FRAUD: TRENDS, CONTROLS AND EDUCATION

CRAIG JEFFERY

Managing Partner, Strategic Treasurer

WHAT

Considering fraud trends, attack methods, effective controls, and the value of fraud training.

WHEN

Monday, May 2, 2022
1:25 - 2:15 PM EDT

WHERE

Live Online Presentation

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.

ADVISE

- Global & Domestic Treasury
- Connectivity & Onboarding
- Working Capital Optimization

RESEARCH

- Industry Surveys
- Benchmarking
- Data Subscription

ASSIST

- Treasury & Risk Technology
- Bank Fee Management
- Temporary Treasury Staffing

INFORM

- Webinars
- Podcasts
- Analyst Reports, eBooks & Executive Summaries

STRATEGIC TREASURER

TOPICS OF DISCUSSION

KEY AREAS OF FOCUS & ANALYSIS

FRAUD SITUATION

ORGANIZATIONS ARE UNDER ATTACK

TRENDS

CRIMINAL OPPORTUNISM

WHAT'S GOING ON

NEW METHODS & THREATS

EXPOSURE POINTS

KNOWING AREAS OF WEAKNESS

HUMAN & TECH

STRENGTHENING YOUR DEFENSES

KEY TAKEAWAYS

AND FINAL THOUGHTS

FRAUD SITUATION

THE NEED FOR HEIGHTENED AWARENESS

Business Email Compromise (BEC)
Get you to send the funds

Ransomware
Lock up data for a payout

Man in the Middle Attacks (MITM)
Take data to steal funds

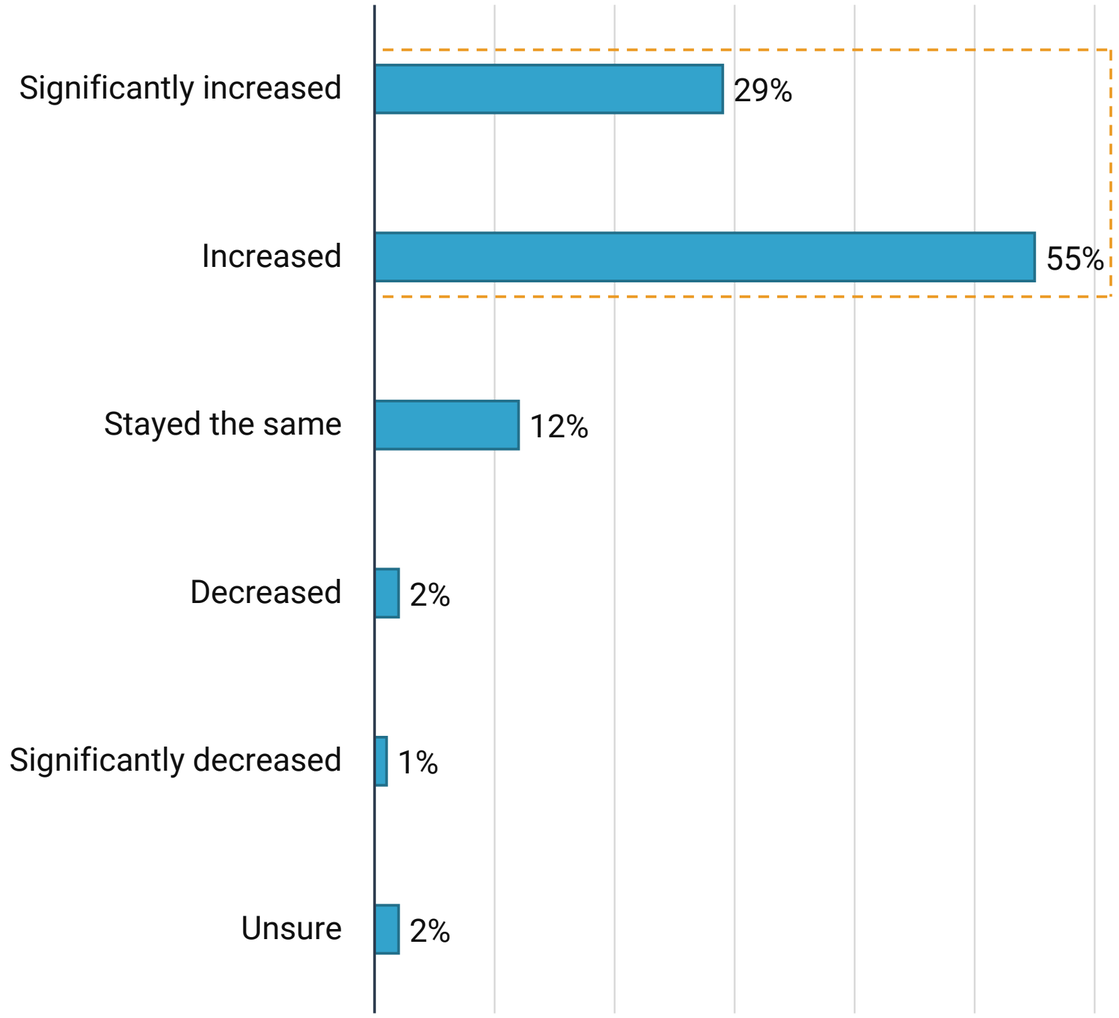
ACH Fraud
Steal funds directly

- What would you do if you knew your organization was about to be attacked and knew how to defend it?
- What can you do to make your team and organization safer?
- What do you need to protect your organization?
- What is at risk by not being protected?

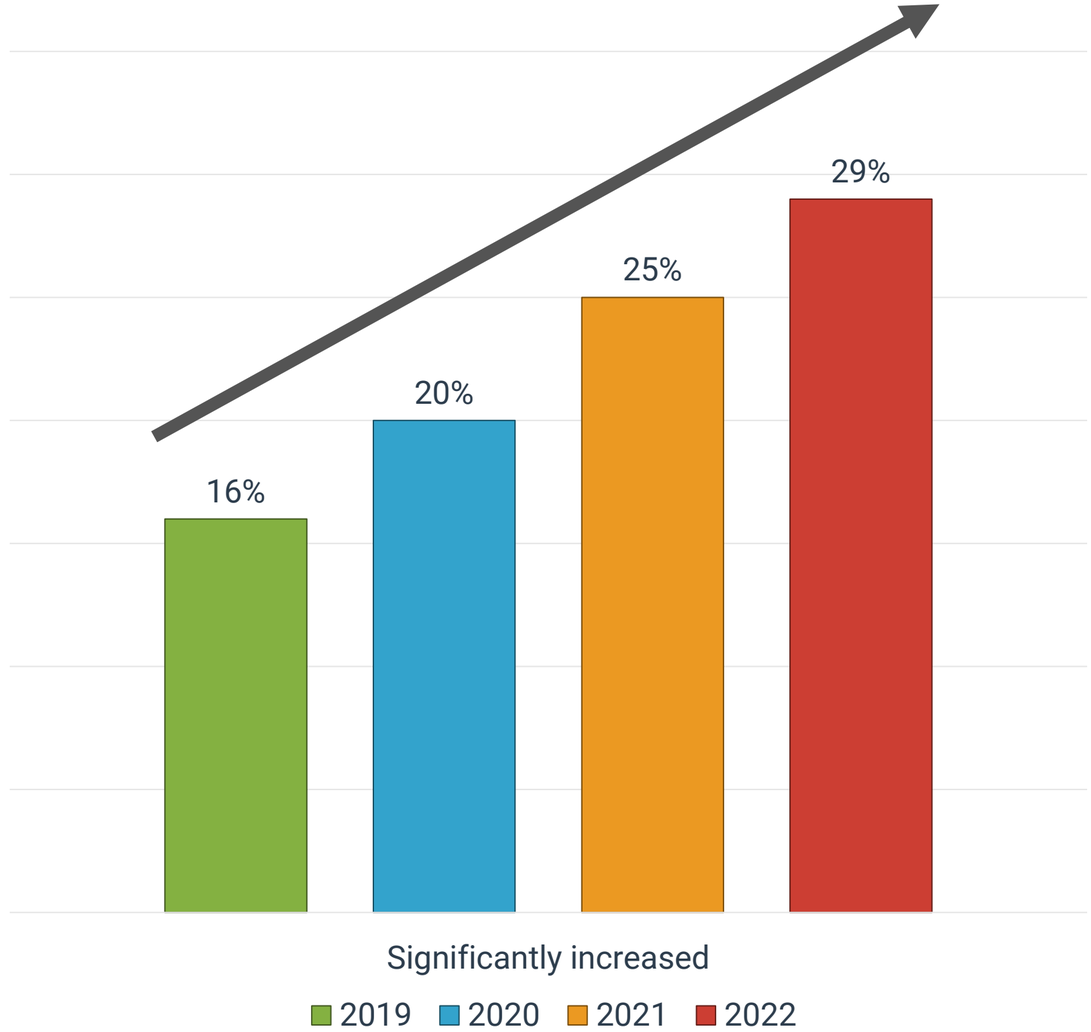
THREAT LEVEL ESCALATION

YOUR PEERS ARE INCREASINGLY CONCERNED

» 84% of survey respondents reported that the threat level of fraud in the past year has increased or significantly increased.



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



- What is driving the increase in an elevated concern over the threat level?
- How should this information and the perspectives of our peers influence us?

Source: 2022 Treasury Fraud & Controls Survey

#GOSTRATEGIC

Strategic Treasurer

WHAT'S GOING ON

YOU ARE A TARGET

DEMOCRATIZATION OF CRIME

Big, little, public, privately owned, government municipality – it doesn't matter. You are at risk.

You ARE being surveilled

You ARE under attack

You ARE NOT flying under the radar

#GOSTRATEGIC

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 individuals.

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

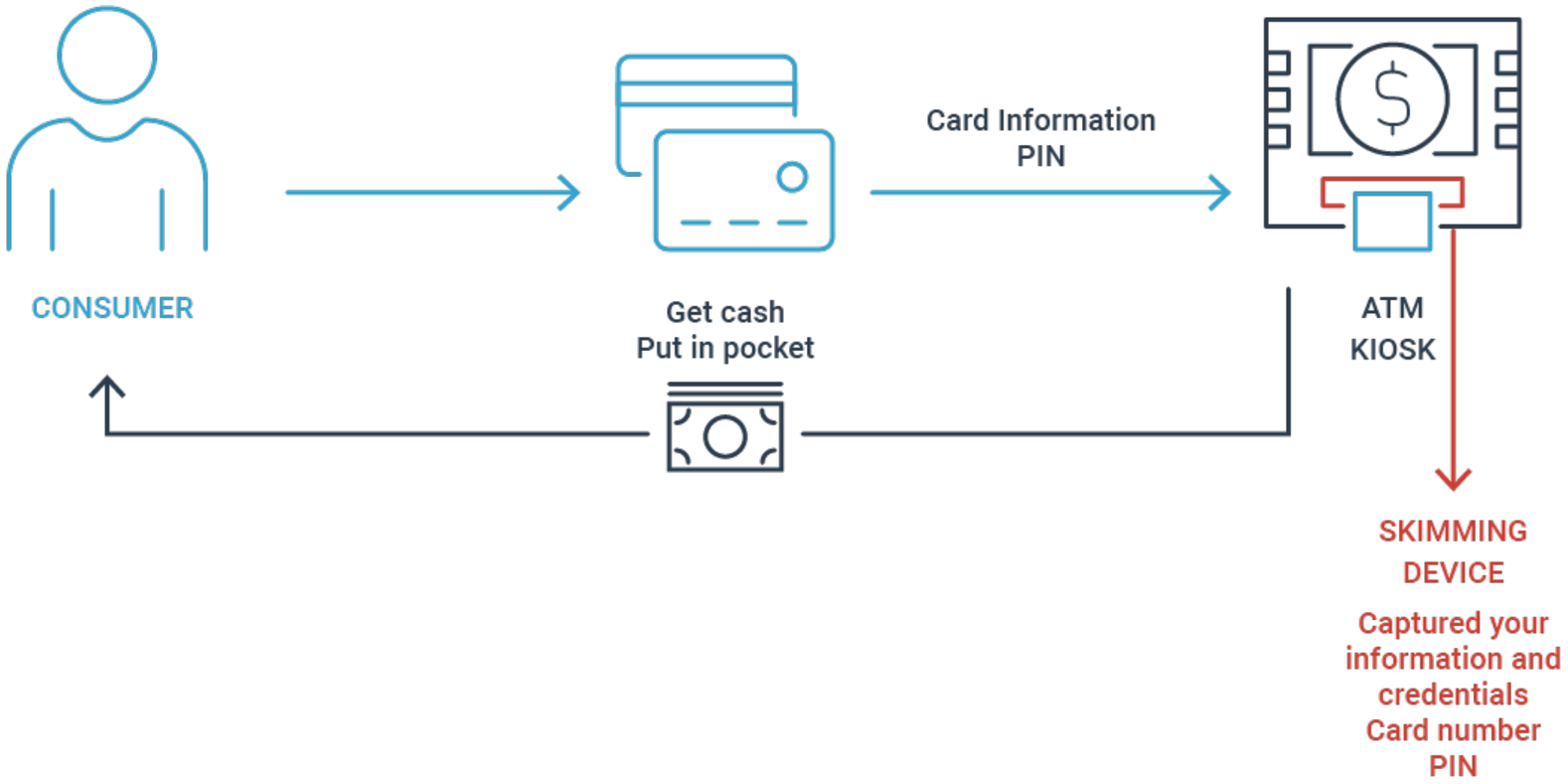
ADAPTIVE
They are not abandoning their tried-and-true methods, but they are consistently adding new methods and adjusting to be most effective.

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.

#GOSTRATEGIC

PHYSICAL ATTACKS

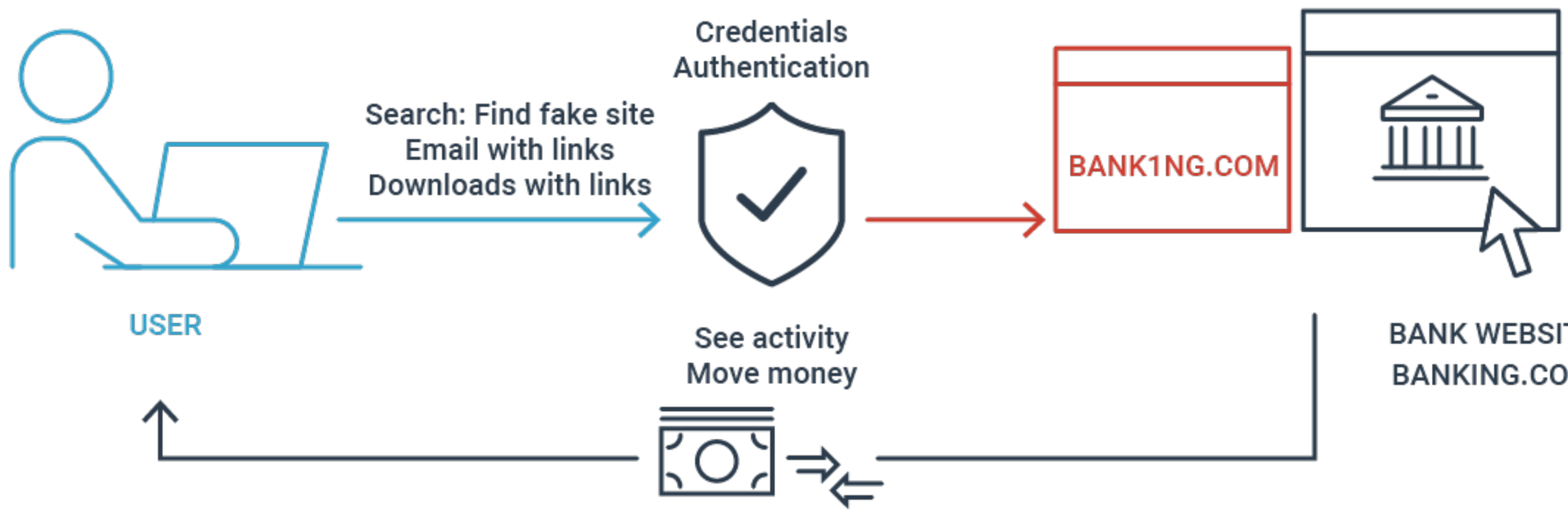
THE OLD WAY OF MITM ATTACKS



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

MAN IN THE MIDDLE

FAKE WEBSITES

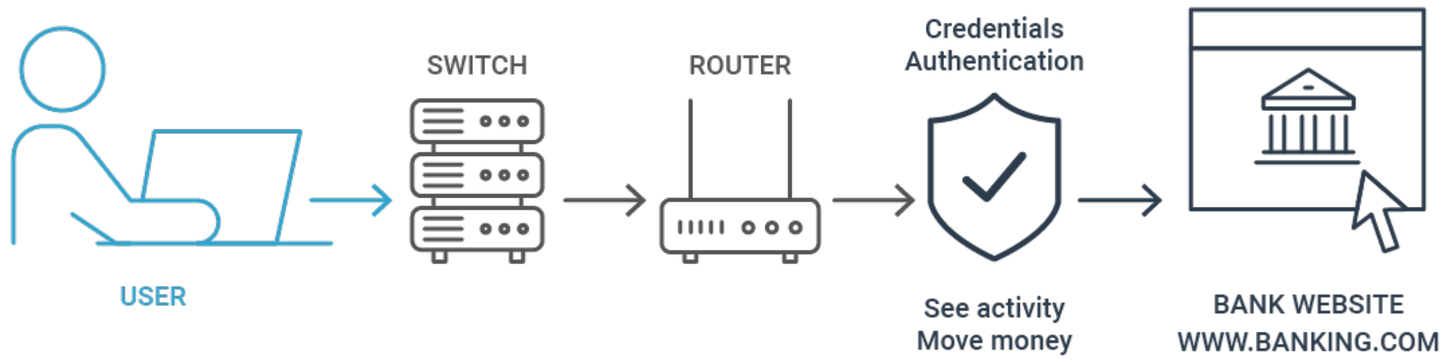


Captures your information and credentials through fake website, passes information on to real website to send confirmation back to user – appears as though nothing is wrong.

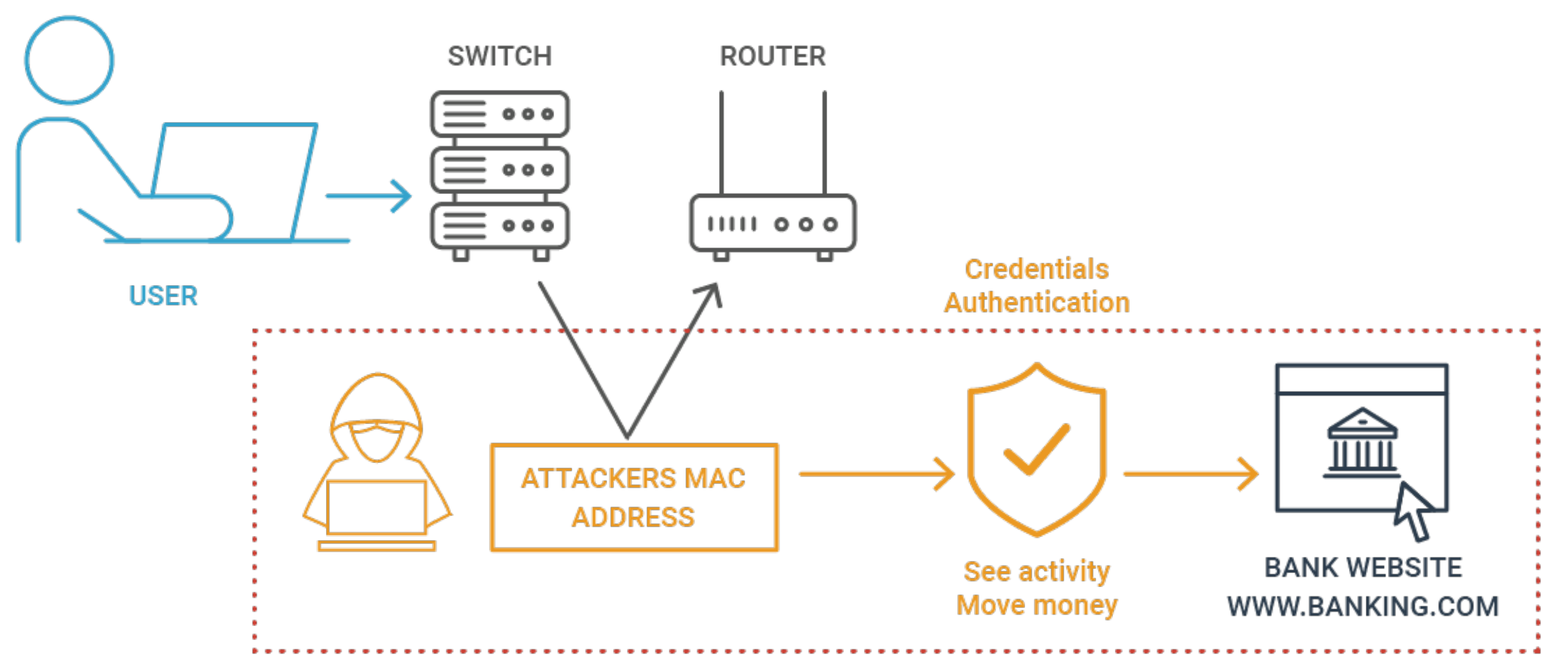
ARP ATTACKS

(SPOOFED) ADDRESS RESOLUTION PROTOCOL

Attacker associates a device MAC address with the IP address of another host. Your computer relies on the ARP and will use that to connect to what is listed as your gateway.



Attacker intercepts communication intended for the network device and fools the devices into connecting to the attacker's machine instead of each other.



STRATEGIC TREASURER

THE FULL SCOPE OF EXPOSURE

KNOW YOUR AREAS OF WEAKNESS

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

Cloud Security

Cyber Security

Segregation of Duties

Transaction & Daily Limits

CORPORATE PERIMETER

INTERIOR

Sensitive Data

Network

Desktop

SAN

TRANSPORT ACCESS

ACCESS CONTROL

EXTERNAL DATA

3rd PARTY

SaaS TMS

Banks

Employees

Temp/Contractors

Partners

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

#GOSTRATEGIC

STRATEGIC TREASURER

BE PREPARED

WITH A PLAN

IDENTIFY

Develop the understanding to manage cybersecurity risk to systems, assets, data, & capabilities.

PROTECT

Design and implement safeguards to ensure delivery of critical infrastructure services.

DETECT

Develop and execute activities to identify the occurrence of a cybersecurity event.

RESPOND

Plan and document the appropriate activities to perform once a cybersecurity event is detected.

RECOVER

Create and maintain plans to restore capabilities or services that may be impaired due to a cybersecurity event.

#GOSTRATEGIC

IDENTIFY, PROTECT & DETECT

DO THE BASICS WELL

- Identify devices, back up data
- Perform regular security evaluations

PARTNER WITH TECHNOLOGY EXPERTS

- Avoid skimping on cyber security budgets
- Review cyber insurance coverage and tap into insurers' expertise
- Prioritize frequent and transparent communication with critical partners

INVEST IN TRAINING

- Bolster the human firewall
- Target payments risk

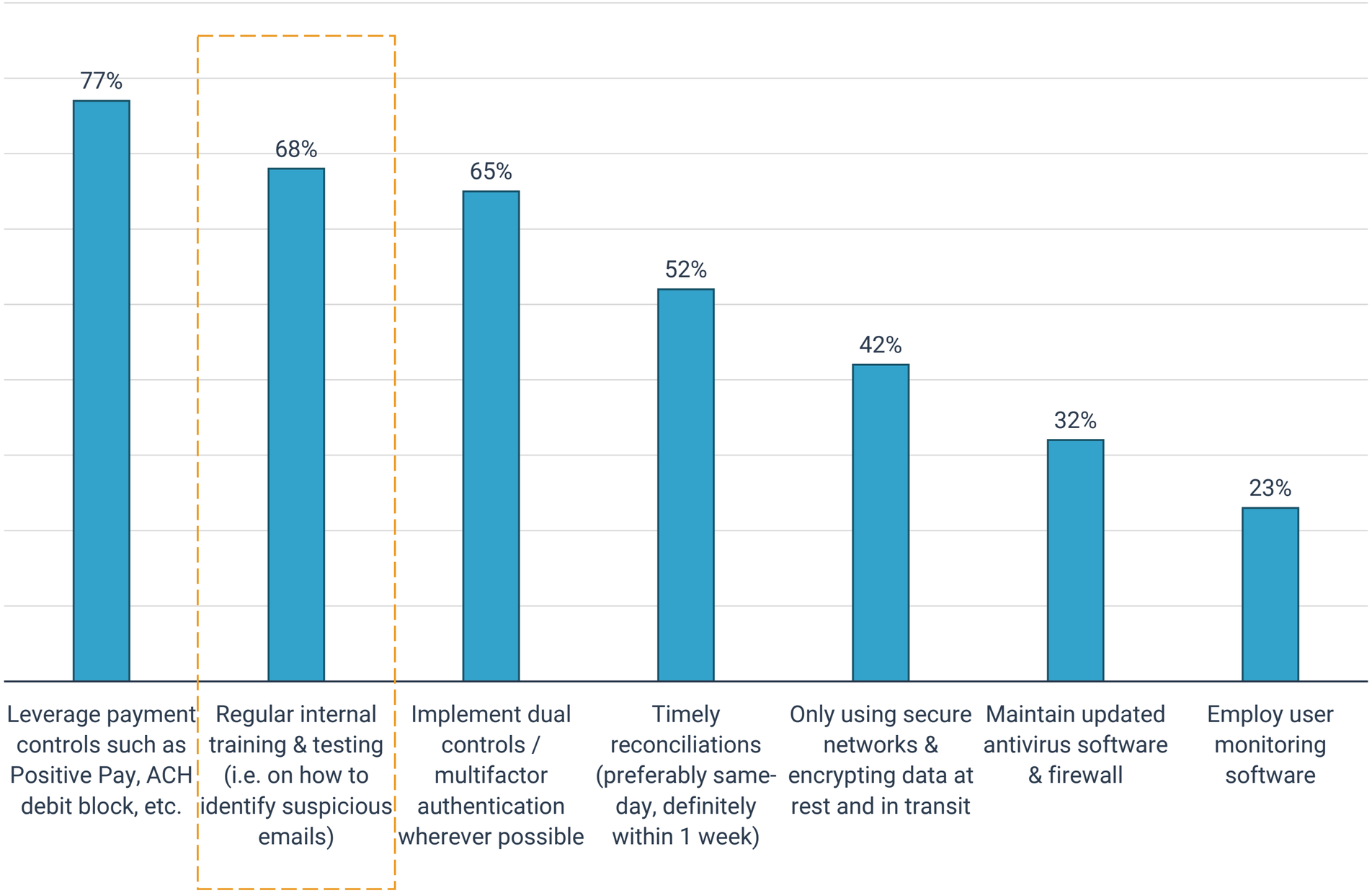
BUILD RESILIENCE

- Foster a risk management culture

SECURITY PRACTICES

BANKS WISH THAT CORPORATES WOULD LEVERAGE

» Bank: *What are the top three security practices or tools you wish all your clients used but that many are not currently leveraging?*

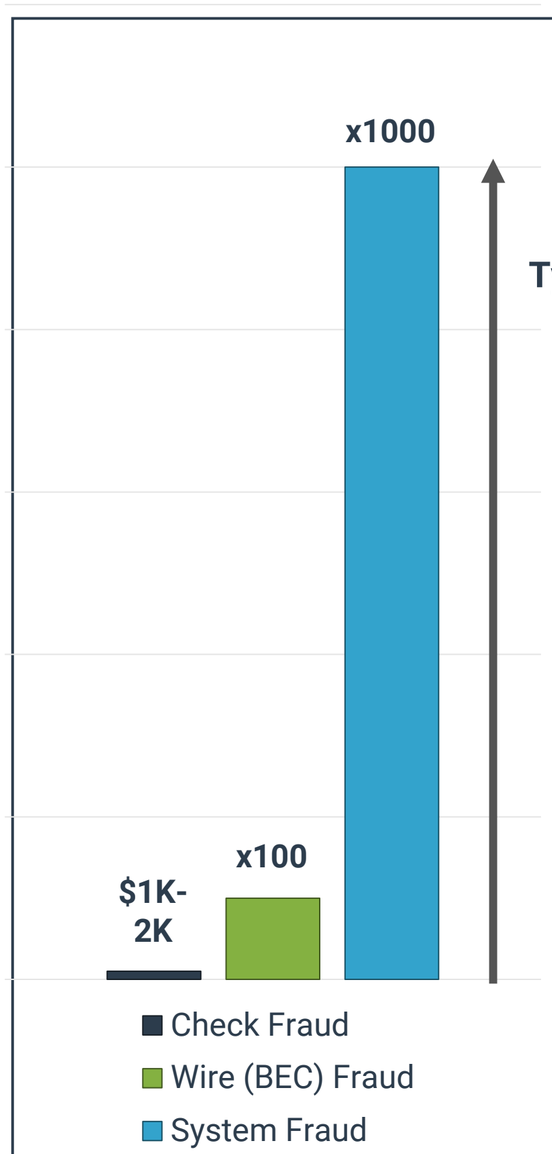


Source: 2022 Treasury Fraud & Controls Survey

STRATEGIC TREASURER

THREATS + DEFENSE

MORE IS BEING LOST TO FRAUD, BUT TRAINING CORRELATES TO LOWER LOSS



Typical Payout Range

SYSTEM FRAUD
$1M-10M+

WIRE (BEC) FRAUD
$130K+

CHECK FRAUD
$1K-2K

The above values are taken from calculations based off FBI, Banking Data and Strategic Treasurer estimates.

RANSOMWARE
averages
$570,000
in loss per payout.

Source: https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/

THE HUMAN ELEMENT

Organizations who train their employees on payment fraud, controls, and cyber fraud have a dramatically lower frequency of reported losses.

NON-TRAINED FIRMS EXPERIENCE MORE LOSSES:

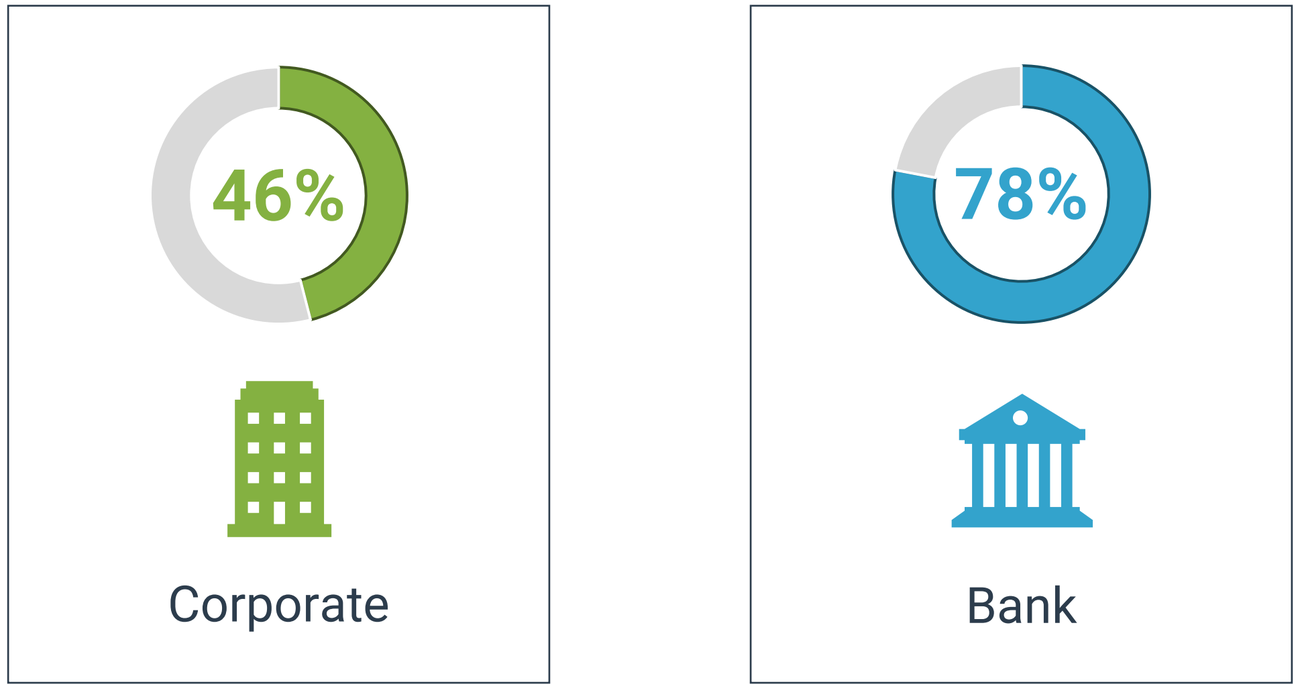
- **1.5X** Payment Diversion
- **2X** ACH Fraud
- **2.5X** System Takeover
- **4X** BEC Fraud
- **5X** Cyberfraud/Malware
- **5X** Ransomware

#GOSTRATEGIC

TREASURY SECURITY TRAINING & TESTING

CORPORATIONS NEED TO CLOSE A SIGNIFICANT GAP IN TRAINING & TESTING

» Of those organizations that provided security training to their employees, what percentage included testing or quizzes to gauge understanding?



Source: 2022 Treasury Fraud & Controls Survey

Strategic Treasurer

CURRENT INDUSTRY PRACTICES

AN EVALUATION

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

RESPOND & RECOVER

Actions to take following event detection – resolve events and foster resilience

Understand the Business Impact of Cyber Fraud

Create a Disaster Recovery Plan

Develop/Update Business Continuity Plans

Broadly Socialize an Emergency Preparedness Plan

Plan and Execute Testing Regularly

STRATEGIC TREASURER

TAKEAWAYS

TO HELP PROTECT YOUR ORGANIZATION'S ASSETS

- **THE BANK WILL NOT CALL/TEXT/EMAIL FOR YOUR CREDENTIALS**
- **DO PAYMENT SECURITY TRAINING & TESTING ANNUALLY**
- **STOP USING PUBLIC WI-FI**
- **VERIFY THE WEBSITE YOU ARE VISITING IS SECURE**
- **BOOKMARK OR FILE BANKING SITES, DON'T DEPEND ON A SEARCH**
- **PLAN FOR AN INCIDENT - STEPS TO TAKE, NUMBERS TO CALL**

#GOSTRATEGIC

STRATEGIC TREASURER

MORE TAKEAWAYS

TO HELP PROTECT YOUR ORGANIZATION'S ASSETS

- PUT BANK OFFERED SECURITY SYSTEMS IN PLACE
- HAVE A DEDICATED PAYMENTS COMPUTER
- MAKE COMPUTER/CYBER HYGIENE PART OF THE ROUTINE
- DESIGNATE RESPONSIBILITY FOR FRAUD PREVENTION
- MEET ON CYBER/PAYMENT SECURITY (TREASURY, CISO, IT)
- BENCHMARK YOUR PRACTICES

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 A. Jeffery,
Managing Partner

craig@strategictreasurer.com

+1 678.466.2222

TD Bank

Adrienne Terpak
Vice-President, Commercial Segment Manager

Adrienne.Terpak@td.com

SecureTreasury™
FRAUD PREVENTION TRAINING

Learn more about **SecureTreasury**

Download the Treasury Perspectives report and infographic:
https://bit.ly/3kqdoxe

Download Report

#GOSTRATEGIC