Building Your Best Defense

Tackling B2B Payment Fraud Risk

Introduction

Are mid-sized companies overconfident in their abilities to detect and prevent fraud? Capital One®-commissioned research, conducted by Accenture, surveyed 225 executives from mid-sized companies ($50 million to $3 billion in annual revenue) to understand their attitudes and approaches to B2B payment security. The survey challenged respondents to answer questions detailing their B2B payment and payment security practices, needs, and preferences. It also delved into their perspectives on fraud and their companies' fraud experiences.

Participants reported overwhelmingly that they were satisfied with their organization's current B2B payment security methods. This by itself is not concerning, but complacency can be dangerous when it leads to inaction.

Almost half (48%) indicated that updating payment security was either not important at this time, or not a main priority. This delay is already hurting businesses, with two-thirds of the surveyed executives reporting that their businesses had experienced payments fraud within the prior two years and four in ten respondents (42%) reported B2B fraud losses above five basis points on B2B payment volume.

42%

reported B2B fraud losses above five basis points on B2B payment volume.

Fraudsters are getting more savvy and have greater access to advanced technology and processing power than ever before. If banks and businesses want to have a fighting chance against these high-tech criminals, they should start seriously evaluating and investing in their own technology and people.

For Informational Purposes Only
These materials are for informational purposes only. These materials do not represent any opinion, guidance or recommendation, whether formal or informal, of Capital One, National Association, or any of its officers, directors, employees, advisors, attorneys, consultants, affiliates or subsidiaries (collectively, "Capital One"). Without limiting the generality of the foregoing, these materials do not represent legal advice or guidance by or from Capital One. In no event may the recipient of these materials rely on these materials for any purpose whatsoever. Nothing contained in these materials shall give rise to, or be construed to give rise to, any obligations or liability whatsoever on the part of Capital One. Nothing contained in these materials shall alter or modify, or be deemed to alter or modify, applicable law (including, but not limited to, the limitations under applicable law of Capital One's obligations and/or liability in applicable matters). The recipient of these materials should consult the recipient's own counsel to understand the recipient's obligations and liability in applicable matters.

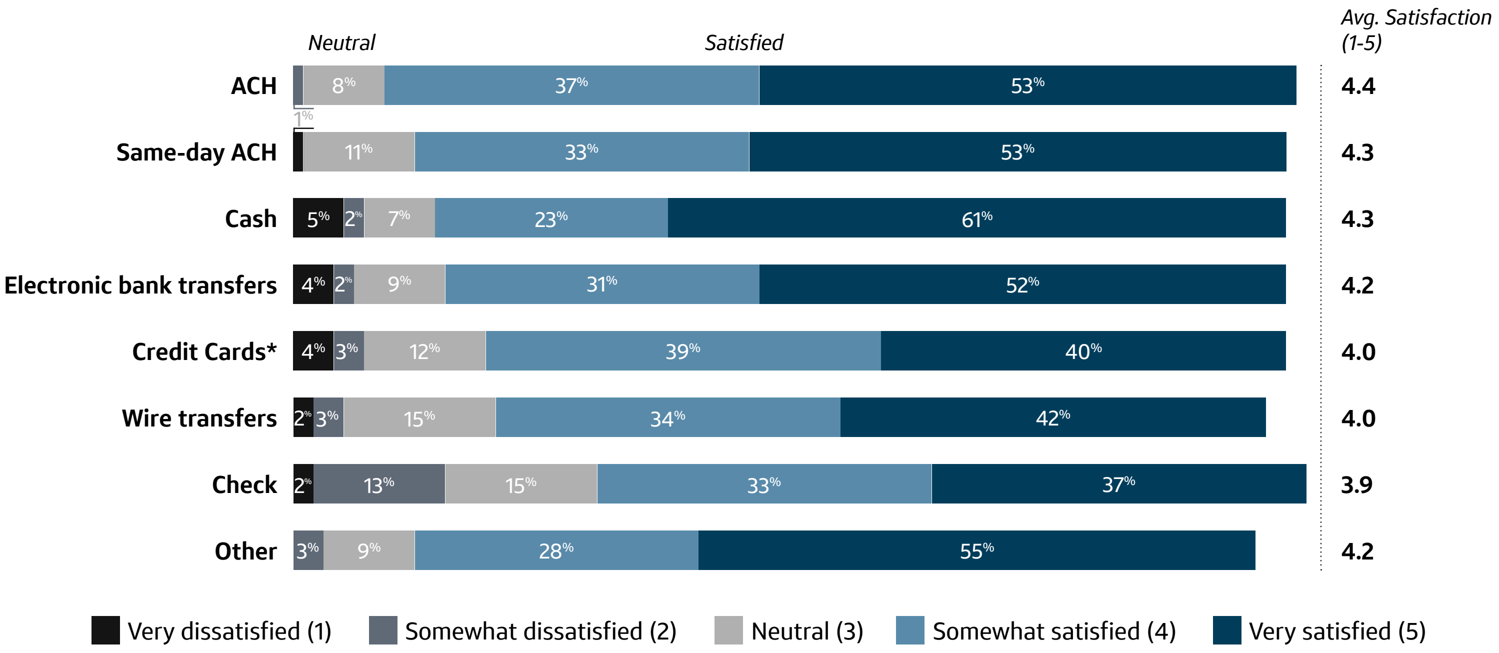
Mid-sized businesses seem content with their current methods for securing B2B payments

So why are these companies forgoing updates to protect their revenue, especially when they've been burned in the past? We saw three common reasons given by executives:

- **Relatively speaking, it's not that important:** "Other problems are more important." "Better security is important but not paramount." "It is on the 'nice-to-do list' over the course of the next several fiscal years."
- **The cost is greater than the value-add:** "The cost is higher than we anticipated and not relevant to our business." "We do not have budget."
- **The status quo is good enough:** "We believe our current processes are adequate." "We already have safeguards in place."

Satisfaction with Security by Payment Method

How satisfied are you with your organization's current methods for securing B2B payments against fraud and cyber-attacks? Please specify your level of satisfaction for each.



*Includes Procurement and Virtual Cards, Other combines ePayables and Cryptocurrency
Source: 2019 B2B Payment Security Survey

Not only are companies not updating their payment security systems, many are not equipping their employees with the right tools to defend themselves against fraud. Just over one-third (36%) of our respondents said they or their employees fell victim to a phishing or business email compromise (BEC) attack within the past two years, and the cost has been stiff: In July 2018, losses from BEC attacks amounted to $12.5 billion globally and $1.2 billion in the US alone[1].

Phishing and BEC issues are directly linked to employee awareness and vigilance. Right now, many companies find themselves in a state where employees are not suitably trained to detect fraud and/or are not sufficiently aware of the red flags indicating a fraud risk.

To avoid falling into a trap of over-optimism and becoming a target for fraudsters, companies should critically evaluate:

- Their security and technology infrastructure; and
- Employee awareness of and behavior toward fraud risks.

[1] *Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), "2018 Internet Crime Report," https://pdf.ic3.gov/2018_IC3Report.pdf*

36%

of our respondents said they or their employees fell victim to a phishing or business email compromise (BEC) attack within the past two years.

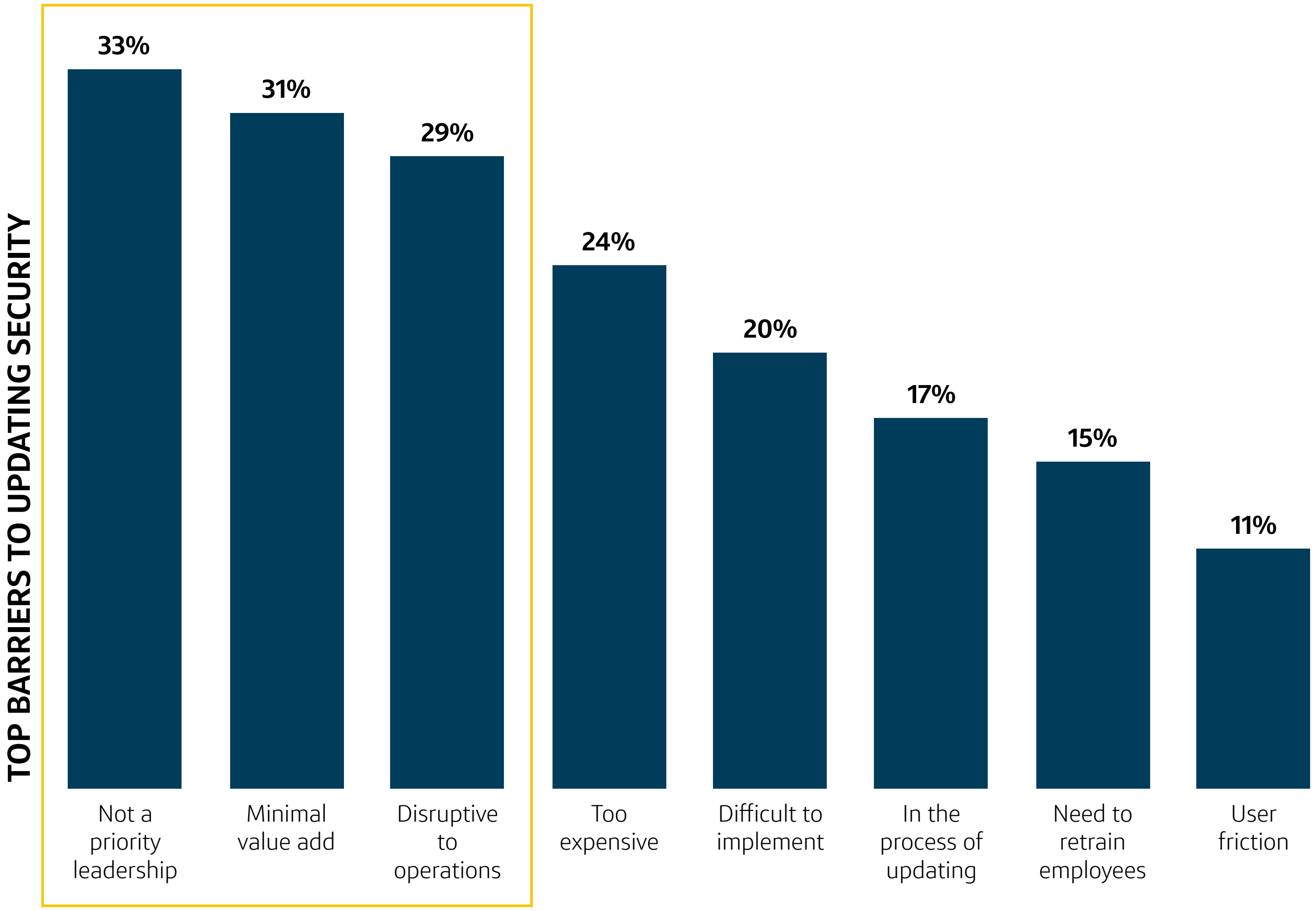


Table of Contents

The Scope of the Threat

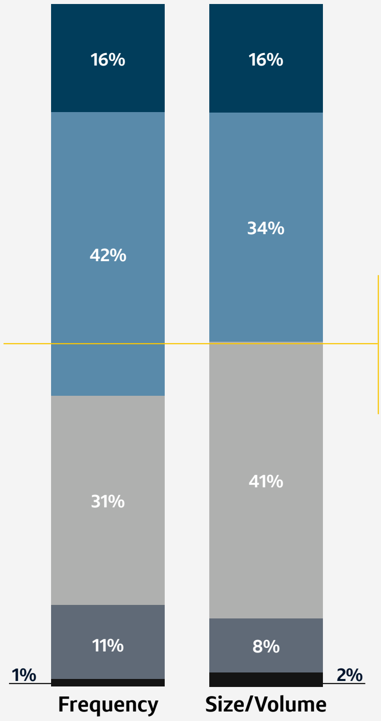
B2B Payments Fraud Is a Growing Threat

Let's face it, fraudsters are smart—they go where the money is. Fraudsters could spend a great deal of time stealing countless credit cards and bank accounts, but why would they when an attack on a single multi-million-dollar company could produce more earnings without similar effort? B2B payment fraud is a rising threat to firms around the world. Our research found that **66% of mid-sized companies** had experienced some form of B2B payments fraud within the past two years and the cost is palpable. (See sidebar, "The Economic Impact of SMB Fraud.")

When looking at firms of all sizes, the situation is even more dire. A 2019 Association for Financial Professionals (AFP) study found that 82% of organizations experienced B2B payments fraud in 2018—a 20% increase from just five years ago[2].

Businesses are fully aware of this threat. Executives of mid-sized companies overwhelmingly ranked "fraud" as the most critical issue facing their company's B2B payments. More than half (58%) indicated that they felt fraud attacks had increased in frequency over the past two years, and 50% noted that they thought fraud attacks had increased in size and volume over the same period.

How can firms adequately deal with this mounting threat? It's a question that all companies, regardless of size, must address—and quickly.



Perception of Fraud Growth Pattern
Do you feel as if fraud attacks targeting B2B transactions has increased in **frequency**? Do you feel as if fraud attacks targeting B2B transactions has **increased in size/dollar volume**?

>50%
of respondents feel fraud attacks are increasing in frequency as well as dollar volume in the past two years

- ■ **Significantly Increased**
- ■ **Somewhat Increased**
- ■ **No noticeable change**
- ■ **Somewhat decreased**
- ■ **Significantly decreased**

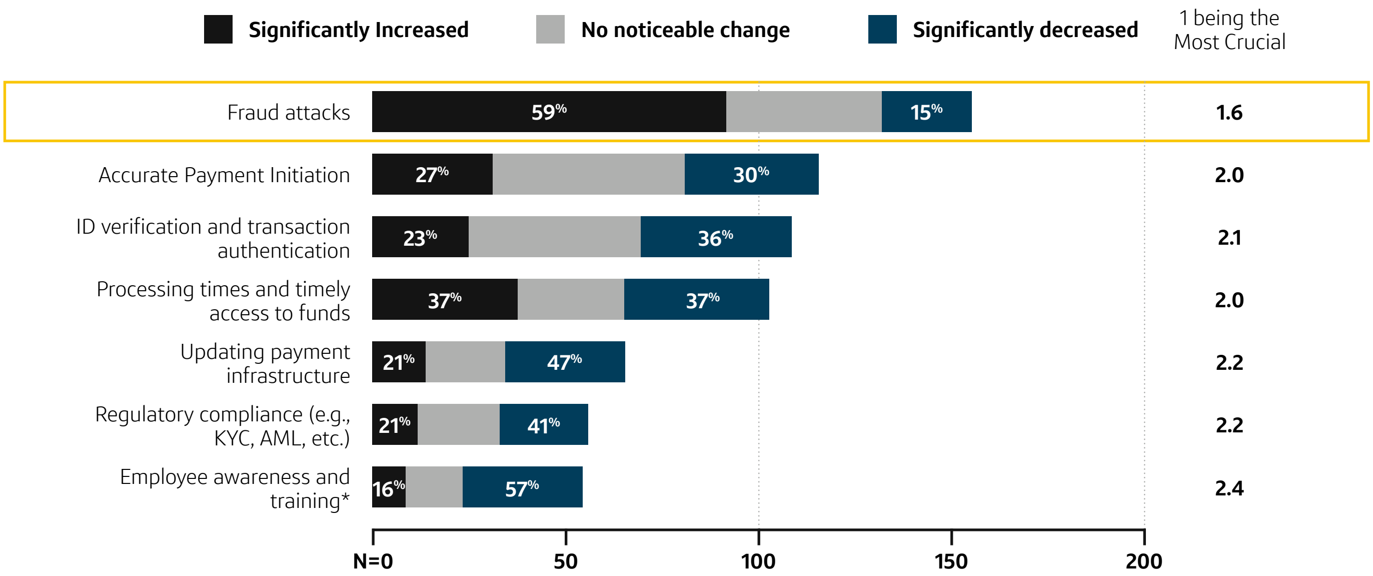
Source: 2019 B2B Payment Security Survey

The Economic Impact of Small and Mid-Sized Businesses

How important is the economic welfare of small and medium-sized businesses? According to the World Economic Forum, in the U.S. alone there are roughly 200,000 companies that have revenues from $10 million to $1 billion. Most of these are privately held or family controlled. Such businesses produce roughly one-third of U.S. GDP.[3]

[2] *Association for Financial Professional (AFP), "2019 AFP Payments Fraud and Control Survey Report," April 2019 Payment Fraud Jumps to Record High*
[3] *World Economic Forum, "Fueling the US economy's middle market growth engine," February 2018*

Top Concerns and Challenges
What are your organization's B2B payment concerns/challenges? Please rank your top three concerns/challenges with 1 being the most crucial.



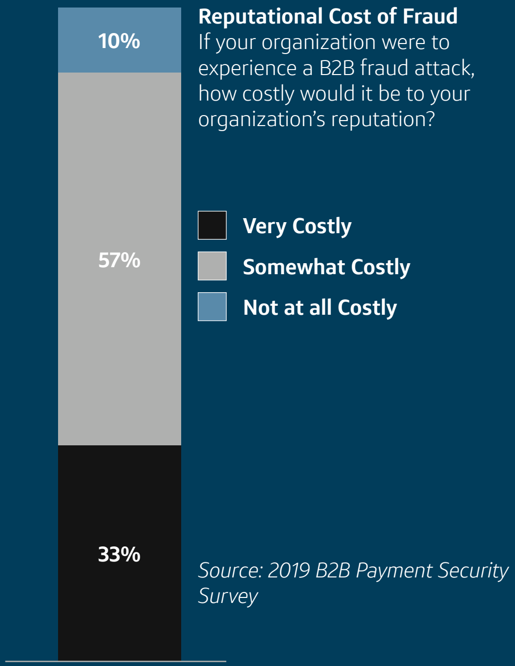
**e.g., onboarding, operations, security best practices*
Source: 2019 B2B Payment Security Survey

The Costs Are Adding Up

According to Accenture's annual Cost of Cybercrime report, U.S. companies are at risk of losing $1.7 trillion to cybercrimes over the next five years. In just the last year, the average cost of cybercrime per a company grew 29%. U.S. companies now lose on average $27.3 million annually to cybercrime.[4]

Our own research found a similarly grave situation when it came to the costs of B2B payment fraud. Three-fourths of respondents who had experienced a fraud attack experienced losses, and about 40% reported annual net B2B payment fraud losses above five basis points (on B2B payment volume).

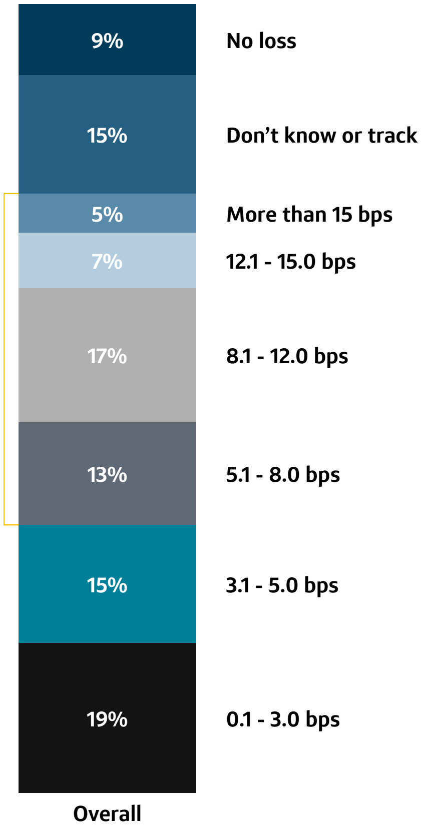
Non-tangible costs need to be accounted for as well—impacts on reputation, investor confidence, customer trust, etc. For example, 90% of respondents noted that a fraud event would be costly to their company's reputation. One-third said it would be "very costly."


Reputational Cost of Fraud
If your organization were to experience a B2B fraud attack, how costly would it be to your organization's reputation?

Source: 2019 B2B Payment Security Survey

[4] Accenture, "Ninth Annual Cost of Cybercrime Study in Banking and Capital Markets 2019 Report." July 2019.

Annual Fraud Losses
(bps on B2B payment volume)



42%
of respondents reported B2B fraud losses above 5bps on payment volume

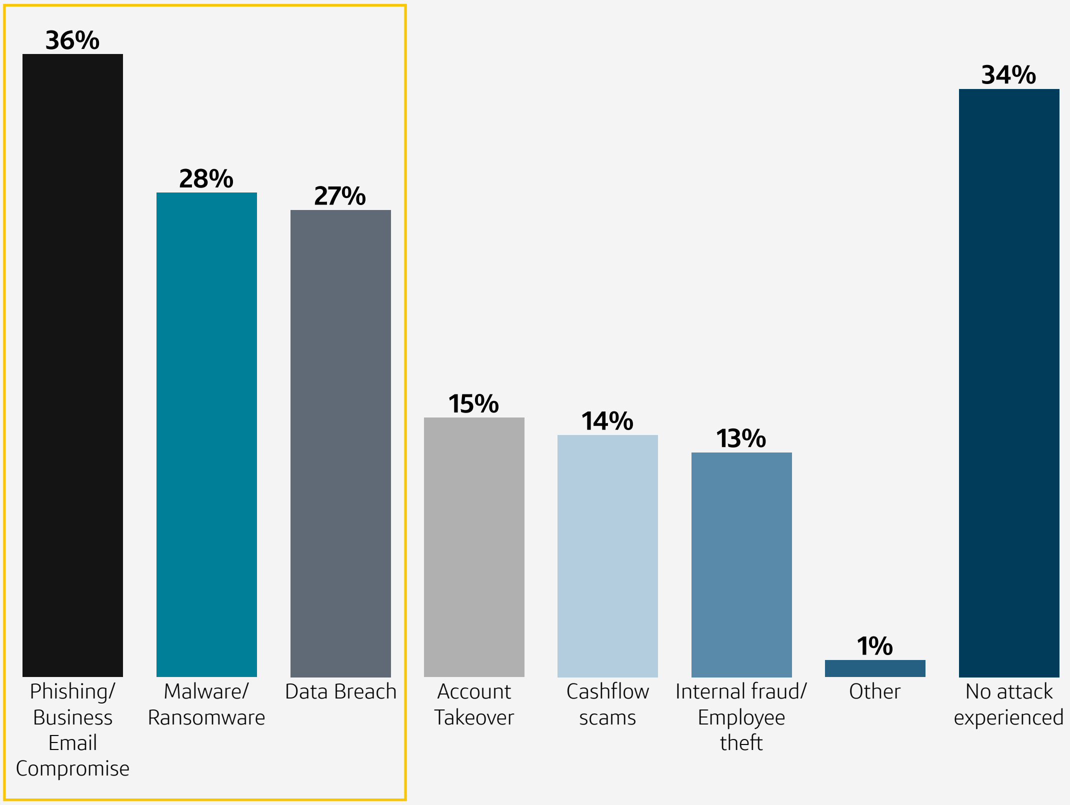
Cyber-Criminals Are Evolving

Complicating the issue, businesses are fighting a moving target. Firms are able to react to conventional fraud, but they have few defenses against novel attacks. The problem is that fraudsters—externally and internally—are creating more sophisticated attacks. Increasingly, shrewder criminals are focusing efforts on large-scale, complex commercial fraud rather than less lucrative retail fraud.

Criminals are organizing and working together to commit more complex commercial fraud attacks than ever before. They can do this by taking advantage of the increased availability of processing power and using sophisticated technologies, such as artificial intelligence, machine learning and automation. With more organized and more technology savvy criminals than ever before, the threat of fraud looms ever greater.

> It is important to note that of the 34% of respondents who did not report any B2B payment fraud attacks, a subset may be unaware that they have fallen victim to an attack - especially if it is recent - and some may have experienced other non-B2B payments forms of fraud.

B2B Payment Fraud by Attack Method
Within the past two years, has your organization experienced any of the below fraud attacks in regard to B2B payments?



66%
of respondents report experiencing some form of B2B payment fraud attack within the past two years

Source: 2019 B2B Payment Security Survey

Types of Security Threats

1. Phishing and Business Email Compromise (BEC)

What are they?

Fraudsters send targeted emails, often pretending to be a vendor or another employee within the company. In this way, they collect personal login information or gain access to a company's data and systems. With access to data and/or systems, fraudsters can make unauthorized payments, install malware or ransomware, or package and resell confidential information (data breach).

Prevalence

High: Affecting 36% of mid-sized companies

2. Malware and Ransomware

What are they?

Victims unknowingly install malicious software designed to damage a computer, server, client, or computer network. In malware attacks, fraudsters threaten victims into paying a fee to avoid activation of the malware or to sell them the solution. In ransomware attacks, fraudsters inhibit operations by holding company systems and/or data hostage until the company pays the hostage fee (often in bitcoin or another cryptocurrency).

Prevalence

High: Affecting 28% of mid-sized companies. (Note: Malware and ransomware attacks are also on the rise. A recent report from McAfee found that ransomware attacks grew 118% in the first quarter of 2019.[6]

3. Data Breaches

What are they?

Data breaches are security events where data is accessed without authorization, often as a result of phishing or BEC attacks.

Prevalence

High: More than one-fourth (27%) of mid-sized companies experienced a data breach within the prior two years. (Note, survey respondents were the most concerned about data breaches. About a quarter of executives indicated that data breaches were a high or moderate risk for their organization.)

4. Account Takeovers

What are they?

A fraudster gains enough personal information to take control of an account to make unauthorized transactions (often changing contact and login information, making it difficult for the true owner to access the account). These are often the result of targeted phishing attacks.

Prevalence

Low: Affecting 15% of mid-sized companies

5. Cashflow Scams

What are they?

Cashflow scams are possible because of a difference between the time it takes for a transaction to clear and when the receiving party has access to funds. For example, a fraudster sends funds that they don't actually have to a second account and then withdraws the funds from the second account. The first transaction bounces because of the lack of funds, but the fraudster already has withdrawn the cash from the second account.

Prevalence

Low: Affecting 14% of mid-sized companies.

6. Internal Fraud Incidents

What are they?

Internal fraud (sometimes also termed "malicious insider attacks") are committed by an employee within an organization. There are many different ways employees may defraud their employer. Some of the most common methods include authorizing funds to be sent to a personal account or selling company data to a fraudster or competitor.

Prevalence

Low: Affecting 13% of mid-sized companies. (Note: Internal fraud often goes unreported and is estimated to be higher than report rates.)

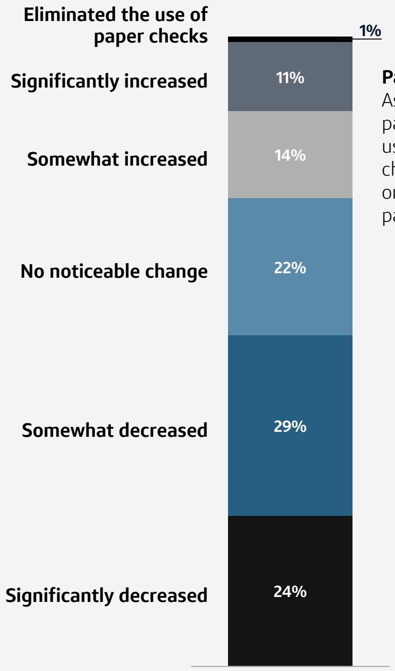
[6] *McAfee Labs Threats Report*

The Role of Technology

Out with the Old and In with the New

Some companies are taking solace in the fact that B2B payments are evolving, and new methods appear to be less susceptible to fraud. For example:

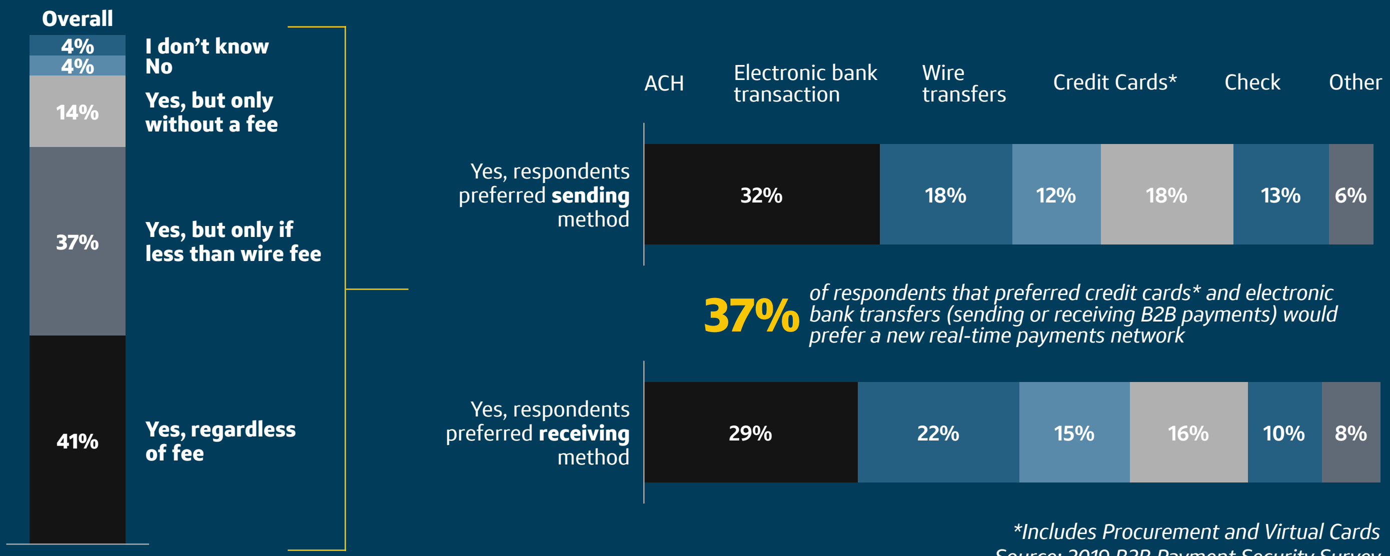
- **Check usage is declining:** Checks are more prone to fraud because they are relatively easy to forge and counterfeit. Half of respondents who listed checks as their most preferred method for sending or receiving B2B payments reported that check usage within their business had somewhat or significantly decreased over the past two years.
- **Real-time payment (RTP) networks are within sight:** Both the Clearing House and the Federal Reserve have announced plans for a real-time payments network. Many expect adoption of these real-time networks could displace some traditional payment methods—wires, ACH, and internal electronic bank transfers—as volume shifts to real-time rails. When asked their preference of either RTP networks or wires, 92% of respondents indicated an interest in using a real-time payment network in place of wire transfers.



Paper Check Usage
As it relates to B2B payments, how has your use of paper checks changed within your organization over the past two years?

Source: 2019 B2B Payment Security Survey

Real-Time Payments Network Interest
If a new real-time payments network was available (e.g. FedNow or The Clearing House's RTP Network), would your organization be more likely to use the new network instead of wire payments for fast transactions/access to funds? Real-time transactions are completed nearly instantaneously (one hour or less) and is different from same-day ACH.



37% *of respondents that preferred credit cards* and electronic bank transfers (sending or receiving B2B payments) would prefer a new real-time payments network*

**Includes Procurement and Virtual Cards*
Source: 2019 B2B Payment Security Survey

Fighting Technology with Technology

New technologies are providing innovative opportunities in B2B payments, but also pose increased threats, as bad actors discover ways to exploit these technologies.

It is important to note that while real-time networks and other alternative payment methods may seem safer now, increased volume over these channels will draw attention from fraudsters. Once volume, and subsequently opportunity, is great enough, fraudsters will likely turn their efforts towards exploiting newer payment channels.

It is thus important to institute these payments changes while simultaneously updating security operations. Below are some of the most promising technologies that are being deployed to combat fraud.

Biometrics

Biometrics is a security enhancement that uses a person's physical features (e.g., thumbprints, retinas, facial data points) for authentication purposes.

According to a report from Gartner, 70% of enterprises, across industries, will combine biometrics with analytics, mobile push notifications and/or embedded public-key credentials by the end of 2022.[7]

Businesses can use biometrics to enhance traditional log-in credentials and badges—e.g., using a thumbprint to unlock a computer or door instead of a password (which can be hacked) or a badge (which can be forged).

Just under half of the companies in our survey (45%) had adopted biometrics.

Behavioral Biometrics

Behavioral biometrics uses non-physical attributes such as voice or device interactions (e.g., how a user holds their phone or types on a keyboard), to identify and authenticate a user. The benefit of behavior-based authentication is that it reduces user friction. For example, trusted devices may default to keeping a user logged in to a payment account, but will lock the account until further authentication is provided if the device detects out-of-the ordinary behavior.

Behavioral biometrics is still in its nascency, however this approach may grow in popularity as companies shift more of their operations to mobile devices.

67%

of mid-sized companies have already adopted multi-factor authentication.

Multi-factor Authentication (MFA)

With multi-factor authentication, access to a system or account requires more than just a password—it can involve a log-in ID plus a secure code sent to an email address or mobile device that must then be entered, or potentially a biometric verification. Because there are multiple layers of security, it is harder for a fraudster to circumvent and gain access to an account and/or sensitive information. We found that a fairly high level of mid-sized companies (67%) have already adopted multi-factor authentication, but there is room for growth.

[7] *Gartner Predicts Increased Adoption of Mobile-Centric Biometric Authentication and SaaS-Delivered IAM*

Artificial Intelligence, Machine Learning and Automation

Artificial intelligence (AI), despite its prevalence in media and corporate conversations, is still often seen as out of reach or unattainable by all but the largest firms. AI—a branch of computer science where machines are programmed to think and adapt instead of just execute instructions—enables programs to solve unfamiliar problems sometimes even better than their human counterparts. AI has the potential to propel security operations into the future.

Machine learning (ML), a subset of AI, has been used to enhance fraud detection engines—finding fraud patterns faster and much more efficiently than humans. Automation (often referred to as "robotic process automation") can streamline back-office operations but may also help prevent phishing and BEC attacks by improving the sorting and filtering capabilities within company email inboxes.

Automation is helping reduce risk by preventing fraudulent emails from ever making it to an employee's inbox, and those that do are often well marked as "suspicious" or "external sender." Over one-third (39%) of mid-sized businesses reported having incorporated AI, ML, and/or automation into their security operations. However, the majority of these most likely have only adopted automation, as other forms of AI and machine learning are more technically difficult (and more expensive).

Decentralized Identities

According to research from Forrester, commissioned by Capital One, a decentralized digital identity is a trusted digital identity that can be shared securely without relying on a central data depository[8]. This includes methods such as avoiding the linkage of an online ID to personal data (e.g., social security number), reducing the risk of compromising information which can lead to fraud.

In our survey, 48% of companies said they have adopted a decentralized approach. However, according to the Forrester research, many companies report a high adoption rate of decentralized identities but also seem to be lacking clarity about what the technology is and how to apply it.

[8] *Embrace Decentralized Digital Identity To Improve Customer Experience And Reduce Risk, a commissioned study conducted by Forrester Consulting on behalf of Capital One, June 2019*

Tokenization

Tokenization is a cryptographic method that replaces sensitive account information with a single-use token that can only be decrypted by the holder of the token vault (i.e., payment and card networks). This makes it harder for fraudsters to steal account information that could be used in account takeover attacks.

Our survey found that the current adoption rate hovers around 41%, although a Gartner study reports that more than 70% of organizations will adopt multiple tokenization-type techniques by 2025.

Blockchain

Blockchain (also referred to as "distributed ledger technology") is a distributed database system that maintains and records data in a way that allows multiple stakeholders to confidently and securely share access to the same data and information. By maintaining a chain across a distributive network, attempting to alter that chain (making an unauthorized transaction or changing account information) would require such a large amount of processing power that it would be theoretically impossible.

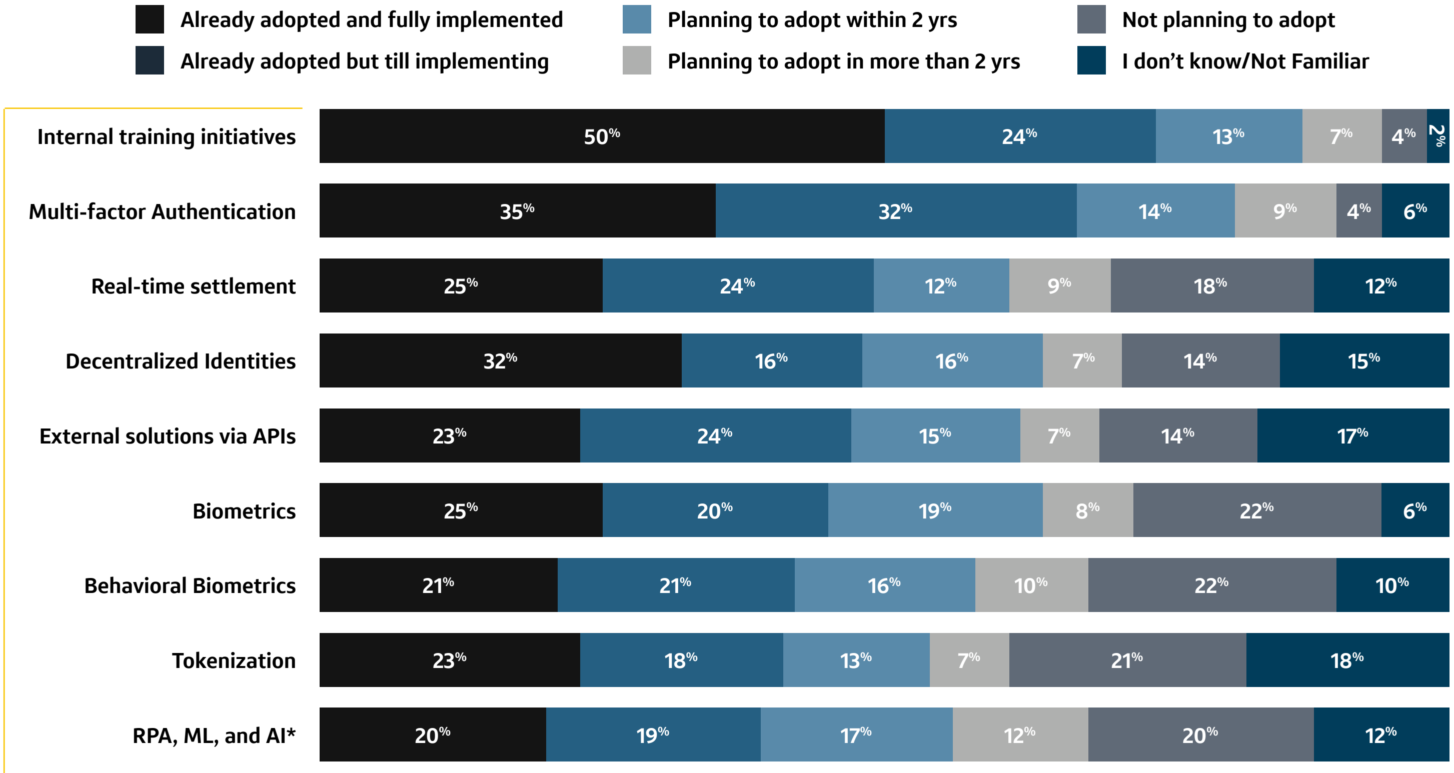
Processing transactions and internal processes across a blockchain could help secure sensitive information.

According to a 2018 Gartner survey, blockchain adoption rates among all industries are barely detectable—1% today and only 8% expected by surveyed CIOs in the short term.[9]

> As companies continue to adopt and implement these technologies, they need to stay vigilant and study the potential ways these technologies could be manipulated or exploited by bad actors. While these technologies present new ways to combat fraud, criminals will be working tirelessly to undermine them.

Technology Adoption to Enhance B2B Payment Security

Has your organization adopted or is planning to adopt the following technology/tolls to enhance B2B payment security?



*Robot Process Automation, Machine Learning, and Artificial Intelligence

Source: 2019 B2B Payment Security Survey

50% of all respondents have already adopted at least one of the listed technologies

The Human Link

For a mid-sized business, many technological advances may not be immediately available. Access to resources—capital, employees, time—make updating security systems difficult, thus they turn to employees as the main line of defense against fraud. Even for companies that are focused on implementing some of these new technologies, these tools are only as good as their weakest link, which in many cases are the humans involved.

Employees may not be properly equipped to fight on the front lines. In some cases, malicious insiders can breach systems to make unauthorized payments to themselves or sell information to criminals completely unbeknownst to their fellow employees. In many others, employee malfeasance isn't the result of maliciousness but rather carelessness.

> Even for companies that are focused on implementing some of these new technologies, these tools are only as good as their weakest link, which in many cases are the humans involved.

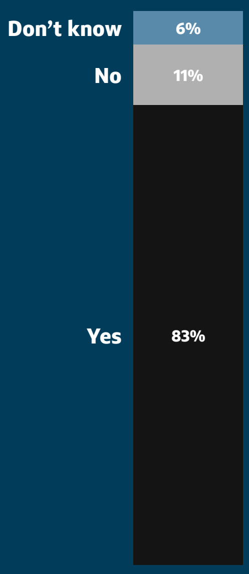
Some of the most common attacks—phishing, BEC, malware, ransomware—are often the result of an employee accidentally clicking a link that they shouldn't, responding to a fraudulent email and disclosing personal information, or visiting an unsafe website. Fraudsters excel at exploiting our human nature and will hide dangerous software in seemingly innocuous places, like websites about top searched celebrities. According to research by McAfee, Gilmore Girls' Alexis Bledel, talk show host James Corden, and Game of Thrones' Sophie Turner took the top three spots for the most dangerous celebrities on the internet in 2019.[10] And as businesses create more connected operating structures, an attack on a single device can infect the entire company as well. We found that 91% of respondents who reported fraud, had experienced at least one phishing/ BEC, malware/ransomware, or data breach within the past two years, indicating employees need to be more vigilant in recognizing and avoiding potential fraud.

Businesses are more likely to be vulnerable and fall victim to phishing and BEC attacks when employees are careless. We found that 36% of mid-sized businesses had experienced a phishing or BEC attack within the prior two years. The high incidence rate suggests that businesses are overly confident in their employees' abilities to identify suspicious messages, and are experiencing losses because of it. According to the US Federal Bureau of Investigation, BEC fraud has resulted in losses of more than $12.5 billion globally since 2018.[11]

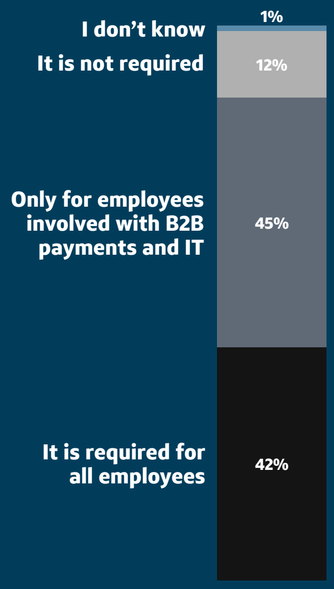
[10] https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/most-dangerous-celebrities-2019/

[11] *Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), "2018 Internet Crime Report,"* https://pdf.ic3.gov/2018_IC3Report.pdf

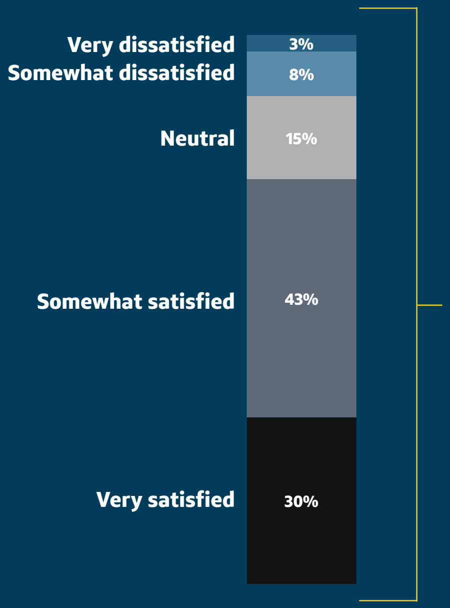
Perception of Employee Security Training
Do you think your organization's employees are properly trained to recognize and alert for fraudulent B2B payment activity for fraudulent B2B payment activity (e.g. suspicious emails, unauthorize payments, etc.)?



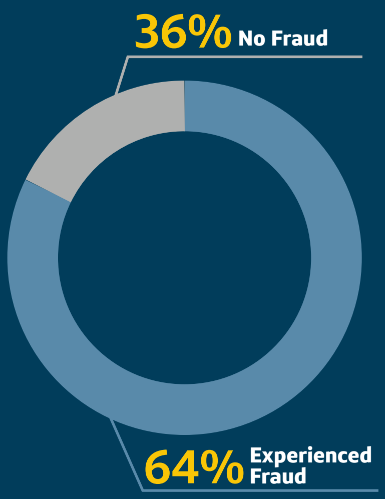
Security Training Requirement
Is B2B payment security/risk mitigation training required for employees at your organization?



Satisfaction with Employee Awareness of Security Protocol
Are you satisfied with the level of B2B payment security protocol/ risk mitigation awareness among employees at your organization in regard to B2B payments?



B2B Fraud Experience With Training
When responding yes to the first question, within the past two years, has your organization experience any of the below fraud attacks in regard to B2B payments?



Source: 2019 B2B Payment Security Survey

And it's not just lower and mid-level employees who constitute a risk. One study found that 42% of email-based cyberattacks occurred because the CEO fell for a scam.[12] So, even changing the behavior of a few key executives could dramatically reduce a company's risk of phishing / BEC fraud.

All of this information begs the question, "If fraud is so common, why aren't companies educating their employees?" The answer is, they are, just not well enough. Three-fourths of respondents reported already adopting internal training initiatives, and 83% felt that their employees were properly trained to recognize and raise alerts for fraudulent B2B payment activity. Yet, when asked who receives security training, only 42% of respondents reported that their organization requires B2B payment security / risk mitigation training for all employees.

As organizations move to fully connected systems, any individual device can become compromised and be used to perpetrate fraud, putting the entire company's systems at risk. Thus, companies need to train all employees, regardless of function or level. If you only train employees from the payments and IT areas, you are leaving your company more vulnerable than it needs to be.

In addition to employee education initiatives, companies should reevaluate their current payment processes and take steps to automate steps wherever possible, to lower the chance of human error. In places where human action is needed, they should make sure the proper controls are in place. This approach should also be taken when implementing new processes.

[12] *PYMNTS.com, "2017 Midyear Security Roundup" report*

In addition to employee education initiatives, companies should reevaluate their current payment processes and take steps to automate steps wherever possible, to lower the chance of human error. In places where human action is needed, they should make sure the proper controls are in place. This approach should also be taken when implementing new processes.

Protecting Your Company Against Fraud

Our research points to three unfortunate truths that mid-size companies should consider when making decisions about their payment security operations:

- **Fraud is increasingly pervasive,** yet companies are often complacent and hold on to the status quo. A study from PYMNTS.com and Stripe found that fraud-related costs amount to 2.2% of annual revenues.[13] For the average mid-sized company that translates into $33 million in losses. That number is nothing to be complacent about.
- **Mid-sized companies are already paying a price.** Our study found that about 66% of respondents had experienced some form of B2B payment fraud within the past two years. About three-fourths reported losses; 42% reported losses above five basis points.
- **Cyber criminals are looking for the low-hanging fruit. That could be you.** Fraudsters may start to target mid-sized companies because they do not have the advanced security of larger firms, yet are still high value. Cyber-criminals don't care if their multi-million-dollar fraud payday comes from a large multi-national or a smaller regional company.

Insurance is a Band-aid Not a Cure-all

It is beneficial for mid-sized companies to seek insurance coverage against fraud. Nevertheless, it is important to state the obvious: Insurance doesn't eliminate the risk. (See sidebar.) Recent attacks have become so large that even the most comprehensive policy will not cover losses entirely.

In addition, insurance companies are not allowing themselves to become the sole protection against fraud losses. Carriers are requiring policy holders to increase their security capabilities and enhance their technology to retain coverage.

Will Insurance Improve Your Loss Rate?
Our research found that loss rates did not vary significantly between the total sample and respondents who reported having sufficient fraud insurance coverage. This underscores the fact that insurance by itself is not the cure to mid-sized companies' fraud woes.

Fighting Back

While the current state of fraud may seem bleak, the situation is not hopeless. There are many best practices that mid-size companies can implement to help reduce their risk of or limit the effect of an attack. The two primary levers companies can pull are (1) technology; and (2) employee awareness and preparedness.

[13] *Payments 2022 Playbook: Building A High-Performing Payments Team For Fraud Detection [PYMNTS.com study in collaboration with Stripe]*

Technology

Companies should want to become more tech-savvy to match cyber-criminals' growing prowess. To help decide which specific solutions your business should adopt, your payments and security teams should consider the following:

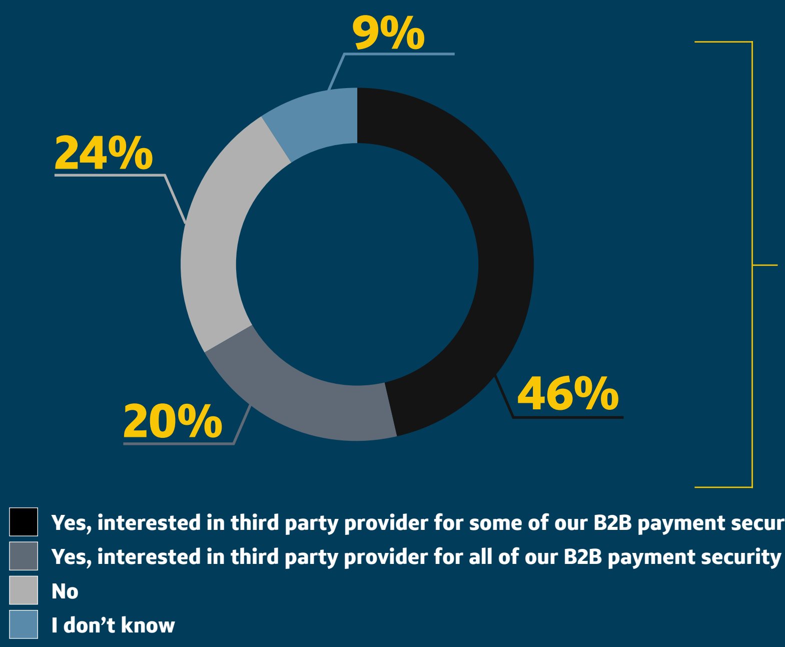
- **Agility.** Your IT and security infrastructure should be designed to be flexible and with change in mind. Technology evolves quickly, so it's vital that your business is agile so it can readily adapt to changing circumstances.
- **Leveraging ecosystem partners.** Using partnerships or managed services relationships can allow your business to access technology that you do not have the resources or wherewithal to build internally. Additionally, leveraging these relationships can also allow mid-sized companies to access the benefits of scale. Not everyone can be an expert at everything. Let experienced security professionals focus on keeping you safe, so you can focus on what makes your business great.

Two thirds of businesses reported interest in using third party providers to manage B2B security, and the overwhelming majority trust banks more than any other provider.

- **Adding MFA.** Multi-factor authentication is a relatively inexpensive and effective way to improve cybersecurity. There are many providers that offer plug-and-play MFA solutions, it does not have to be built internally.
- **Investing in intelligent automation capabilities.** Intelligent automation (also referred to as robotic process automation, or RPA) can reduce human error and free up your employees to focus on more "thinking-intensive" tasks.
- **Engaging a "red team."** Many companies are hiring white hat hackers to test the limits of their security systems. These teams can help find vulnerabilities and remedivate them before a fraudster exploits them.

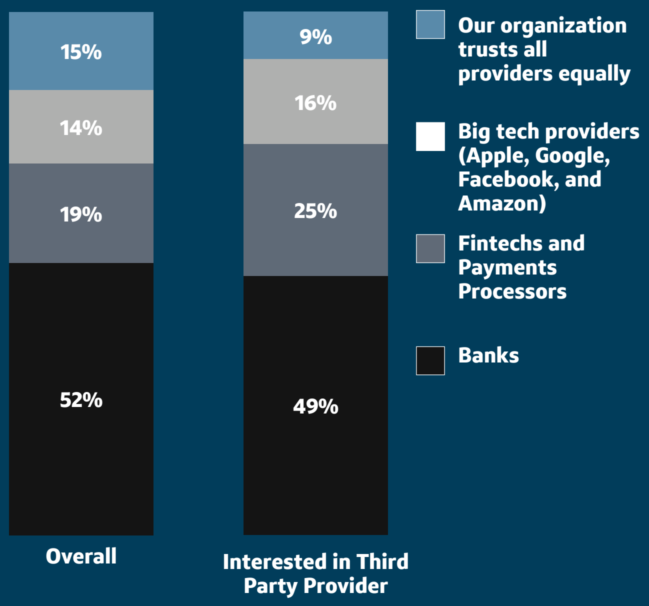
Interest in Third Party Providers

Would your organization be interested in using a third-party provider to manager your B2B payment security?



Security Provider Trust

Whom do you trust most as a B2B payments security provider? If you are interested in a third-party, whom do you trust as a provider?



Source: 2019 B2B Payment Security Survey

Employee Awareness and Preparedness

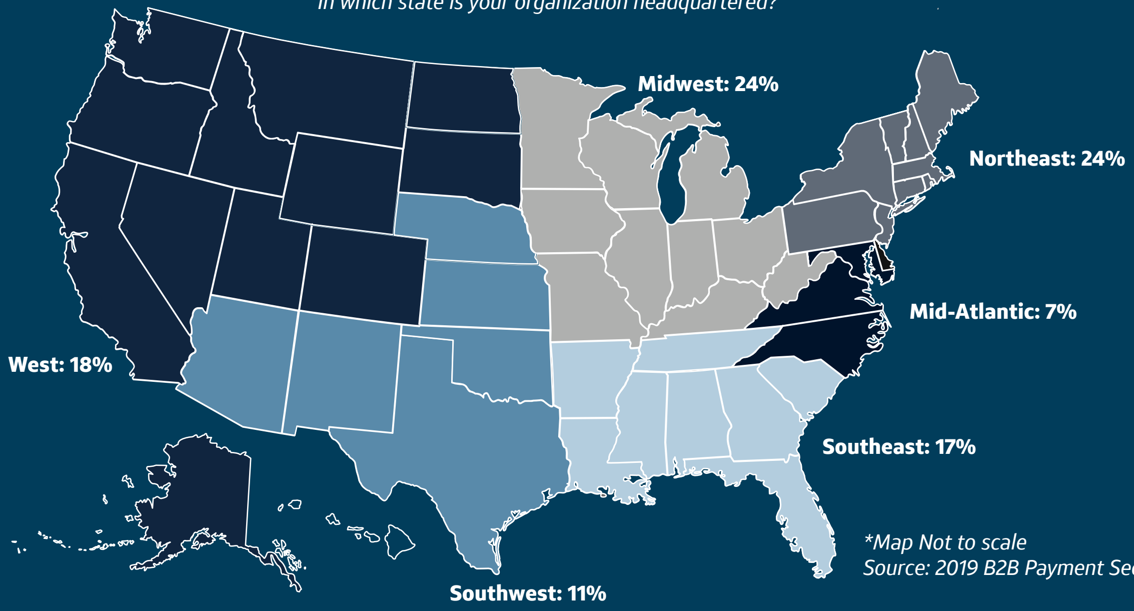
Investing in your employees may give you the most 'bang for your buck' in the fight against fraud. Making some simple changes could have a major impact on your bottom line.

- **Changing behaviors, not just information.** Learning programs about cybersecurity should move beyond the classroom, whether that classroom is physical or virtual. Educational material should not just give employees the facts about 'security best-practices,' but provide an opportunity for them to test their knowledge. Having employees complete simulations or case studies may help them when they encounter the real thing.
- **Educating all employees.** With connected and cloud systems, all company computers/devices are vulnerable. Fraudsters only need one vulnerable employee to gain access to entire systems. By educating all employees, not just the payments and IT teams, companies may be able to reduce the risk of fraudsters gaining access to or damaging the company data.
- **Limiting the use of company devices for personal use.** Limiting devices for personal use can prevent employees from exploring unsafe websites or opening a dangerous email from their personal account. If you decide to allow employees to use company devices for non-work needs, consider limiting usage to well-known sites and having a strong firewall in place. Making employees aware of the dangers involved with surfing the internet may also reduce this unsafe behavior.
- **Testing the human factor.** Having an internal team (which might include third-party providers) send out fake phishing emails or request suspicious transactions can help determine how and which employees need to improve awareness and change their behaviors.
- **Making reporting easy.** Having a built-in button for reporting suspicious emails and ensuring 'help' resources are easily accessible can increase the rate your employees alert your security team to attempted attacks. If your security team is aware of these attempts, they can be on high alert for others.
- **Balancing your priorities.** The best path forward is typically to increase initiatives across both the technology and employee learning axes. But if your budget is limited, starting with employee awareness and preparedness is often the least expensive and can yield strong results.

About the Research

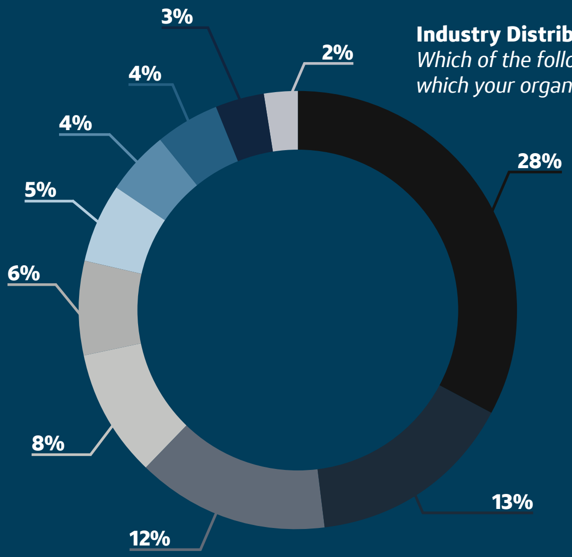
Capital One® engaged Accenture to conduct an online survey of middle market executives with financial and payment responsibilities. The survey consisted of 41 questions and for the purpose of the study, middle-market companies were defined as firms with operations in the United States with annual revenues between $50 million to $3 billion in annual revenue. The 225 responses represent this population with a margin of error of 6.5 points at 95% confidence.

Headquarters Location
In which state is your organization headquartered?



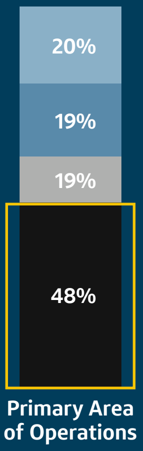
**Map Not to scale*
Source: 2019 B2B Payment Security Survey

Industry Distribution
Which of the following best describes the industry in which your organization operates?



Not all respondents visualized
Source: 2019 B2B Payment Security Survey

Operating Region
Where does your organization primarily operate?



About Us

Capital One Financial Corporation (www.capitalone.com) is a financial holding company whose subsidiaries, which include Capital One, N.A., and Capital One Bank (USA), N.A., had $262.7 billion in deposits and $390.4 billion in total assets as of December 31, 2019. Headquartered in McLean, Virginia, Capital One offers a broad spectrum of financial products and services to consumers, small businesses and commercial clients through a variety of channels. Capital One, N.A. has branches located primarily in New York, Louisiana, Texas, Maryland, Virginia, New Jersey and the District of Columbia. A Fortune 500 company, Capital One trades on the New York Stock Exchange under the symbol "COF" and is included in the S&P 100 index.

Take the Next Steps

Whether insulating your company from a disruptive event, facilitating an R&D expansion or acquiring new online and mobile payment solutions, a strong banking relationship is key. As a top-10 U.S. bank* housing a digital innovation lab, we're committed to providing you the resources, tools and expertise needed in promoting innovation across your business.

Let's discuss the possibilities.

Capital One®, National Association
299 Park Ave., New York, NY 10171

Visit **capital.one/tm** to learn more.

Capital One®

*Note: Rank excludes banks with high non-loan asset concentrations: Goldman Sachs, Morgan Stanley, BONY, State Street, Charles Schwab. Ranks as of 12/31/2019. Based upon total gross loans and total aggregated domestic deposits for bank holding company. Sources: SNL, FDIC, company reports.