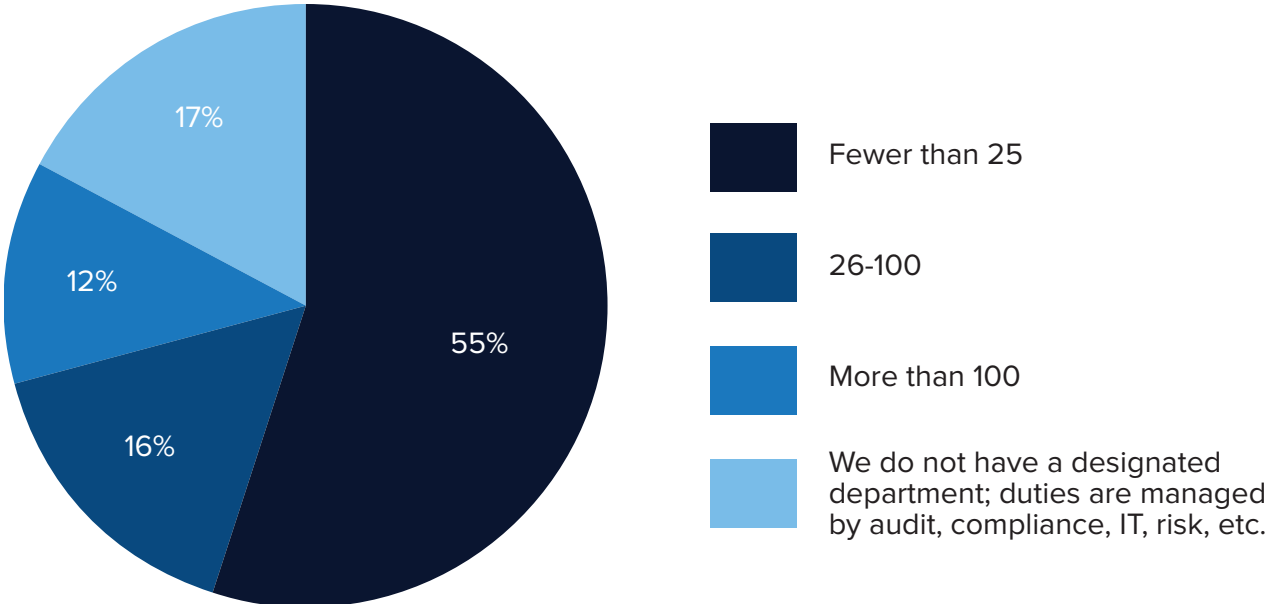
The vast majority of survey participants – 81 percent – purchase anti-fraud solutions from one to five vendors, with 15 percent purchasing from six to 10 vendors. Just 4 percent purchase anti-fraud solutions from 11 or more vendors.

How do you expect your budget dedicated to fraud prevention to change in the next year?



Budgets for fraud prevention are expected to increase in the next year. Some 45 percent expect a 1 percent to 5 percent increase, and 22 percent expect a 6 percent to 10 percent increase. A quarter expect no change, and just 3 percent anticipate a decrease in available budget.

How large is your organization's department assigned to fraud prevention and detection?



The majority of financial institutions have a team of fewer than 25 people working on fraud prevention and detection. Perhaps more concerning – 17 percent of survey participants state that their financial institution doesn't have a designated department for this purpose; the duties are carried out by other teams.

Conclusions and Recommendations

In reaching conclusions about the survey results, it's important to reflect again upon the goals of this study, which were to help to determine:

- The top forms of fraud affecting financial institutions in 2019;
- The biggest gaps in organizations' efforts to mitigate fraud;
- Where today's financial institutions are focusing their investments on fraud prevention technologies for the coming year.

To review some top-level findings:

- Financial institutions have the support of C-level executives for investment in tools enabling threat mitigation. In fact, nearly three-quarters of survey participants were confident or very confident that the executive suite understands the importance of the right fraud mitigation tools.
- Further, more than half of survey respondents were confident or very confident that employees are educated and aware of how to mitigate fraud.

However ...

- The number of fraud incidents increased to 47 percent in the current survey from 39 percent the previous year.
- Time to uncover fraud increased, this survey shows, yet the speed of mitigation decreased. Some 20 percent of fraud is now detected in real time, compared with just 12 percent a year ago. But real-time mitigation has dropped to 13 percent from 17 percent a year ago.

Why is this?

The Pervasive Silo Problem

Banks are notoriously siloed and this handicaps timely remediation efforts; 65 percent of security professionals surveyed say cultural barriers are impeding the ability to get a consolidated view of activities across banking channels. The same percentage report that technical controls are not good at "talking to one another" across separate parts of the institution.

The Fraud Arms Race

Fraud schemes are evolving faster than the ability to educate and train staff. This applies to internal staff, but also to third-party entities that today's businesses are increasingly reliant upon. Some 60 percent of participants say that today's fraud schemes evolve too quickly for us to keep pace, while 57 percent say that the lack of awareness of socially engineered fraud schemes among customers and partners is a serious concern.

Opacity of Phishing Attacks

While just over half of organizations have "detailed visibility" into the impact of a phishing attack, a concerning 45 percent have limited visibility and 3 percent have no visibility. The inability to connect the dots between attacks and the repercussions presents a challenge in articulating the scale of the damage in terms that business executives understand: direct financial losses, reputational damage, customer churn and employee turnover.

The Perennial Staffing Crisis

It is no secret that there is a significant skills shortage in the cybersecurity industry. The majority of financial institutions have a team of fewer than 25 people working on fraud prevention and detection. Perhaps more concerning – 17 percent of survey participants state that their financial institution doesn't have a designated department for this purpose; the duties are carried out by other teams.

So what's the solution?

Emerging Technologies Are Key to Mitigating Emerging Fraud Schemes

There is clearly no silver bullet for ending financial services fraud. Fraudsters will continue to flock to "where the money is." And despite seemingly more attention and budget from executive teams to mitigate fraud, the challenges of connecting the dots between cause and effect mean that it will remain challenging to win support for budget increases. Most survey participants anticipate an anemic annual budget increase of between 1 percent and 5 percent for fraud prevention tools.

In summary, security teams in financial services will need to make discerning choices when it comes to allocating budget for solutions that enable them to work smarter with existing resources – such as artificial intelligence, machine learning and big data analytics – and continue to educate and train customers (both internal and external) on fraud schemes that cause the greatest damage, such as business email compromise and spear phishing.

For more analysis on how to put the survey results to work, see the interview that follows.

The New Faces of Fraud Survey

The Challenging Disconnect Between Information and Action

NOTE: In preparing this report, ISMG's Nick Holland discussed the findings with Mike Lopez from the survey sponsor, AppGate, who addressed how organizations can best put them to use to improve fraud detection and response. This is an excerpt of that conversation. For the full interview, please click here.

First Impressions

NICK HOLLAND: First of all, what was your gut reaction to this year's survey? What surprised you?

MIKE LOPEZ: My gut reaction Nick, is that financial institutions are finally starting to really comprehend the threat landscape and the challenges that they're facing.

Interestingly enough, throughout the survey, though, you're seeing that while they've identified where they need to go, there seems to be a little bit of a struggle with the execution on that.

In terms of specifically what surprised me, the industry has talked a lot about spear phishing and business email compromise. Statistically, it's been said that more than 90 percent of all the cyberattacks or fraud attacks are initiated via spear-phishing campaigns. Yet interestingly enough, most of the respondents stated that they have not seen spear phishing or business email compromise that has resulted in fraud losses. That might be potentially a situation where there is a disconnect.

HOLLAND: I completely agree with you. I thought that was actually a really interesting point. They know that the fraud is happening but there doesn't seem to be the dots connecting.

LOPEZ: Correct. They have the visibility into the initiation of the attack. There may just be issues with correlating that to whether there is an account takeover, actual fraud losses, subsequently happening with that.

The Mobile Security Angle

HOLLAND: Another interesting finding was around mobile. Tell us about what we saw there.

LOPEZ: It's interesting that still approximately a quarter of the respondents are saying that they don't have visibility into their mobile channel, which is somewhat surprising.

In terms of mobile, what we're seeing is there has been a reduction in the number of mobile attacks, but the mobile attacks that we are seeing are very targeted and very deliberate. They are extremely complex in nature, so financial institutions cannot assume that traditional mitigating or identifying controls will work the same as they did perhaps on the desktop. They need to be very cognizant of the fact that they're going to have to implement controls that are different from that – maybe focusing on the identity and the posture of those devices specifically so that they can create controls on the back end.

Mike Lopez

"Financial institutions are finally starting to really comprehend the threat landscape and the challenges that they're facing."

"You're seeing much more investment in terms of artificial intelligence and machine learning, which is critical."

Balancing Security and Customer Experience

HOLLAND: One of the things we talked about was zero trust and how the mobile device doesn't lend itself very well to some of the traditional things you might see on a laptop in terms of recognizing fraud. But there are things we can do from a technology standpoint that will make the mobile experience frictionless, but also a lot more secure.

LOPEZ: There's a lot of talk around zero trust as it relates to the enterprise. I think there's the opportunity to take that same model and apply it to the consumer.

To your point, in terms of the mobile channel, there's the opportunity to leverage significant intelligence and device attribution to than create a device posture and then an identity around the user.

And then once you've identified the user, authenticated the user and created that secure access, you can then determine what level of entitlement you want the user to have on the back end – the ability to create a zero trust posture within the consumer framework.

Budget Issues

HOLLAND: In terms of some of the budget allocation questions we were asking, what would be some of your takeaways?

LOPEZ: First of all, we are finally seeing that the C-level executives understand that there is a need to invest. As a banker for 15 years, that was not always the case. The fact that we're getting C-level buy-in is impressive.

In terms of the investments, I think we are seeing the right approach this year. You're seeing much more investment in terms of artificial intelligence and machine learning, which is critical because the attacks that we're seeing today are extremely complex and can adapt and change at a very high rate of speed. If you have manual processes, you will not be able to keep up.

Along with that, the budget items around multifactor authentication are impressive. We have not seen that before. It seems like financial institutions are finally focusing on moving away from SMS and listening to what NIST is saying in terms of the security issues around SMS.

Multifactor Authentication

HOLLAND: Obviously there have been things like PSD2 in Europe driving things like multifactor authentication, but banks seem to be voluntarily doing it at this point in time.

LOPEZ: To your point earlier on zero trust, SMS in terms of a multifactor authentication doesn't provide the best user experience. And this is telling us that it's not the most secure. If you again, incorporate that secure access, zero trust methodology with implementing stronger MFA via push or in-channel capabilities, it's a better user experience.

"The key advice that I would give practitioners would be we need to focus on orchestration."

Next Steps for Practitioners

HOLLAND: What would you say are the key takeaways for security practitioners? And what advice would you give based on the findings of the survey?

LOPEZ: The key advice that I would give practitioners would be we need to focus on orchestration.

We heard a lot throughout the survey that there are still cultural and technology barriers. Financial institutions need to figure out how to break down those barriers and leverage the intelligence that is coming out from the departments to create more actionable data and to create the ability to make stronger decisions.

And we've talked about the importance of building a zero trust, secure access framework for the consumer. Create less friction throughout the transaction or throughout the session process while simultaneously creating stronger authentication factors behind that. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io