PAYMENT SECURITY

ASSESSING & RESPONDING TO AN ESCALATING THREAT

CRAIG JEFFERY
Founder & Managing Partner
Strategic Treasurer

Certified Treasury Professional®

FP&A® Certified Corporate Financial Planning & Analysis Professional

WHAT

The current situation, the threat levels of various types of fraud, and the tactics for constructing a solid defense.

WHEN

Thursday, July 15, 2021
2:30 PM – 3:30 PM EST

WHERE

Live Online Presentation
Replays at StrategicTreasurer.com

STRATEGIC TREASURER

This presentation is provided by Strategic Treasurer

ABOUT THE SPEAKER

GET TO KNOW TODAY'S SUBJECT MATTER EXPERT

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.

STRATEGIC TREASURER

Strategic Treasurer was founded in 2004 by Craig Jeffery, a financial expert and trusted advisor to executive treasury teams since the early 1990s. Partners and associates of Strategic Treasurer span the US, the UK and continental Europe.

This team of experienced specialists are widely recognized and respected leaders in treasury. Known for their expertise in treasury technology, risk management, and working capital as well as cash management and banking, they efficiently identify issues, creatively explore ideas and options, and provide effective solutions and implementations for their valued clients.

Strategic Treasurer

TOPICS OF DISCUSSION

KEY AREAS OF FOCUS

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

CURRENT STATE

CRIMINAL PLAYBOOK

THE TECHNIQUES

FRAUD TYPES

MITM ATTACKS

EXPOSURE POINTS

IN THE PAYMENT PROCESS

LEVERAGING TECH

RESPONDING TO VULNERABILITIES

CASE STUDY

WIRECARD

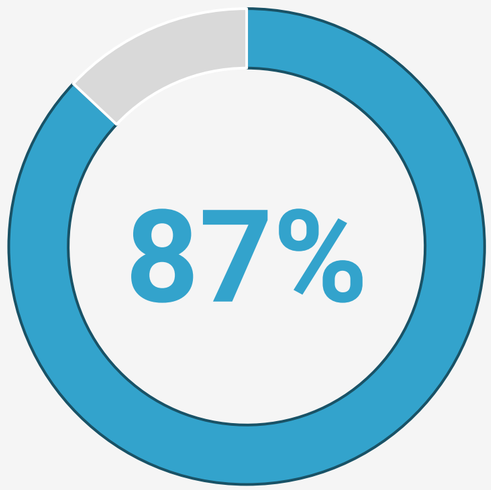
*#GO**STRATEGIC***

Strategic Treasurer

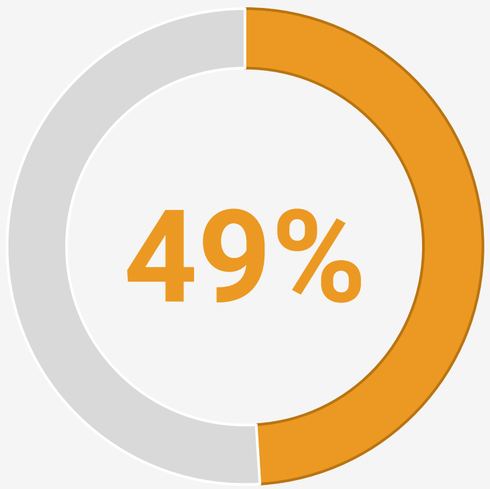
THE CURRENT STATE OF FRAUD

NOT AS SECURE AS WE THINK WE ARE

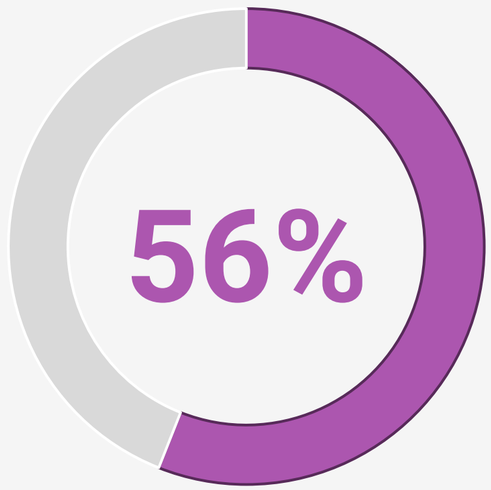
> *I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.*
>
> *- Robert Mueller, Former FBI Director*



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.

Source: 2021 Treasury Fraud & Controls Survey

CRIME PAYS

AND CRIMINALS ARE NOT GIVING UP

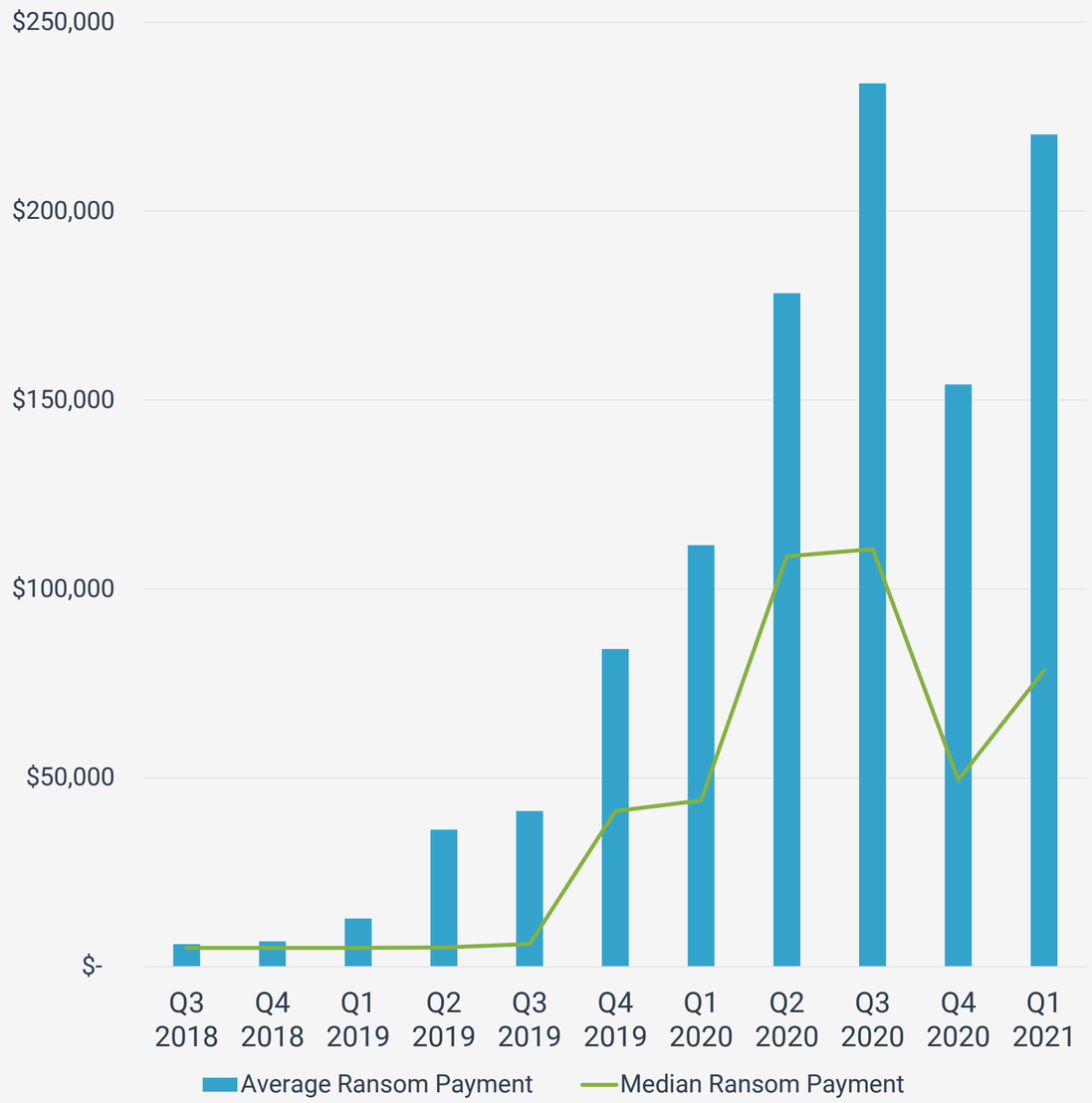
Automation has helped criminals scale their attempts and improve their success rates.

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

Ransomware
A third of firms experienced attempts, with about one out of ten incurring a loss.

System Level Fraud
About a third of firms experienced attempts, with 4% incurring a loss.

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



Source: ST Survey, Coveware Quarterly Ransomware Report

STRATEGIC TREASURER

WFH FRAUD INCREASE

MEASURING FRAUD THROUGHOUT THE PANDEMIC

The Global Recovery Monitor was a frequent mini-survey on 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 2020

36%
reported an increase

Period 15
September 2020

64%
reported an increase

Period 16
October 2020

53%
reported an increase

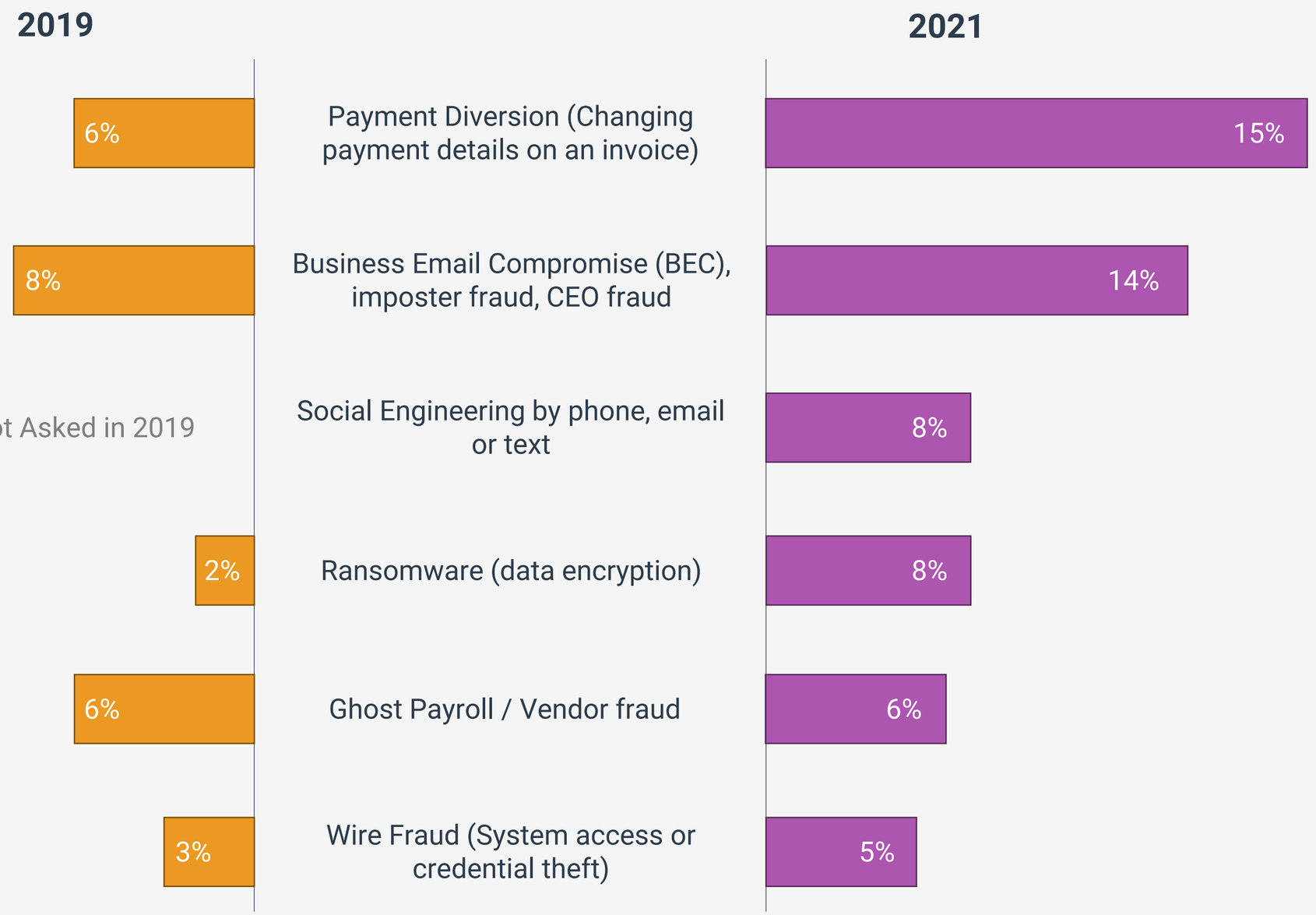
Period 18
January 2021

40%
reported an increase

THEN & NOW

LOSSES FROM FRAUD

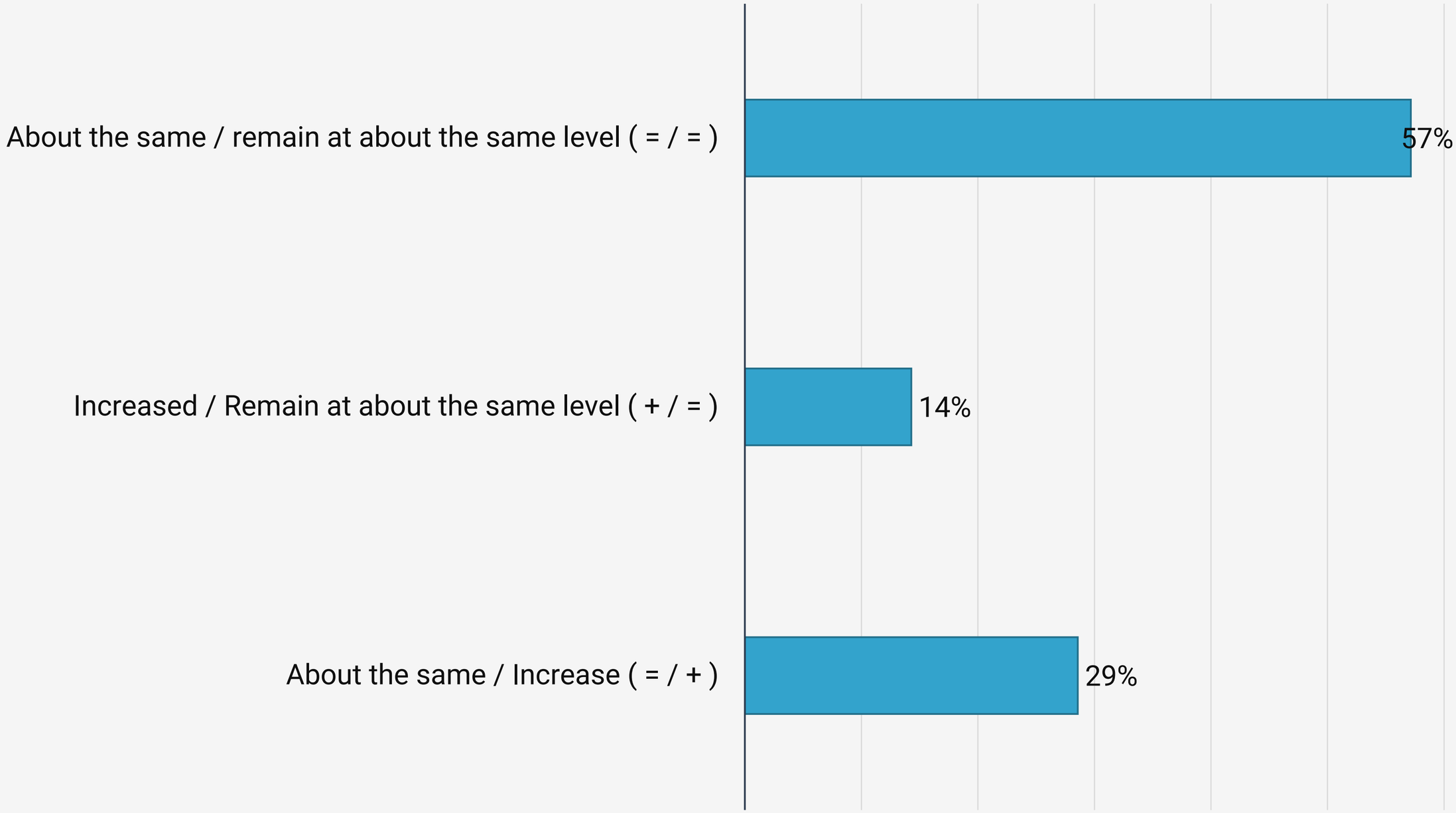
Fraud attempts are increasing along with the losses. Those that report suffering a loss in the last 12 months have significantly increased over a two-year period.



Note: Only top 6 responses from 2021 displayed

POLL QUESTION

Our spending and plans to spend on technology for payment security for the prior year versus your expectations for the next year.



Strategic Treasurer

CYBERCRIMINAL METHODOLOGY

TODAY'S CRIMINAL OPERATES EFFICIENTLY

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

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

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

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

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

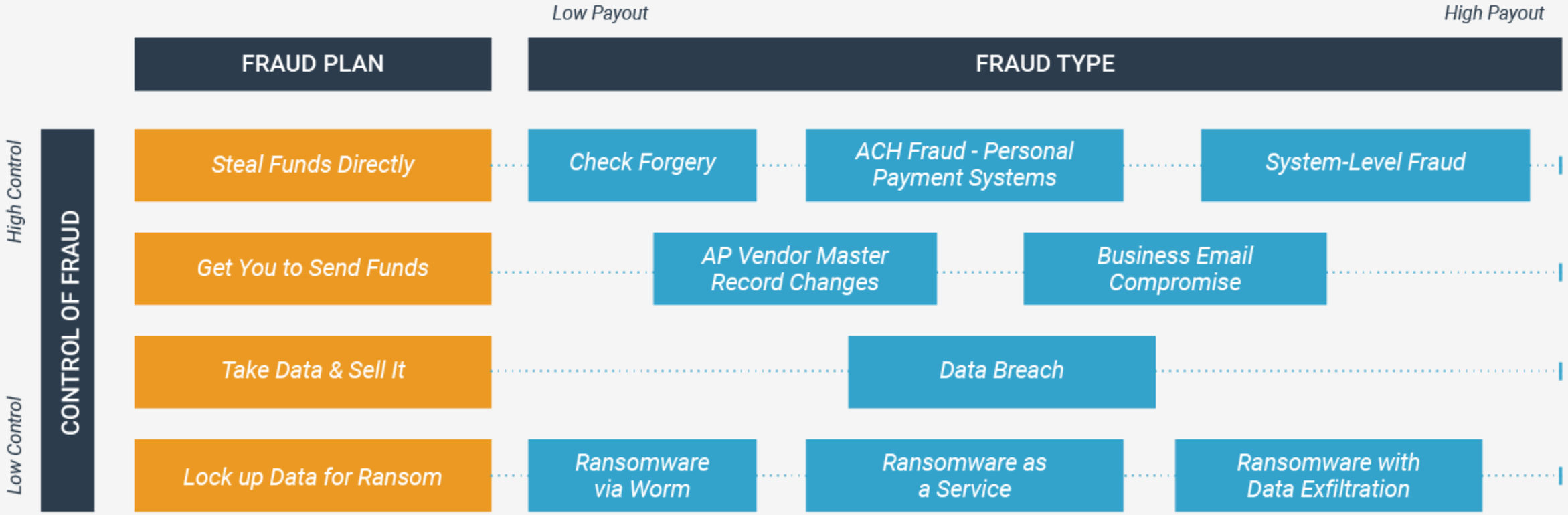
PATIENT
They will watch for the ideal time to strike and are willing to steal encrypted data today with the confidence that technological advances will allow for an eventual payout.

*#GO**STRATEGIC***

STRATEGIC TREASURER

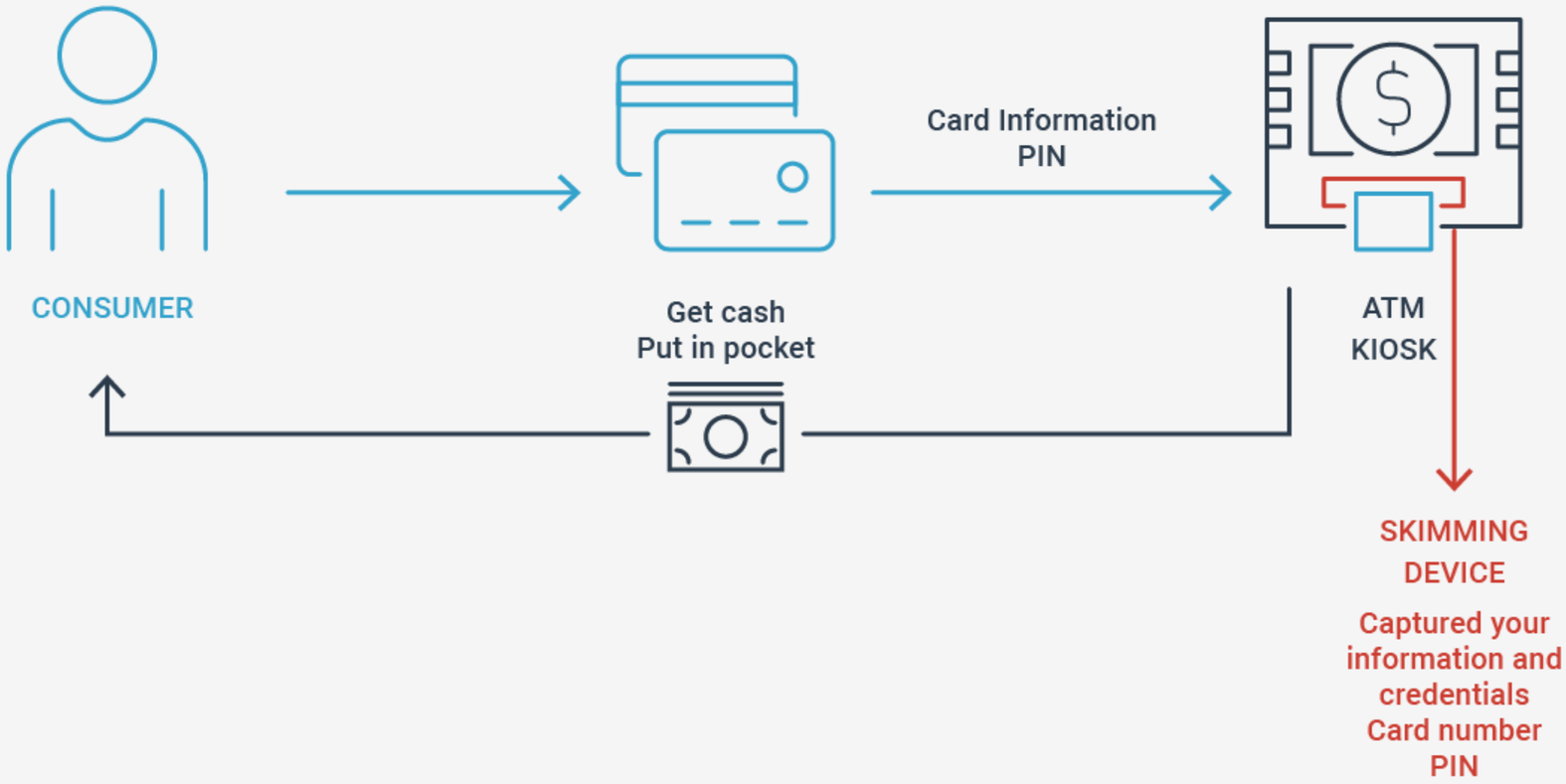
FRAUD TYPES

AND ASSOCIATED INTENTIONS



PHYSICAL MITM ATTACKS

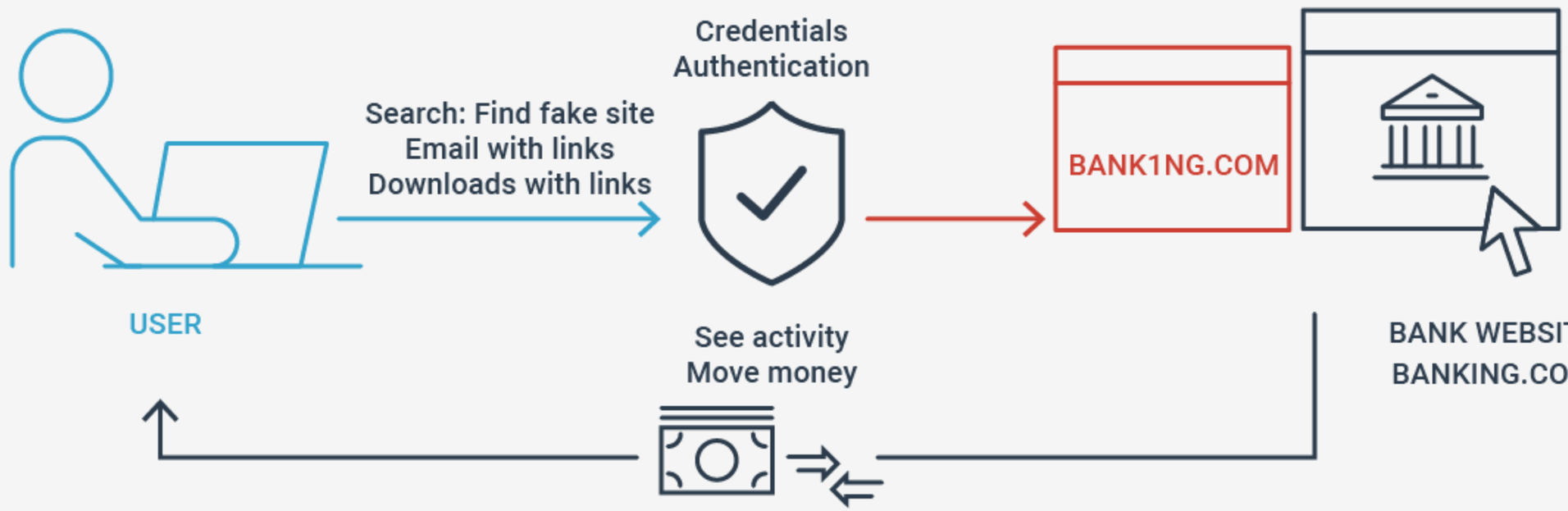
THE OLD WAY OF MAN IN THE MIDDLE ATTACKS



- Objects and devices are visible, more expensive and have limited reach.
- Must be in close proximity to accounts.

DIGITAL MITM ATTACKS

FAKE WEBSITES



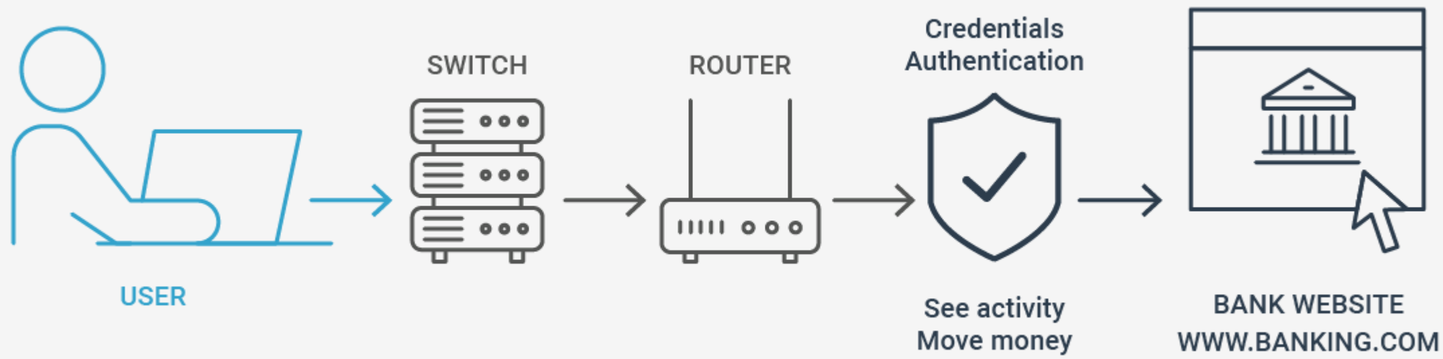
Captures your information and credentials through fake website, passes information on to real website to send confirmation back to user – appears as though nothing is wrong.

STRATEGIC TREASURER

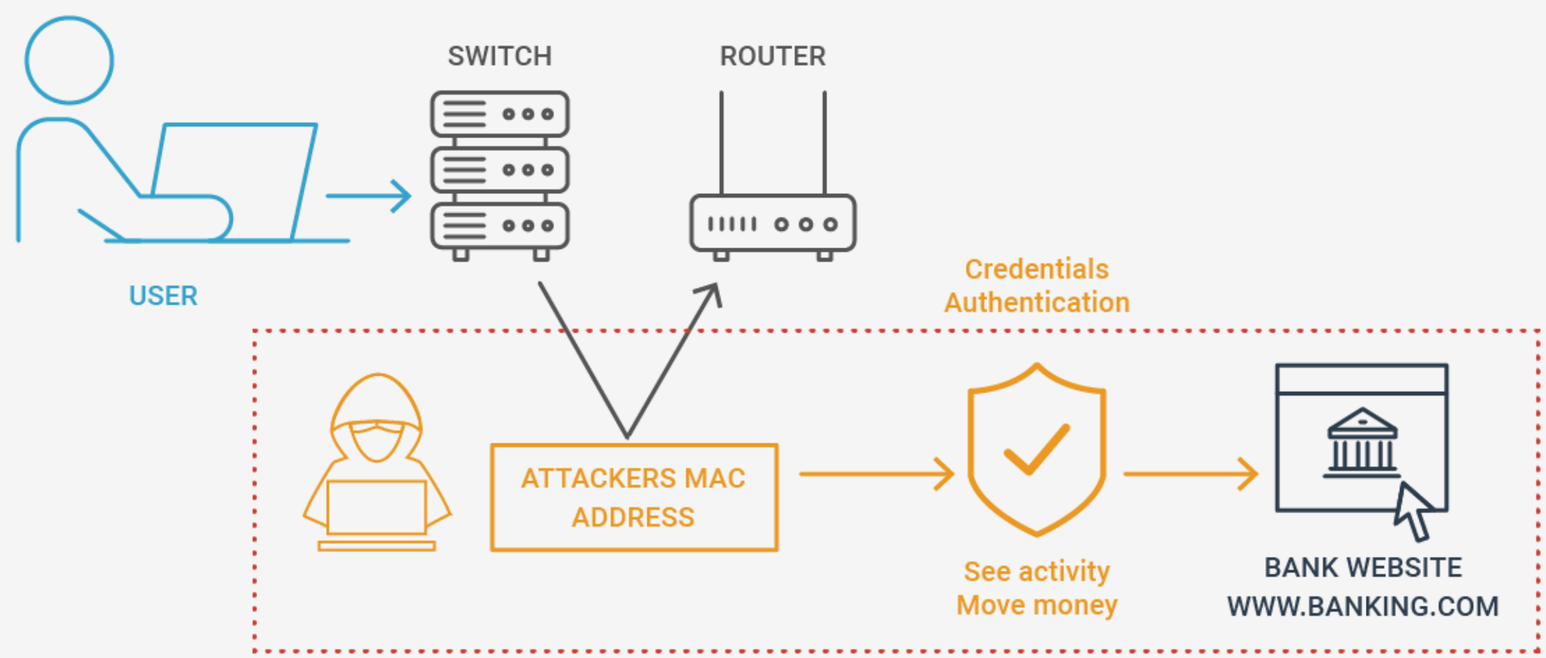
ARP ATTACKS

(SPOOFED) ADDRESS RESOLUTION PROTOCOL

Links the attacker's MAC address to the IP address of some other host. Your computer thinks it's your real gateway and now is connected to the attacker's device.



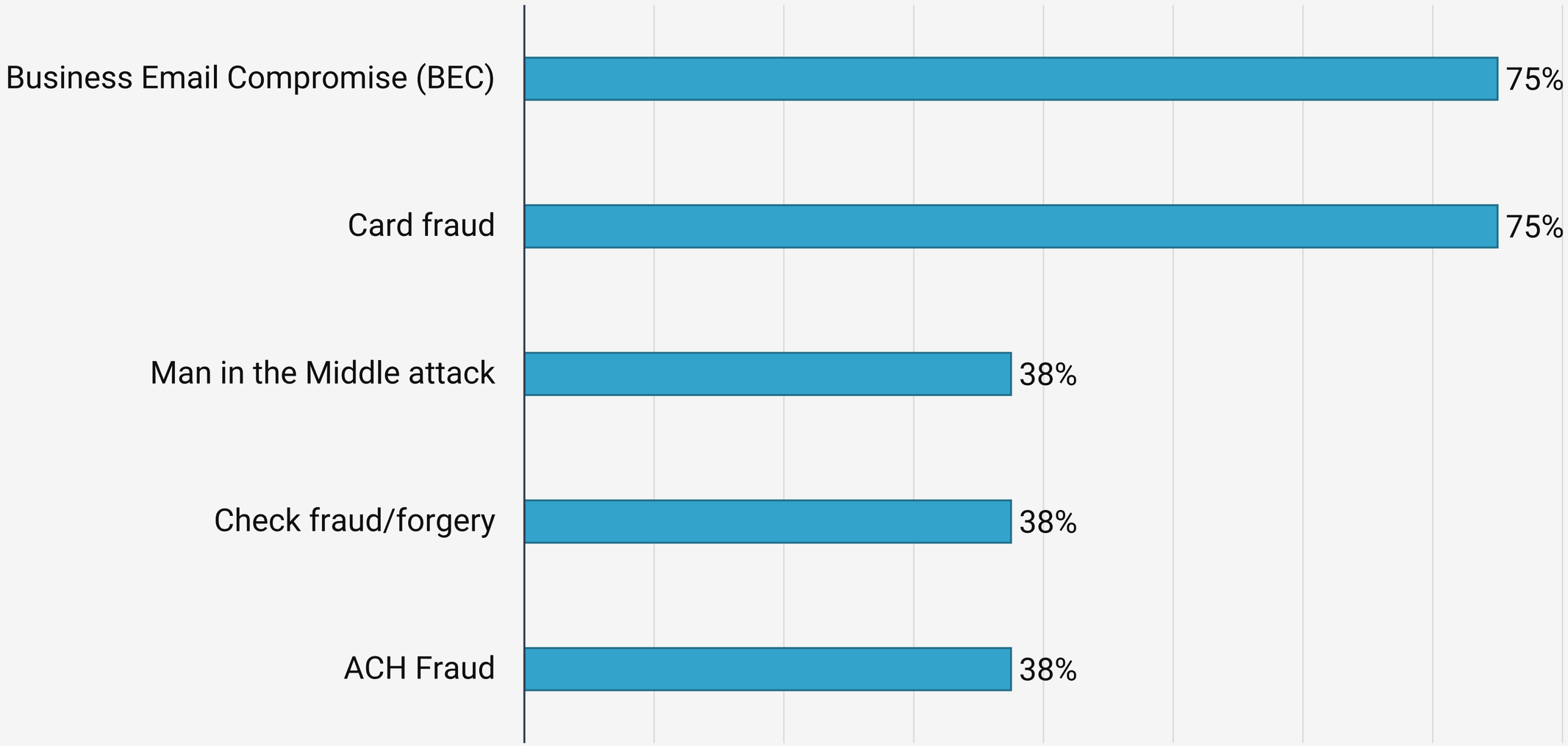
Attacker can read communication between network devices.



#GO***STRATEGIC***

POLL QUESTION

Thinking of the last twelve months, which of the following types of fraud has your company experienced (both unsuccessful or successful)?



Strategic Treasurer

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**

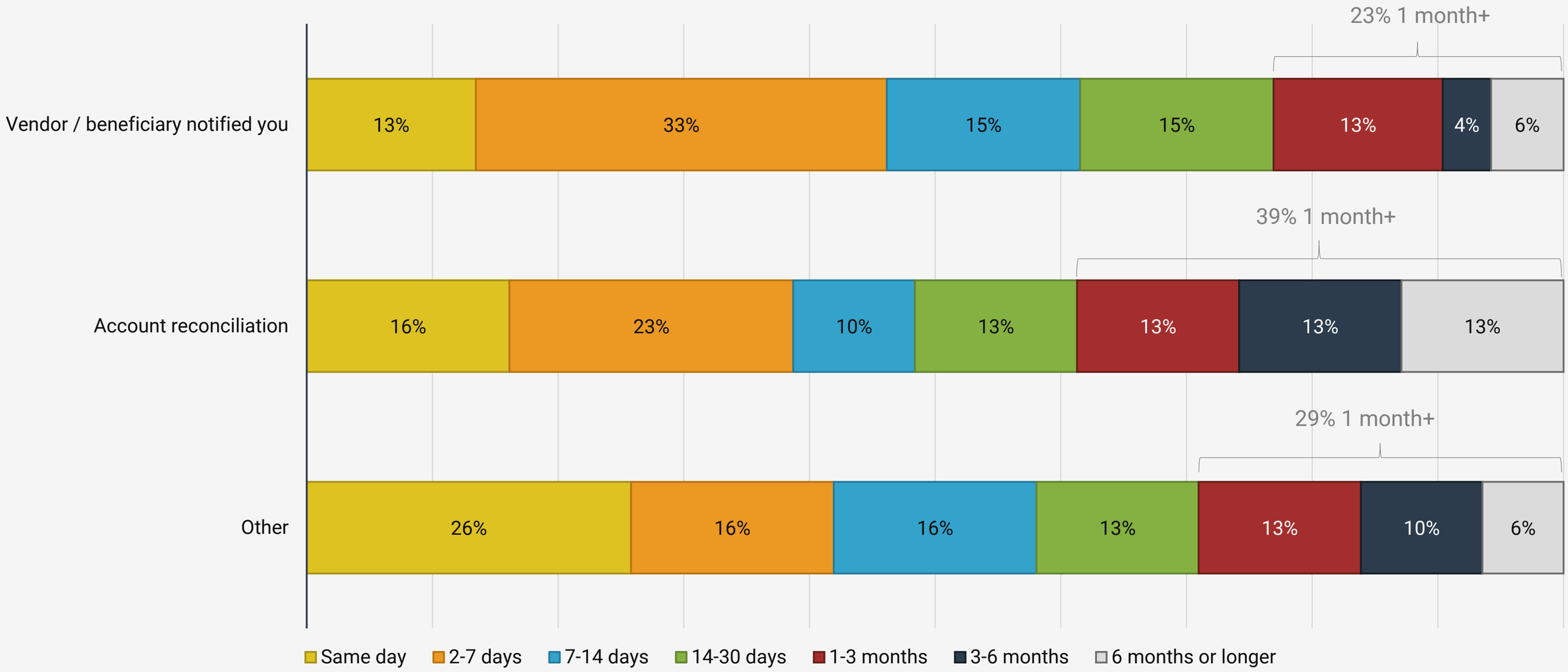
*#GO**STRATEGIC***

PAYMENT HAS LEFT THE BUILDING

AND IT'S TAKING A WHILE TO REALIZE IT

Nearly a third (32%) of corporates reported having an ACH or wire fraud that left the building this year, up from 25% in the previous survey.

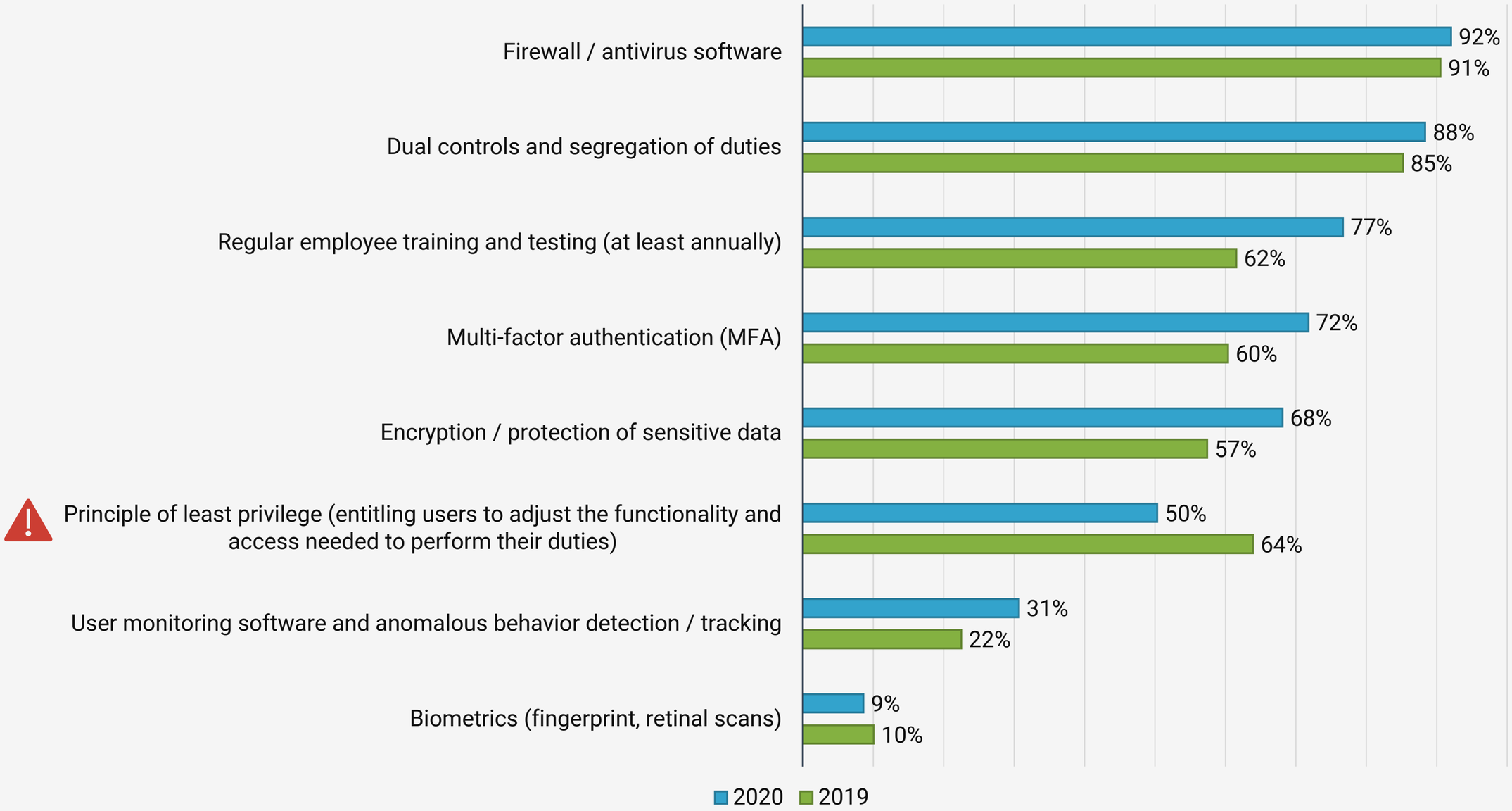
» Specifically considering your largest ACH or wire fraud incident, how long did it take you to detect it and by what method did you detect it?



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

STRATEGIC TREASURER

RISKS IN THE PAYMENT PROCESS

MANAGING THE FULL SCOPE OF EXPOSURES

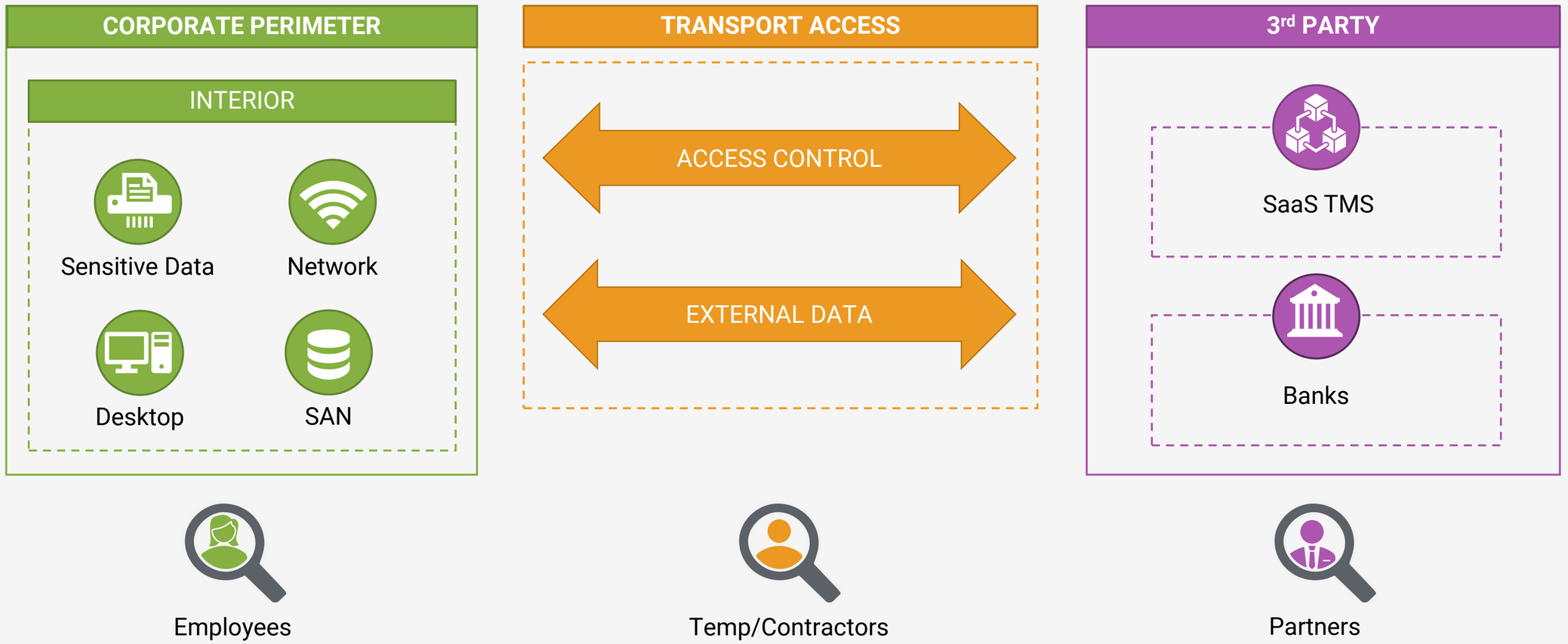
Incident Response — Employee Management — Treasury Security Framework — Access Control — Banking Design

Cloud Security

Cyber Security

Segregation of Duties

Transaction & Daily Limits



Lockdown Playbook — Assessment & Benchmarking — Duties & Policies — Communications — Liability Management

STRATEGIC TREASURER

TREASURY ACCESS POINTS

SECURING THE “GATES”

While many security elements of the payment process are not directly related to treasury, a few areas of exposure do fall within treasury’s role. To ensure proper handling, treasury needs to have their own security framework outlining the management of their own vulnerabilities and controls.

BANK ACCOUNT MANAGEMENT

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

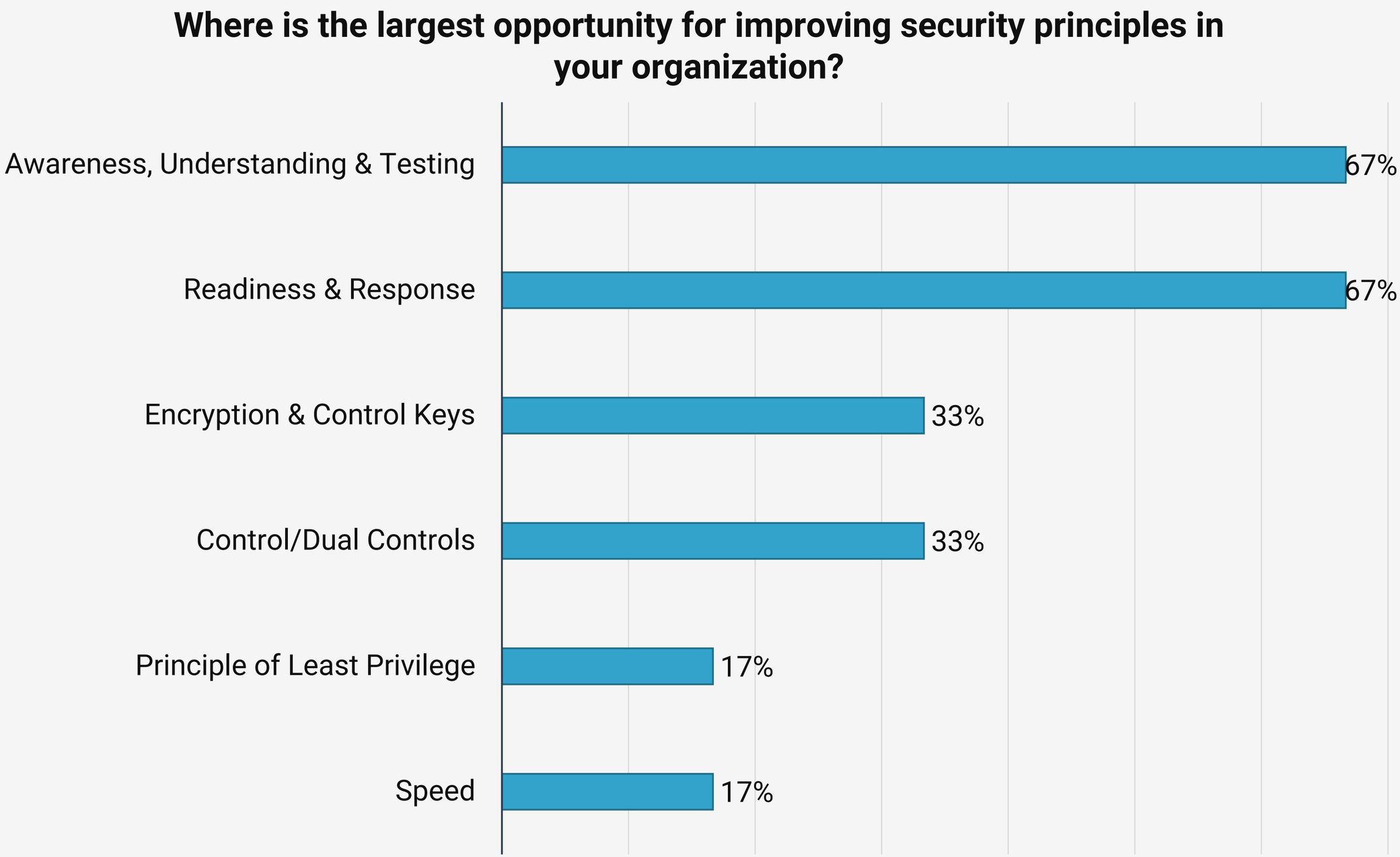
ACCOUNT ARCHITECTURE

- Intentional Organization
  - Header Account
    - Collection Accounts
      - Concentration Account
        - Disbursement Accounts
    - Special Categorization

CONTROLS

- Account-Level & Transaction-Level
- Allow Lists
- Block Lists
- Debit Filters
- Debit Blocks
- Positive Pay
- ACH Positive Payment/Electronic Pre-Authorization
- Reconciliation
- Automated Detection Processes

POLL QUESTION



CASE STUDY

WIRECARD

WHAT HAPPENED

- Ernst & Young refused to sign off on financial statements in June of 2020
- E&Y audits showed €1.9B ($2.1B USD) missing from financial statements

FAILURES OF DEFENSE

- Internal controls were insufficient/ faulty as several parties were creating fictitious activity
- Proper bank account management would have detected ‘missing’ cash

FRAUD METHODS

- Investigation still ongoing
- Falsified financial statements, inflating revenue and overstating cash
- Collusion is suspected and charges being pursued

OUTCOME

- It was determined the funds never existed
- Wirecard dropped over 60% in value in a single day and declared bankruptcy
- The CEO resigned and was arrested

For more information on this case study and what treasury groups can learn from it, please see our video on YouTube.

Strategic Treasurer

TAKE-AWAYS

IDEAS AND POINTS TO BRING BACK TO THE OFFICE

EVERYONE IS NOW A TARGET

- Train & test employees on payment security
- Assign specific people to particular areas of security

ASSESS THE PAYMENT PROCESSES

- Identify and address security issues
- Review exposures from WFH workarounds that were “temporarily” adopted

TIME TO BENCHMARK

- Measure yourself against others (benchmarks) and against leading industry standards

INVEST IN TECHNOLOGY

- Your adversaries are using tech to attack
- Identify and acquire payment tools that support security objectives

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.

Click o add text

STRATEGIC TREASURER

Craig A. Jeffery,
Managing Partner

craig@strategictreasurer.com

The Treasury Update Podcast

linkedin.com/in/strategictreasurer/

EBOOK

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.

This eBook is intended to help treasury understand and fill that role most effectively by covering the current situation, the threat levels of various types of fraud, common areas of vulnerability, and frameworks and tactics for constructing a solid defense.

Request eBook

*#GO**STRATEGIC***