



Cybersecurity Strategies for Preventing Business Fraud

Hosted by Rockland Trust

Featuring Citrin Cooperman Advisors, LLC

Housekeeping

- This event being hosted live through Zoom.
- To cut down on background noise, all attendees are muted.
- Have questions? Enter them in the Q&A tab on your screen – we will be answering questions at the end of our webinar.
- Contact information for our speakers will also be included at the end of this webinar for reference.
- We will share this recorded presentation with everyone in roughly two business days.



Speakers



Stacey Coyne

VP, Institutional Banking & Treasury
Management Team Leader
Rockland Trust



Kevin Ricci, CISM, CISA, CRISC, MCSE, QSA

Partner
Citrin Cooperman



Agenda

- The Cyber Threat Landscape
- Costs and Causes of a Data Breach
- Best Practices
- Micro Risk Assessment
- Questions

Cybersecurity Overview

Let's establish a baseline...

1. What is cybersecurity?

- “Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information”

2. What does cyber security awareness mean?

- Being cybersecurity aware means you understand what the threats are, and you take the right steps to prevent them



Today's Cyber Threat Landscape

40+ Billion Records Were Lost, Stolen, or Exposed In 2021

Increase In the Compromised Records in 2021 vs 2020: 4 Billion

2022 Global Average Cost per Breach: \$4.35M

43% of Cyber Attacks Target Small Organizations

91% of Breaches Are the Result of Phishing Attacks

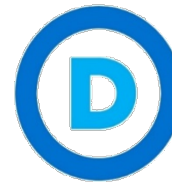
Average Cost of a Breach Is 61% Less When Unprepared

Ransomware attacks cause an average of 21 days of downtime







Average Days to Detect a Breach: 207
Average Days to Contain a Breach: 70



Once More Unto the Breach

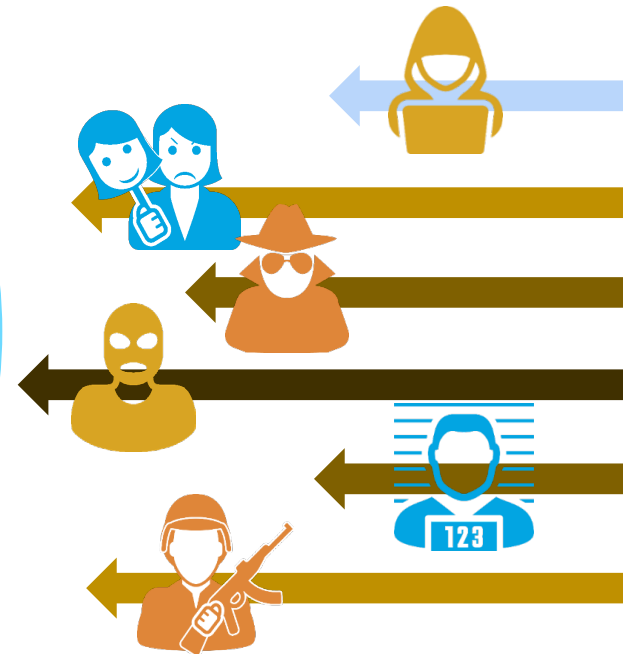
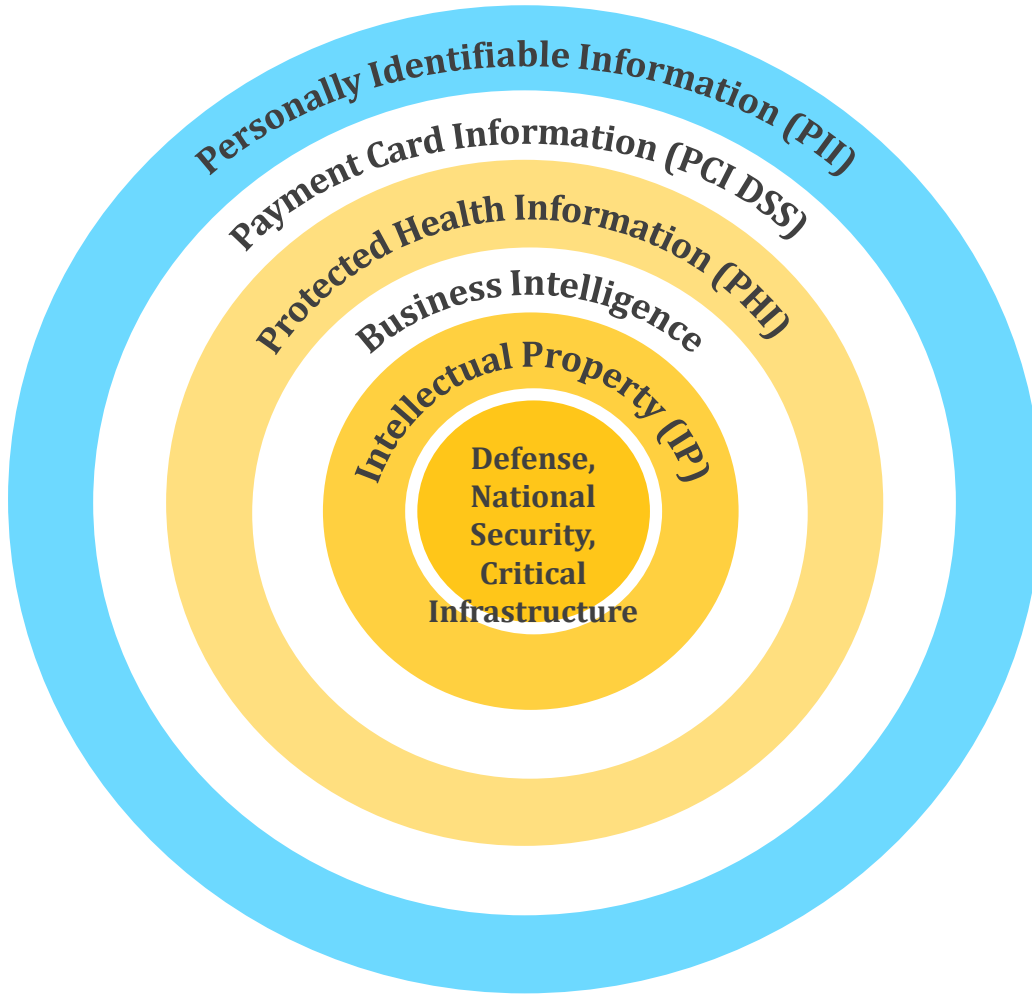


Looking Under the Hoodie

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hackers might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

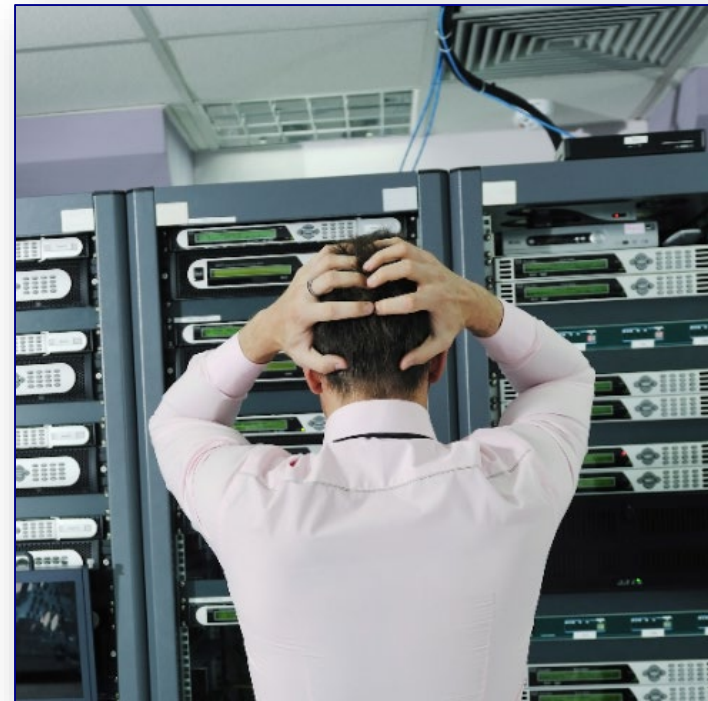


Motivations & Incentives



What Are Some Causes of Data Breaches?

- Malicious insider
- Physical security compromise
- Cloud or server misconfiguration
- Compromised credentials
- **Social engineering**

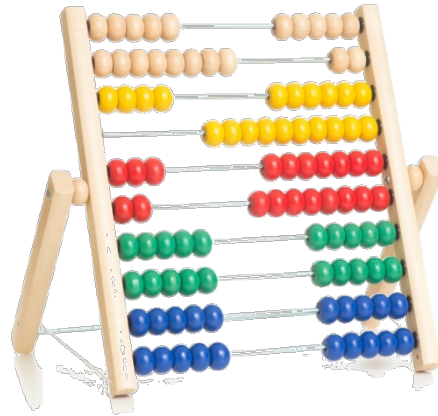


Another Day at the Breach

- ✈ Fines and penalties
- ✈ Technology expenditures
- ✈ Forensics
- ✈ Legal counsel
- ✈ Notification
- ✈ Downtime
- ✈ **Reputation**



Plan A: Go Old School



Plan B: Implement Cybersecurity Best Practices

- Assess, remediate, repeat
- Password hygiene & multi-factor authentication
- Continuous monitoring
- Service Organization Controls (SOC) reports
- Update your technology
- Work from home controls
- Penetration & vulnerability tests
- Incident response preparation
- Awareness training
- Spear phishing simulations



Spear Me the Details

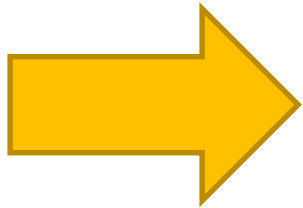
- Phishing has evolved into spear phishing
- The email appears safe but has a sinister purpose
- Awareness and education are the best weapons against this threat



Gone Phishin'

The key question to ask when receiving an email that :

- asks you to provide sensitive information
- click on a link or open an attachment
- request to change financial data/payment instructions



Did I expect this request from this person at this time?

If you are unsure, then your next step is to contact the sender by phone to confirm the legitimacy.

It is critical to **ALWAYS** verify financial account details or wire instructions with your vendors by phone, every time there is a change to financial data.



Common Threats



Jane in your accounting department receives an email from Joe, a well-known vendor



The email looks legitimate and the writing seems like Joe's. Joe asks Jane to update payment information to a new bank account



Joe may have sent the email, it is possible that someone else could have intercepted the email and changed the account numbers before it got to Jane



A King's Ransom

- Dangers of ransomware
 - Encryption
 - Data is publicly exposed
- Dangers of paying
- Ransoms can be negotiated



Getting Off the Hook

- Trust but verify
- Enable warning banners for external senders



WARNING: This email originated from outside the organization.

- For many companies providing spear phishing training, they do not cover the other modes of social engineering:
 - **SMiShing** is an attack via text message
 - **Vishing** is a voice attack via a phone call



Getting Off the Hook (continued)

- Look for errors

From: Mary Scanlan <Mary.Scanlan@R0cklandTrust.com>

Sent: Wednesday, March 3, 2021 12:20 PM

To: Jane Johnson <Jane.Johnson@RocklandTrust.com>

Subject: RE: New Wire Transfer

Hi Jane,

Thanks so much! Please send the wire to:

Jack Smith

101 Main Street

Boston, MA

Routing #: 123456789

Account #: 987654321

Payment Amount: \$35,000

Memo: Invoice Payment for #555

Please send this as soon as you can and let me know when this is done!

Best,
Mary

R0cklandTrust.com
is **NOT** the correct
domain name – be
sure to check the
full email



Farewell Sweet Prince

Police arrest alleged 'Nigerian prince' email scammer in Louisiana

USA TODAY NETWORK Charles Ventura, USA TODAY Published 6:22 a.m. ET Dec. 30, 2017 | Updated 9:46 a.m. ET Dec. 30, 2017



Louisiana man charged with 269 counts of wire fraud and money laundering



What is Payments Fraud?

Payments fraud –

- When financial information is stolen from a business by a fraudulent party (fraudster) and is used to complete illegal transactions
- The top vulnerabilities are:

**Credit Card/
Merchant
Services Fraud**

Wire Fraud
Fraud committed
through
electronic
communication
means

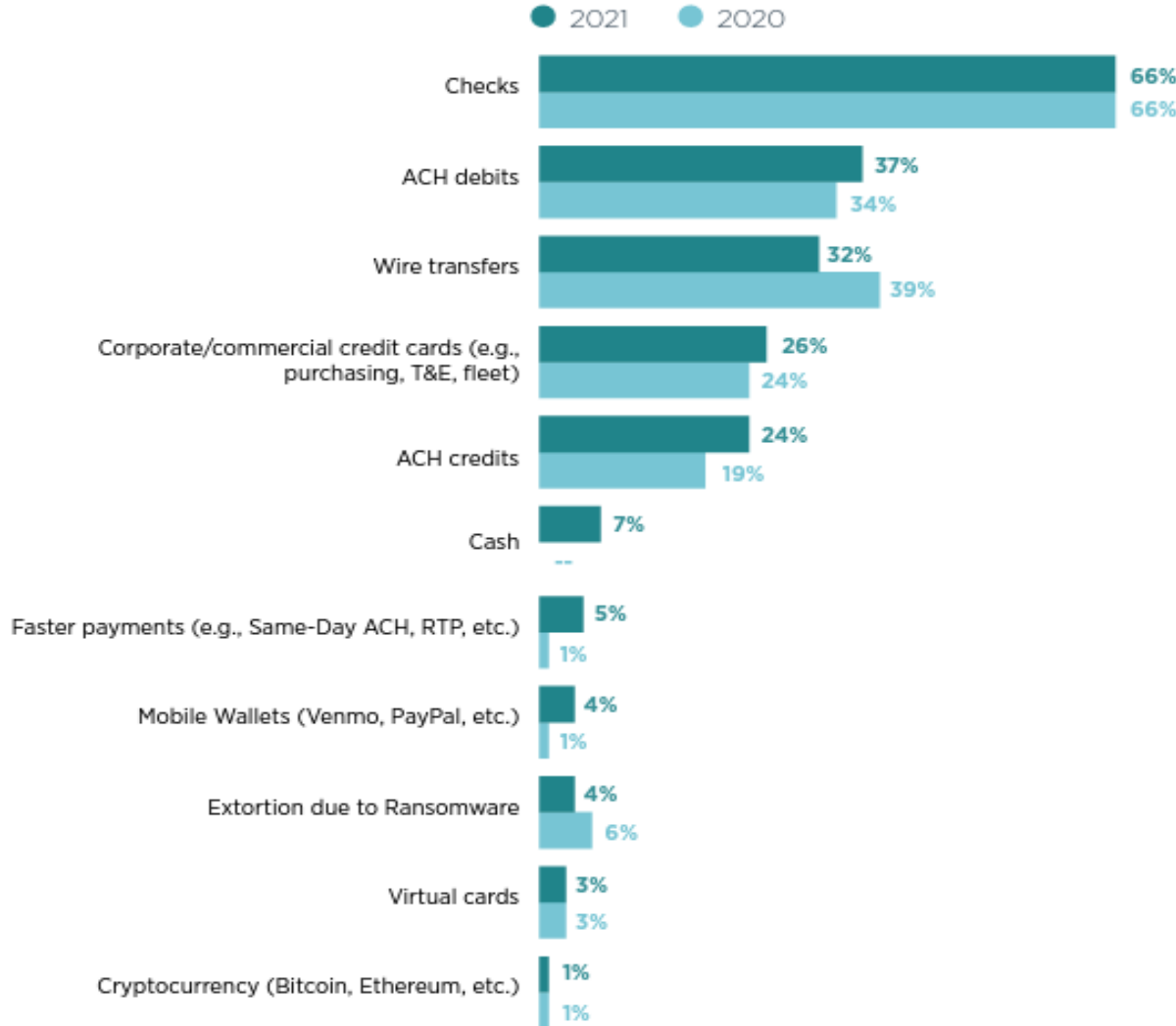
**Check
Fraud**
Fraud committed
through the use
of paper checks

ACH Fraud
Fraud committed
through the
Automated
Clearing House
network



Payments Fraud

Payment Methods Subject to Attempted/Actual Payments Fraud
(Percent of Organizations)



Prevention Strategies

Three basic, but **key rules**, that our treasury management team stresses are:

Rule #1: Always verify new or updated payment information over the phone with a known contact

Rule #2: Think twice before you click

Rule #3: Work with a banker to implement fraud prevention tools

➤ Ex. Positive Pay

The chances of recovering lost funds is significantly reduced after 24 hours.


If your business suspects or has experienced fraud – call your bank immediately!



The SCORE Report



Let's put your business to the test...



CITRINCOOPERMAN
FOCUS ON WHAT COUNTS

SCORE Report™ Risk Summary Dashboard

ABC Company

Security, Compliance, and Operations Risk Evaluation

Category	Item	Status	Score
IT Operations	Staffing	↓	Low
	IT policies and procedures	↓	Low
	Steering committee	○	Low
	Security event history	↓	Low
Physical Security	Entrance security	↓	Low
	Access tracking	↓	Low
	Environmental controls	↓	Low
Logical Security	User ID assignments	↓	Low
	User ID review	↑	Low
	Password strength	↓	Low
	Password change frequency	↓	Low
	Handling of terminated users	↓	Low
	Network equipment passwords	↓	Low
Automated login requirement	↑	Low	
Mobile Devices	Policies	○	Low
	Phone and tablet security	○	Low
	Laptop security	○	Low
Recovery	Policies	↓	Low
	Backup power	↓	Low
	Redundant ISP	↓	Low
	Proper backup scope	↓	Low
	Frequency	↓	Low
	Offsite procedures	↓	Low
	Backup security	↓	Low
	Viability testing	○	Low
	Disaster recovery policies	○	Low
Cyber insurance	↓	Low	
Network Security	Web filtering	↓	Low
	Email filtering	↓	Low
	Email encryption	○	Low
	Firewall and antivirus	↓	Low
	Wireless security	↓	Low
Online Security	Cloud data policies	↓	Low
	Cloud data backups	↑	Low
	Cloud data security	↑	Low
	Website policies	○	Low
	Website backups	○	Low
	Website security	↓	Low
Social media policies	↑	Low	
Data Privacy and Security Compliance	PII policies and security	↓	Low
	PII training	○	Low
	PII breach response plan	↑	Low
	PHI policies and security	↑	Low
	PHI training	↑	Low
	PHI breach response plan	↑	Low
	PCI DSS policies and security	↑	Low
PCI DSS training	↑	Low	
PCI DSS breach response plan	↑	Low	
System and Hardware Controls	RAID configurations	↓	Low
	Warranties and support	○	Low
	Data encryption and disposal	○	Low
	Equipment life cycle	↓	Low
	Copier security	○	Low
	Server monitoring	↓	Low
	Change management	○	Low
Remote computing policies	↓	Low	

This communication is intended only for the information and use of the management of ABC Company, and is not intended to be and should not be used by anyone other than those specified parties. The observations contained in the SCORE Report above were the result of limited inquiries performed during our comprehensive high-level risk assessment. These inquiries do not take the place of a full comprehensive IT risk assessment, which if engaged to perform such assessment, may change or increase the number of observed control deficiencies.



The SCORE Report





CITRINCOOPERMAN®
FOCUS ON WHAT COUNTS

SCORE Report™ - Hot Spots

ABC Company

Security, Compliance, and Operations Risk Evaluation

Section	Issue	Risk	Solution	Risk Level
Data Privacy and Security Compliance				
PII Training	There is no formal training in place to provide guidance regarding the protection of personally identifiable information (PII).	As a business that maintains PII, the Company is required to comply with state security and privacy regulation (e.g. Massachusetts's data security regulation 201 CMR 17) requirements. These regulations typically require, among other things, ongoing employee training on the proper use of the computer system and the importance of PII. Lack of training could result in significant fines while also hindering employees from making good security decisions.	Provide periodic security and privacy training to all employees that covers best practices on protecting PII.	High
PII Breach Response Plan	There is no formal response plan in place to provide remediation steps in the event of a personally identifiable information (PII) data breach.	Without a set of periodically tested breach response procedures in place, the response may not be organized and the remediation time may be significantly extended.	Document all PII breach response policies and procedures, with detailed descriptions and action steps. Test, to the fullest extent possible, the plan on an annual basis. Update the documentation as policies and procedures change.	High
PCI DSS Training	There are no formal policies or training in place to provide guidance regarding the protection of cardholder data.	This is a requirement of PCI DSS v3.1. In the event of a data breach, lack of such policies and training would result in the organization being considered not in compliance with the PCI DSS and could result in significant fines and penalties. It also hinders employees from making good security decisions.	Complete the requirements of the PCI DSS SAQ that addresses the needs of the regulations surrounding the care of cardholder data. Update the documentation as policies and procedures change and submit on annual basis. Provide periodic training to all employees on the importance of protecting cardholder data.	High
PCI DSS Breach Response Plan	There is no formal response plan in place to provide remediation steps in the event of a cardholder data breach.	Without a set of periodically tested breach response procedures in place, the response may not be organized and the remediation time may be significantly extended.	Document all PCI DSS breach response policies and procedures, with detailed descriptions and action steps. Test, to the fullest extent possible, the plan on an annual basis. Update the documentation as policies and procedures change.	High

The SCORE Report

For remote connectivity and cloud applications, is multi-factor authentication required?

Do you perform viability testing on your backups on a periodic basis?

Do you provide security awareness training as part of the onboarding process?

Do you periodically test your end users' ability to detect and avoid spear phishing attacks?

If you have a multifunction copier, does it have a security solution installed?



The SCORE Report

Are key IT procedures and credentials documented and accessible by trusted and authorized members of the company?

Do you have a third-party risk management system to evaluate your vendor's cybersecurity efforts?





Do you review event logs for suspicious activity on a regular basis?

Are your servers and workstations running operating systems that are supported by the vendor (e.g., no Microsoft Windows Server 2008 or Windows 7)?

Do you perform penetration tests or vulnerability scans on a periodic basis?



The SCORE Report

Number of "YES" Answers	Risk Level
10	 A semi-circular gauge with five segments: Very Low (green), Low (light green), Moderate (yellow), High (orange), and Very High (red). The needle points to the Very Low segment.
7 - 9	 A semi-circular gauge with five segments: Very Low (green), Low (light green), Moderate (yellow), High (orange), and Very High (red). The needle points to the Low segment.
4 - 6	 A semi-circular gauge with five segments: Very Low (green), Low (light green), Moderate (yellow), High (orange), and Very High (red). The needle points to the Moderate segment.
0 - 3	 A semi-circular gauge with five segments: Very Low (green), Low (light green), Moderate (yellow), High (orange), and Very High (red). The needle points to the High segment.





Exclusive offer! For viewers of this webinar:

Citrin Cooperman is offering a 50% discount on the SCORE Report, the proprietary cybersecurity risk assessment that's designed to identify and help remediate the risks that threaten your business before cybercriminals can take advantage of them

Contact Kevin Ricci (kricci@citrincooperman.com) to take advantage of this offer!



Thank You!



Stacey Coyne

VP, Institutional Banking & Treasury Management
Team Leader
Rockland Trust

Office: 508.732.3382
Stacey.Coyne@RocklandTrust.com



Kevin Ricci, CISM, CISA, CRISC, MCSE, QSA

Partner
Citrin Cooperman

Office: 401.421.4800
kricci@citrincooperman.com



Questions

