



PROTECTING PAYMENTS.

New Challenges to Treasury



DEBBI DENISON

Senior Consultant, Strategic Treasurer

MELODY HART, CPA, CTP, FP&A

Senior Consultant, Strategic Treasurer



WHAT.

A review of the processes and controls to protect payment processes.



WHEN.

Thursday, October 15, 2020
12:45 PM – 1:45 PM EDT



WHERE.

Live Online Presentation
Replays at StrategicTreasurer.com



FP&A

Certified Corporate
Financial Planning &
Analysis Professional



This presentation is provided by Strategic Treasurer to Ft. Worth AFP

SPEAKERS.

GET TO KNOW YOUR SUBJECT MATTER EXPERTS.



DEBBI DENISON

Debbi has over two decades of experience at the senior level in corporate treasury, with global, multinational and Fortune 500 corporations. Her industry experience includes utility, airline, consumer products and pharmaceuticals. As a senior leader, Debbi is responsible for leading client projects and relationships across working capital, cash management, liquidity management, treasury technology and risk domains. She is one of the firm's primary trainers at client and industry events covering a range of executive and operational topics. Debbi is a SWIFT Certified Trainer.

Debbi received her MBA from Kennesaw State University following a BA in Finance from Georgia State University. She has served on the Board of Directors at Crohn's & Colitis Foundation (CCFA) – Georgia Chapter, and is a past officer of The Association for Financial Professionals – Greater Atlanta.



MELODY HART

Melody has over 30 years of global treasury experience at a senior level, including as a Treasurer, covering a variety of organization types, including consumer products, automotive, and retail. She is recognized as an expert in streamlining processes, instituting controls and policy, managing financial risks, evaluating credit and liquidity needs, and negotiating favorable credit terms, as well as managing diverse and complex financial systems and processes.

Melody is a member of the Northern Ohio Association of Financial Professionals. She received her MBA from Keller Graduate School in Chicago. She has a BS in TV Journalism from Bradley University in Peoria, Illinois, and studied Corporate Financial Management and Pension Benefits Management at the University of Michigan's Executive Education Program.

TOPICS OF DISCUSSION.

KEY AREAS OF FOCUS &
ANALYSIS.



FRAUD IN CONTEXT

Recent statistics on treasury fraud.



PROACTIVE

Preparing for payment and fraud attacks before they strike.



EFFECTIVE TRAINING

Training and cross-training your team at all levels domestically & globally.



PROTECTION

Activities receiving focus during COVID-19 crisis.



UPDATE

Review security policies and procedures.



LOOKING AHEAD

Best practices, training, and plans.



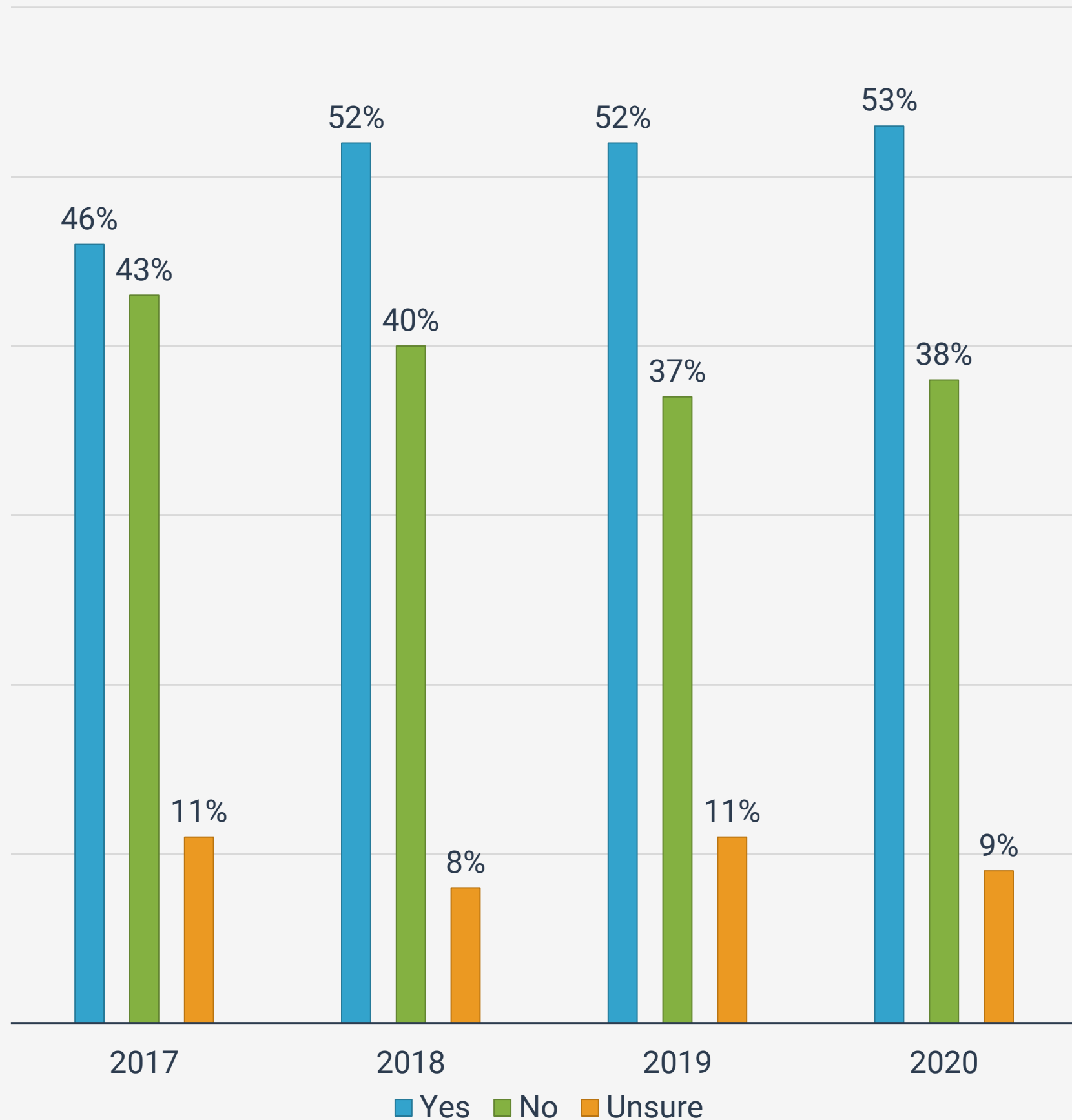
SECTION 1

FRAUD IN CONTEXT

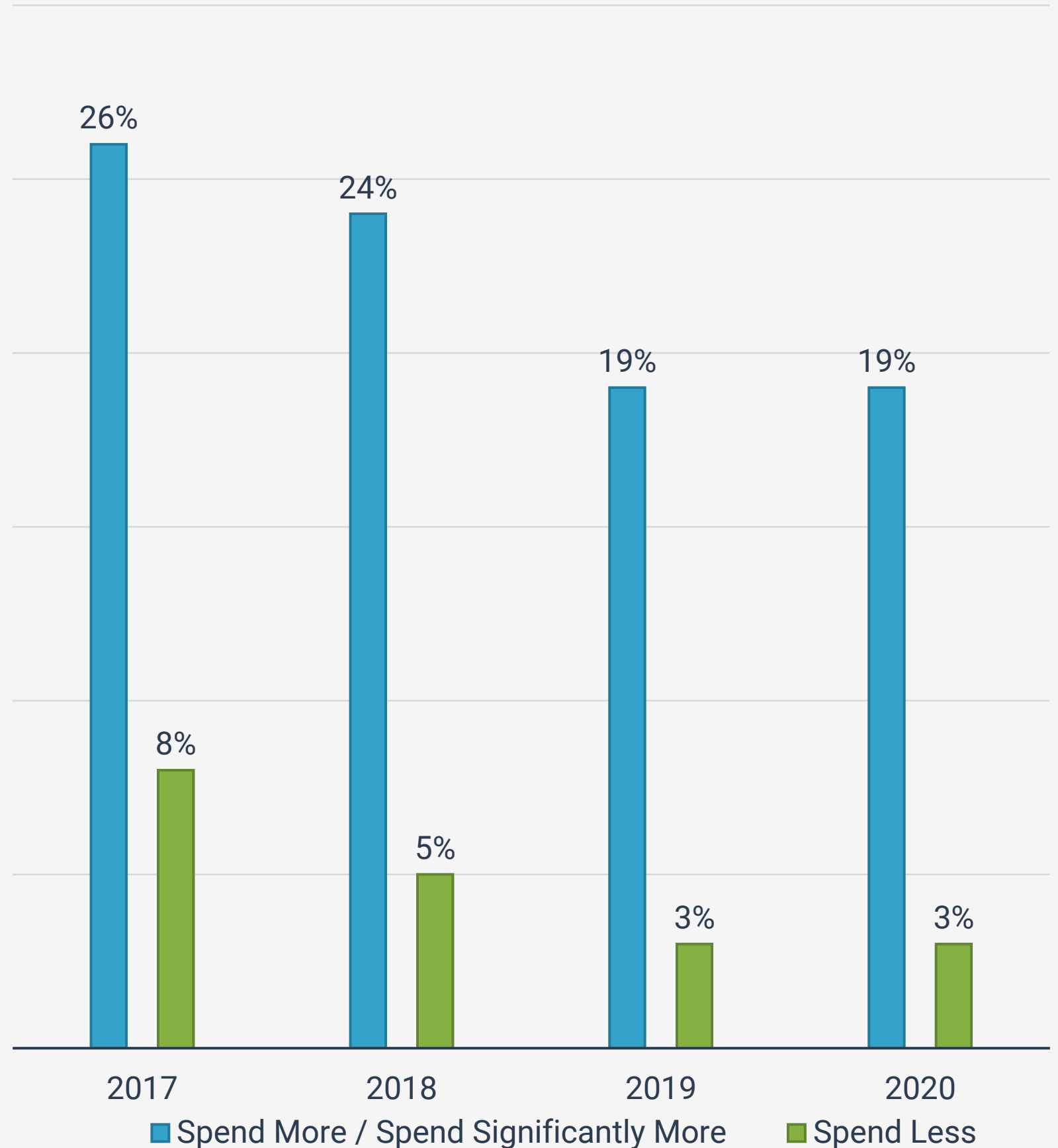
BEING PROACTIVE IS NECESSARY.

Criminals Are Not Giving Up!

» Have you experienced fraud in the last 12 months?



» What are your spending plans for treasury fraud prevention, detection, and controls?

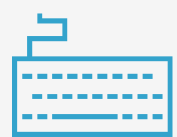


CRIME PAYS.

Leaders in Success.

Automation has helped the criminals scale their attempts and is clearly outpacing high-touch and high-exposure attack methods. The larger payoffs are attracting more sophisticated criminals who want to ensure that crime keeps paying.

Fraud Type	Success Rate
BEC	18%
Ransomware	19%
System-Level Fraud (System Takeover)	20.5%
Wire Fraud	23.5%
Check	25%



Leverage Automation



Target Weak Areas



Secure Medium to Large Payoffs

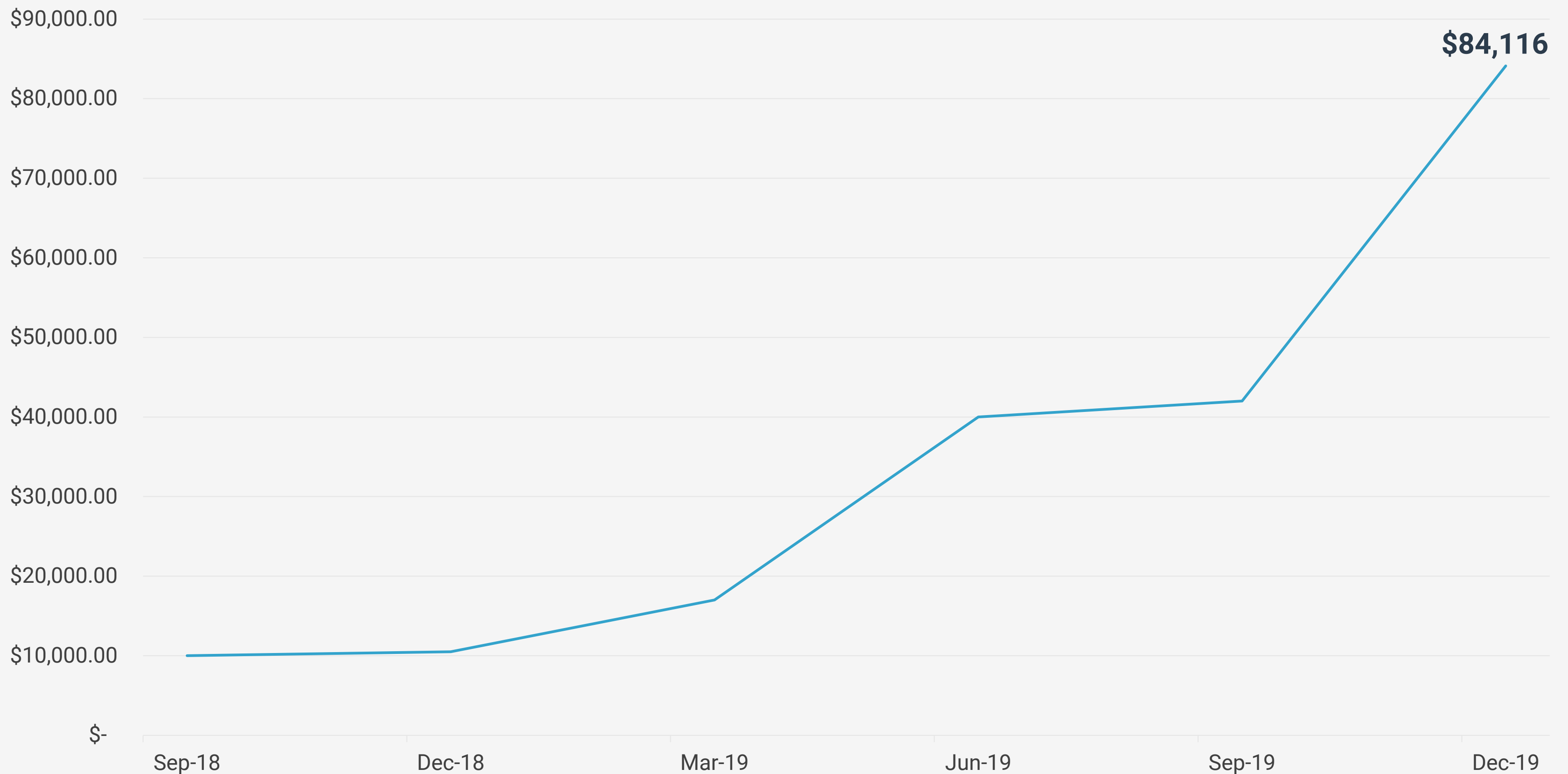


Go Where the Money Is

STRATEGIC BLACKMAIL.

Payment to Release Files Spikes.

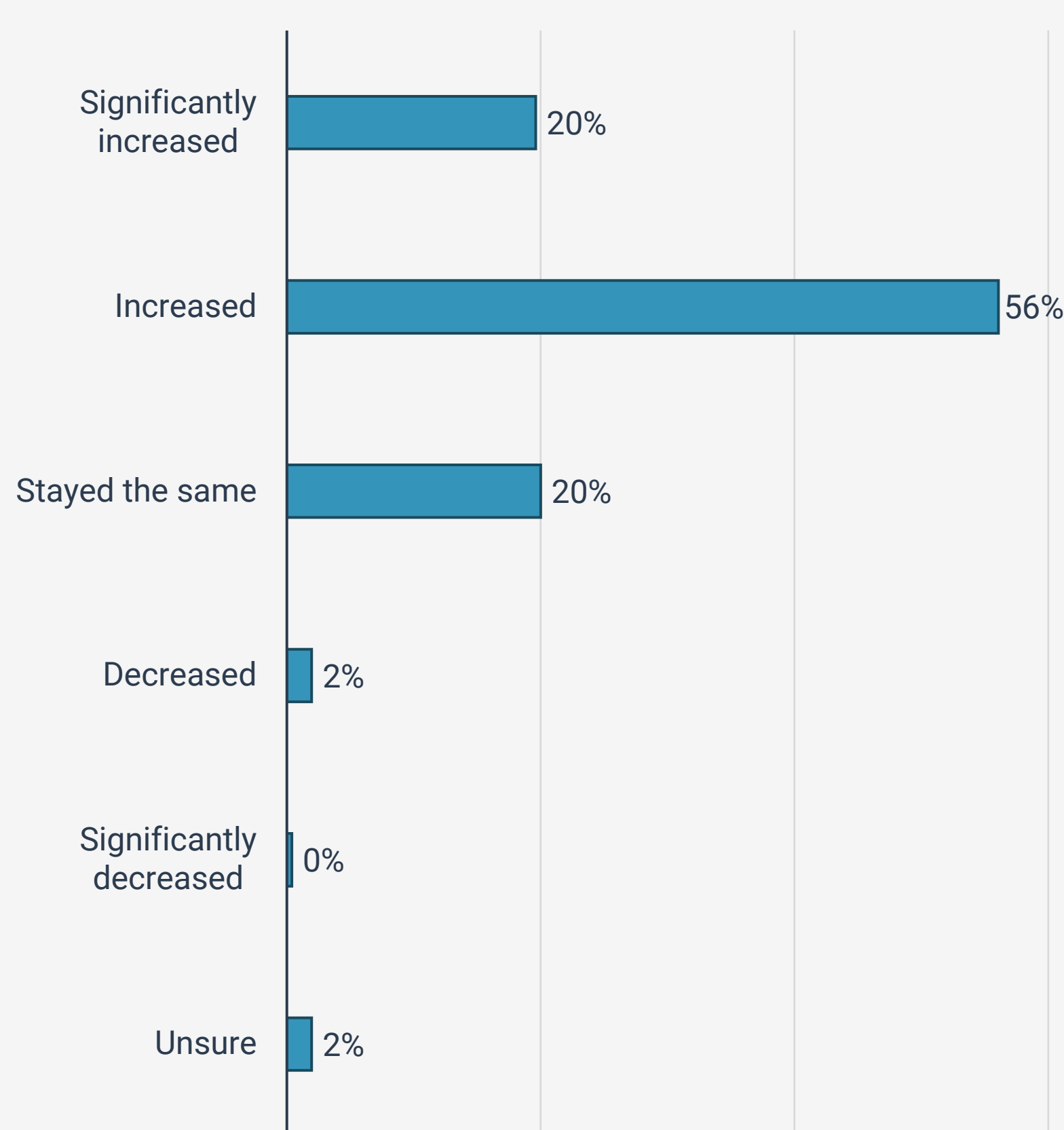
Average Payment Made by Ransomware Victims



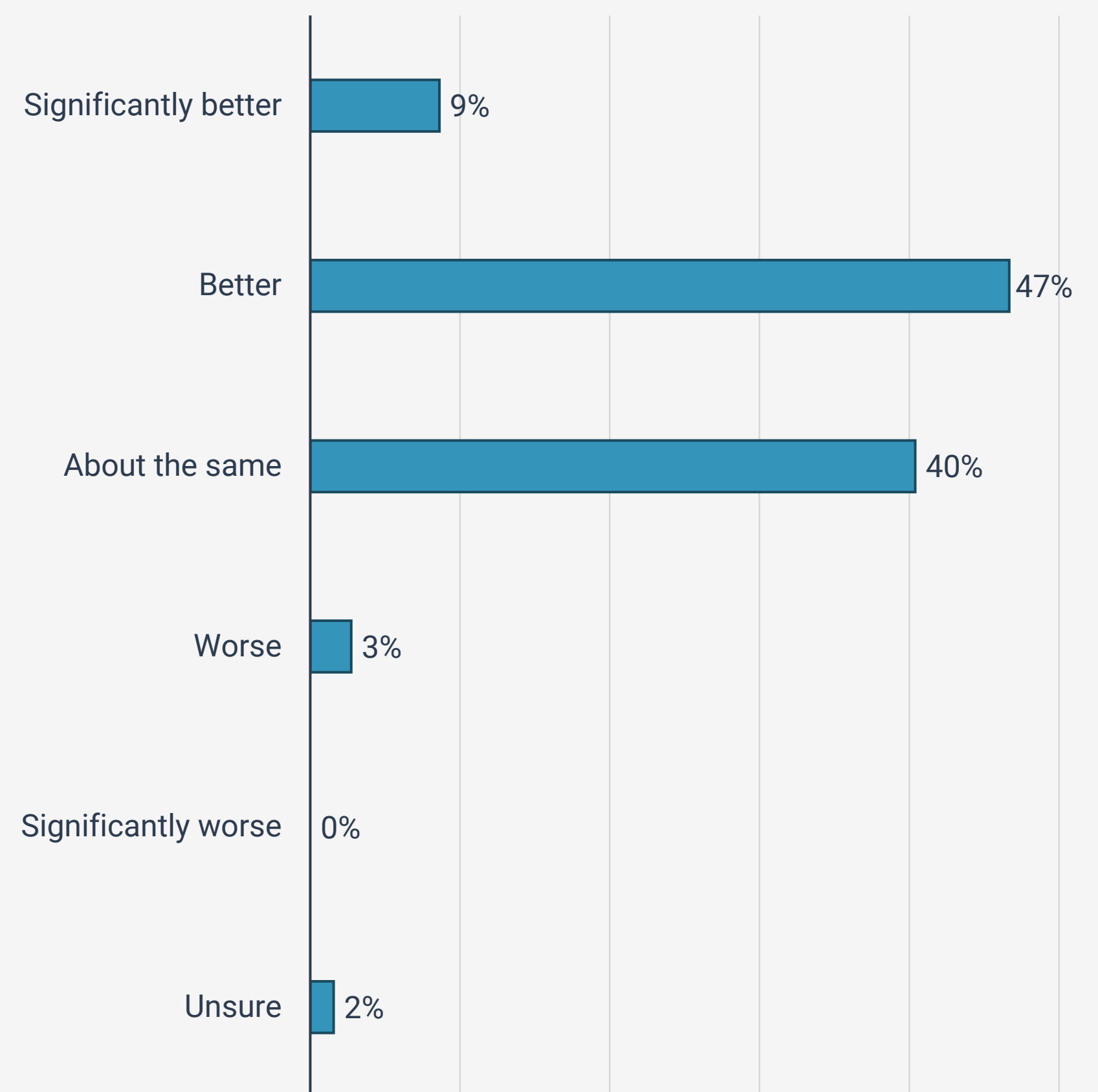
AWARE & PREPARED.

Threat Level vs. Confidence.

» In the past year, I think that the threat level of fraud has:



» With regard to the threat level associated with fraud and considering our current security posture, we are in a(n) _____ position as compared to last year.

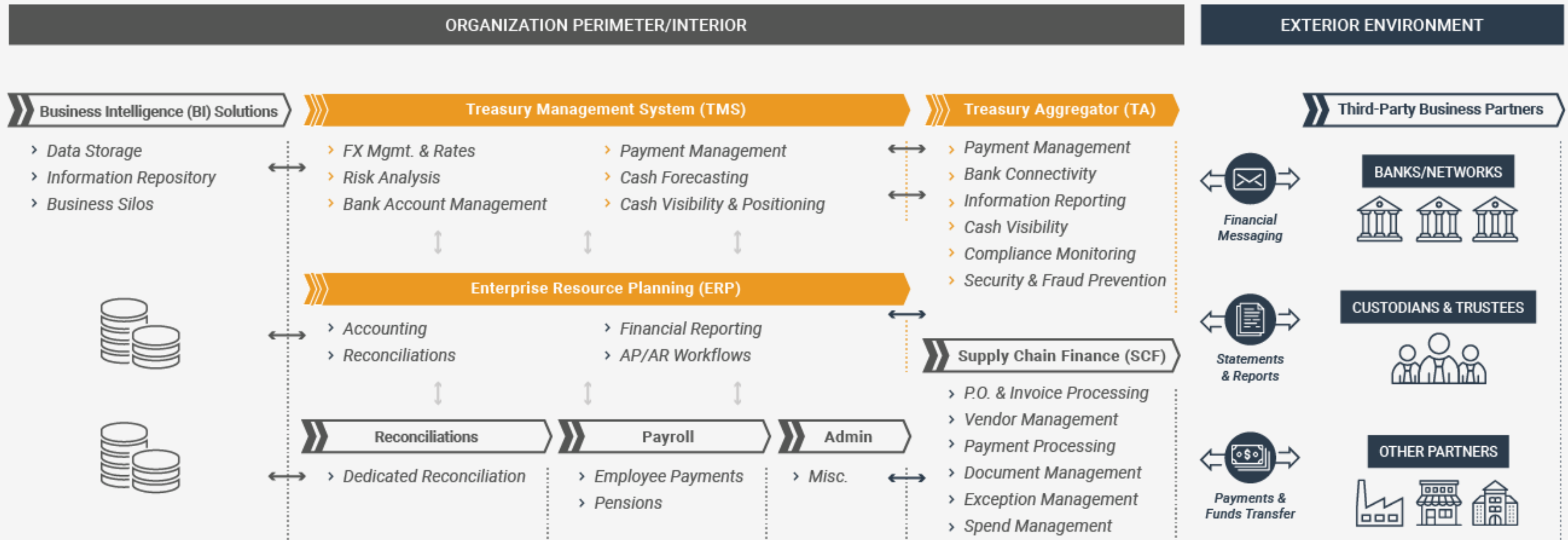




SECTION 2
PROACTIVE

THE FRAUD BATTLEFIELD.

Are You Prepared?

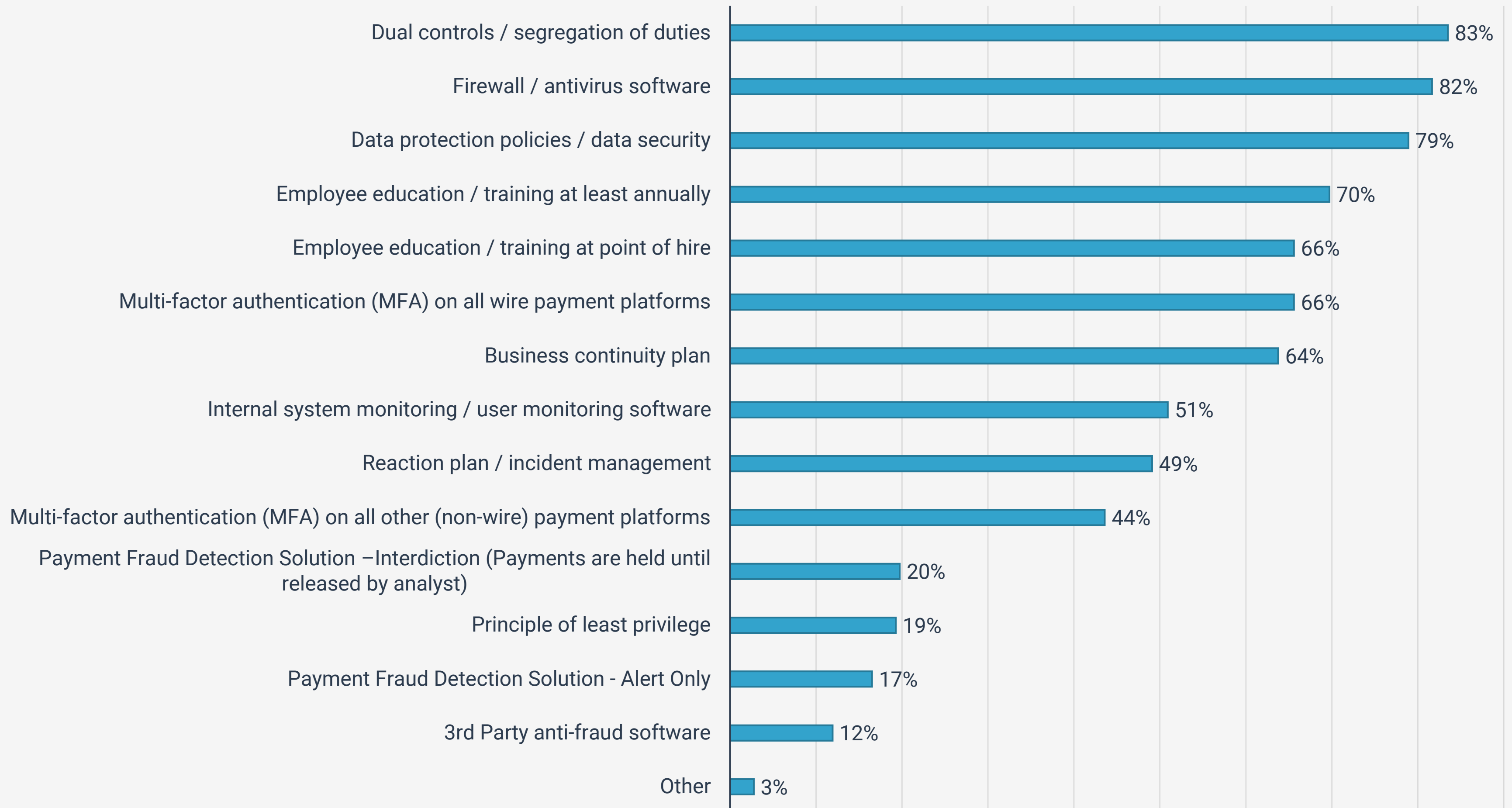


Managing the Full Scope of Exposures. Considering the entire scope of back-office solutions, workflows, and processes that comprise any organization's internal architecture, it is understandable that complications regarding the development of a comprehensive security framework would arise. Each system represents a potential exposure point, and personnel (both IT and individual users, including treasury) must ensure that access to the system is restricted and that workflows are designated in such a manner that a single employee or actor cannot override the controls. Additionally, there are elements of the exterior environment (business partners, information in transit, etc.) where exposures arise and fraud can occur; these areas must be evaluated as well if a comprehensive controls framework is to be developed.

LOOKING AT PREVENTION.

Room for Improvement.

» What controls do you have in place to prevent fraud? (Select all that apply)



WFH FRAUD INCREASE

ARE FRAUD ATTEMPTS REALLY INCREASING?

Five out of nine companies increased their communication about fraud/attempted fraud since moving to the Work from Home (WFH) posture.

Was this an overreaction? When we look at the fraud issues, the concern seems to have been well-founded. Of those who knew, more than one-third of respondents indicated that there had been an increase.

Additional communication, compensating controls and enhanced training seem to be in order in the new environment.



Fraud Communications

Has your team's communication about fraud / attempted fraud changed in the WFH environment?

Yes.

The communication level has increased **55.7%**



Fraud Attempts

Has your organization seen a change in attempts of fraud or cyber-fraud? (Other than unsure)

Yes.

An Increase of **36%**

No.

About the same **64%**



SECTION 4

EFFECTIVE TRAINING

TRAINING PAYOFF.

Investing in the Human Element.



The Payoff








There are several strong correlations between lower losses and organizations who train their employees on payment fraud, controls and cyberfraud. These firms have a dramatically lower frequency of reported losses than their non-trained peers. For those that DON'T train their employees, here is the factor for losses:

- ✓ **1.5x** Payment Diversion Fraud
- ✓ **2x** ACH fraud
- ✓ **2.5x** System Level Fraud (system takeover)
- ✓ **4x** Business Email Compromise
- ✓ **4x** Bank Mandate Fraud
- ✓ **5x** Cyberfraud/Malware
- ✓ **5x** Ransomware








EVALUATING CURRENT INDUSTRY SECURITY PRACTICES.

Technology vs. Human Security Coverage. While many organizations have begun placing a closer emphasis on their technology security components, there has been less headway made in the area of human (staff/personnel) security training and awareness. Given the prevalence of BEC schemes and other criminal tactics that count on human error and confusion to provide payouts, the human element of security must be given further attention, particularly within the corporate realm.

Technology Security Components

-  **Firewall & Antivirus**
-  **Multifactor Authentication**
-  **User Monitoring Tools**
-  **Biometrics**
-  **Encryption**
-  **Tokenization**
-  **SAML 2.0**

Human Security Components

-  **Security Training**
-  **Employee Testing**
-  **Whistleblower Policy**
-  **Clean Desk Policy**
-  **Dual Controls**
-  **Segregation of Duties**
-  **Principle of Least Privilege**



SECTION 3
PROTECTION

WHAT SHOULD TREASURY LOOK LIKE?

THE SCOPE OF PAYMENT SECURITY.

What Should Treasury Security Look Like?

- An efficient and effective treasury security framework provides coverage at every juncture throughout treasury's day-to-day workflows and operations.
- This includes a robust "perimeter," as well as encryption of data when it is in transit and ensuring that vendors and business partners are adhering to stringent security procedures as well.
- Both human and technology components should be evaluated so that systems are kept secure and staff know how to identify fraud and what to do in the event of a breach.

Developing a Comprehensive Security Framework

Internal Files in Transit

Data accessed through a cloud or SaaS solution should only be available to recognized/verifiable users, and protected via VPN/SFTP connections.

CLOUD-BASED STORAGE

Most data centers in use today have received SSAE 18 (SOC 1 & SOC 2) certifications, meaning they are annually inspected and approved by an independent third-party.

BANK INFORMATION

Payment details and statements routed from a bank are typically encrypted using the bank's security components.

CORPORATE PERIMETER

Corporates must protect information used within their perimeter through the installation of robust firewalls and anti-virus protection, as well as regular staff training and testing on new fraud and security developments.

BANK SECURITY

Banks typically provide and manage their own security components for sending and storing payment details and client information.

Files in Transit

To protect information in transit, common industry practices include hashing payment totals, use of e-signatures to lock payment details, and use of VPN or SFTP secure connections.

INTERNAL SYSTEMS

Entry to a company's internal systems, including TMS and Aggregator portals, should be secured using a "multifactor" approach, such as username/password combination coupled with a unique USB or key fob.

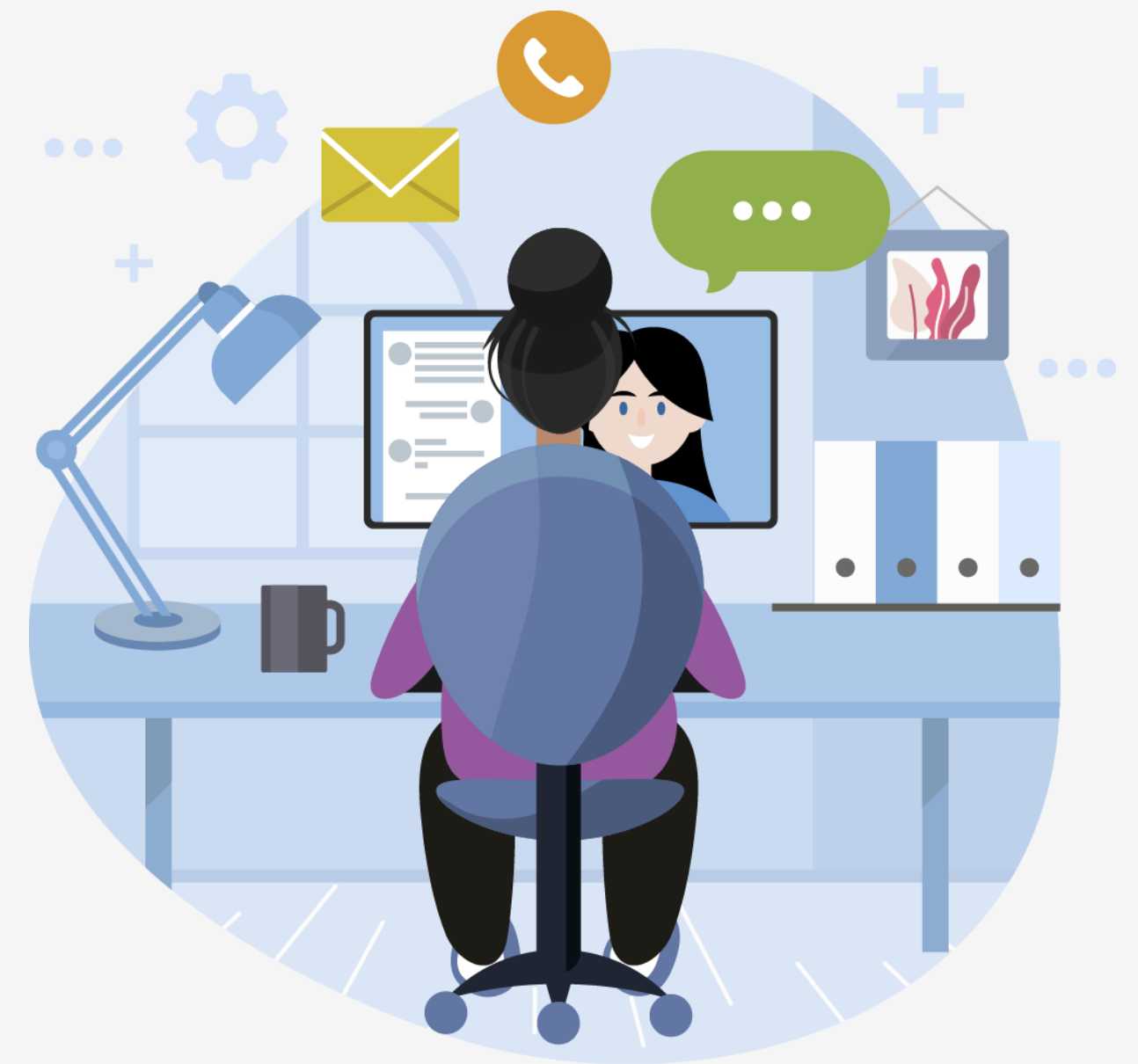


PROTECTION IN A WFH ENVIRONMENT.

A Change Some Were Not Fully Prepared For.

Activities Receiving Focus During COVID-19

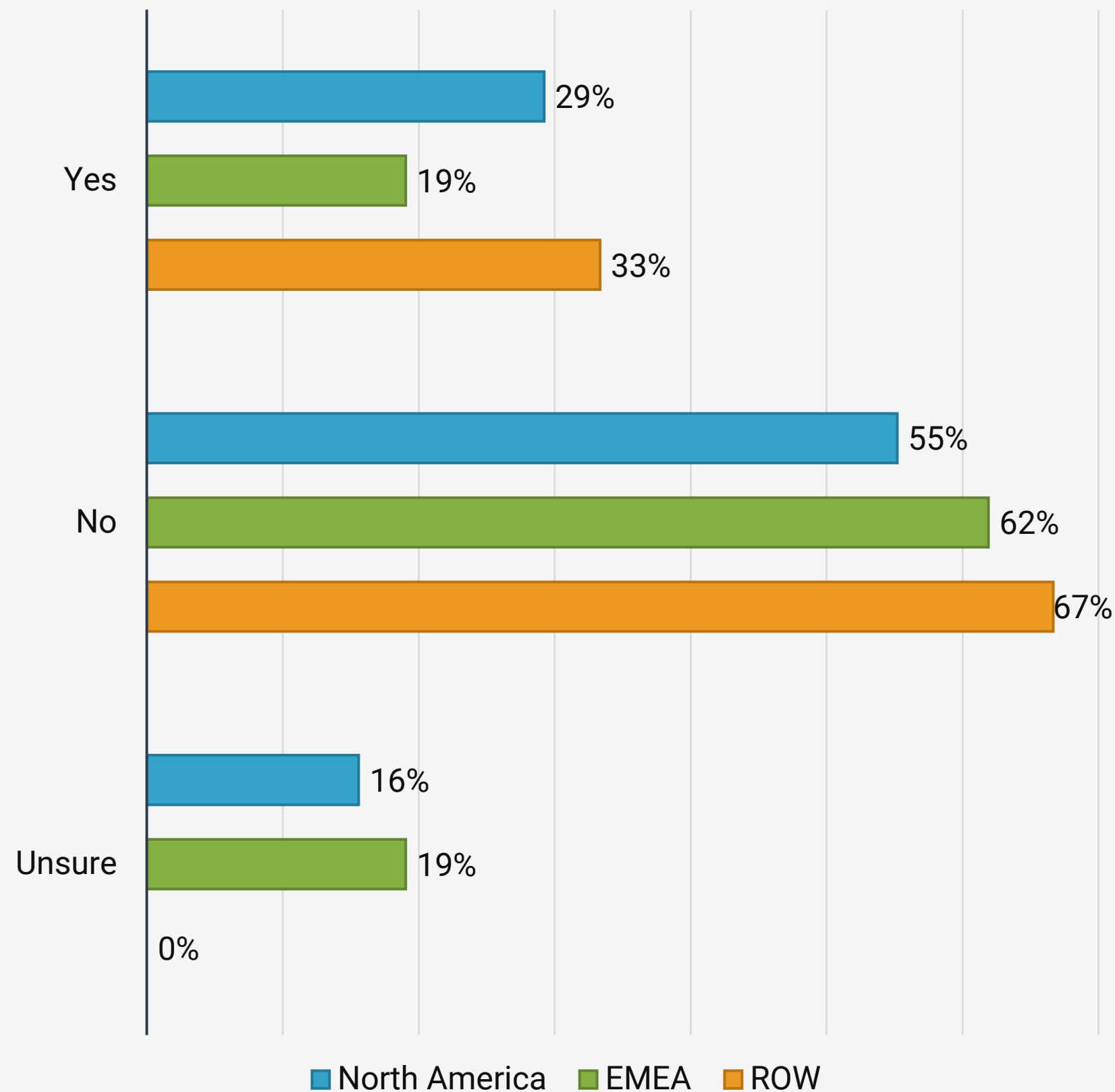
- The completeness of Business Continuity Plans and security framework were immediate concerns in the mass transition to WFH.
- 81% of respondents indicated that projects HAVE been reconsidered due to the current crisis. Of those with reconsidered projects, 40% were increasing their attention to Payment Process / System Security. Another 28% were increasing their Payment Security Training.
- The importance of cross-training became very evident with concerns of multiple team members becoming sick or being out caring for ill family members. Deepening the bench strength is needed in many organizations.
- Managing staff responsibility in a WFH environment and accessing all necessary IT applications from home were two challenges identified by about half of respondents.



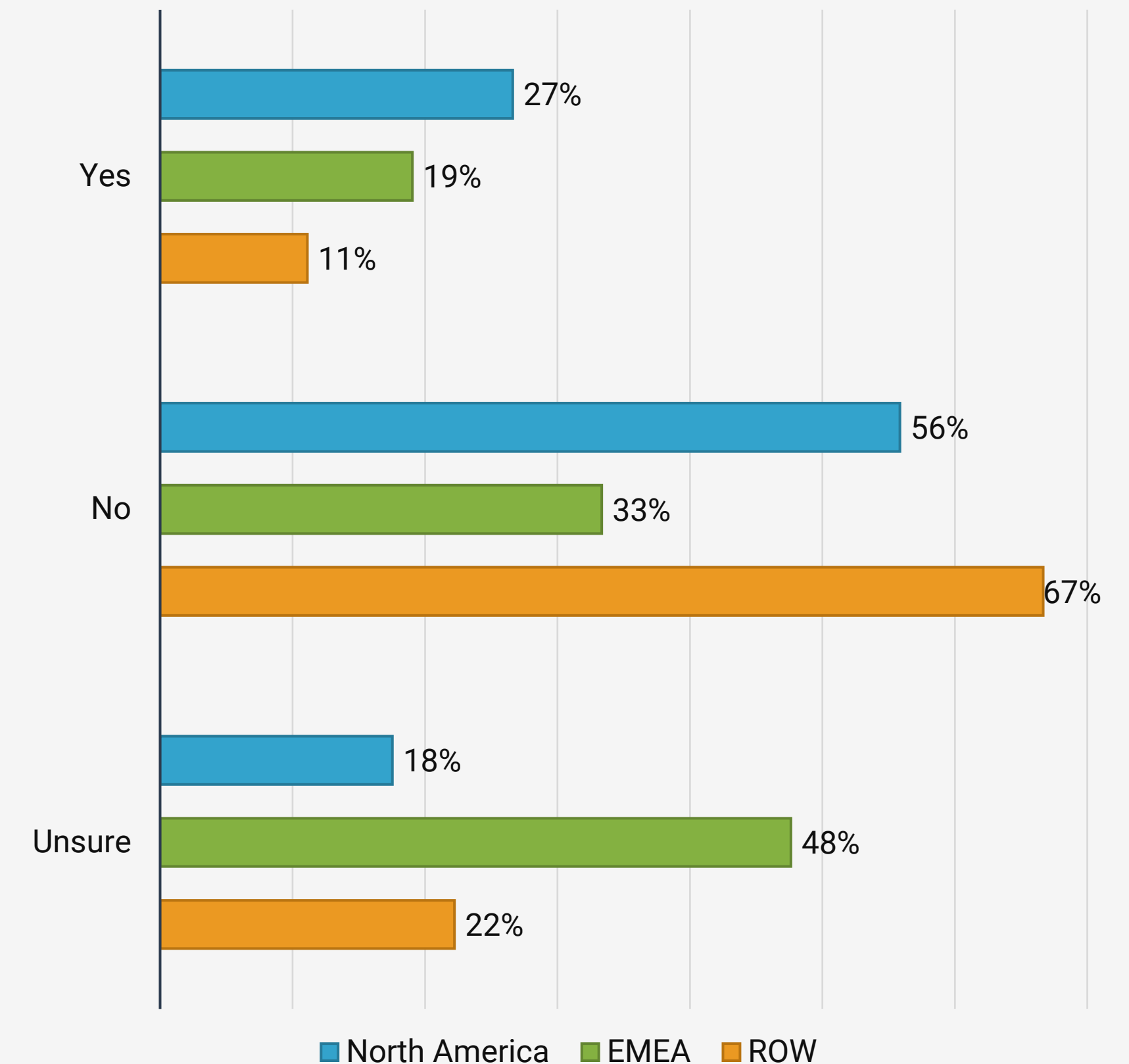
THE PAYMENT HAS LEFT THE BUILDING.

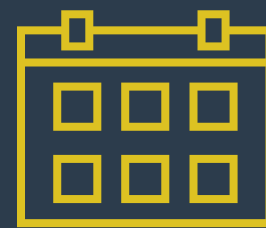
Some Get Lucky.

» Do you utilize a payment monitoring solution that will detect potentially fraudulent payments BEFORE they leave the building?



» Have you had a prior ACH or Wire Fraud that left the building?





SECTION 5
UPDATE

REVIEW & UPDATE.

Evaluate Security Policies and Procedures From Top to Bottom.

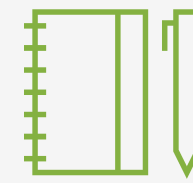
Why have a policy? A simple, focused and easily understood policy is an effective way to illustrate your organization's commitment to combat fraud.

Communicate plan to all staff (FT & PT), contractors and suppliers.



IDENTIFY AREAS OF EXPOSURE

- Perimeter – e.g., firewall, Wi-Fi, antivirus (all devices), BYOD
- Interior – e.g., all desktops (including payment-only computers for some companies), passwords, confirmations, etc.
- Network – e.g., secure areas (access reports), security settings (antivirus, data backup), user access, etc.
- Transport: Transporting files – e.g., payment files, critical files, etc.
- Third-Party Systems – e.g., TMS, trading platforms & banking systems



DEFINE & DOCUMENT

- Actions that are deemed to be fraudulent
- Formal procedures for employees to follow if fraud is suspected
- Who is responsible for taking action and what steps to follow
- Staff procedures
- Reporting to bank
- Reporting to policy
- Frequency of ongoing training and who is to be trained
- Respond and Recover procedures



Don't Forget:

- Background check employees and contractors
- Perform ongoing training with testing

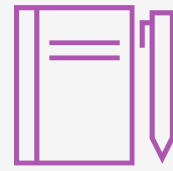


SECTION 6

LOOKING AHEAD

NEXT STEPS.

What Can Treasury Do to Protect Themselves?



EDUCATE

yourself about the methods and techniques used by criminals to initiate fraud.



IDENTIFY

inventory all the access points and areas of exposure within your organization.



DETECT

additional points of exposure externally (partners, 3rd party, etc.).



CREATE

A layered approach works best, so that multiple blocks are set up to prevent any fraud attempt.



TEST & EVALUATE

your security regularly to ensure it is up to date and running smoothly.



IMPLEMENT

If not already done, implement treasury security & fraud best practices, training, and plans.

LET'S CONNECT.

DON'T LET THE LEARNING END HERE...
CONTACT US WITH ANY FUTURE QUESTIONS.

Thank you for your interest in this presentation and for allowing us to support you in your professional development. Strategic Treasurer and our partners believe in the value of continued education and are committed to providing quality resources that keep you well informed.



STRATEGIC TREASURER

Debbi Denison,
Senior Consultant

✉ debbi@strategictreasurer.com

Melody Hart, CPA, CTP, FP&A
Senior Advisor

✉ melody@strategictreasurer.com

LIVE SURVEY



2021 GLOBAL SURVEY:
FOR CORPORATES & BANKS

Underwritten by
STRATEGIC TREASURER **Bottomline**

TREASURY FRAUD & CONTROLS

- Fraud Experience
- Structure & Bank Account Management
- Reconciliation & Visibility
- Control Framework
- Cyber Risk Management & Data Protection

CHANCE TO WIN:
One of Three \$50, \$100, \$200
Amazon.com Gift Cards

This survey seeks to evaluate the current and projected impact of fraud on the finance and treasury environment. The data is compiled annually and used to educate the industry as to how the fraud landscape is evolving, and how practitioners can better protect themselves and their organizations against attacks.

Take the Survey