PROTECTING PAYMENTS FROM FRAUD

NEW CHALLENGES FOR U.S. COMPANIES

CRAIG JEFFERY
Founder & Managing Partner, Strategic Treasurer

ALEXA COOK
Consultant, Strategic Treasurer

WHAT.
A review of the processes and controls to protect payments.

WHEN.
Tuesday, February 23, 2021
11:00 AM – 12:00 PM EST

WHERE.

Live Online Presentation

Certified Treasury Professional®

STRATEGIC TREASURER

fiserv.

This presentation is provided by Strategic Treasurer for Fiserv.

ABOUT THE SPEAKERS

GET TO KNOW TODAY'S SUBJECT MATTER EXPERTS

CRAIG JEFFERY

Craig Jeffery formed Strategic Treasurer in 2004 to provide corporate, educational, and government entities direct access to comprehensive and current assistance with their treasury and financial process needs.

His 30+ years of financial and treasury experience as a practitioner and as a consultant have uniquely qualified him to help organizations craft realistic goals and achieve significant benefits quickly.

ALEXA COOK

Alexa brings a wealth of knowledge to clients based on her domestic and global background in financial reporting, forecasting, cash management, compliance, bank fee analysis, technology solutions, connectivity, and more.

Alexa worked at a Fortune 500 automotive company and managed a full-blown technology implementation and a multilateral netting program that spanned across more than 30 countries with six different currencies. She was also selected for the company's leadership fast-track and tasked with an expatriate assignment in Germany, where she worked alongside leadership in a manufacturing plant. Alexa received a Bachelor of Science in Finance, followed by an MBA from Oakland University in Rochester, MI.

TOPICS OF DISCUSSION

KEY AREAS OF FOCUS & ANALYSIS

With fraud on the rise and payment processes scattered throughout different departments, a treasurer must function as the 'superintendent' of payment security, overseeing the policies, controls and practices others are putting into action.

FRAUD IN CONTEXT

Recent statistics on treasury fraud.

PROACTIVE

Preparing for payment and fraud attacks before they strike.

PROTECTION

Activities receiving focus during the COVID-19 crisis.

EFFECTIVE TRAINING

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

LEVERAGING TECH

Responding to the vulnerabilities.

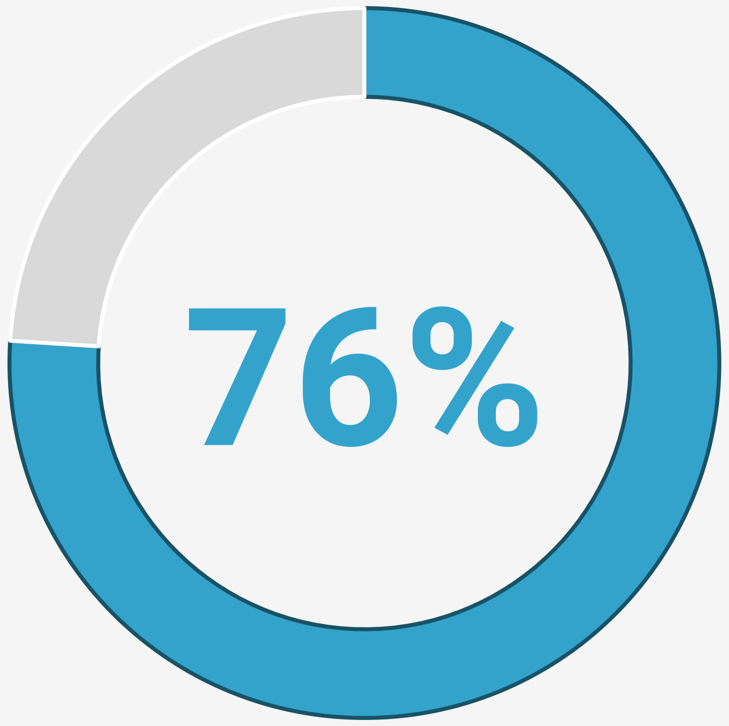
LOOKING AHEAD

Best practices, training and plans.

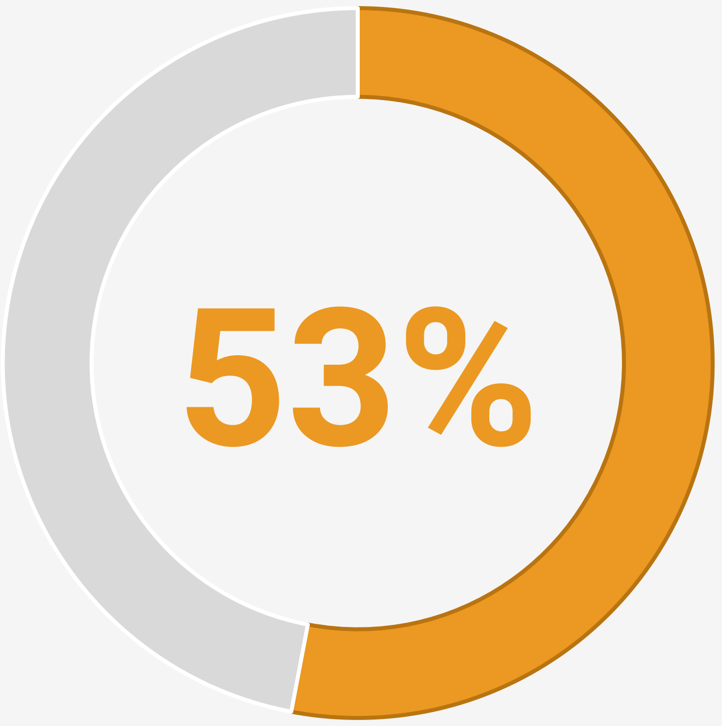
THE CURRENT STATE OF FRAUD

NOT AS SECURE AS WE THINK WE ARE

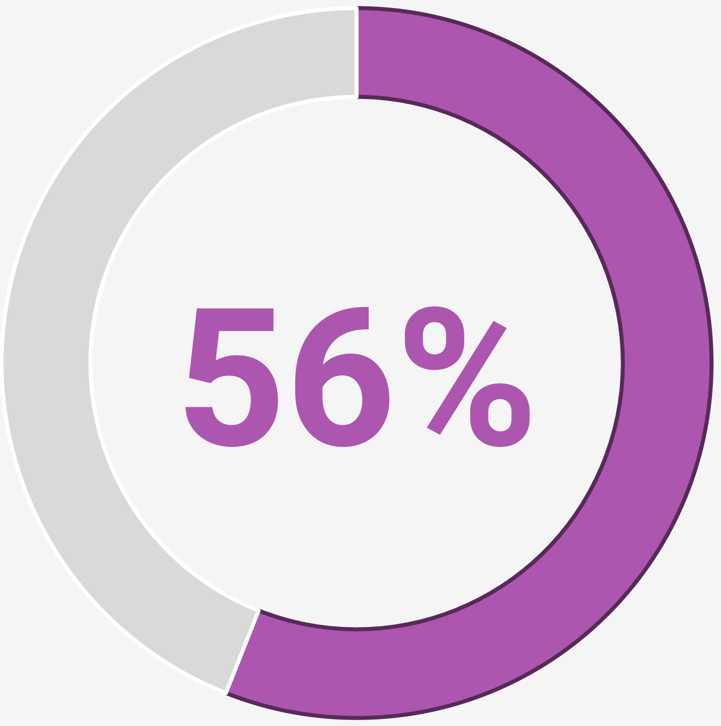
> “ *I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.* ”
>
> *- Robert Mueller, Former FBI Director*



Felt the threat level of fraud had increased or significantly increased in the past year.



Companies had experienced fraud over the course of the past year.



Stated that they were in a better or significantly better position regarding fraud compared to the prior year.

POLL QUESTION

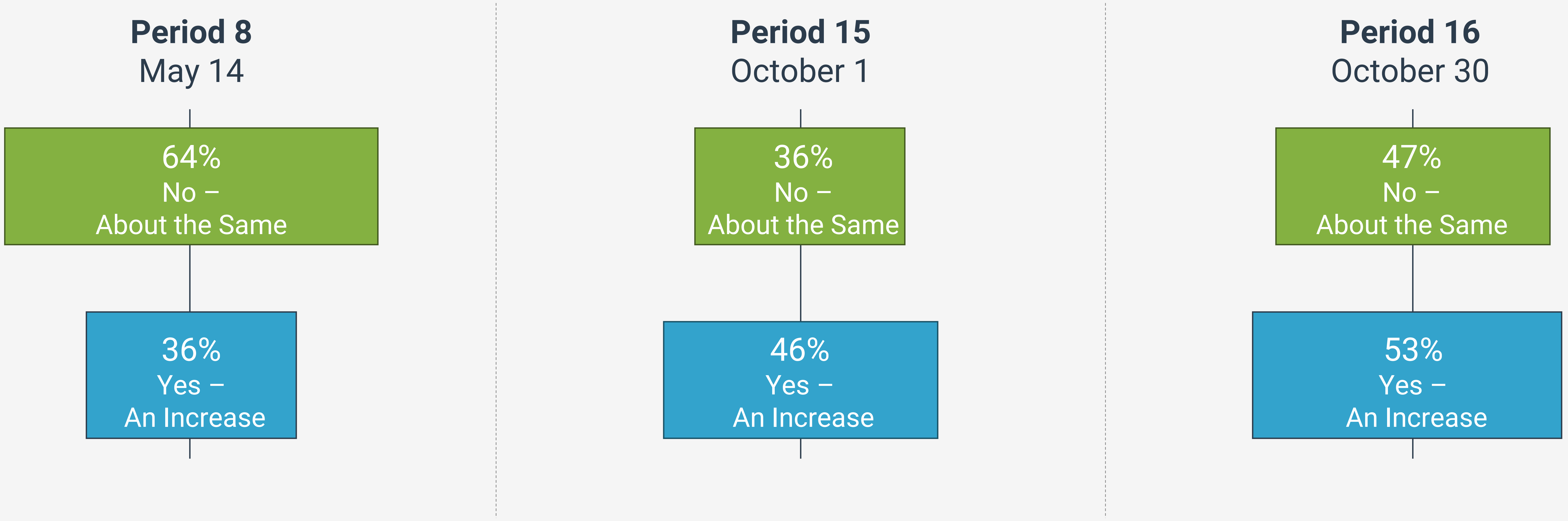
STRATEGIC TREASURER

fiserv.

FRAUD ON THE RISE

MEASURING FRAUD THROUGHOUT THE PANDEMIC

MANY SAW FRAUD INCREASE IN THE PANDEMIC. The Global Recovery Monitor Survey is an ongoing survey of the impact of COVID-19 and response of treasury. Respondents were asked if their organization had seen a change in attempts of fraud or cyberfraud at various points throughout the pandemic.



Period 8
May 14

64%
No –
About the Same

36%
Yes –
An Increase

Period 15
October 1

36%
No –
About the Same

46%
Yes –
An Increase

Period 16
October 30

47%
No –
About the Same

53%
Yes –
An Increase

Source: Global Crisis Monitor Survey, Treasury Coalition Note: “unsure” responses not displayed

#GO***STRATEGIC***

Strategic Treasurer

fiserv.

CRIME PAYS

AND CRIMINALS ARE NOT GIVING UP

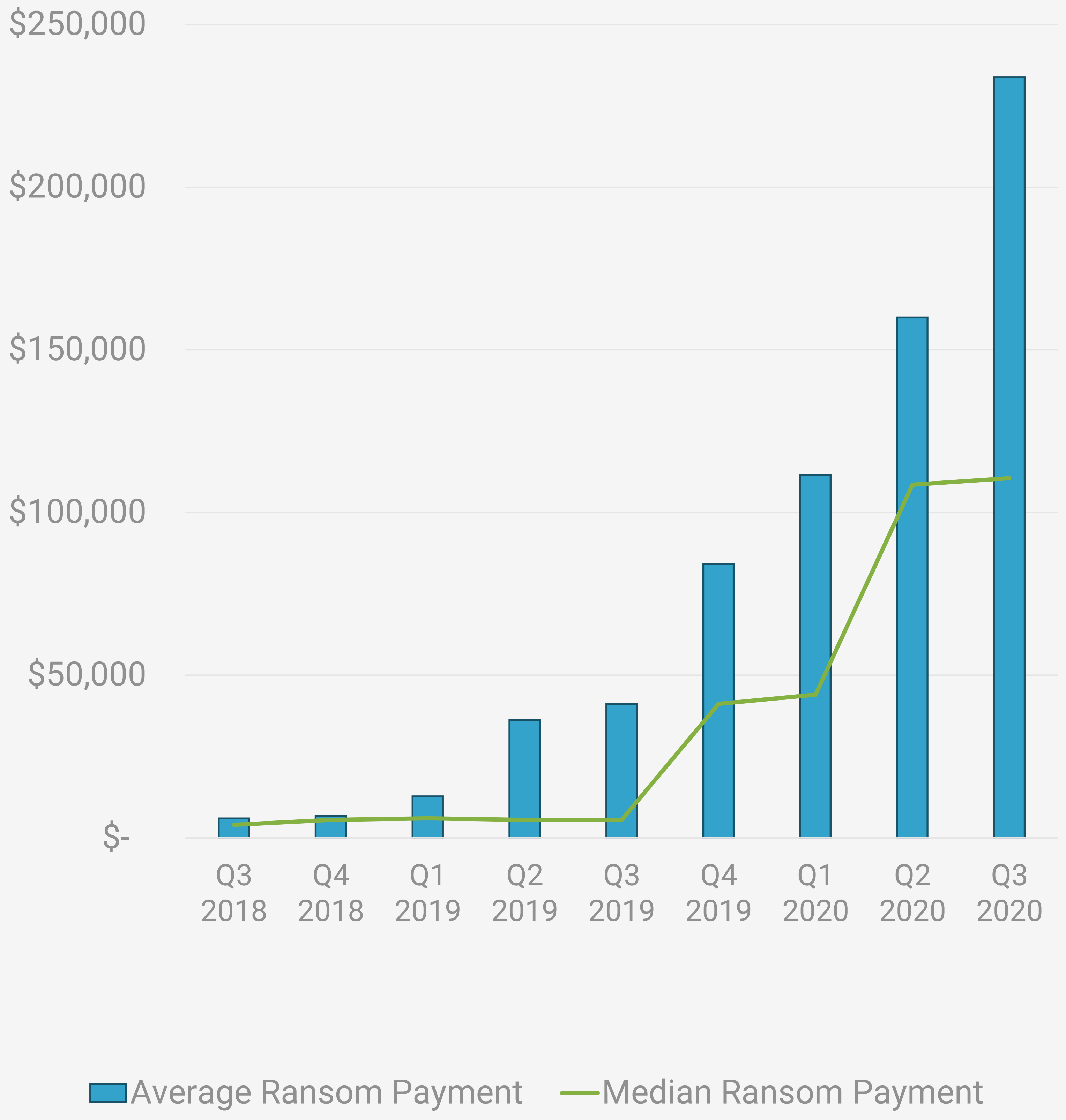
Automation has helped criminals scale their attempts and improve their success rates.

Business Email Compromise (BEC)
9 out of 10 firms experienced attempts, with 18% experiencing a loss.

Ransomware
Over a quarter of firms experienced attempts, with 19% incurring a loss.

System Level Fraud
About a third of firms experienced attempts, with 20.5% incurring a loss.

Ransom payments increase by more than a third in one quarter.



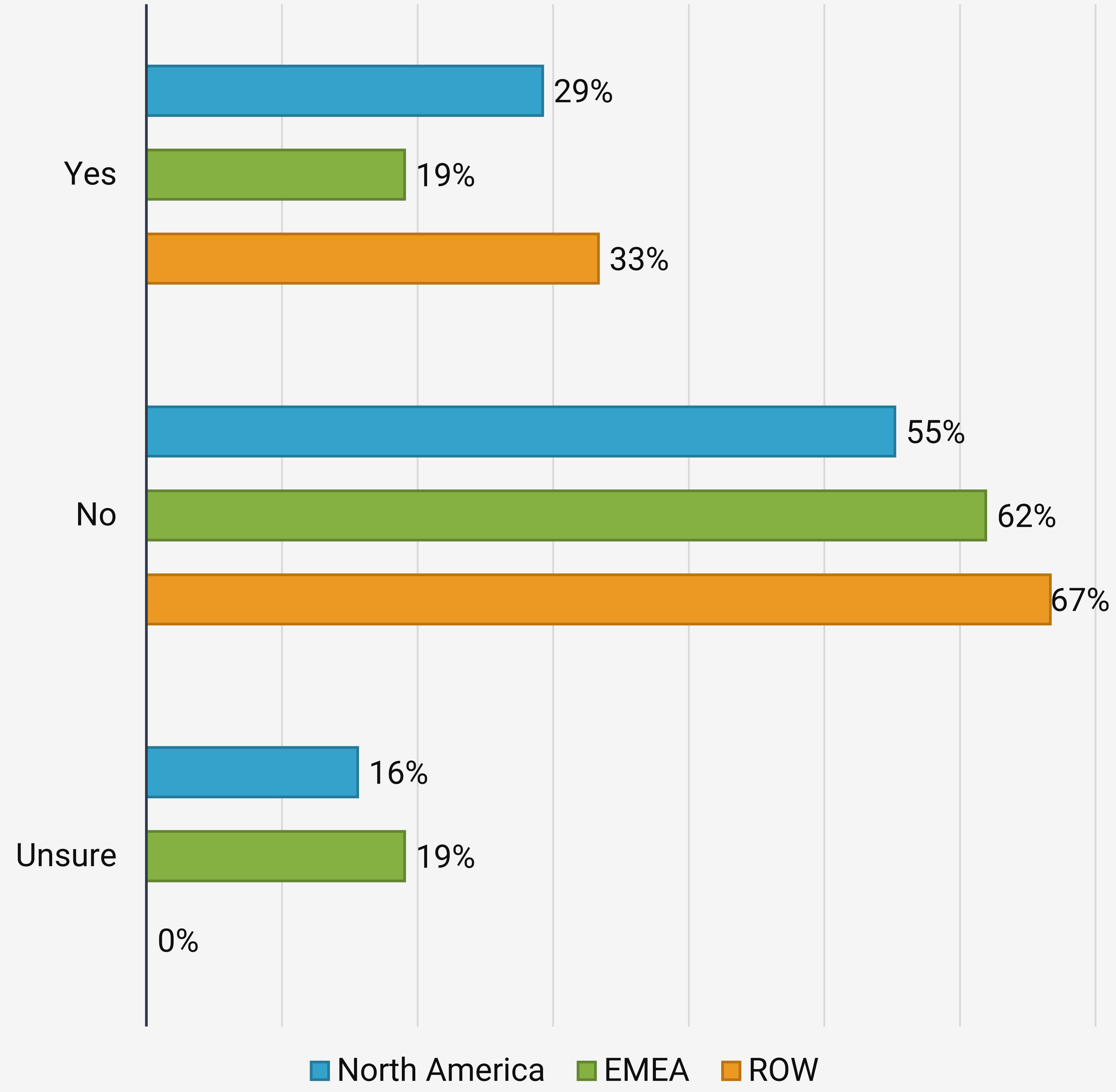
Source: ST Survey, Coveware Quarterly Ransomware Report

#GOSTRATEGIC

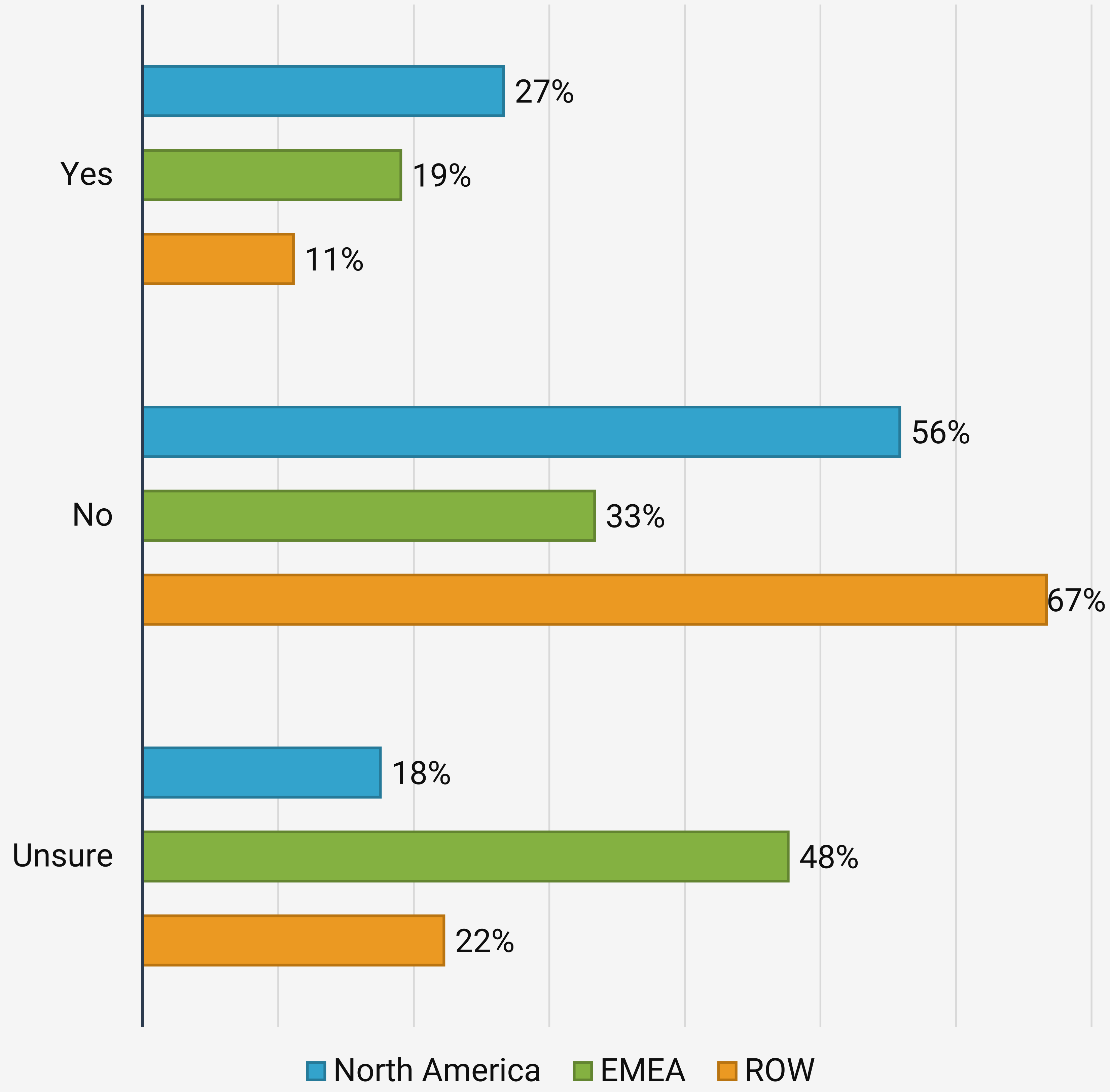
THE PAYMENT HAS LEFT THE BUILDING

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?



Source: 2020 Treasury Fraud and Controls Survey

#GO**STRATEGIC**

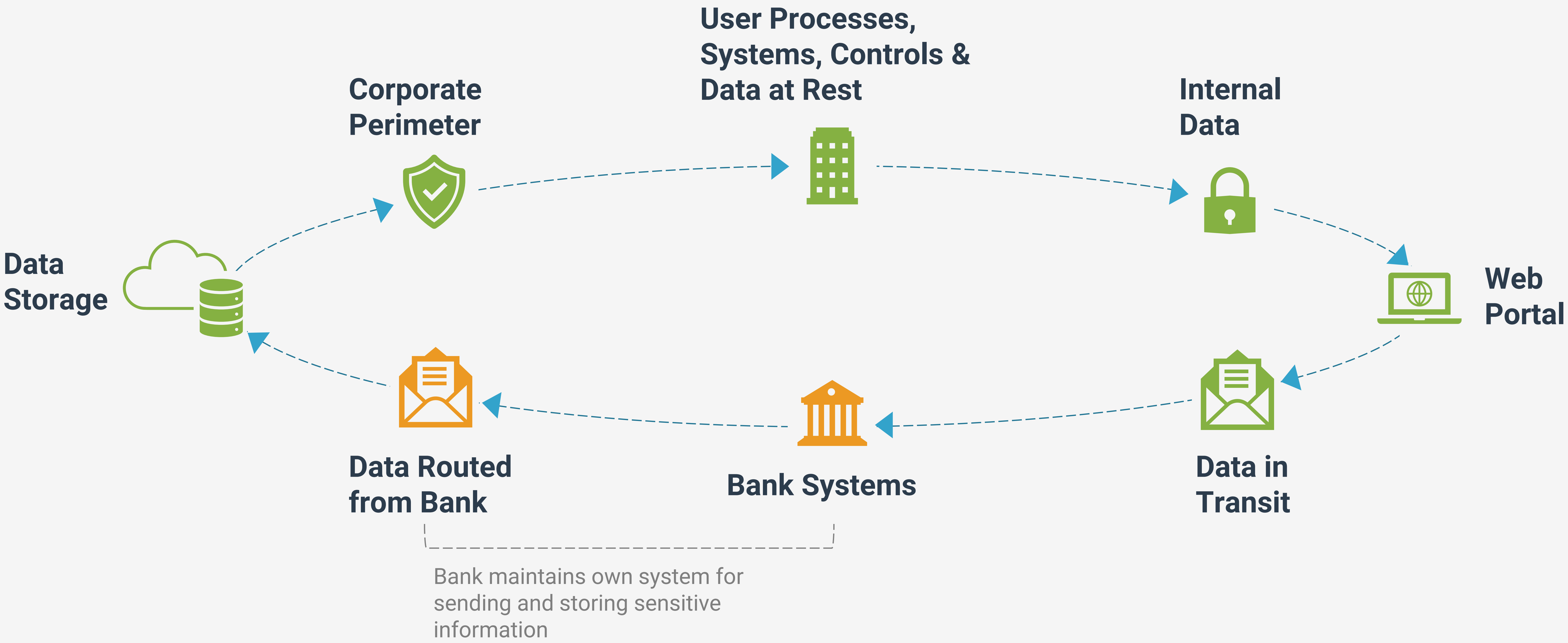
STRATEGIC TREASURER

fiserv.

RISK IN PAYMENT TECHNOLOGY

SECURITY COMPONENTS

The complex defense required by every increasing exposure cannot be solved simply with more people and more compensating controls, as this is both difficult to accomplish and inadequate in its effects. Instead, treasury must work to drive the complexity into consistent and efficient processes. This is where the TMS can step in.


Data Storage

Corporate Perimeter

User Processes, Systems, Controls & Data at Rest

Internal Data

Web Portal

Data in Transit

Bank Systems

Data Routed from Bank

Bank maintains own system for sending and storing sensitive information

#GOSTRATEGIC

CYBERCRIMINAL METHODOLOGY

TODAY'S CRIMINAL OPERATES EFFICIENTLY

PERSISTENT

Constantly adjusting their attack methods until they find an angle that is successful.

TARGETED

Broad tactics are still being utilized, but activities are also being tailored to identify weaknesses and penetrate vulnerable individuals.

ADAPTIVE

They are not abandoning their tried-and-true methods, but they are consistently adding new methods and adjusting to be most effective.

SOPHISTICATED

Attempts are increasingly more convincing and better executed with intricate technology.

AUTOMATED

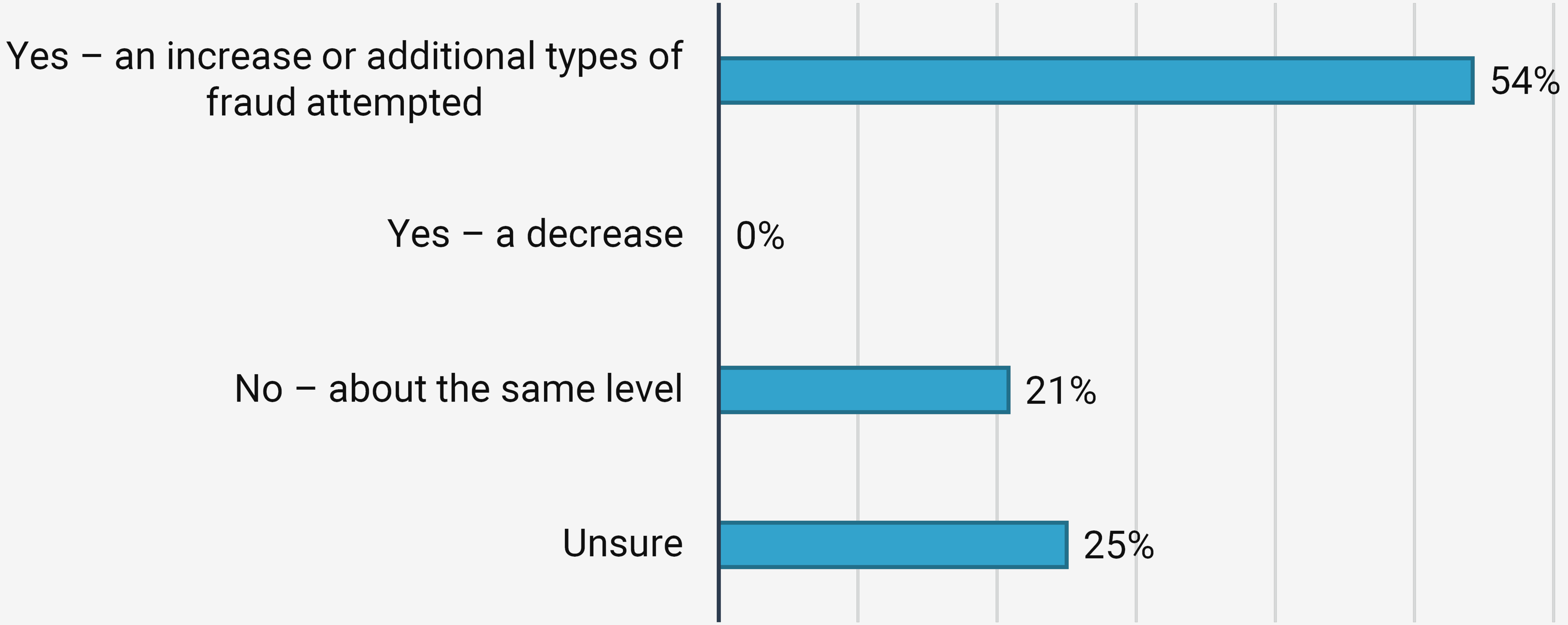
Use software to increase efficiency and effectiveness by continually probing targets and uncovering weaknesses.

PATIENT

They will watch for the ideal time to strike and are willing to steal encrypted data today with the confidence that technological advances will allow for an eventual payout.

POLL QUESTION

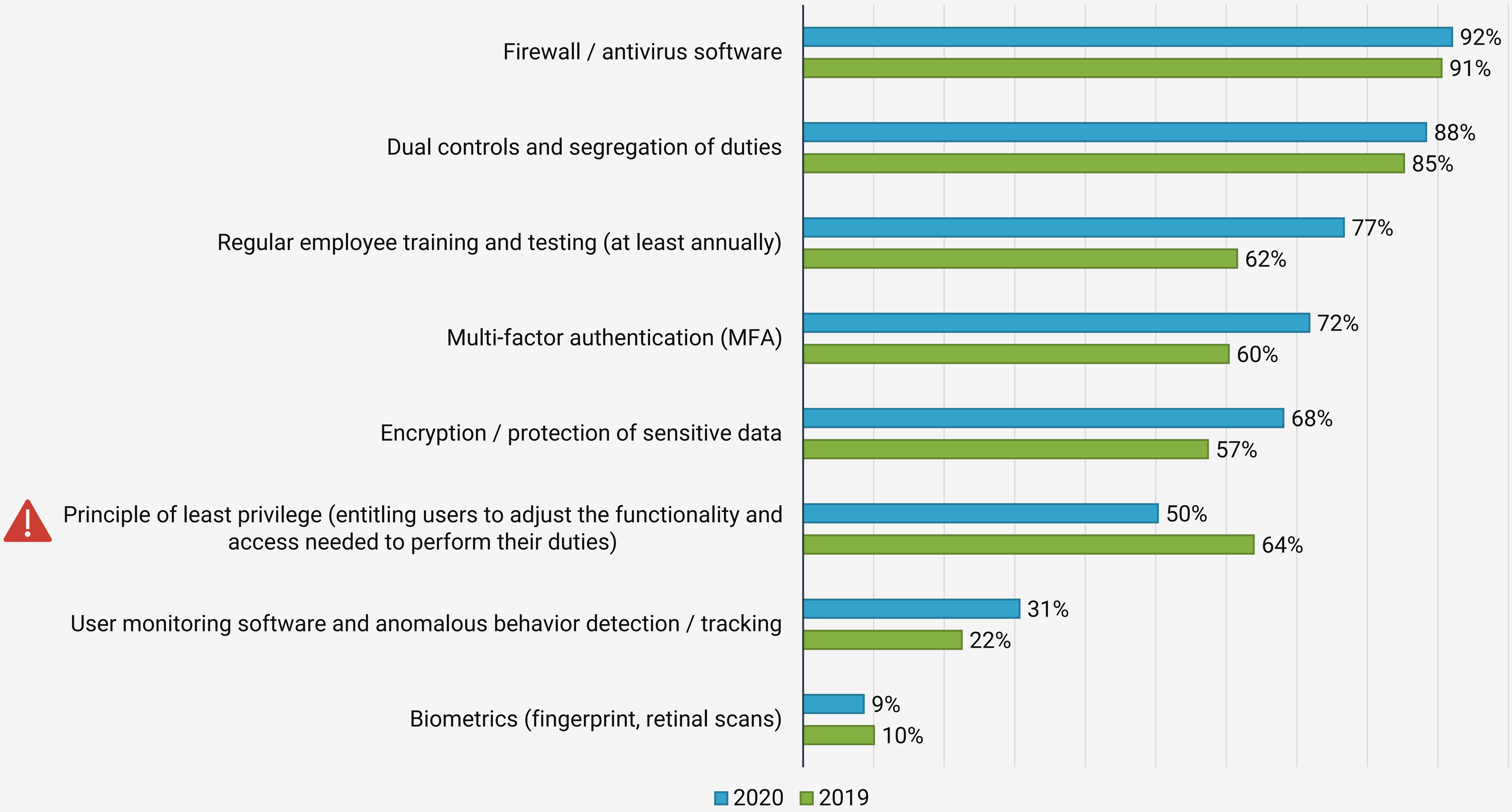
Has your organization seen a change in attempts of fraud or cyberfaud since the start of COVID-19?



CONTROLS

GROWING USE, BUT ROOM FOR WIDER ADOPTION

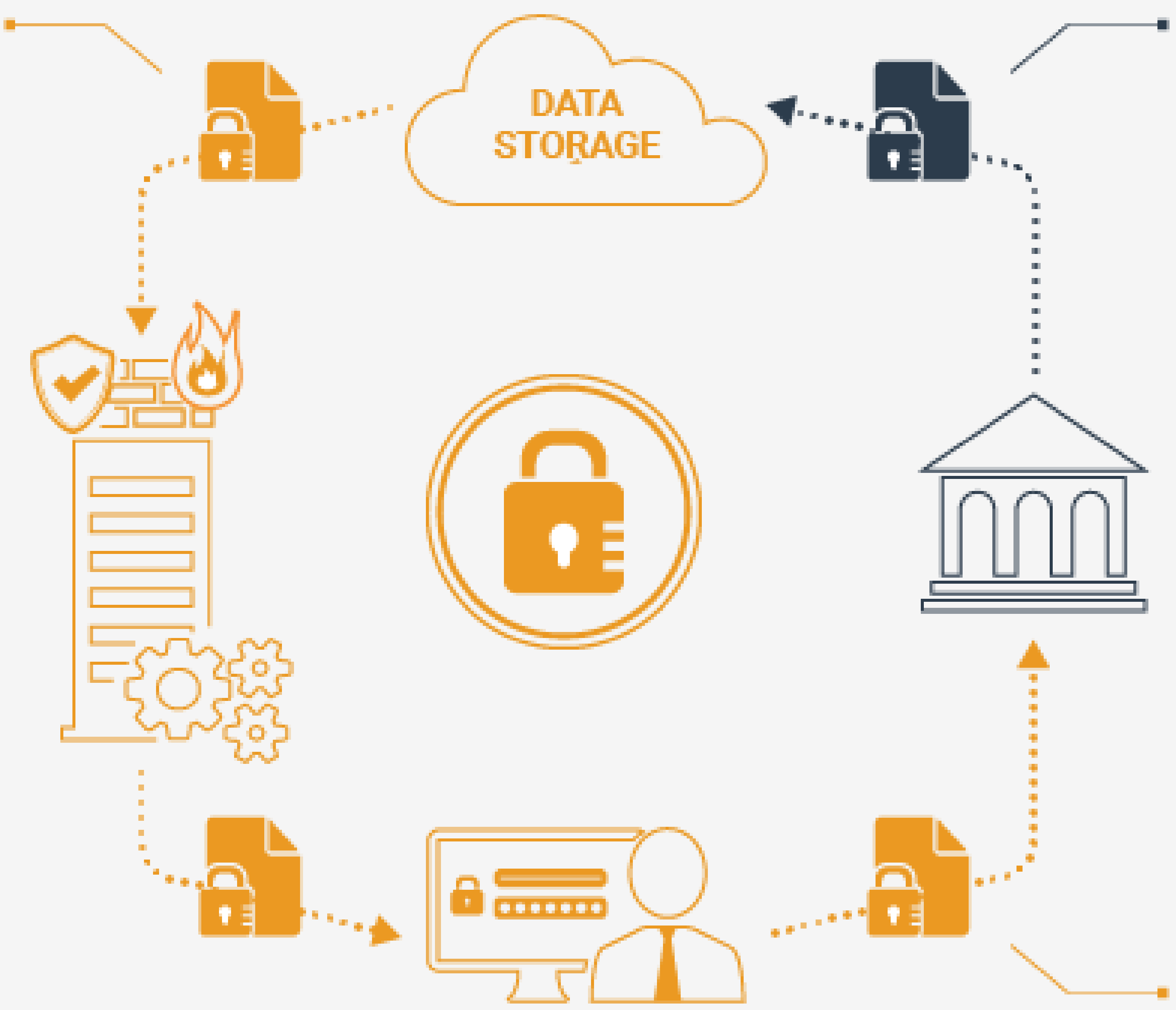
What controls does your organization have in place to prevent fraud / cyber-attacks?



Source: Treasury Perspectives Survey

WHAT DOES PAYMENT SECURITY INCLUDE?

- 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.



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.

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.

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.

PROTECTING AGAINST FRAUD

LOCKING THE GATE

Many security elements of the payment process touch on payables, receivables and banking. To ensure an appropriate level of care finance must be thoughtful with their: banking structure, bank account management process, services from banks, and controls they manage. These must be properly established and maintained.

ACCOUNT ARCHITECTURE

- Intentional Organization
  - Concentration Account
  - Header Account
    - Collection Accounts
    - Disbursement Accounts
    - Operating Accounts

BANK ACCOUNT MANAGEMENT

- Tracking
  - Every Bank Account
  - Every Signer
- Top Level Controls
  - Debit Filters
  - Vendor Verification
  - Banking Services

SERVICES & CONTROLS

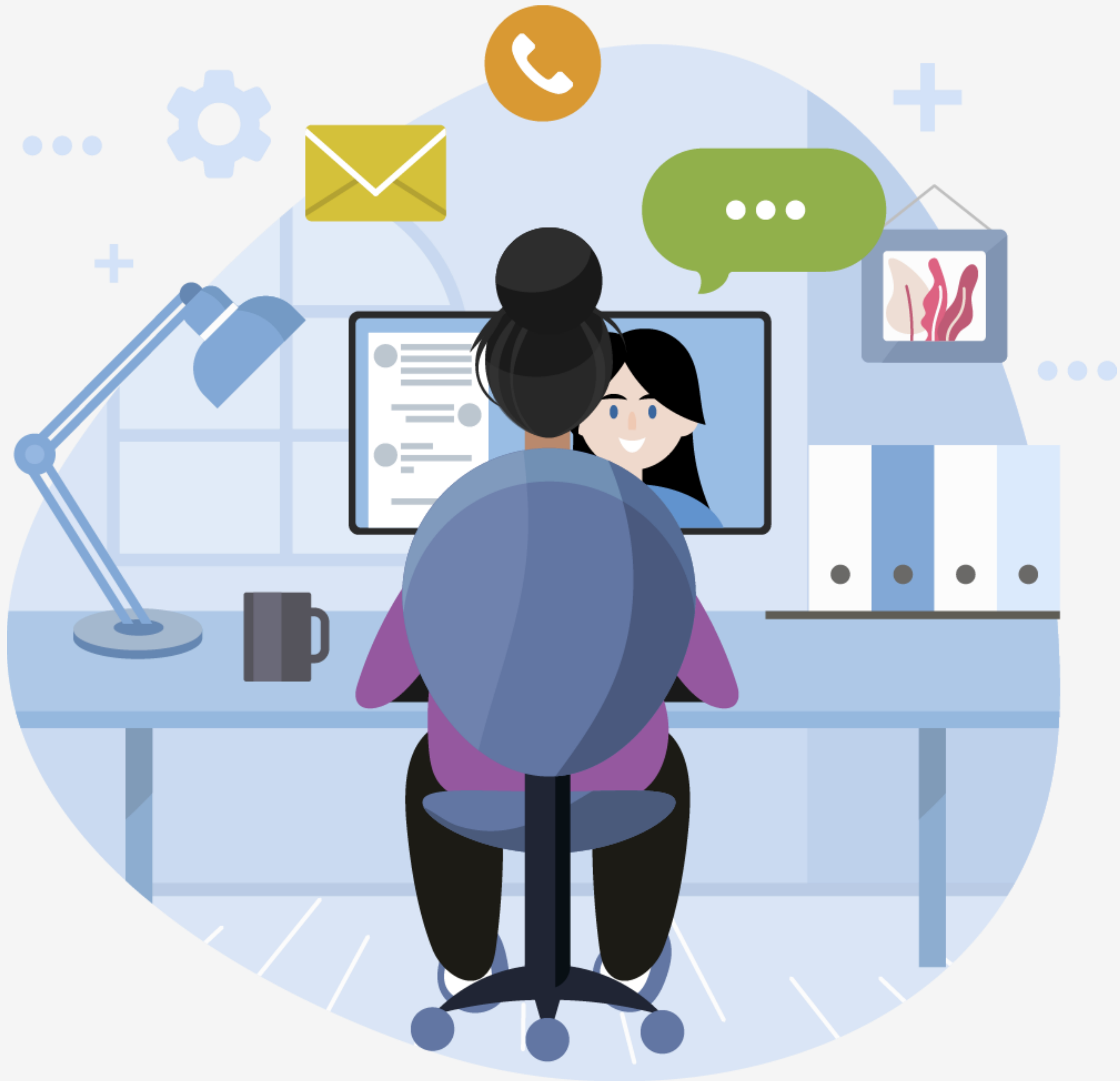
- Account and Transaction Level
  - Allow & Block Lists
  - Debit Filters and Blocks
  - Positive Pay/Payee Match
  - ACH Positive Payment / Electronic Pre-Authorization
  - Confirmation services
- Reconciliation (daily)
- Visibility
- Automated Detection Processes

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 work from home (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.



Source: Global Crisis Monitor Survey, Treasury Coalition

#GO**STRATEGIC**

TRAINING PAYOFF

INVESTING IN THE HUMAN ELEMENT

THE PAYOFF: LOWER LOSS

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

Source: 2020 Treasury Fraud and Controls Survey

LEVERAGING TECHNOLOGY

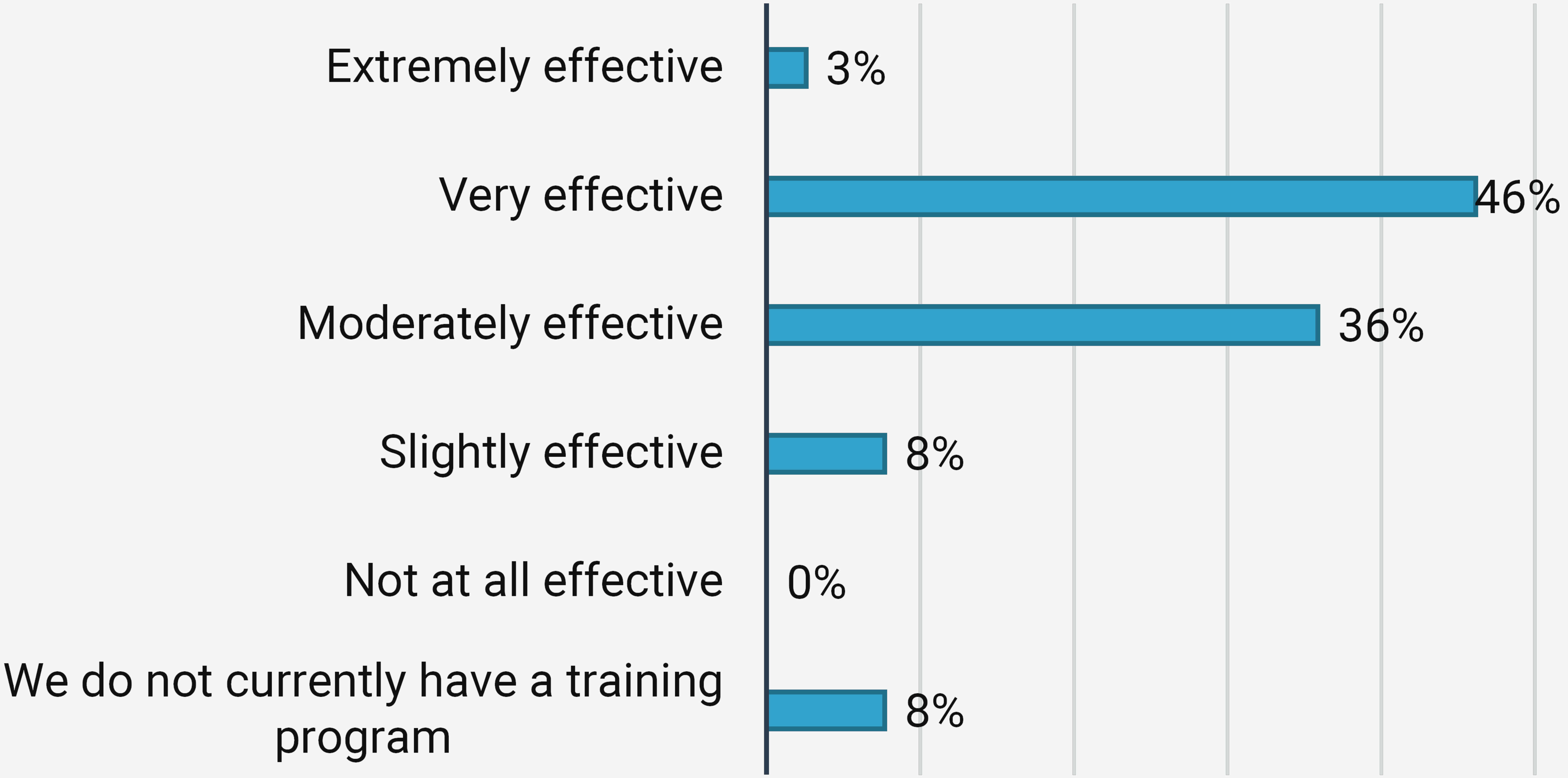
CRIMINALS ARE USING IT – SO SHOULD YOU

Treasury doesn't need to fully understand all the technical details behind a system, but they do need a comprehensive understanding of major factors.

- Where and How Your Payment Data Is Saved
- The Methods for Processing Your Payments Data
- The Shape Your Data Takes When Processed
- Who Has Permission to Approve and Release Payments
- Who Has Access to Your Payments Data
- How You Can Control Who Receives a Payment

POLL QUESTION

How would you rate the effectiveness of your security, fraud and payment training?



DON’T IGNORE THE HUMAN ELEMENT

TECH CAN ONLY DO SO MUCH

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	Human Security Components
Firewall & Antivirus	Security Training
Multifactor Authentication	Employee Testing
User Monitoring Tools	Whistleblower Policy
Biometrics	Clean Desk Policy
Encryption	Dual Controls
Tokenization	Segregation of Duties
SAML 2.0	Principle of Least Privilege

TAKE-AWAYS

IDEAS AND POINTS TO BRING BACK TO THE OFFICE

FOCUS ON TRAINING

- Learn more about the methods and techniques used by criminals
- Train and test staff on threats – too easy to forgo in the WFH environment

ASSESS PAYMENT PROCESSES

- Identify all exposure points within your organization
- Examine other exposure points with external parties

PLAN & IMPLEMENT

- Address security issues
- Layering your defenses so multiple blocks must be overcome for fraud to succeed

BENCHMARK YOUR SECURITY

- Evaluate your security to ensure it is up to date with leading practices
- Rinse and Repeat. Reexamine every 12-24 months

#GO***STRATEGIC***

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

Craig Jeffery, CCM, FLMI
Founder & Managing Partner

✉ craig@strategictreasurer.com

Alexa Cook,
Consultant

✉ alexa@strategictreasurer.com

FEB 3 - MAR 31
2021
Global Recovery Monitor
An Ongoing Survey of COVID-19 Response and Economic Recovery
TREASURY
COALITION
...from Crisis to Recovery...

GLOBAL RECOVERY MONITOR SURVEY

Investing only 5 minutes every eight weeks will help your organization and our profession. Arm yourself with the most current, necessary information for treasury and finance teams in near real-time.

Take GRM Survey