



When Worlds Collide:

A cybersecurity discussion between an FBI Cyber Analyst and an Ethical Hacker

WELCOME

Michael Camacho, CPA, CIA

PARTNER

mcamacho@citrincooperman.com



CITRINCOOPERMAN®

Accountants and Advisors



THE FACTS:

Approx. 4.5 billion
records stolen in first
6 months of 2018

Average Cost per
Record Stolen:
\$148/record

Average Days to
Detect Breach: 191

Average Days to
Contain Breach: 66

Likelihood of
recurring breach:
27.9%

Average cost of
breach is 37% higher
when a Company is
not prepared

INTRODUCTIONS



Jacqueline Nolan
Cash Management Business Development Officer
Jacqueline.Nolan@RocklandTrust.com



Lisa Morrissey
VP/Treasury Management Sales Officer
Lisa.Morrissey@RocklandTrust.com



Tom Doyle
BFI Intelligence Analyst
tdoyle2@fbi.gov



Matt Wagenknecht, CISSP, CREA, CEH
Director / Cybersecurity
mattw@citrincooperman.com



Kevin Ricci, CISA, MCSE, CRISC, QSA
Director / Cybersecurity
kricci@citrincooperman.com

Fraud 101: Protecting Your Business



Member FDIC

How did we get here?

Situation: The landscape in banking is changing. Fraud prevention and cyber security awareness is top of mind.

Impact: Typically financial institutions are reacting to customer exposure after the fact.

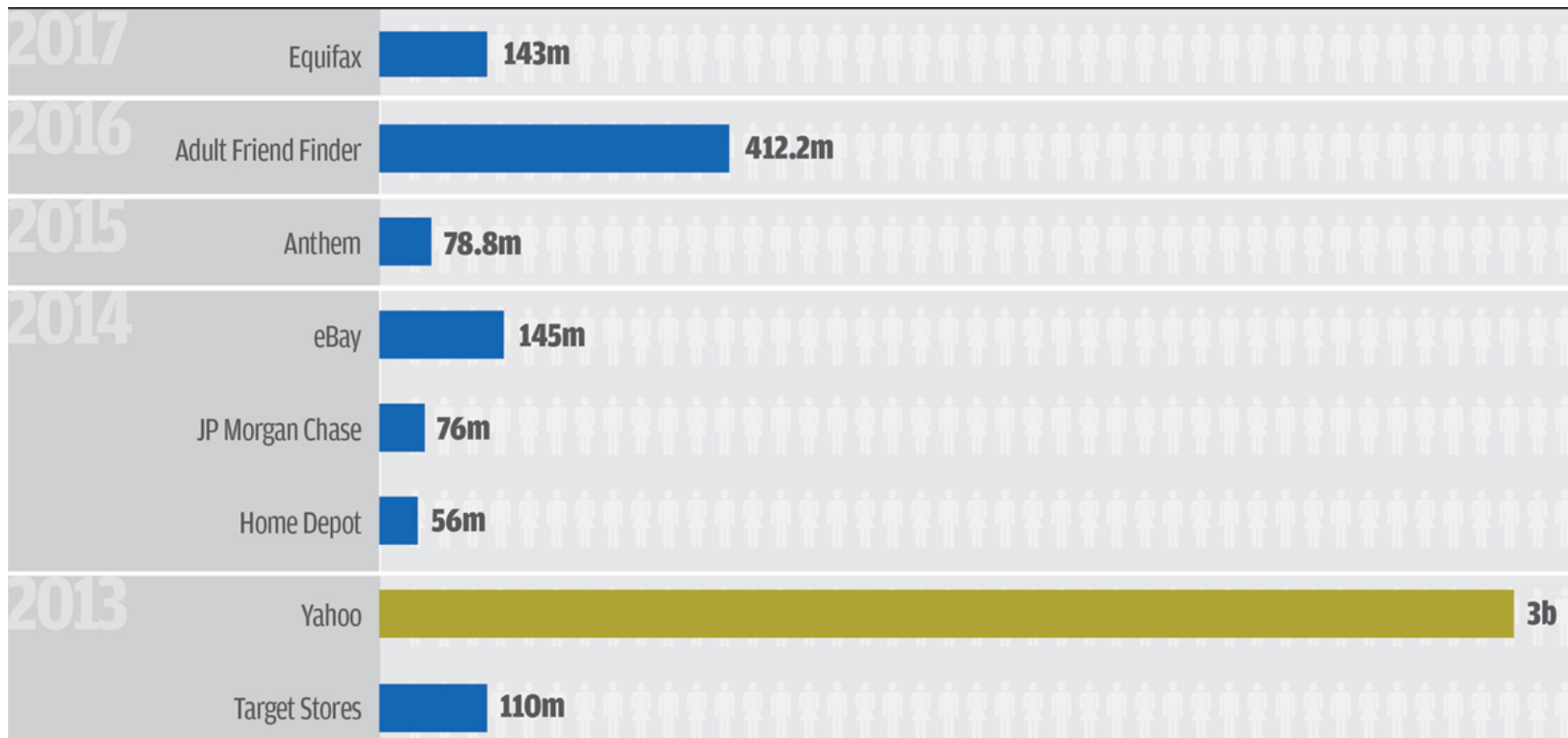
Goal: Mitigate fraud by providing a hands-on approach -- educating the business community to be vigilant against potential threats.

Solution: Rockland Trust Bank - Where Each Relationship Matters[®].

Reputation at Risk?

54% of companies believe it can take up to **2 years** to restore a company's reputation following a **breach of customer data**.

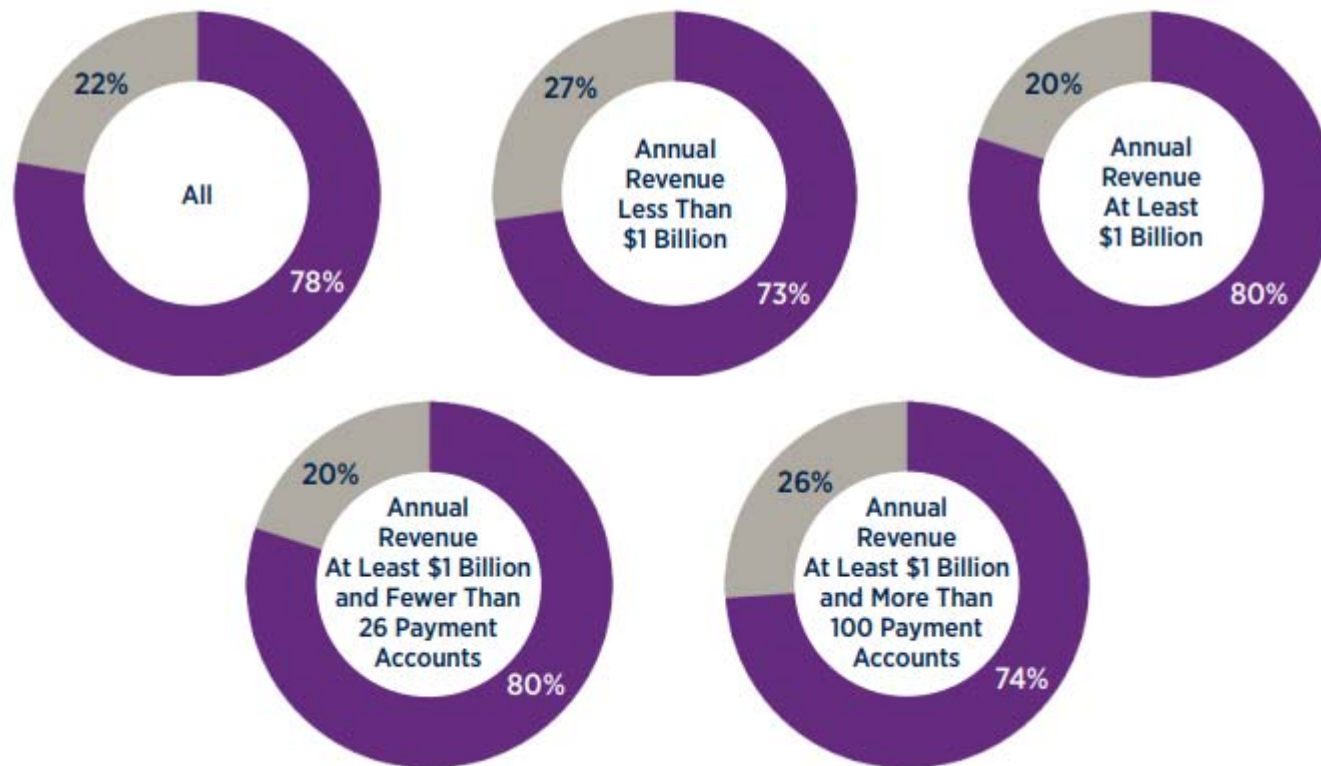
The biggest names to suffer a data breach since 2013 include:



Payments Fraud Types

Checks continue to be the payment method most often exposed to fraudulent activity.

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud in 2017



Member FDIC

■ Experienced attempted/actual Payment Fraud Activity

2018 AFP [Payments Fraud and Control Survey](#)

Phishing



Rockland1rust.com is not
the correct domain name

From: Stacey.Coyne@Rockland1rust.com
Sent: Monday, May 23, 2016 2:16 PM
To: Lisa.Morrissey@Rocklandtrust.com
Subject: RE: Wire Transfer

Great!

Send the wire to:

Alfred Smith
345 Main St
Phoenix, AZ
Routing #: 011304568
Account #: 12345678

Please send \$35,364.82
Memo: Payment for Invoice # 89D5

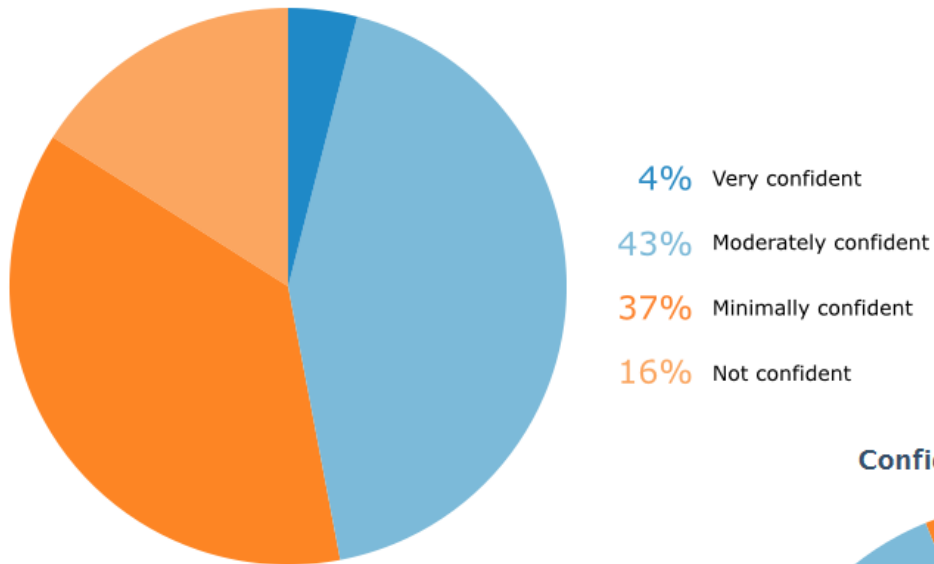
Please let me know as soon as it's done.

Thank you!

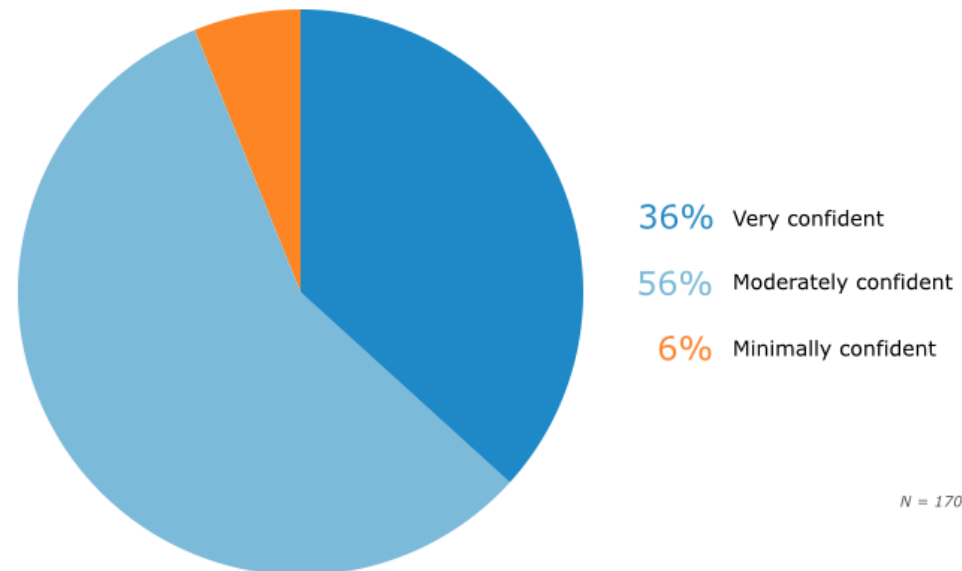
Stacey M. Coyne
Vice President

Why Employees Click

Confidence in Co-Workers' Ability to Avoid Phishing Attack



Confidence in Personal Ability to Avoid Phishing Attack



N = 170

Scary Statistic

“What is fascinating – and disheartening – is that over **95%** of all incidents investigated recognize “**human error**” as a contributing factor.”

The More You Know...

According to UCC Regulation, liability for fraud is no longer just the responsibility of the bank:

Customers must also exercise “***ordinary care***” measures. The absence of these measures, such as timely account reconciliation, lack of internal controls, minimal security procedures, to name a few, ***puts your Company at risk for being held liable for all, or a substantial portion, of any given loss.***



Best Practices to Safeguard Your Business

- Fraud Prevention Tools
 - Positive Pay: Safeguards against fraudulent check activity
 - ACH Debit Blocks / Filters: Safeguards against unauthorized ACH transactions
- Clean desk policy – lock up sensitive data
- Keep antivirus / malware protection current
- Place a call – validate communications to change financial data
- Separation of duties – establish internal controls
- Practice due diligence – know with whom you're doing business
- Provide ongoing employee training and awareness
- Practice email etiquette



ETHICAL HACKER

MATT WAGENKNECHT



Primary Attack Methods

- Misconfigurations/Default Settings
- Easy-to-guess passwords
- Social Engineering Attacks
- Wireless Attacks

Misconfigurations/Default Settings

- Active Directory
 - Password stored in memory on Servers and Workstations
 - Backwards Compatibility (Windows 7)
 - Network Shenanigans and General Tomfoolery
- Default passwords on devices :: admin/admin or admin/calvin
- Poor Perimeter Hygiene
- [DEMO] <http://images.shodan.io>



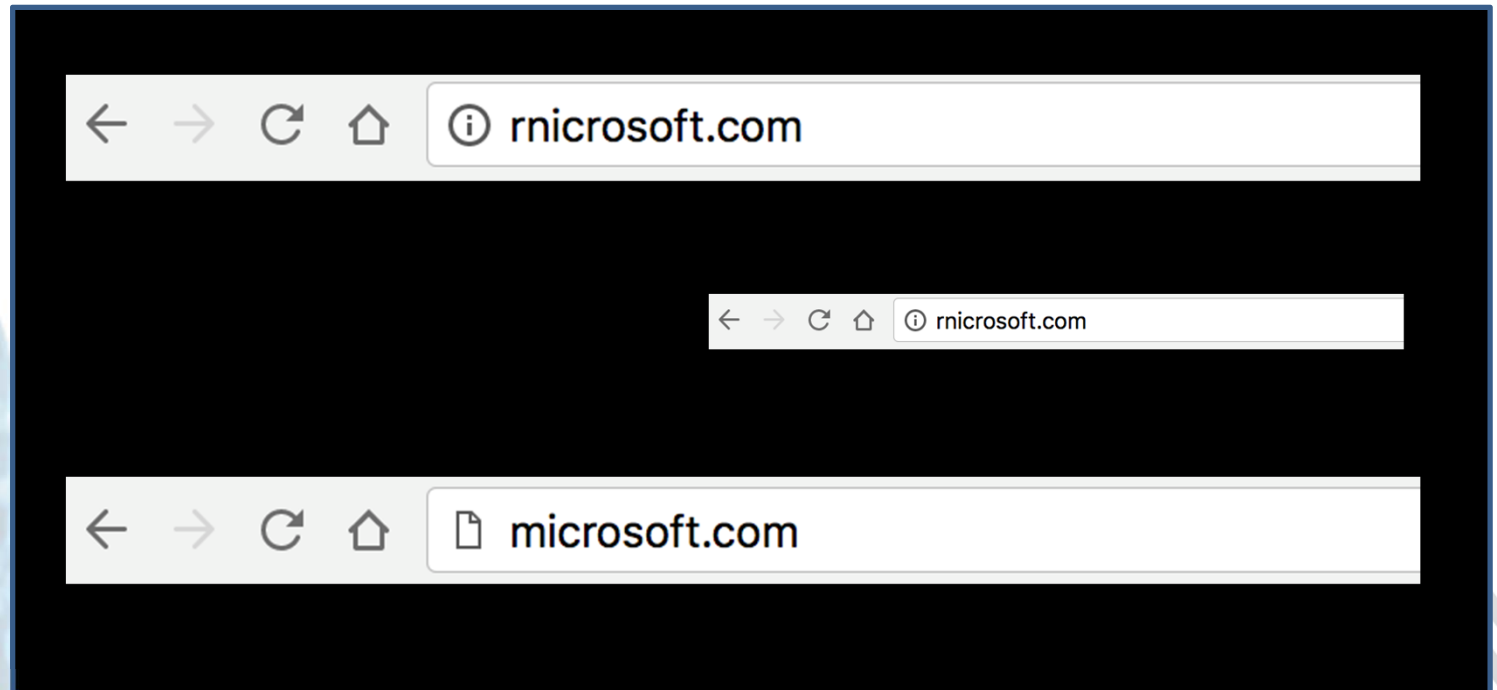
Easy-to-guess Passwords

- External Websites
- Remote Administration ports (SSH, Telnet, RDP)
- Bad User Practices
 - Odometer-Style Password Rotation
 - Password storage (spreadsheets, sticky notes, whiteboards)
 - [DEMO]

Social Engineering Attacks

- Phishing Methods
 - Email attachments – doc, pdf, js, vbs, zip
 - URL Substitution

URL - Minor Difference Substitution



URL - Minor Difference Substitution




← → ↻ 🏠  apple.com

= apple.com



← → ↻ 🏠  apple.com

= appie.com



It's what you **don't** see that
ultimately gets you.

...and you can't know what you don't see
until someone makes you see it.



TRUST, BUT **VERIFY**

Question? Comments?



Intelligence Analyst
Tom Doyle
Email: tdoyle2@fbi.gov

Panel Discussion and Q&A



MODERATOR

Kevin Ricci, CISA, MCSE, CRISC, QSA
Director / Cybersecurity
kricci@citrincooperman.com



Matt Wagenknecht, CISSP, CREA, CEH
Director / Cybersecurity
mattw@citrincooperman.com



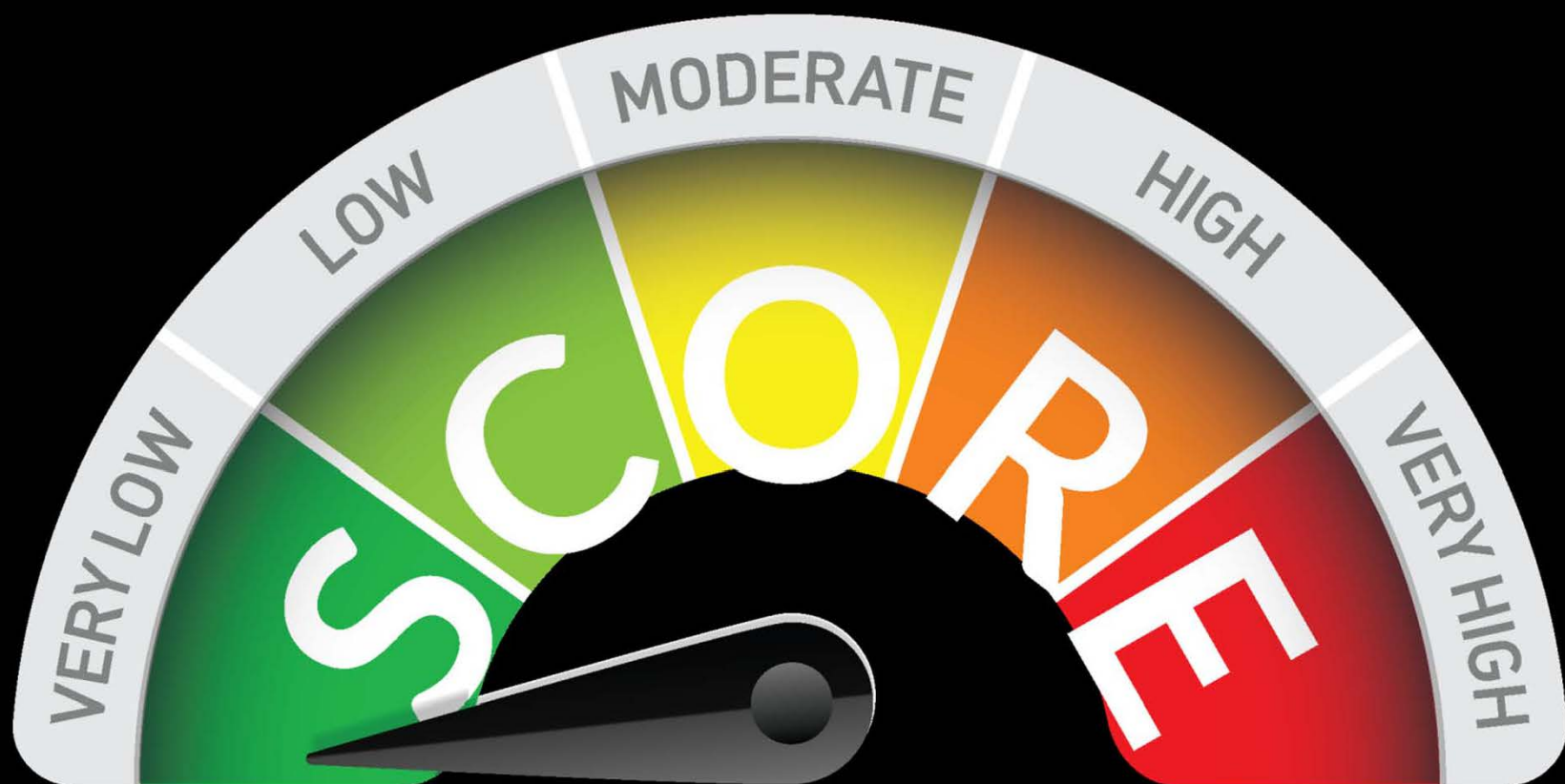
Lisa Morrissey
VP/Treasury Management Sales Officer
Lisa.Morrissey@RocklandTrust.com



Jacqueline Nolan
Cash Management Business Development Officer
Jacqueline.Nolan@RocklandTrust.com



Tom Doyle
BFI Intelligence Analyst
tdoyle2@fbi.gov



REPORT

THE SCORE REPORT



SCORE Report™ Risk Summary Dashboard

ABC Company

Security, Compliance, and Operations Risk Evaluation

IT Operations

Staffing



IT policies and procedures



Steering committee



Security event history



Physical Security

Entrance security



Access tracking



Environmental controls



Logical Security

User ID assignments



User ID review



Password strength



Password change frequency



Network Security

Web filtering



Email filtering



Email encryption



Firewall and antivirus



Wireless security



Online Security

Cloud data policies



Cloud data backups



Cloud data security



Website policies



Website backups



Website security



Social media policies



THE SCORE REPORT



SCORE Report™ - Hot Spots ABC Company

Security, Compliance, and Operations Risk Evaluation

Section	Issue	Risk	Solution	Risk Level
Password Strength	There is no minimum password length requirement, no password complexity requirement, no restriction on using prior passwords, and no lockout after a series of incorrect password attempts.	A password that is not complex, does not have at least an 8 character minimum length, can be used repeatedly, and is not locked out after repeated invalid attempts greatly increases the chances of the account being compromised.	Best practices for a strong password is to enforce complexity, mandate a minimum password length of 8 or more characters, restrict usage of the last several passwords, and disable the account after a series of invalid login attempts. These requirements can be enforced throughout the Company using group policy. Note: Turbines has password policies in place that meet best practice standards.	High
Password Change Frequency	Passwords are not required to be changed after a set number of days.	In the event that a password was compromised, the perpetrator could access the account indefinitely.	Implement a policy so that passwords are required to be periodically changed, with best practice being every 90 days. A potential alternative to traditional passwords is to utilize biometrics (fingerprint readers) to cut down on forgotten passwords while increasing security. Note: Turbines has password policies in place that meet best practice standards.	High
PII Policies and Security	A Data Security Compliance Officer has not been appointed by the Company to administer the care of personally identifiable information (PII).	As a business that maintains PII, the Company is required to comply with all applicable state security and privacy regulation (e.g. Rhode Island's Identity Theft Protection Act) requirements. Not having a Data Security Compliance Officer in place increases the risk of PII being compromised as there is no one dedicated to keeping up to date with the regulations and insuring that proper security is in place. If a data breach occurs, the fines and penalties as well as damage to reputation, among other ramifications, can significantly impact an organization.	Appoint a Data Security Officer and provide them with the necessary training so that they can properly administer PII security.	High
PII Policies and Security	The Company has not developed a Written Information Security Program (WISP). There is no encryption or a formal risk-based information security program 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 all applicable state security and privacy regulation (e.g. Rhode Island's Identity Theft Protection Act) requirements. These regulations typically require, among other things, encryption and a risk-based information security program. Lack of these required elements could result in significant fines while also hindering employees from making good security decisions.	Encrypt all systems that have any interaction with PII and create a WISP that addresses the needs of the regulations surrounding the care of PII and update the documentation at least annually, or as policies and procedures change.	High
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 all applicable state security and privacy regulation (e.g. Massachusetts 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 Policies and Security	The Company may not be compliant with the Payment Card Industry Data Security Standards (PCI DSS). The lack of evidence artifacts and no self assessment questionnaire (SAQ) are examples of potential concern.	By accepting credit cards, the Company is required to comply with PCI DSS. Not having proper security controls in place increases the risk of cardholder data being compromised. If a data breach occurs, the fines and penalties, potential inability to accept credit cards until compliant, damage to reputation, and ongoing increased compliance requirements, among other ramifications, can significantly impact an organization.	Perform a Gap Assessment to identify all missing elements in accordance with PCI DSS, as outlined by the Company's associated PCI DSS self assessment questionnaire (SAQ). Remediate all gaps and implement a plan for continued compliance going forward. Maintain a repository of all PCI-related screen captures and other backup documentation and update them as settings or documentation changes.	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

THANK YOU

