



Exclusive offer for attendees of the CFMA New England event:

Citrin Cooperman is offering a 50% discount on the SCORE Report, our 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 at kricci@citrincooperman.com to take advantage of this limited time offer



Preventing Hackers By Constructing A Strong Cybersecurity Foundation

October 4th, 2022





Welcome & Introduction

KEVIN RICCI, CISM, CISA, CRISC, MCSE, QSA

Partner

Citrin Cooperman

kricci@citrincooperman.com

401-421-4800

AGENDA

The Cyber Threat Landscape

01

Costs and Causes of a Data Breach

02

Best Practices

03

Micro Risk Assessment

04

Questions

05

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

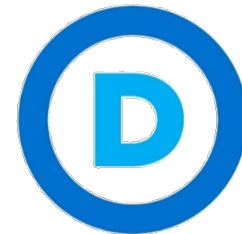
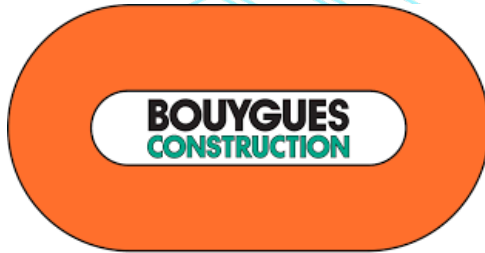
91% of Breaches Are the
Result of Phishing Attacks

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



Construction in the Crosshairs

Cybersecurity for Contractors: 6 Ways Your Company Is Opening Doors for Hackers

Cyber Threats: Why the Construction Industry Could be the Next Big Target

Tech adoption makes construction industry top target for cyberattacks

Is the Construction Industry the Next Big Cybercrime Target?



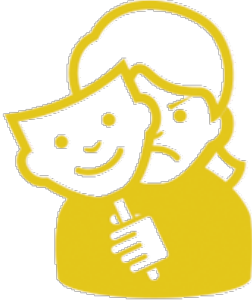

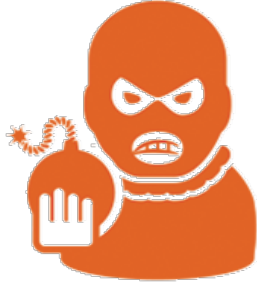

Increasing cyber attacks in the construction industry are causing disruptions and delays

Construction firms are being viewed as easy pickings for cyber criminals

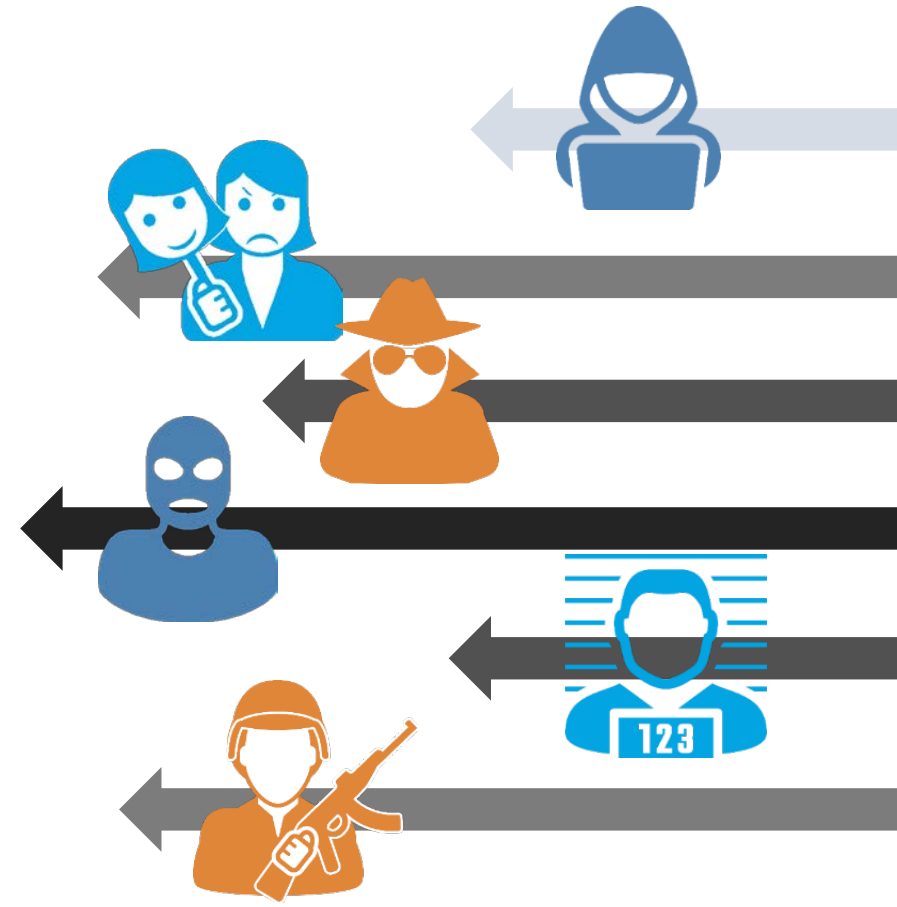
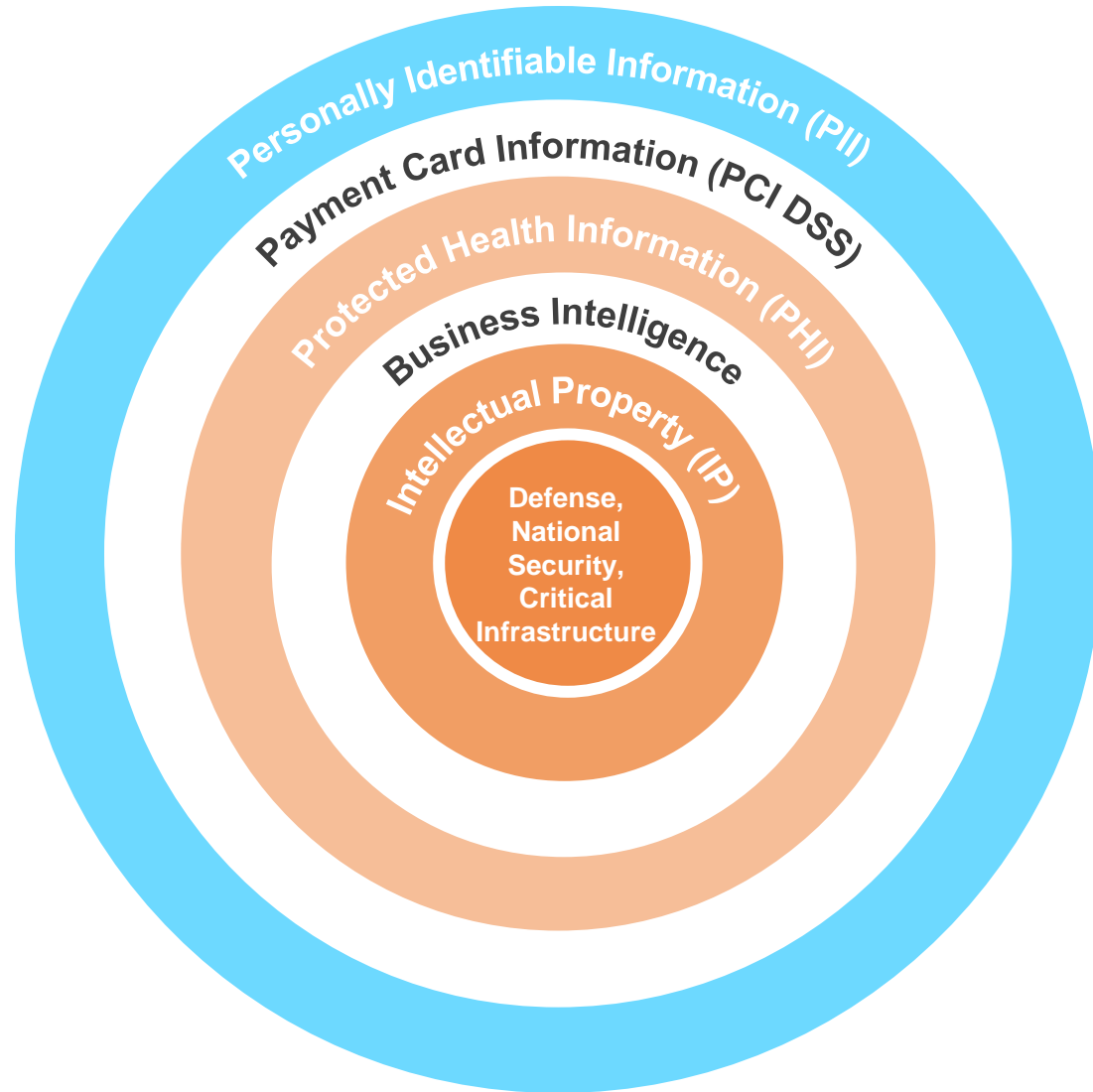
Stats The Way It Is

- Construction is the number one industry hit by ransomware (NordLocker)
- 74% of construction companies are not prepared for cyberattacks (IBM)
- 75% of construction companies reported they fell victim to a cyber incident within the last 12 months (Forrester)
- 97% of cyber presentations will feature someone in a hoodie (Kevin Ricci)

Looking Under the Hoodie

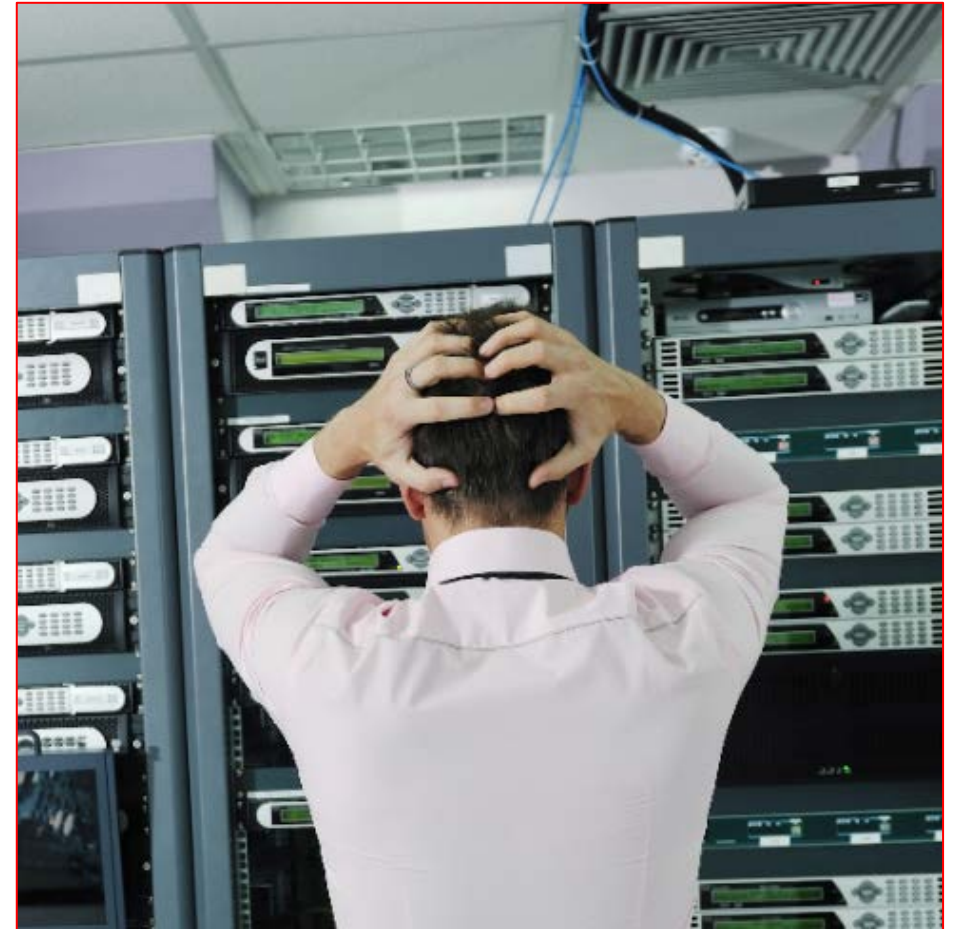
		HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS							
ACTIONS		Hactivists might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat 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 a Data Breach?

- Malicious Insider
- Physical Security Compromise
- Cloud or Server Misconfiguration
- Compromised Credentials
- Social Engineering

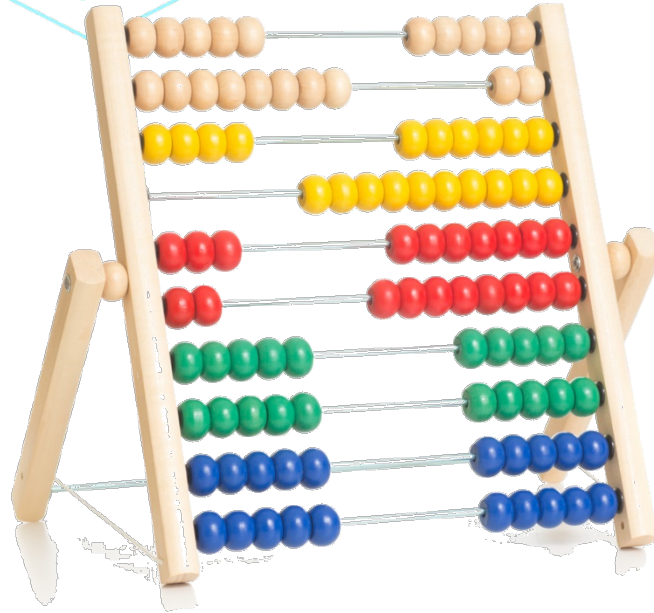


Another Day at the Breach

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



Plan A: Go Old School



Option 2: Implement Cybersecurity Best Practices

- Assess, remediate, repeat
- Password hygiene and 2FA
- Continuous monitoring
- SOC Reports
- Update your technology
- Work from home controls
- Penetration and 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'

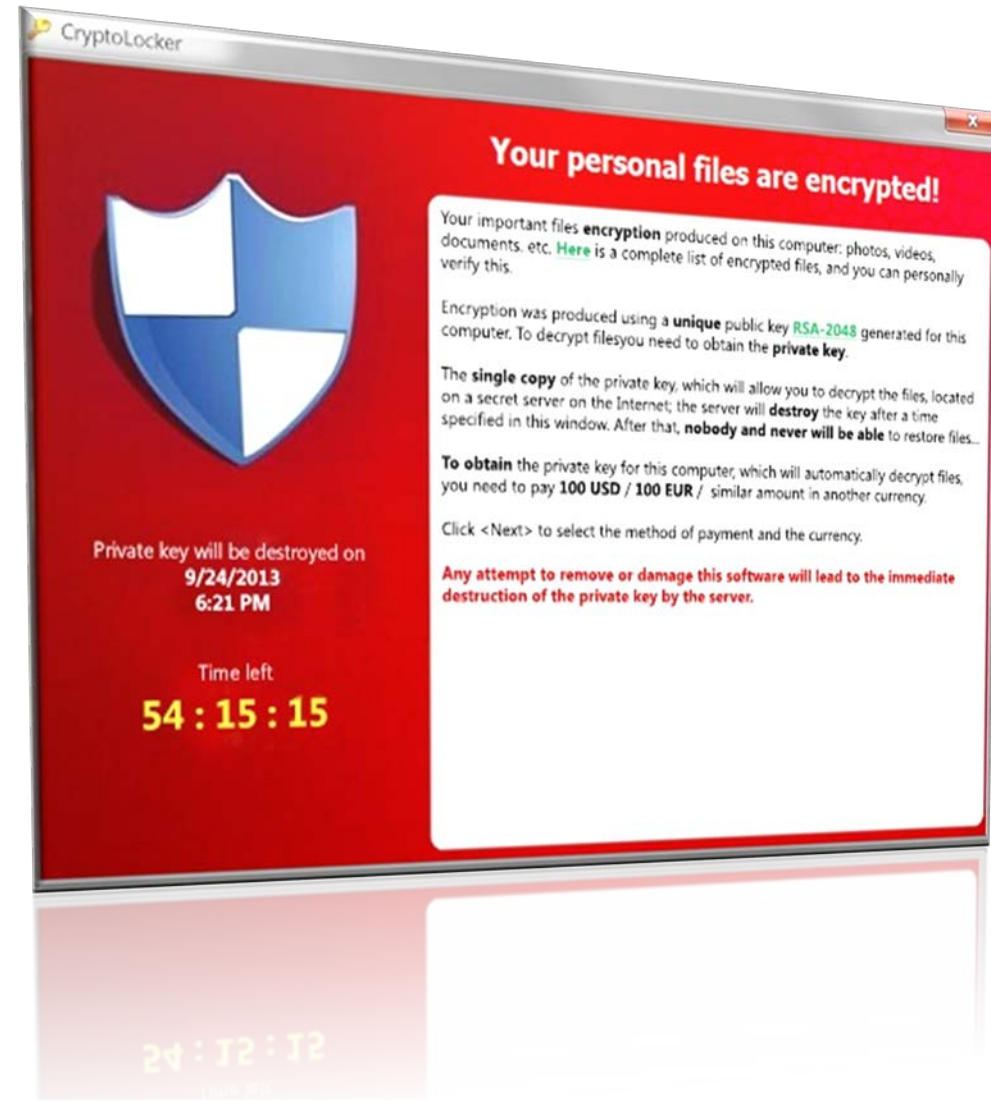
- The key question to ask when receiving an email that asks you to provide sensitive information, click on a link or open an attachment:

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

- If you are not 100% certain that the answer is “yes”, contact the sender by phone or in a separate email

A King's Ransom

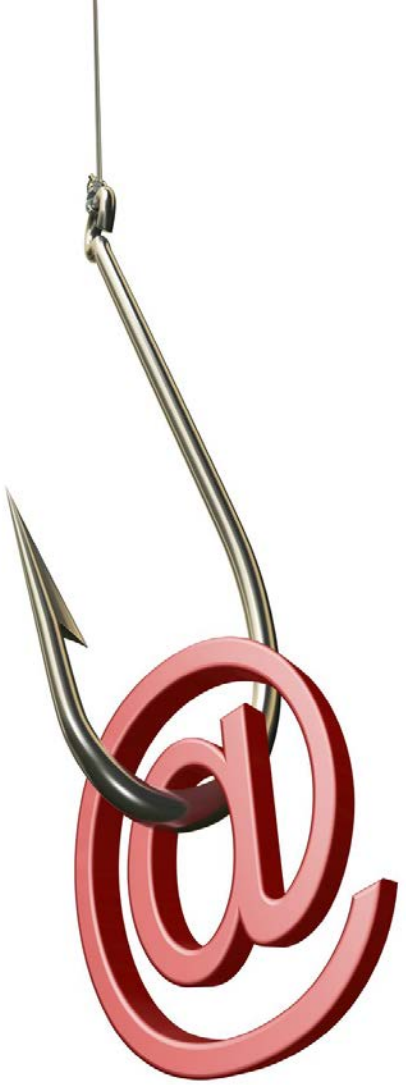
- Dangers of ransomware
 - Encryption
 - Data is publicly exposed
- Dangers of paying
- Ransoms can be negotiated



Get Off The Hook

- Trust but verify
- Look for suspicious signs
 - INFO@cfrra.org
 - 1NF0@cfrra.org
- 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



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



67-year-old Michael Neu of Louisiana was charged with 269 counts of wire fraud and money laundering



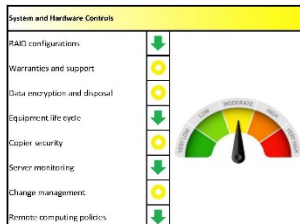
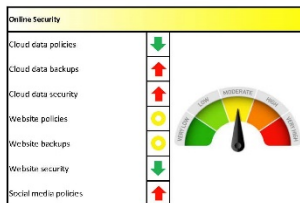
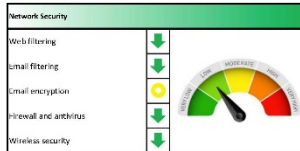
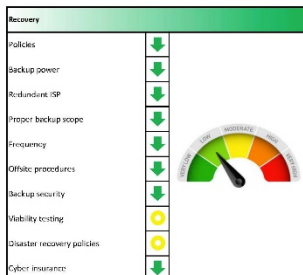
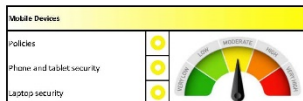
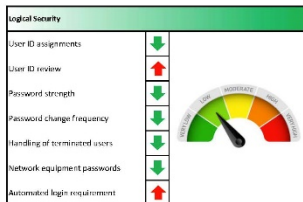
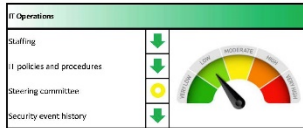
THE SCORE REPORT

CITRIN COOPERMAN
FOCUS ON WHAT COUNTS

SCORE Report™ Risk Summary Dashboard

ABC Company

Security, Compliance, and Operations Risk Evaluation



This information is intended solely for the internal use of the management of ABC Company. It is not to be used by anyone who has been unauthorized. The information contained in this SCORE Report is not to be used for any other purpose, including but not limited to, marketing, sales, or other business development purposes. The information contained in this SCORE Report is not to be used for any other purpose, including but not limited to, marketing, sales, or other business development purposes.

CITRIN COOPERMAN
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



CITRINCOOPERMAN
FOCUS ON WHAT COUNTS

SCORE Report™ Risk Summary Benchmarking ABC Company

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%	↑
Information Security	85.7%	77.9%	+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?

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	
7 - 9	
4 - 6	
0 - 3	



Questions?

KEVIN RICCI, CISM, CISA, CRISC, MCSE, QSA

kricci@citrincooperman.com

401-421-4800

Thank You

"Citrin Cooperman" is the brand under which Citrin Cooperman & Company, LLP, a licensed independent CPA firm, and Citrin Cooperman Advisors LLC serve clients' business needs. The two firms operate as separate legal entities in an alternative practice structure. Citrin Cooperman is an independent member of Moore North America, which is itself a regional member of Moore Global Network Limited (MGNL).





About Us

Citrin Cooperman is one of the nation's largest professional services firms. Citrin Cooperman & Company, LLP, a licensed independent CPA firm that provides attest services and Citrin Cooperman Advisors LLC which provides business advisory and non-attest services, operate as an alternative practice structure in accordance with the AICPA's Code of Professional Conduct and applicable laws, regulations and professional standards. Clients are in all business sectors and leverage a complete menu of service offerings. The entities include more than 275 partners and over 1,600 employees across the U.S. For more information, please visit citrincooperman.com, and be sure to follow us on LinkedIn, Twitter, Facebook, Instagram, and YouTube.

"Citrin Cooperman" is the brand under which Citrin Cooperman & Company, LLP, a licensed independent CPA firm, and Citrin Cooperman Advisors LLC serve clients' business needs. The two firms operate as separate legal entities in an alternative practice structure. Citrin Cooperman is an independent member of Moore North America, which is itself a regional member of Moore Global Network Limited (MGNL).