

Navigating the Digital Minefield of 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



Lisa Morrissey

VP, Treasury Management Team Leader
Rockland Trust



Kevin Ricci

Partner
Citrin Cooperman Advisors LLC

Credentials - Licenses include:

- ISACA Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Microsoft Certified Systems Engineer (MCSE)
- Qualified Security Assessor (QSA)
- Certified Information Security Manager (CISM)



Lumi Taiwo

Manager
Citrin Cooperman Advisors LLC



Key Topics

- Defining Cybersecurity
- Today's Cyber Threat Landscape
- Identifying Fraud Threats
- Best Practices for Your Business
- 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 cybersecurity awareness mean?

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



Today's Cyber Threat Landscape

22+ Billion Records Were Lost, Stolen, or Exposed In 2022

4,100 Publicly Disclosed Data Breaches

2023 Global Average Cost per Breach: \$4.45M

43% of Cyber Attacks Target Small Organizations

91% of Breaches Are the Result of Phishing Attacks

82% of Data Breaches Involved Data Stored in the Cloud

Ransomware attacks cause an average of 21 days of downtime

Average Days to Detect a Breach: 204
Average Days to Contain a Breach: 73



Once More Unto the Breach



LastPass



CNA

EQUIFAX



GEICO



Marriott
HOTELS · RESORTS · SUITES

Capital One



YAHOO!

Sabre

T Mobile



Anthem

Progress
MOVEit



Another Day at the Breach

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



Common Fraud Strategies

A few of the most prevalent strategies include:

Malware: “Software used to gain unauthorized access to IT systems in order to steal data, disrupt system services or damage IT networks”

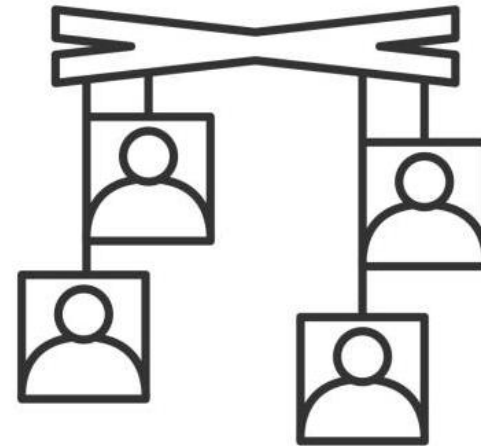
- **Ransomware:** A “type of malware identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided”



Common Threats

Social Engineering: When an attacker “uses human interaction (social skills) to obtain...information about an organization”*

- **Phishing:** A form of social engineering where attackers use “email or malicious websites to solicit personal information or to get you to download malicious software by posing as a trustworthy entity”**



*Source: [CISA.gov, Avoiding Social Engineering and Phishing Attacks](https://www.cisa.gov/avoiding-social-engineering-and-phishing-attacks)

**Source: [CISA.gov, Phishing General Security Postcard](https://www.cisa.gov/phishing-general-security-postcard)



Spear Me the Details

- Phishing has evolved into **Spear Phishing**
- Targets a specific individual, often with information relevant to them
- The email appears safe but has a sinister purpose



A King's Ransom

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



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



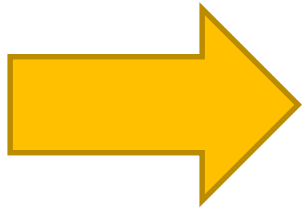
Louisiana man charged with 269 counts of wire fraud and money laundering



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



Getting Off the Hook

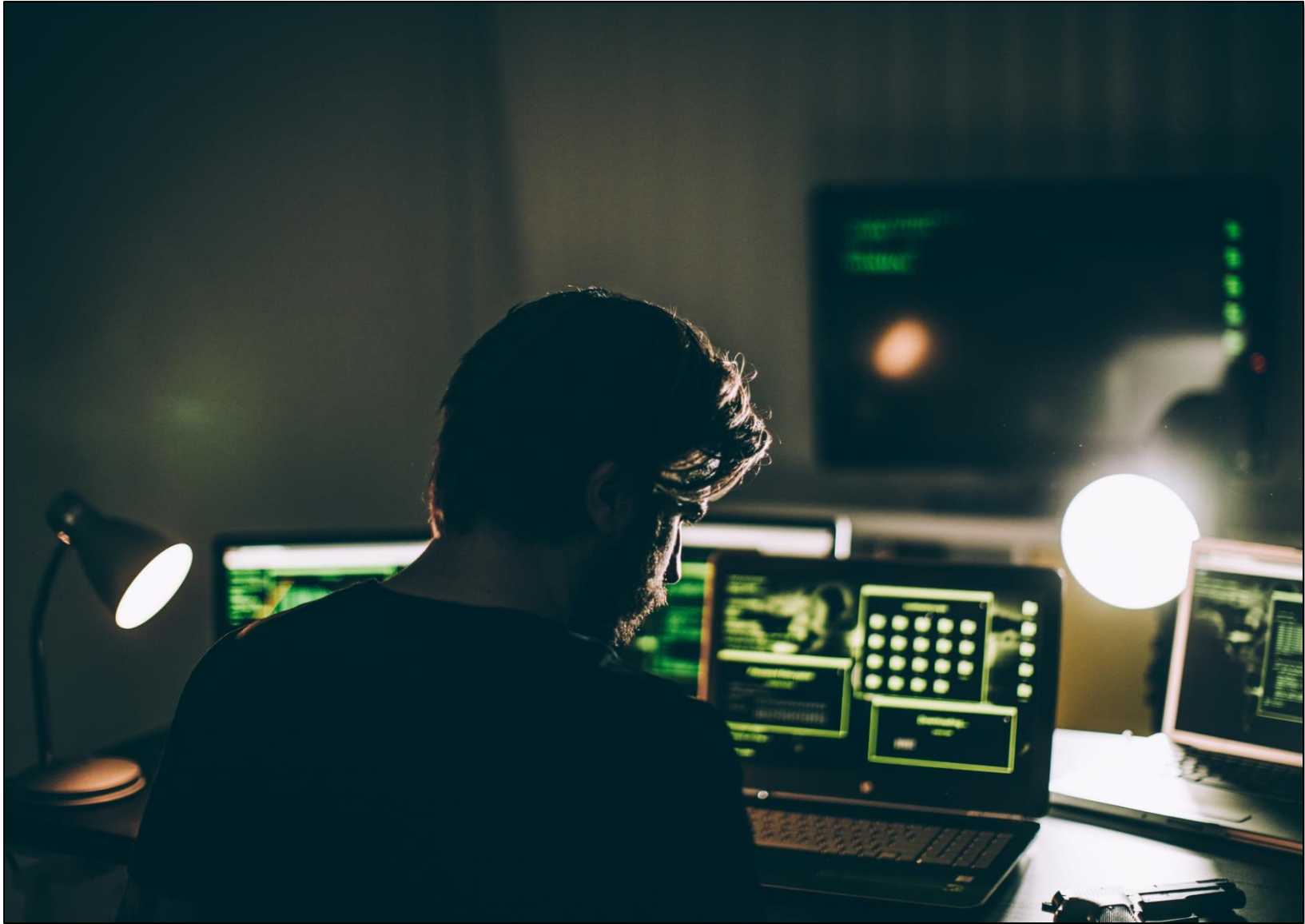
- Look for errors or suspicious signs
 - INFO@email.org
 - INF0@ernail.org
- Trust, but verify
- Enable warning banners for external senders

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



Penetration Testing



A Look at Artificial Intelligence (AI)

Access to AI gives fraudsters the ability to:

- Instantly generate sophisticated social engineering attacks
 - Create malware with minimal effort and coding skills
 - Create websites hosting legitimate AI tools to access your data
-

Be aware that:

- There are few safety mechanisms in place to prevent the upload of sensitive information to AI chatbots
- Chatbots are susceptible to hackers, so be aware of what information you and your team provide on these sites



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**

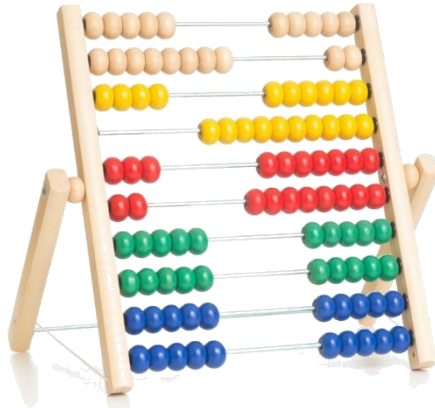
Wire Fraud
Fraud committed
through
electronic
communication
means

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

ACH Fraud
Fraud committed
through the
Automated
Clearing House
network



Plan A: Go Old School



Plan B: Implement Cybersecurity Best Practices

Assess, remediate, repeat

Password hygiene & multi-factor authentication

Continuous monitoring

Third-Party Risk and Service Organization Controls (SOC) reports

Update your technology

Work from home controls

Penetration & vulnerability tests

Incident response preparation (insurance)

Awareness training

Spear phishing simulations



Plan B: Work with Your Bank

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 **preventative tools**, including Positive Pay, purchase limits, and ACH filters/blocks

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



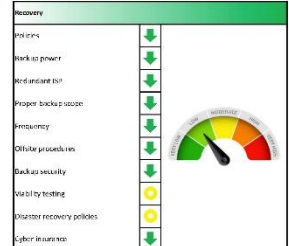
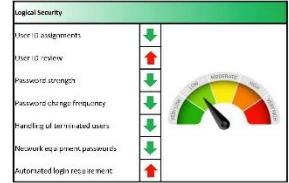
Let's put your business to the test...



The SCORE Report



SCORE Report™ Risk Summary Dashboard
ABC Company
Security, Compliance, and Operations Risk Evaluation



ABC Company and its subsidiaries are not licensed by any state as the administrator of ABC Company and its subsidiaries. ABC Company and its subsidiaries are not licensed by any state as the administrator of ABC Company and its subsidiaries. This report is for informational purposes only and does not constitute an offer of any financial product or service.

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

Security, Compliance, and Operations Risk Evaluation

	Your SCORE	Average SCORE	Difference	
IT Operations	87.5%	67.5%	+20.00%	↑
Physical Security	100.0%	78.3%	+21.70%	↑
Logical Security	85.7%	77.0%	+7.80%	↑

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?

For each of your critical cloud applications, do you request and review a System and Organization Controls (SOC) report?



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?





If you accept credit card payments, is your business compliant with the Payment Card Industry Data Security Standard (PCI DSS)?

Are your servers and workstations running operating systems that are supported by the vendor (e.g., Microsoft Windows Server 2012)?

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 Advisors LLC 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 to take advantage of this offer!



Speakers



Lisa Morrissey

VP, Treasury Management Team Leader
Rockland Trust

Office: 781.982.6336
Lisa.Morrissey@RocklandTrust.com



Kevin Ricci

Partner
Citrin Cooperman Advisors LLC

Office: 401.421.4800
kricci@citrincooperman.com



Lumi Taiwo

Manager
Citrin Cooperman LLC



Questions



Additional Resources

- [What You Need to Know About Business Email Compromise](#)
- [Working with your Bank to Prevent Wire Fraud for Your Business](#)
- [8 Ways to Protect Yourself from Fraud](#)

