Building Defenses Against Fraud and Cybercrime

Fraud Mitigation Strategy for Payments Risk

Presented by:

- Carla Krieman, District Sales Manager, TD Bank
- Adrienne Terpak, CTP, Segment Manager, TD Bank
- Danny Bizjak, Sr. Treasury Management Officer, TD Bank

Featuring Subject Matter Expert:

- Denise DeRosa, Asst. Business Administrator, Middletown Township School District

TRUST | ADVICE | SECURITY

TD Bank, N.A. | Bank Deposits FDIC Insured

Agenda

Welcome and Introduction

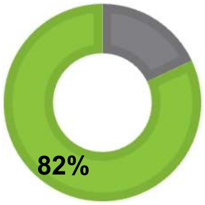
- Why We're Here
- Fraud Trends and Insights
- Fraud Mitigation and Payments Optimization
- Questions

"**Humans have the opportunity to be the greatest defense against cyberattacks**, but most are often **found to be the weakest link** in the chain. Lack of **proper training** and prioritization of a **strong security posture** leave employees vulnerable to accidentally releasing attacks into the business."

Source: McAfee Labs Threats Report

Fraud Defenses:

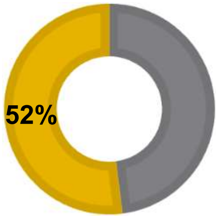
Scale Up, Never Let Your Guard Down



Fraud Susceptibility Rises for AP/AR but Declines for Treasury and Payroll

AP has again been identified as the area most susceptible to fraud (82%), representing a further deterioration since 2019 when 67% of respondents expressed this concern. Meanwhile, the perception of treasury's susceptibility to fraud has improved, dropping from 53% to 46%. This indicates AP is now the most susceptible area for fraud by a factor of almost two times any other area. Procurement also saw a sizable jump in susceptibility, from 17% to 28%, while payroll made notable improvements (26% to 12%).

Companies scale up their fraud defenses:
To combat potential fraud exposure, which has significantly increased in this remote work environment, firms have bolstered their fraud defenses by adopting multi-factor authentication (MFA), encryption and monitoring software/anomalous behavior detection/tracking. Concerns about AP fraud grew in 2020, with 82% of organizations identifying it as the most susceptible group while treasury and payroll fraud concerns notably subsided.



Supply Chain and Cyberfraud Remain Top Industry Concerns

Of their top three global economic and operational risk concerns, 81% of corporate respondents listed a global health pandemic that could affect the supply chain as their top concern, followed by cyberfraud (52%) and trade conflict with China (48%). These responses reflect current economic challenges that have led to an increase in cyberfraud. Banks mirror corporate responses regarding the pandemic's impact on the supply chain and cyberfraud, but differ in their third most pressing concern of interest rates (51%).

Notable Cyber Threats

Threats identified as "sever key themes" are part of TD's risk and threat mapping

Cyber Fraud Against Customers

Customers targeted by phishing, banking trojans, and social engineering for financial gain such as Business Email Compromise (BEC) or Email Account Compromise (EAC).

Cyber Attacks on Network, Systems, & Employees

Networks, systems, and employees targeted which could result in business disruption, data loss, or cyber-fraud losses

Third Party & Insiders Leverage Privileged Access

Access by unauthorized entities could result in data breaches containing sensitive internal and customer information

PAYMENT FRAUD LANDSCAPE

Actions:

Education:

- ✓ All vulnerable staff are trained

Prevention:

- ✓ Dual authentication
- ✓ Access and admin controls
- ✓ IT Security

Detection:

- ✓ Automation
- ✓ Reconciliation

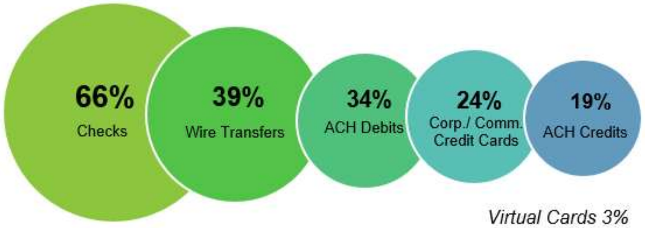
Targeting:

- 80% of businesses targeted
- Susceptible regardless of business size

Sources of Fraud:

- Business Email Compromise (61%)
- Outside Individual – forged check or stolen card (58%)
- Related Third Party - vendor or service provider (26%)

Payment Methods Targeted for Fraud:



Virtual Cards 3%
Faster & 3rd Party Pay 3%
eWallets, Crypto 2%

Source:
2021 AFP Payments Fraud and Control Survey

PHISHING CAMPAIGNS

Actions:

- ✓ Optimizes controls for quick detection and remediates live phishing and malware threats
- ✓ Employee report suspicious button is used to decrease click rate and increase report rate incrementally
- ✓ Proactively identify phishing sites using JavaScript Web Beacon

Targeting:

- Email
- Telephone
- Text message

Sensitive Data:

- PII
- Banking details
- Passwords

Well-Known Brands used in Phishing Scams:

- World Health Organization (WHO)
- Country-specific health agencies
- Companies

Business Email Compromise (BEC) is the most-often reported source of payments fraud attacks

TRUST | ADVICE | SECURITY

TD Bank | Building Fraud and Cybercrime Defenses

COVID-19 CYBER FRAUD

Actions:

- ✓ Tracking and reporting on COVID-19 related fraud and attacks
- ✓ Engaged in collaborative sharing with key external partners
- ✓ Produced a report on "Cyber & Privacy Risks Associated with Zoom"

Targeting:

- Stimulus check fraud
- Relief and unemployment payments
- New small business loans

Video Conference and Communication Platforms:

- 500k Zoom accounts sold on the Dark Web

Working from Home Risks:

- Increase and uncontrollable data exposure through personal as well as work-issued devices

RANSOMWARE

Actions:

- ✓ Tracks groups, attacks, and new developments
- ✓ Produced Ransomware Playbook
- ✓ Produces profiles on ransomware and attack stages

Targets:

- Major organizations
- Third-parties

Biggest Ransomware Attacks of 2020:

- FBI $1B USD
- Public & Private Sectors $144MM USD

Extortionist Tactics:

- Searching networks and steal the data before they encrypt the system
- Select information is shared on "name and shame" sites

TRUST | ADVICE | SECURITY

Denise DeRosa, Asst. School Business Administrator and Assistant Board Secretary
Middletown Township School District

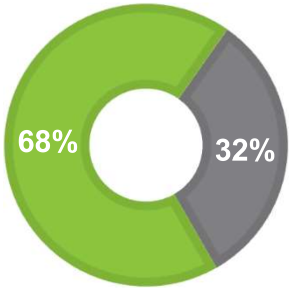
Total Revenue Budget: $171.73 million

Student Population: ~9,500

Number of Schools: 16
(includes 3 middle schools and 2 high schools)

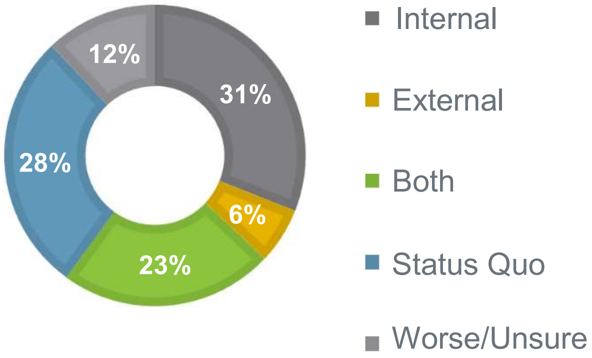
2020
TREASURY PERSPECTIVES
Survey Report

Working Capital Management:
Focus Bears Results



Over two-thirds of organizations place a heavy emphasis on optimizing working capital, which could be reflective of the challenging operational environment.

Sixty percent of firms noted improvements in working capital, while 28% have remained even, and only 4% indicated working capital deterioration during this timeframe. **Internal initiatives alone or with external financing (54%) showed the largest improvement.**



Managing Working Capital Beyond 2020

Five Key Changes:

- **Improve visibility to increase responsiveness** - streamline metrics and reporting, focus on key indicators.
- **Increase the frequency scenario modeling** for cash flow forecasting and develop proactive contingency plans.
- **Accelerate technology adoption and digital transformation** – increase operational efficiencies and embrace virtual, technology-enabled ways of working.
- Revisit service delivery models - **increase flexibility, resilience, and agility** to understand and manage risks across the supply chain and their impact on cash flow.
- Make working capital management a **cross-functional responsibility** and minimize activities that will jeopardize liquidity.

Source: Hackett Group 2020 Working Capital Study

Taking the first steps…where to begin

Build a strategy to optimize the use of various "Payment Rails"

- Commercial Credit Card* – efficient for both payer and payee; monetize payables with float and revenue opportunities
- ACH Transactions – economical and versatile
- Checks – Resource-intensive, time-consuming and expensive
- Wires – some transactions simply call for a Fedwire

Optimize your business payments to improve working capital and reduce operational costs.

*Not a revolving credit line

Cost-Benefit of Optimizing Payment Rails

Creating a (Virtual) Card Program	Converting Check to ACH	Outsourcing Checks
Cost Savings	**Cost Savings**	**Cost Savings**
Cost of a check: $3.00 $1,500 Monthly (500 Checks)	Cost of a check: $3.00 $1,500 Monthly (500 Checks)	Cost of a check: $3.00 $1,500 Monthly (500 Checks)
Avg Cost of a Card Payment: $1.50 $750 Monthly (500 Payments)	Cost of an ACH Payment: $.29 $145 Monthly (500 Payments)	Cost of a Bank issued Check: $2.34 $1,170 Monthly (500 Payments)
Cost Savings: $750/month	Cost Savings: $1,355/month	Cost Savings: $330/month
Revenue Opportunity Average Rebate: 100bps – 60bps Revenue Opportunity $1MM - $10K - $6K $2MM - $20K - $12K $3MM - $30K - $18K **ROI = +$19K – $15K (Annually)**	**Not all Checks can become Card or ACH. Some vendors remain in a world where checks are required. Overall, there is an "Optimization" of these rails and that is unique to every business.**	**In this scenario, all of the time and effort is reduced to one file that gets sent to the bank for processing.**

Optimization Strategy

Take the time to review your current payment mix

- Analyze where your payments are focused today.

Explore potential benefits of a (virtual) card program

- Offset expenses by monetizing a portion of spend.

Find the right payment solution for your business

- Consider your evolving needs to gain efficiencies.

Capitalize on the opportunity to streamline

- Implement your strategy with key partners.

Track the results and report benefits to key stakeholders.

Fraud Mitigation Strategy

Fraud Strategy: Layer 1 – Account Structure

For example:

4 Accounts comprised of:

Account 1: Check and ACH activity

Account 2: ACH Only

Account 3: Check only

Account 4: No Check or ACH

Check Positive Pay with Payee Verification

ACH Positive Pay

ACH Block

Check Block

Fraud Strategy: Layer 2 – Account Information

For example:

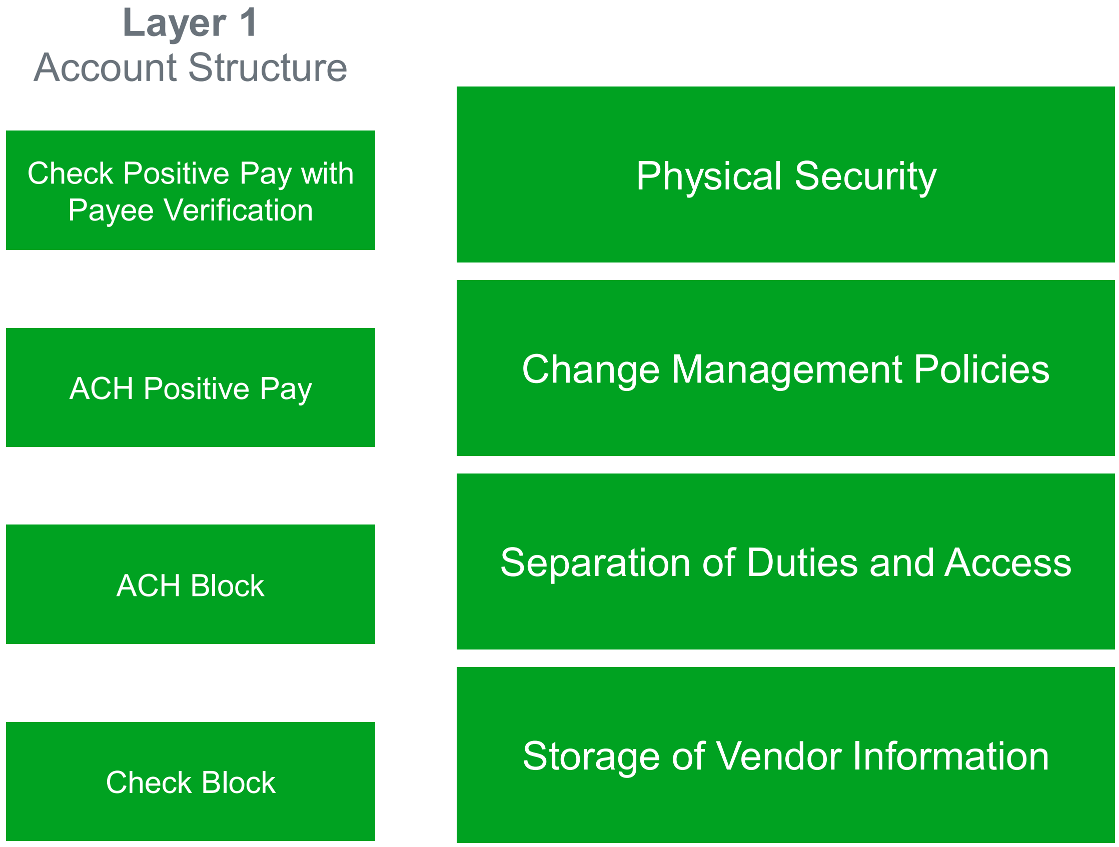
4 Accounts comprised of:

Account 1: Check and ACH activity

Account 2: ACH Only

Account 3: Check only

Account 4: No Check or ACH



Layer 1
Account Structure

Check Positive Pay with Payee Verification

ACH Positive Pay

ACH Block

Check Block

Physical Security

Change Management Policies

Separation of Duties and Access

Storage of Vendor Information

Fraud Strategy: People and Processes

For example:

4 Accounts comprised of:

Account 1: Check and ACH activity

Account 2: ACH Only

Account 3: Check only

Account 4: No Check or ACH

Layer 1 Account Structure	**Layer 2** Account Information	
Check Positive Pay with Payee Verification	Physical/Network Security	**Training and Education**
ACH Positive Pay Blocks/Filters	Change Management Policies	**Individual Resiliency**
ACH Block	Separation of Duties and Access	**Establishing a Risk Management Culture**
Check Block	Storage of Vendor Information	**Daily Reconcilement**

Overall Fraud Strategy

Layer 1 Account Structure	Layer 2 Account Information	Layer 3 People and Processes
Check Positive Pay with Payee Verification	Physical/Network Security	Training and Education
ACH Positive Pay Blocks/Filters	A/P Change Management Policies	Individual Resiliency
ACH Block	Separation of Duties and Access	Establishing a Risk Management Culture
Check Block	Storage of Vendor Information	Daily Reconcilement

Legend: Bank-Offered Products/Services | Dual Bank / Customer Approach | Customer Process/Tactics

Become More Resilient

In 2020, 74% of financial professionals reported that their organizations had been *victims of attempted or actual* fraud attacks, with 61% indicating that Account Payable is the most vulnerable business unit. Help safeguard your business through:

Technology

Deploy innovative technologies that enhance your company's safety and security

Tradecraft

Develop information sharing platforms, intelligence products, and operational playbooks that inform executive action and decision-making

Teamwork

Implement leading management practices and initiatives to maximize collaboration, learning, and innovation across functional areas

Build the Right Culture.

Robust technology and static fraud prevention processes are not enough.

Leaders must **build a culture in which fraud awareness is second nature** for the whole team.

Moreover, that culture must support teams to stay abreast of the latest threats, with a clear understanding of how to spot and avoid them.

> **“Establishing a culture of risk management and accountability ensures that security becomes part of the business and not an afterthought.”**

Source: McAfee Labs Threats Report

Thank You!

Cheryl Griffith
TD Bank, America's Most Convenient Bank®
SVP, Government Banking Group Manager
M: (908) 552-9442
Email: Cheryl.Griffith@td.com

Gordon Thomas
TD Bank, America's Most Convenient Bank®
Government Banking Relationship Manager
M: (609) 634-9599
Email: Gordon.Thomas@td.com

Carla Krieman
TD Bank, America's Most Convenient Bank®
District Sales Manager, Treasury Mgmt.
M: (610) 945-8199
Email: Carla.Krieman@td.com

Melissa D'Alessandro
TD Bank, America's Most Convenient Bank®
Government Banking Relationship Manager
M: (609) 502-1209
Email: Melissa.a.Dalessandro@td.com

Daniel Rodriguez
TD Bank, America's Most Convenient Bank®
Government Banking Relationship Manager
M: (201) 966-9777
Email: Daniel.Rodriguez@td.com

Lisa Semple
TD Bank, America's Most Convenient Bank®
Government Banking Relationship Manager
M: (908) 406-0343
Email: Lisa.Semple@td.com

Appendix

TRUST | ADVICE | SECURITY

Resources at your Fingertips

Resource	Link[1]
Cybersecurity and Infrastructure Security Agency (CISA)	Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data
	Webinar - K 12 Education Leaders' Guide to Ransomware Prevention, Response, and Recovery
	https://www.cisa.gov/ransomware-reference-materials-k-12-school-and-school-district-it-staff
	Security Tip (ST04-014)_Avoiding Social Engineering and Phishing Attacks
	https://www.cisa.gov/publication/secure-video-conferencing-schools
	https://www.cisa.gov/ransomware-trainings-and-webinars
Treasury Perspectives Survey (2020) Strategic Treasurer and TD Bank	https://strategictreasurer.com/2020-treasury-perspectives/

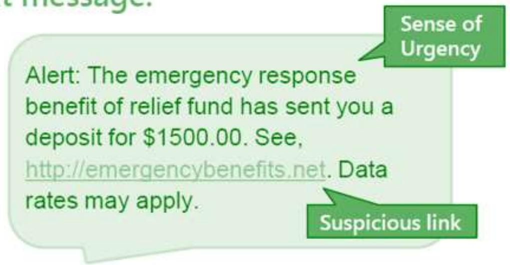
[1] TD Bank does not control the content or privacy policies associated with any third-party websites provided.

10 Common Risk Management Practices

- **Cultivate a Risk Management Culture** within the organization
- **Mandate Process Controls** including dual control and segregation of duties
- **Validate the origin and security of a website's URL** especially for banking and payments
- **Pick up the Phone** to authenticate **ALL** payment requests (internal & vendor)
- **Inspect Bank Accounts Daily** and reconcile frequently to spot potential fraud
- **Structure Bank Accounts** to isolate activities and leverage inherent controls
- **Use Fraud Deterrent Banking Services** like Positive Pay, ACH Blocks/Filters, etc.
- **Monitor Information** with credit reporting agencies and state record databases
- **Initiate Background Checks** on **ALL** employees and contractors
- **Notify the Bank & Law Enforcement** if you are under attack

Cyber Threats: Phishing

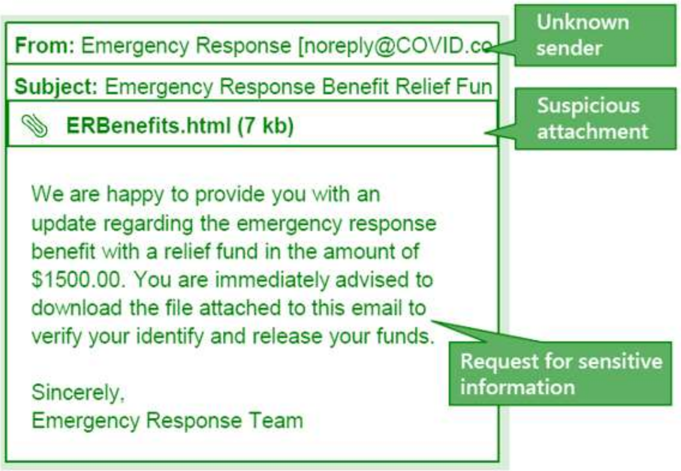
Text message:



Alert: The emergency response benefit of relief fund has sent you a deposit for $1500.00. See, http://emergencybenefits.net. Data rates may apply.

Sense of Urgency
Suspicious link

Email message :



From: Emergency Response [noreply@COVID.co

Subject: Emergency Response Benefit Relief Fun

ERBenefits.html (7 kb)

We are happy to provide you with an update regarding the emergency response benefit with a relief fund in the amount of $1500.00. You are immediately advised to download the file attached to this email to verify your identify and release your funds.

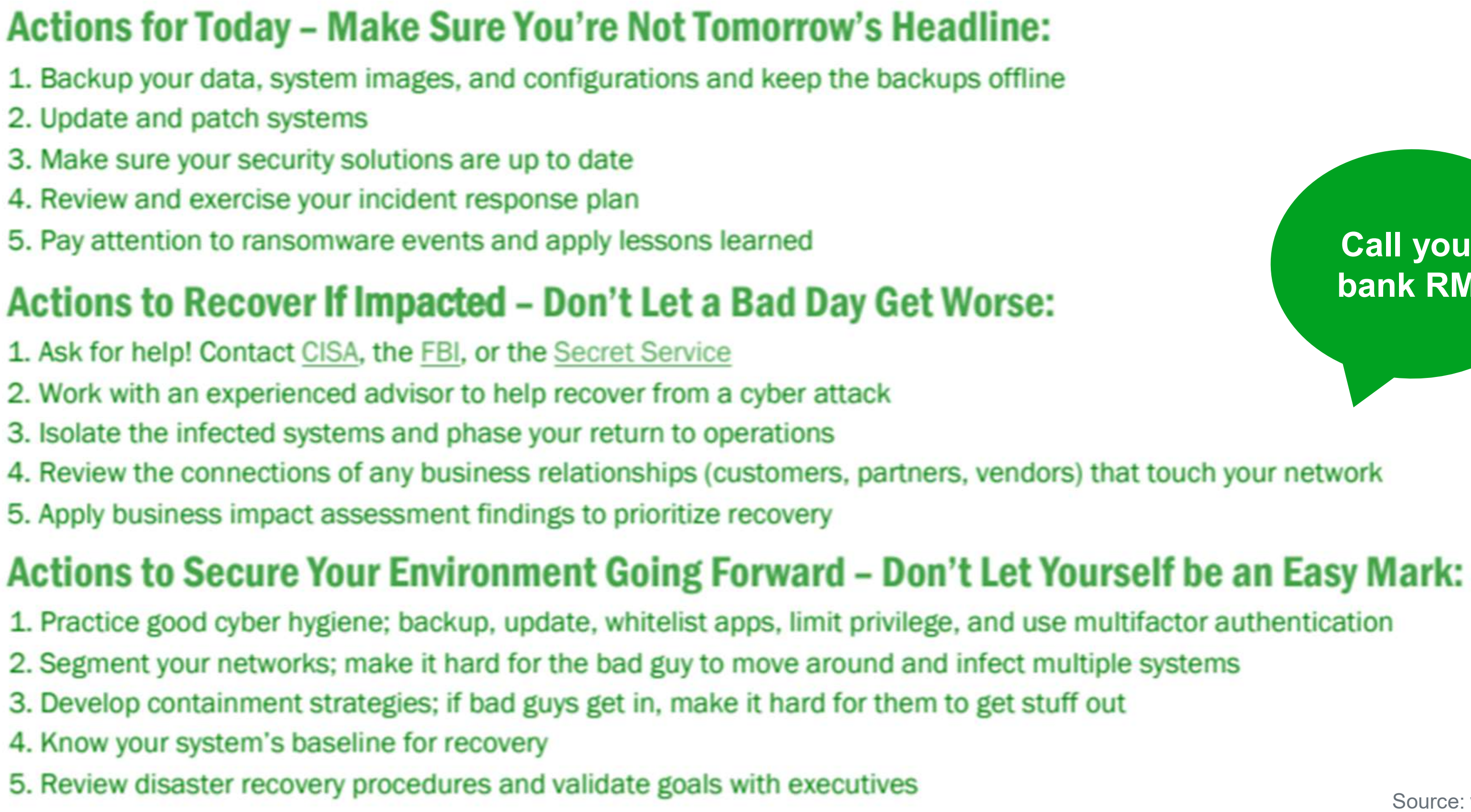
Sincerely,
Emergency Response Team

Warning Signs for Suspicious Messages:

- ☑ Unknown senders
- ☑ Generic greetings
- ☑ Hidden email senders or suspicious links
- ☑ Attachments with suspicious extensions
- ☑ Requests for sensitive information
- ☑ Urgency or call to action
- ☑ Errors, or something being "off"

TRUST | ADVICE | SECURITY

Ransomware Mitigations – Defend Today, Secure Tomorrow



Actions for Today – Make Sure You're Not Tomorrow's Headline:

1. Backup your data, system images, and configurations and keep the backups offline
2. Update and patch systems
3. Make sure your security solutions are up to date
4. Review and exercise your incident response plan
5. Pay attention to ransomware events and apply lessons learned

Actions to Recover If Impacted – Don't Let a Bad Day Get Worse:

1. Ask for help! Contact CISA, the FBI, or the Secret Service
2. Work with an experienced advisor to help recover from a cyber attack
3. Isolate the infected systems and phase your return to operations
4. Review the connections of any business relationships (customers, partners, vendors) that touch your network
5. Apply business impact assessment findings to prioritize recovery

Actions to Secure Your Environment Going Forward – Don't Let Yourself be an Easy Mark:

1. Practice good cyber hygiene; backup, update, whitelist apps, limit privilege, and use multifactor authentication
2. Segment your networks; make it hard for the bad guy to move around and infect multiple systems
3. Develop containment strategies; if bad guys get in, make it hard for them to get stuff out
4. Know your system's baseline for recovery
5. Review disaster recovery procedures and validate goals with executives

Call your bank RM!

Source: www.CISA.gov