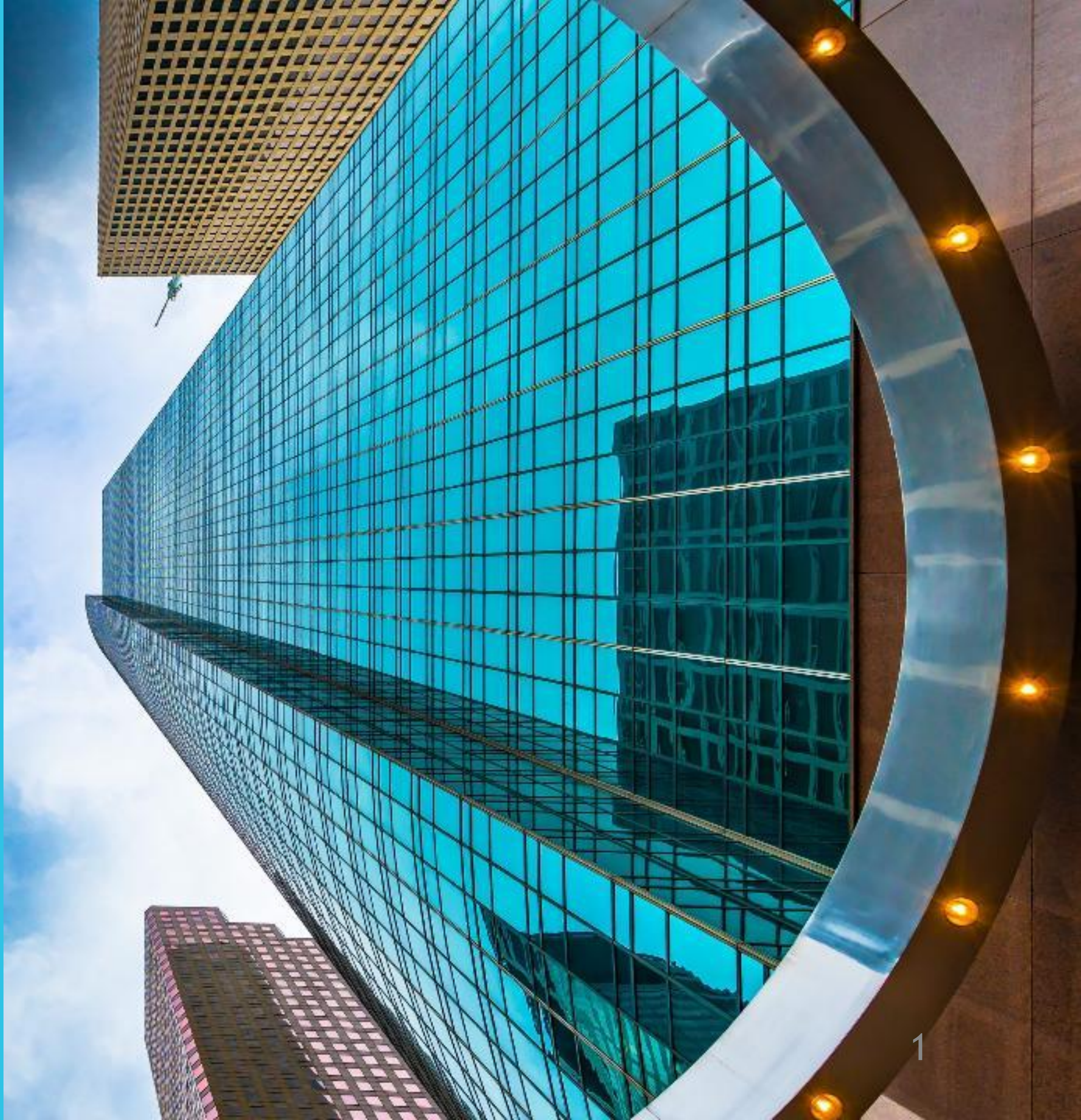
iFA INTERNATIONAL FRANCHISE ASSOCIATION

Franchises Under Fire: Securing Your Business From Cybersecurity Threats

March 17, 2026

CITRINCOOPERMAN



Kevin Ricci

CISM, CISA, CRISC, MCSE, QSA

Partner

Citrin Cooperman

kricci@citrincooperman.com

401-421-4800

Agenda

- Threat Landscape
- Cost of a Data Breach
- AI Security Risks
- Cybersecurity Services
- Micro Risk Assessment
- Questions & Answers

Today’s Cyber Threat Landscape

2.6 Billion Records Were Lost, Stolen, or Exposed In 2025, a 23% increase over 2024

3,322 Publicly Disclosed Data Breaches In 2025

2025 Average Breach Cost:

Global: $4.44M

USA: $10.88M

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

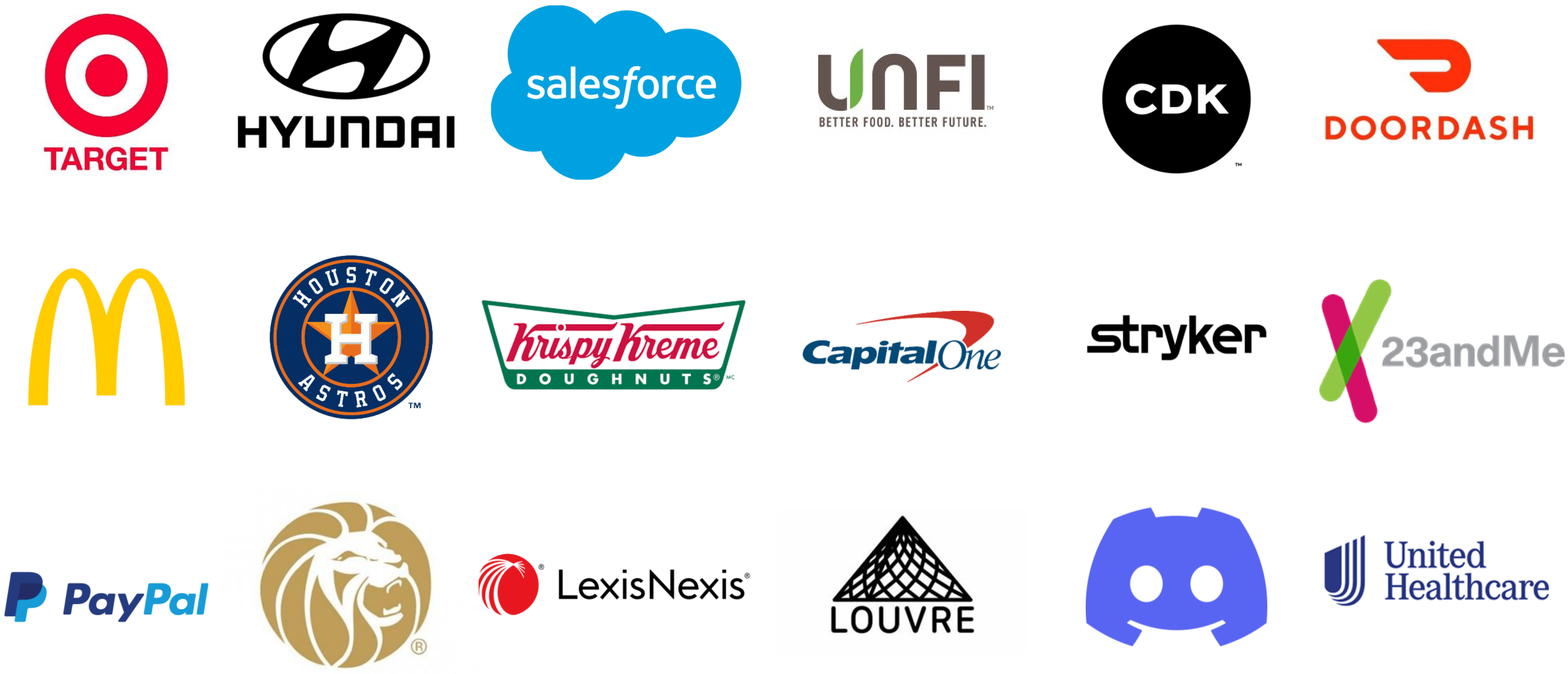
2025 Average Days to Detect a Breach: 181

2025 Average Days to Contain a Breach: 60

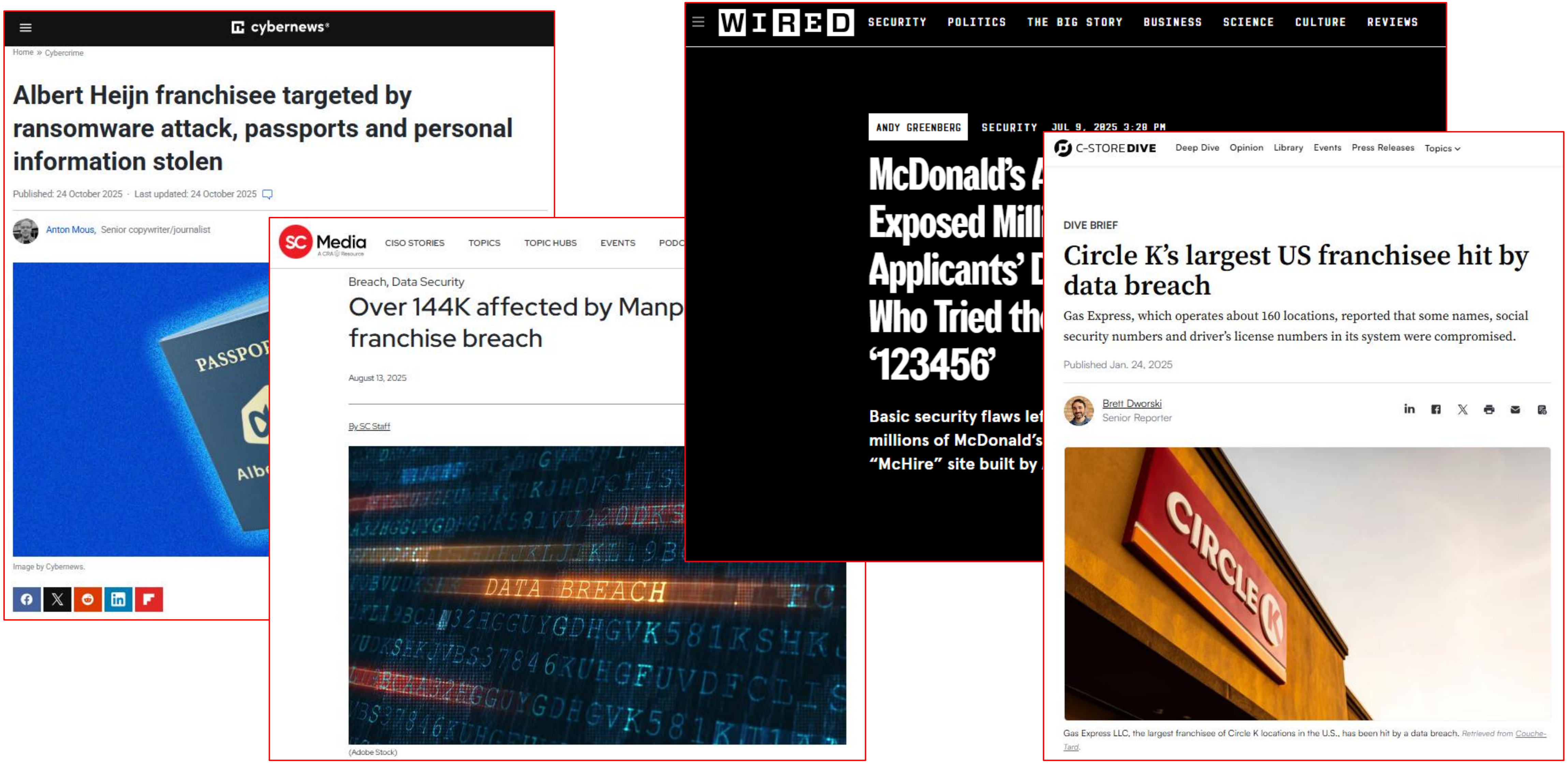
Statistics from the IBM Ponemon Data Breach Report, CSHub, KnowBe4, and CompariTech

"Once More Unto the Breach"

- William Shakespeare, 1599
- Kevin Ricci, last Tuesday



Franchise Horror Stories



cybernews®

Home » Cybercrime

Albert Heijn franchisee targeted by ransomware attack, passports and personal information stolen

Published: 24 October 2025 · Last updated: 24 October 2025

Anton Mous, Senior copywriter/journalist

Image by Cybernews.

SC Media

CISO STORIES TOPICS TOPIC HUBS EVENTS PODC

Breach, Data Security

Over 144K affected by Manp franchise breach

August 13, 2025

By SC Staff

(Adobe Stock)

WIRED SECURITY POLITICS THE BIG STORY BUSINESS SCIENCE CULTURE REVIEWS

ANDY GREENBERG SECURITY JUL 9, 2025 3:28 PM

McDonald's A Exposed Milli Applicants' D Who Tried th '123456'

Basic security flaws lef millions of McDonald's "McHire" site built by

C-STORE DIVE Deep Dive Opinion Library Events Press Releases Topics

DIVE BRIEF

Circle K's largest US franchisee hit by data breach

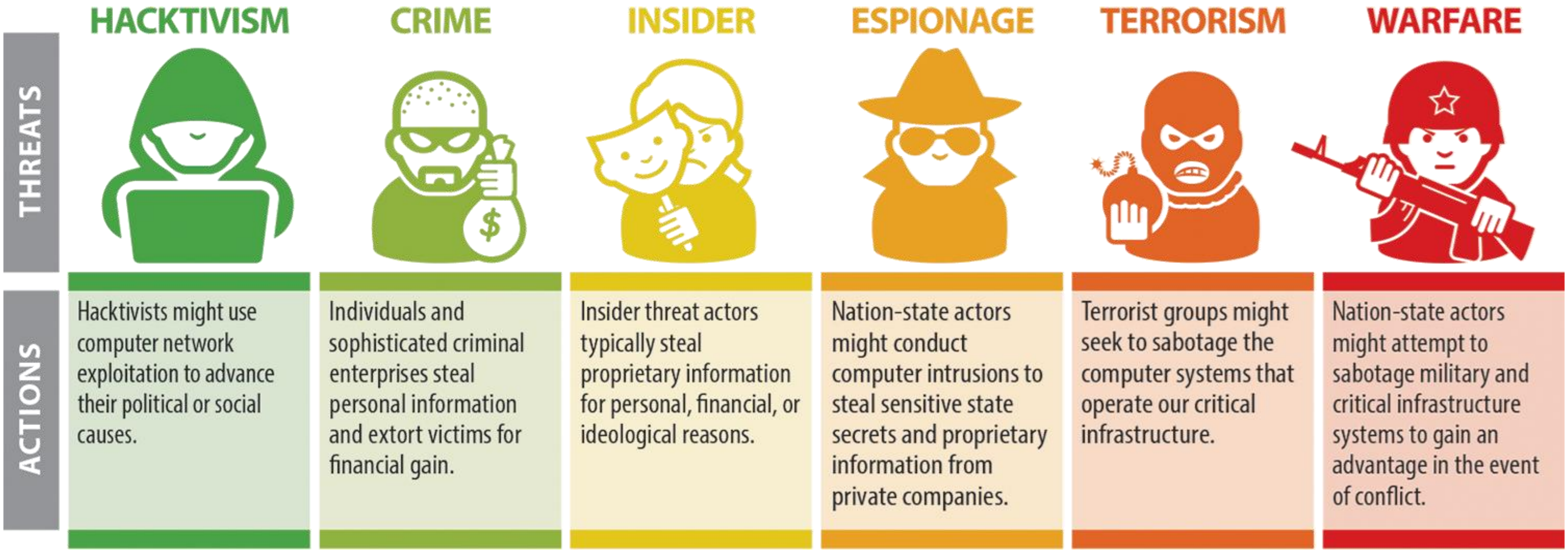
Gas Express, which operates about 160 locations, reported that some names, social security numbers and driver's license numbers in its system were compromised.

Published Jan. 24, 2025

Brett Dworski
Senior Reporter

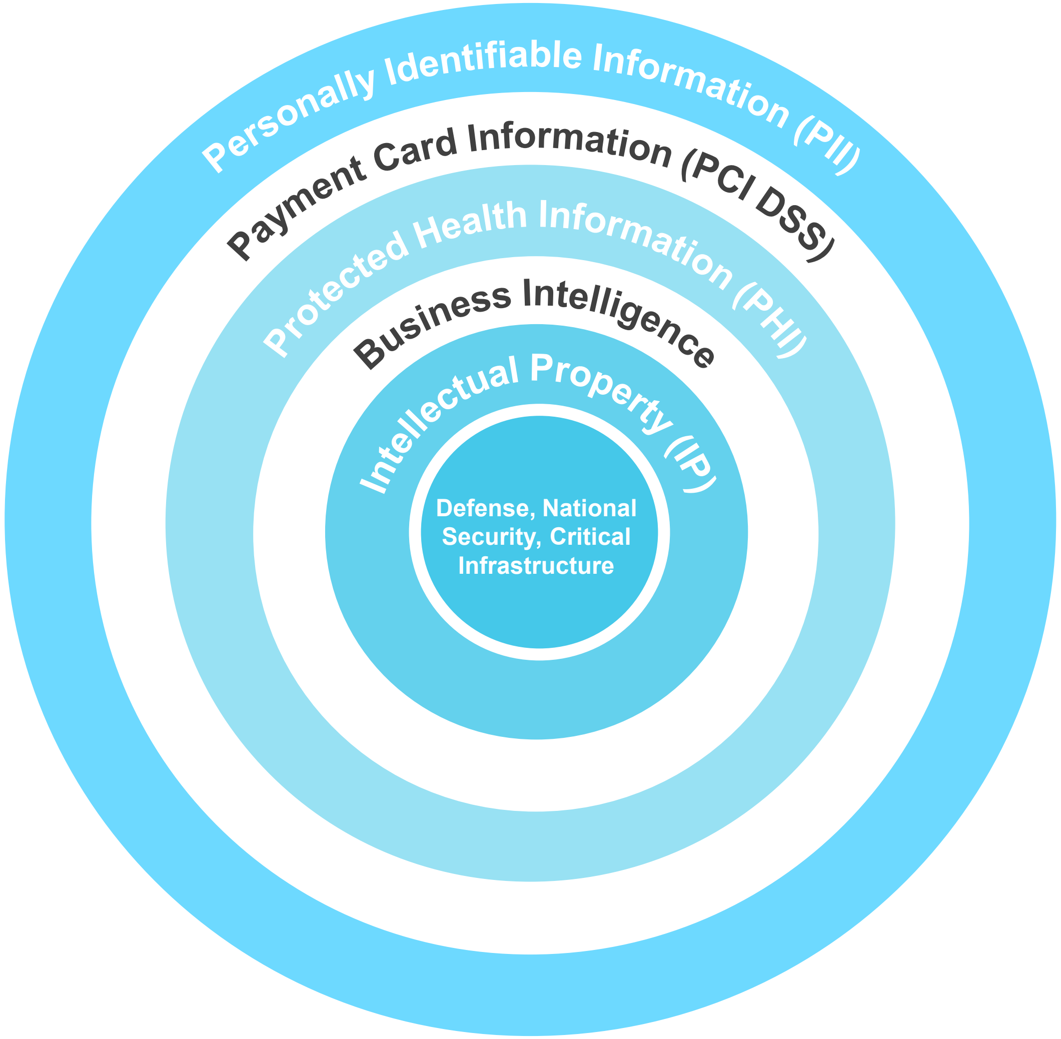
Gas Express LLC, the largest franchisee of Circle K locations in the U.S., has been hit by a data breach. *Retrieved from Couche-Tard.*

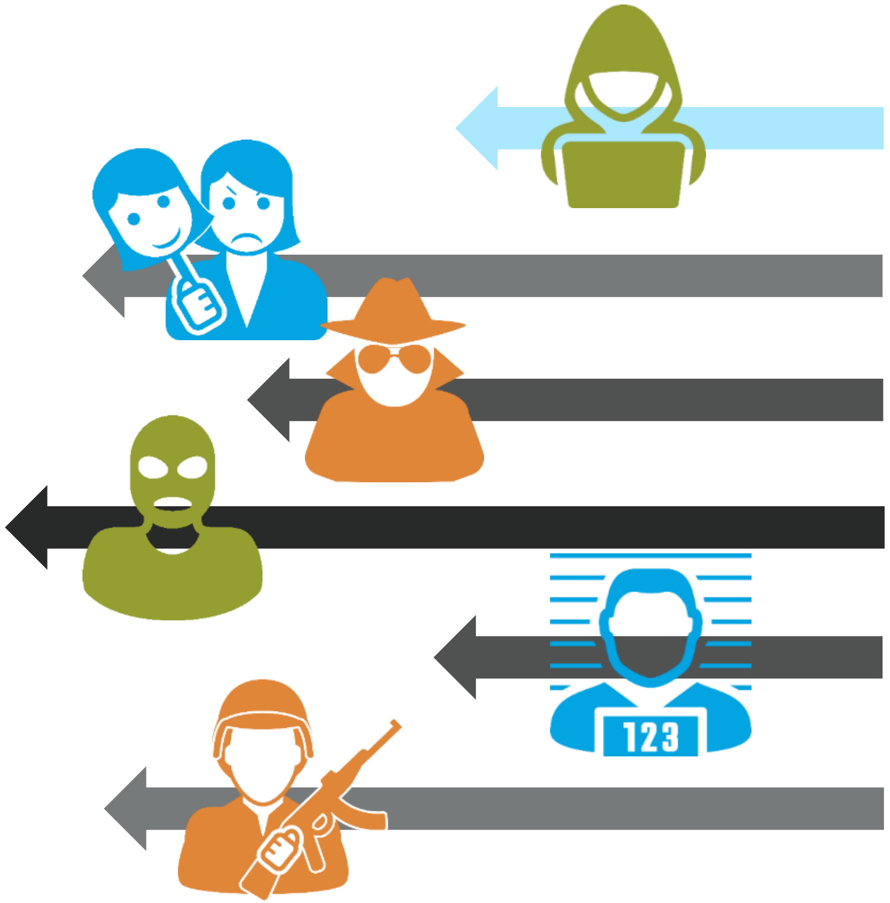
Let’s Look Under the Hoodie



	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hacktivists 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.

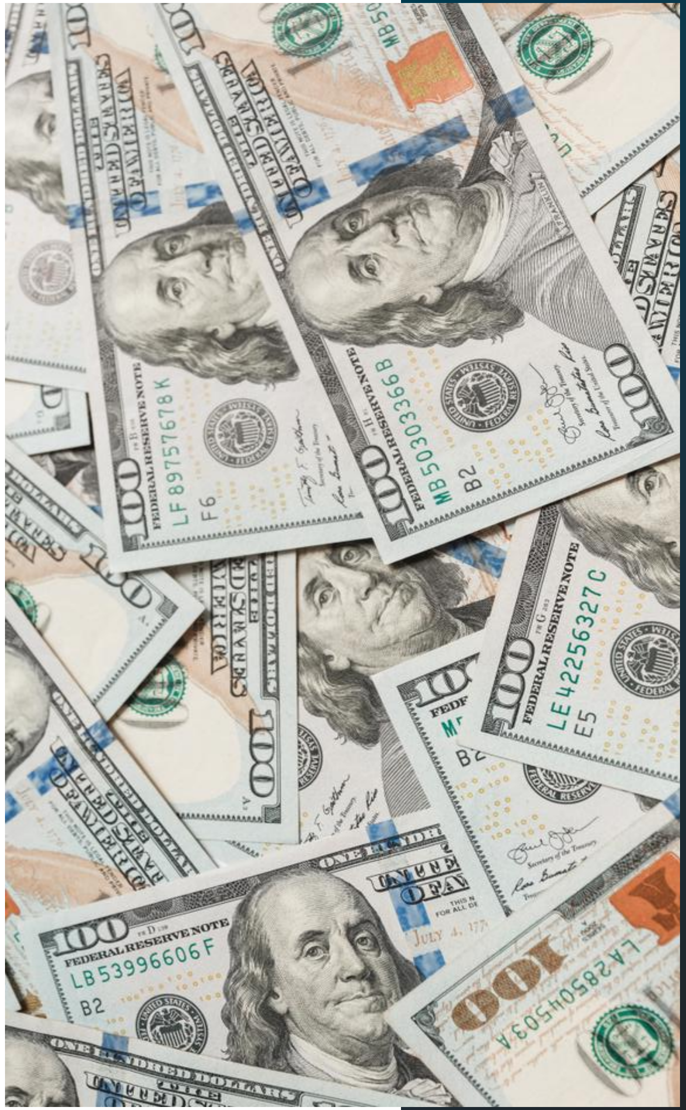
Motivations & Incentives

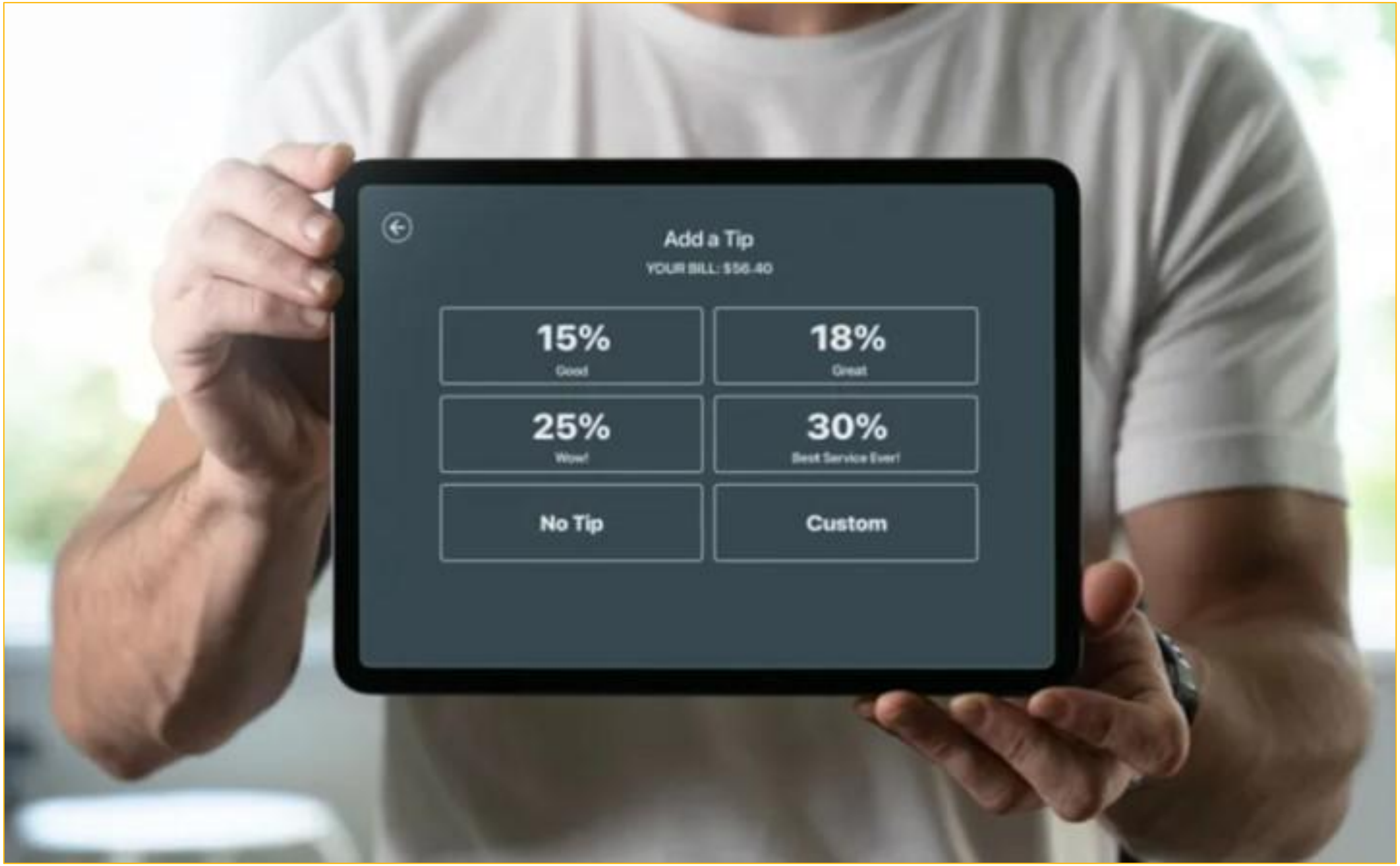

Personally Identifiable Information (PII)
Payment Card Information (PCI DSS)
Protected Health Information (PHI)
Business Intelligence
Intellectual Property (IP)
Defense, National Security, Critical Infrastructure



- Fines and penalties
- Technology expenditures
- Forensics
- Legal counsel
- Notification
- Downtime
- Reputational

Cost of a Breach





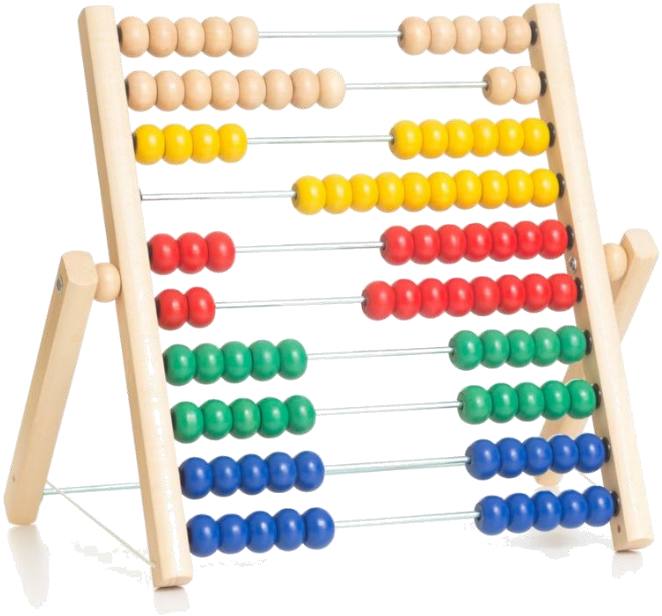
Add a Tip

YOUR BILL: $56.40

AI Threats Are Anything But Artificial

- Instant generation of sophisticated social engineering attacks
- New strains of malware can be generated with minimal effort and coding skills
- Criminals have set up fake websites that appear to host legitimate AI tools
- Data poisoning attacks
- AI has supercharged the deepfake capabilities used by cybercriminals
- There are limited safety mechanisms in place to prevent the upload of sensitive information to AI chatbots, which are susceptible to hackers

Plan A: Go Old School



Plan B: Implement Cybersecurity Best Practices

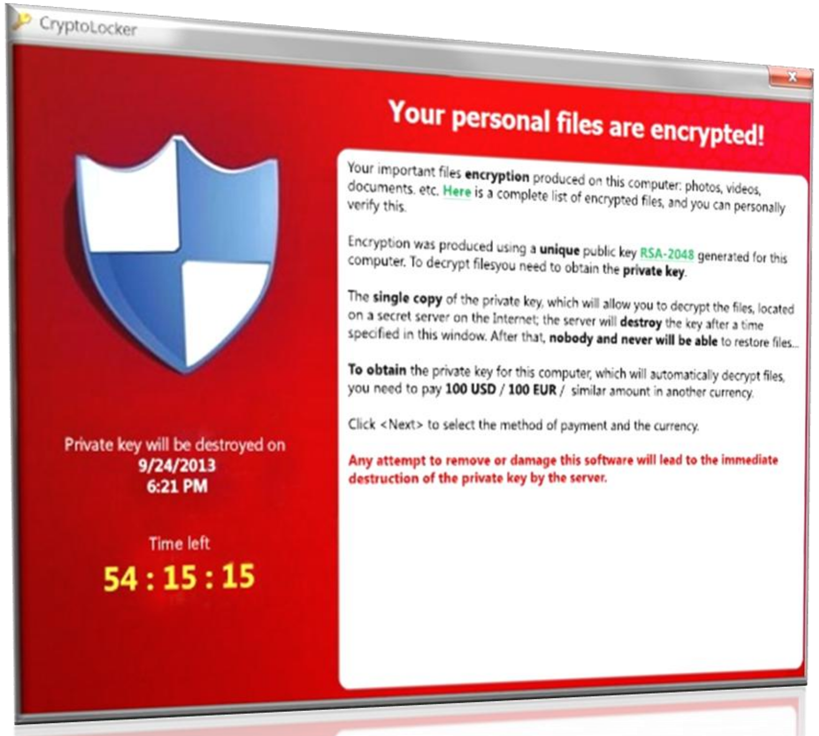
- Assess, remediate, repeat
- Password hygiene and MFA
- Work from home defenses
- Continuous monitoring
- TPRM and SOC Reports
- Update your technology
- Penetration and vulnerability tests
- Incident response preparation
- Viable backups
- Training, policies, and phishing simulations

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

A King's Ransom

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



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Gone Phishin’

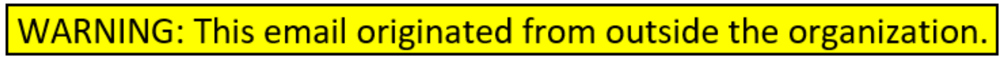
- The key question to ask when receiving an email that asks you to provide sensitive information, click on a link or open an attachment:

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

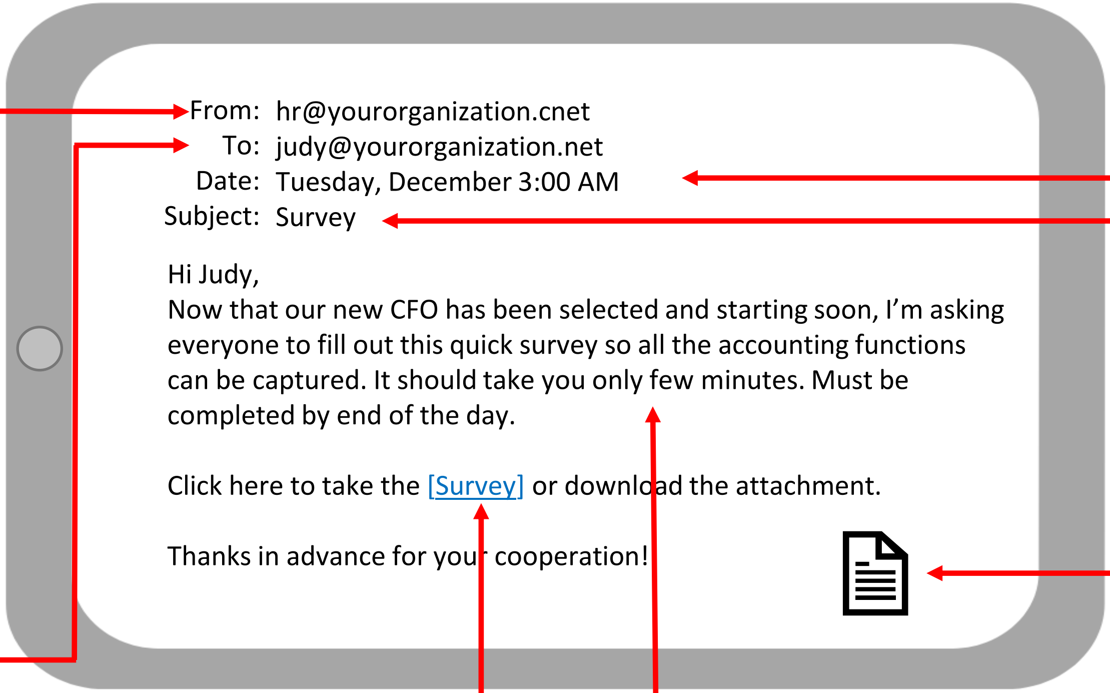
Getting Off The Hook

- Look for suspicious indicators
- Inspect the sender’s email address
  - INF0@FRANCHISE.org
  - lNF0@FRANCHlSE.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 (SMS) message
  - Vishing is a voice attack via a phone call
  - Quishing is an attack via a QR code

Spear Phishing Red Flags



From: hr@yourorganization.cnet

To: judy@yourorganization.net

Date: Tuesday, December 3:00 AM

Subject: Survey

Hi Judy,

Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by end of the day.

Click here to take the [Survey] or download the attachment.

Thanks in advance for your cooperation!

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with.**
- This email is **from someone outside my organization, and it's not related to my job responsibilities.**
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character.**
- Is the sender's email address from **a suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is **an unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but **the link-to-address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, www.bankofarnerica.com-- the "m" is really two characters– "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

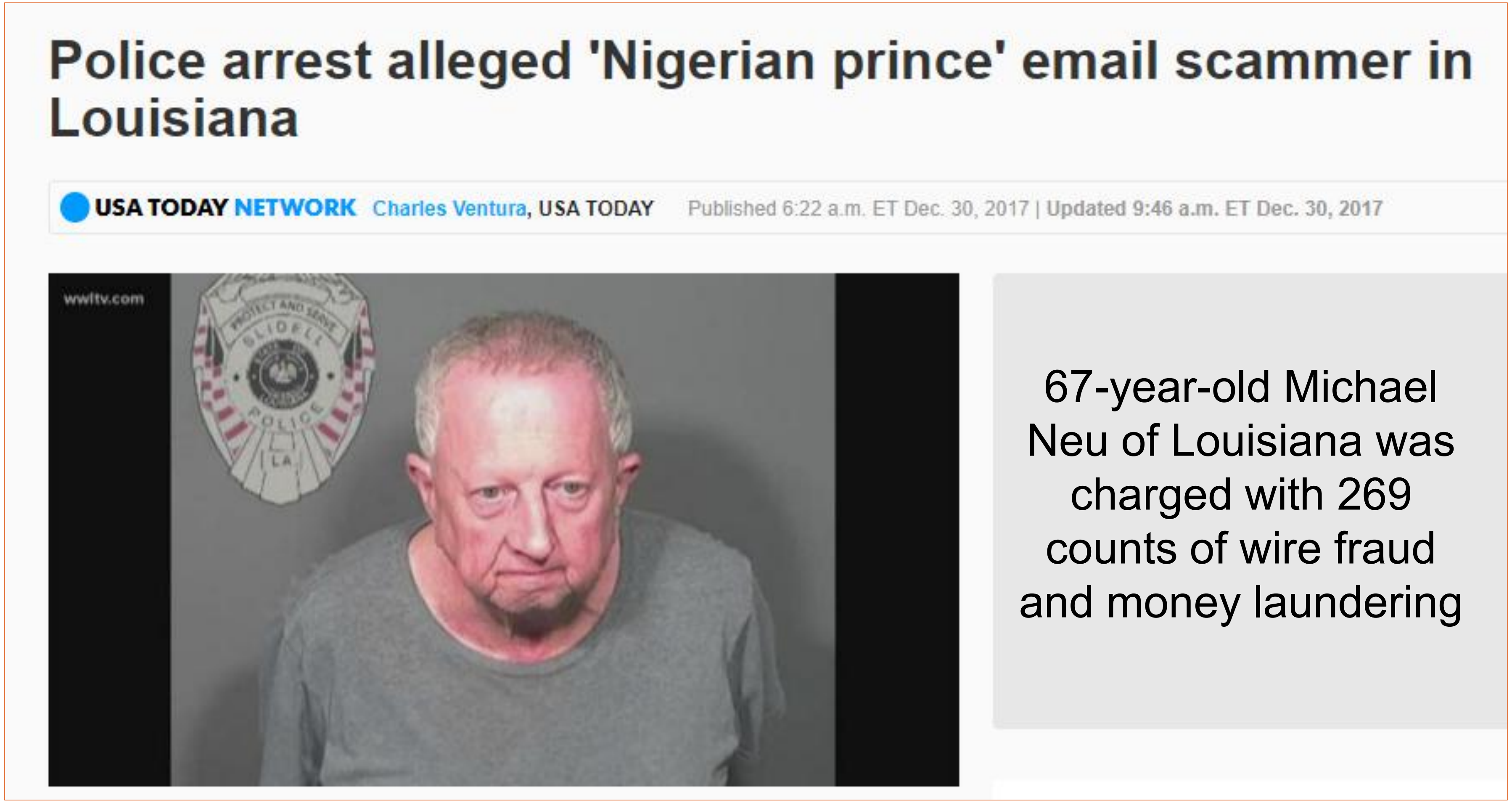
ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that makes no sense to me in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary** or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click on a link or open an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Farewell Sweet Prince



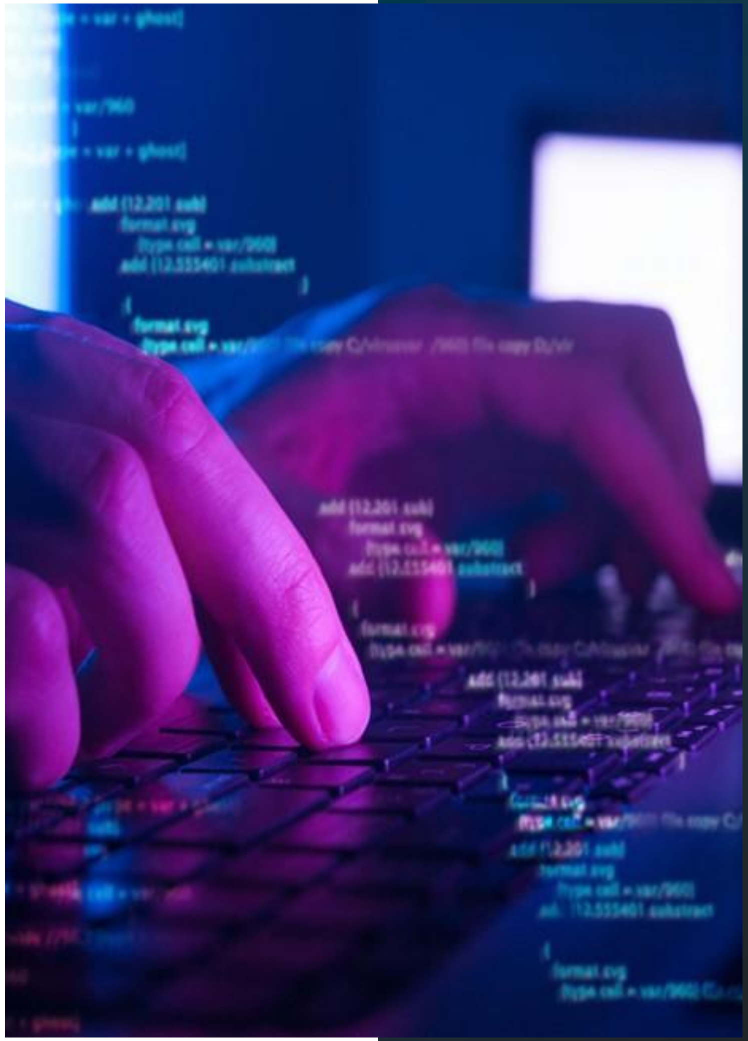
Police arrest alleged 'Nigerian prince' email scammer in Louisiana

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

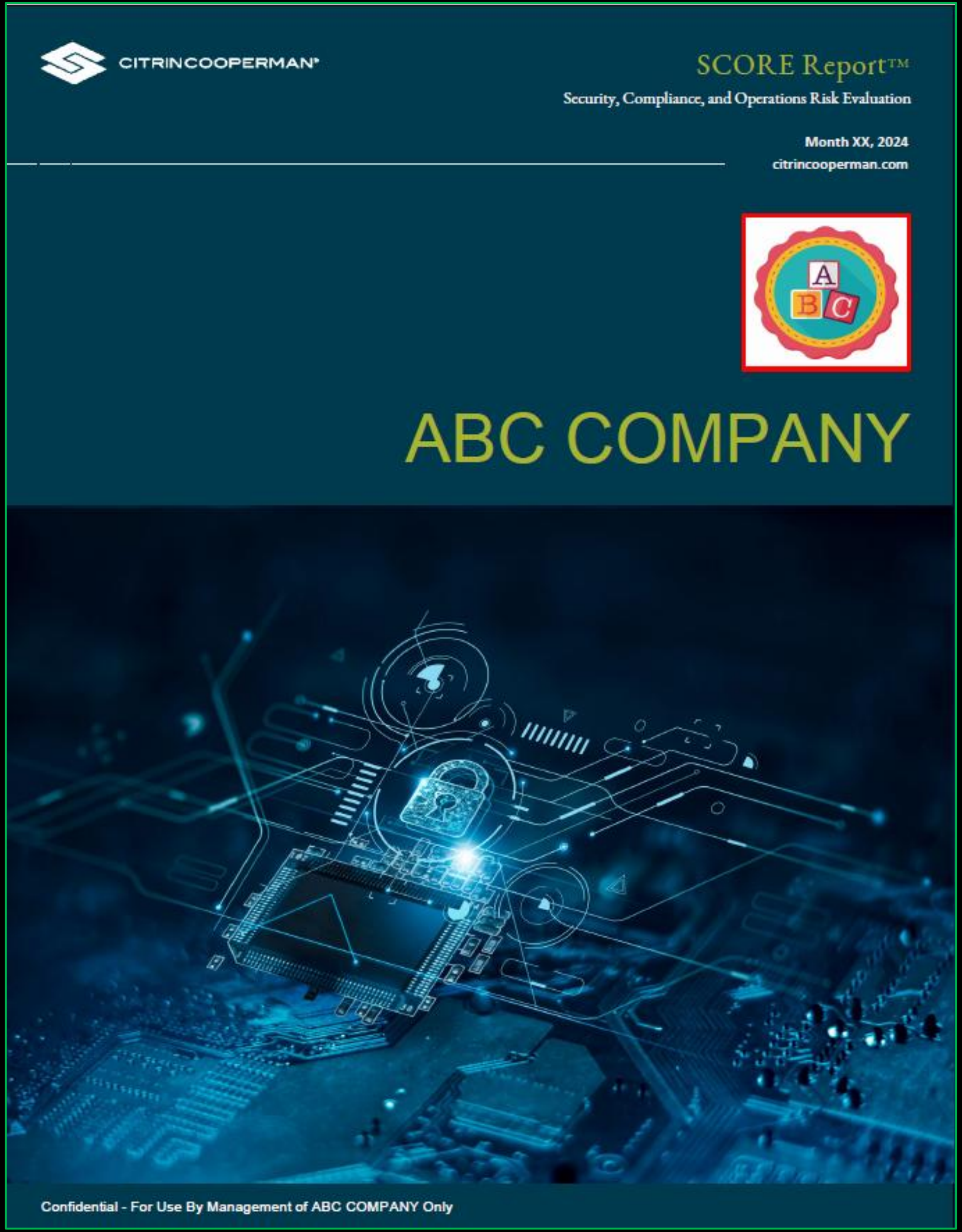
67-year-old Michael Neu of Louisiana was charged with 269 counts of wire fraud and money laundering

Risk Advisory Services

- **Cybersecurity**
  - SCORE Report Cybersecurity Assessments
  - Vulnerability Scanning
  - Penetration Testing
    - Internal, External, Physical
  - Incident Response and Disaster Recovery Planning
  - Awareness Training and Spear Phishing Simulations
  - vCISO
- **Cyber Compliance**
  - Compliance Assessments and Validation
    - PCI DSS, HIPAA, CMMC, State Data Security
    - Policy and Procedure Development
- **Traditional Risk Advisory**
  - Internal audit (outsourced / co-sourced)
  - IT Audit
  - SOX 404
  - Third-party assurance (SOC 1, 2, 3)
  - Due diligence (internal control or IT)



THE SCORE REPORT



CITRINCOOPERMAN®

SCORE Report™

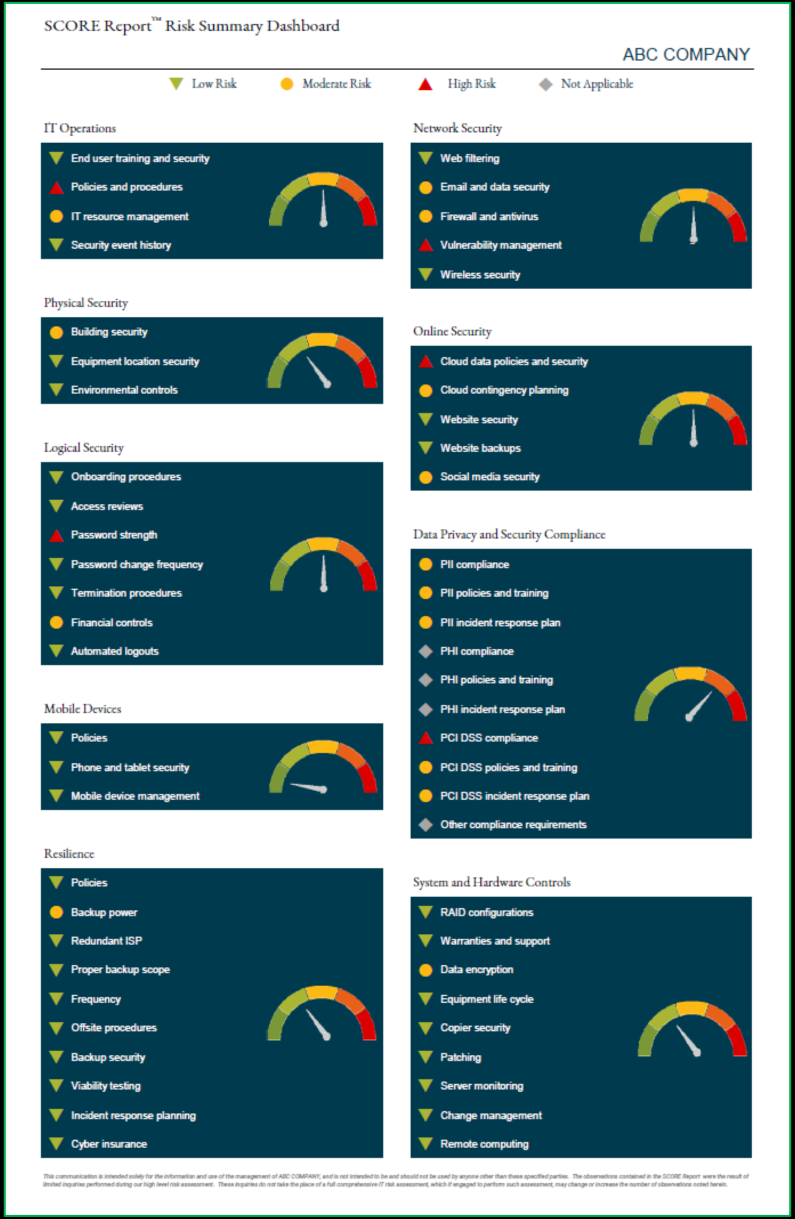
Security, Compliance, and Operations Risk Evaluation

Month XX, 2024
citrincooperman.com

ABC COMPANY

Confidential - For Use By Management of ABC COMPANY Only

THE SCORE REPORT



SCORE Report™ Risk Summary Dashboard

ABC COMPANY

▼ Low Risk ● Moderate Risk ▲ High Risk ◆ Not Applicable

IT Operations

- ▼ End user training and security
- ▲ Policies and procedures
- ● IT resource management
- ▼ Security event history

Physical Security

- ● Building security
- ▼ Equipment location security
- ▼ Environmental controls

Logical Security

- ▼ Onboarding procedures
- ▼ Access reviews
- ▲ Password strength
- ▼ Password change frequency
- ▼ Termination procedures
- ● Financial controls
- ▼ Automated logouts

Mobile Devices

- ▼ Policies
- ▼ Phone and tablet security
- ▼ Mobile device management

Resilience

- ▼ Policies
- ● Backup power
- ▼ Redundant ISP
- ▼ Proper backup scope
- ▼ Frequency
- ▼ Offsite procedures
- ▼ Backup security
- ▼ Viability testing
- ▼ Incident response planning
- ▼ Cyber insurance

Network Security

- ▼ Web filtering
- ● Email and data security
- ● Firewall and antivirus
- ▲ Vulnerability management
- ▼ Wireless security

Online Security

- ▲ Cloud data policies and security
- ● Cloud contingency planning
- ▼ Website security
- ▼ Website backups
- ● Social media security

Data Privacy and Security Compliance

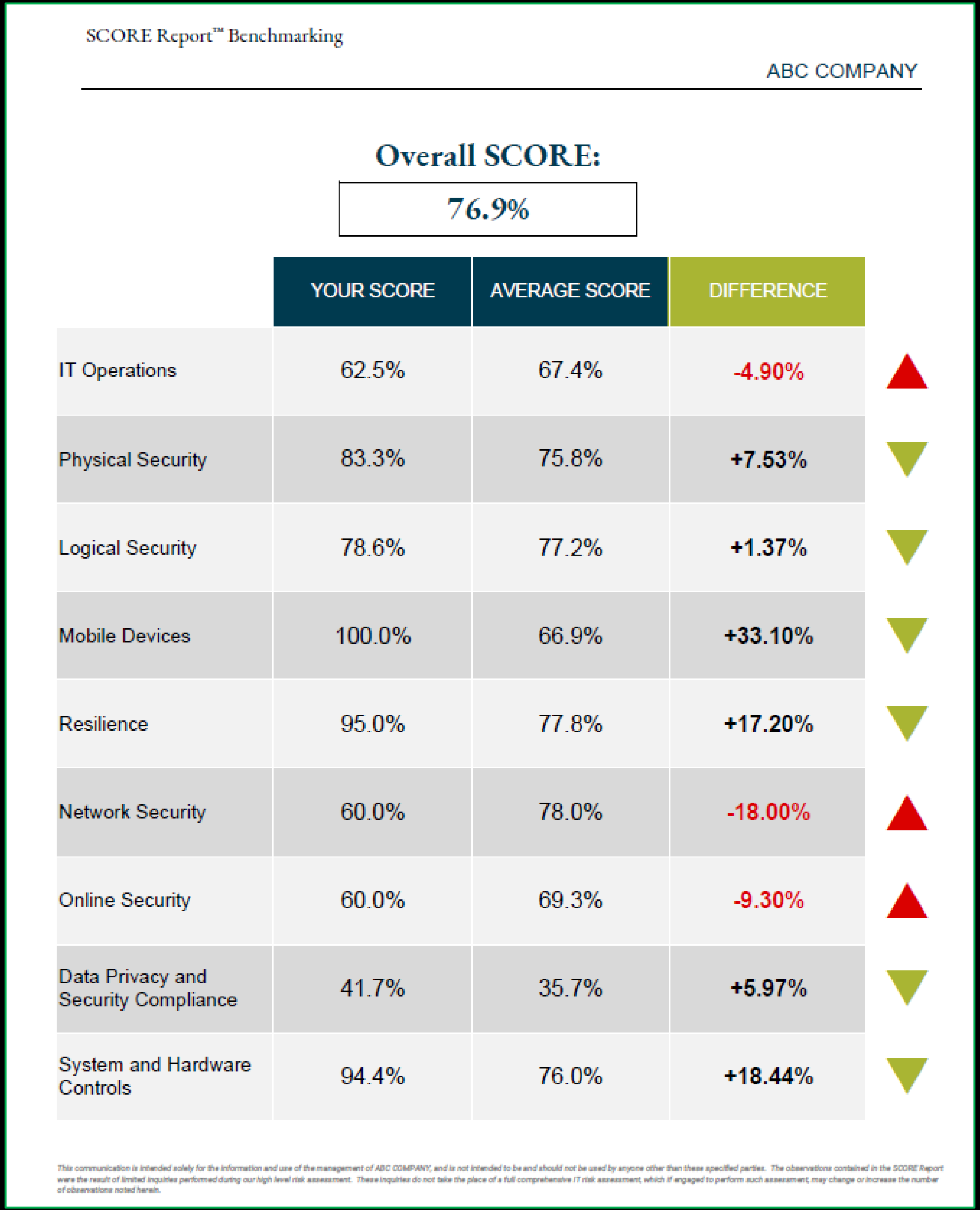
- ● PII compliance
- ● PII policies and training
- ● PII incident response plan
- ◆ PHI compliance
- ◆ PHI policies and training
- ◆ PHI incident response plan
- ▲ PCI DSS compliance
- ● PCI DSS policies and training
- ● PCI DSS incident response plan
- ◆ Other compliance requirements

System and Hardware Controls

- ▼ RAID configurations
- ▼ Warranties and support
- ● Data encryption
- ▼ Equipment life cycle
- ▼ Copier security
- ▼ Patching
- ▼ Server monitoring
- ▼ Change management
- ▼ Remote computing

This communication is intended solely 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 these specified parties. The observations contained in the SCORE Report were the result of limited inquiries performed during our 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 observations noted herein.

THE SCORE REPORT



SCORE Report™ Benchmarking

ABC COMPANY

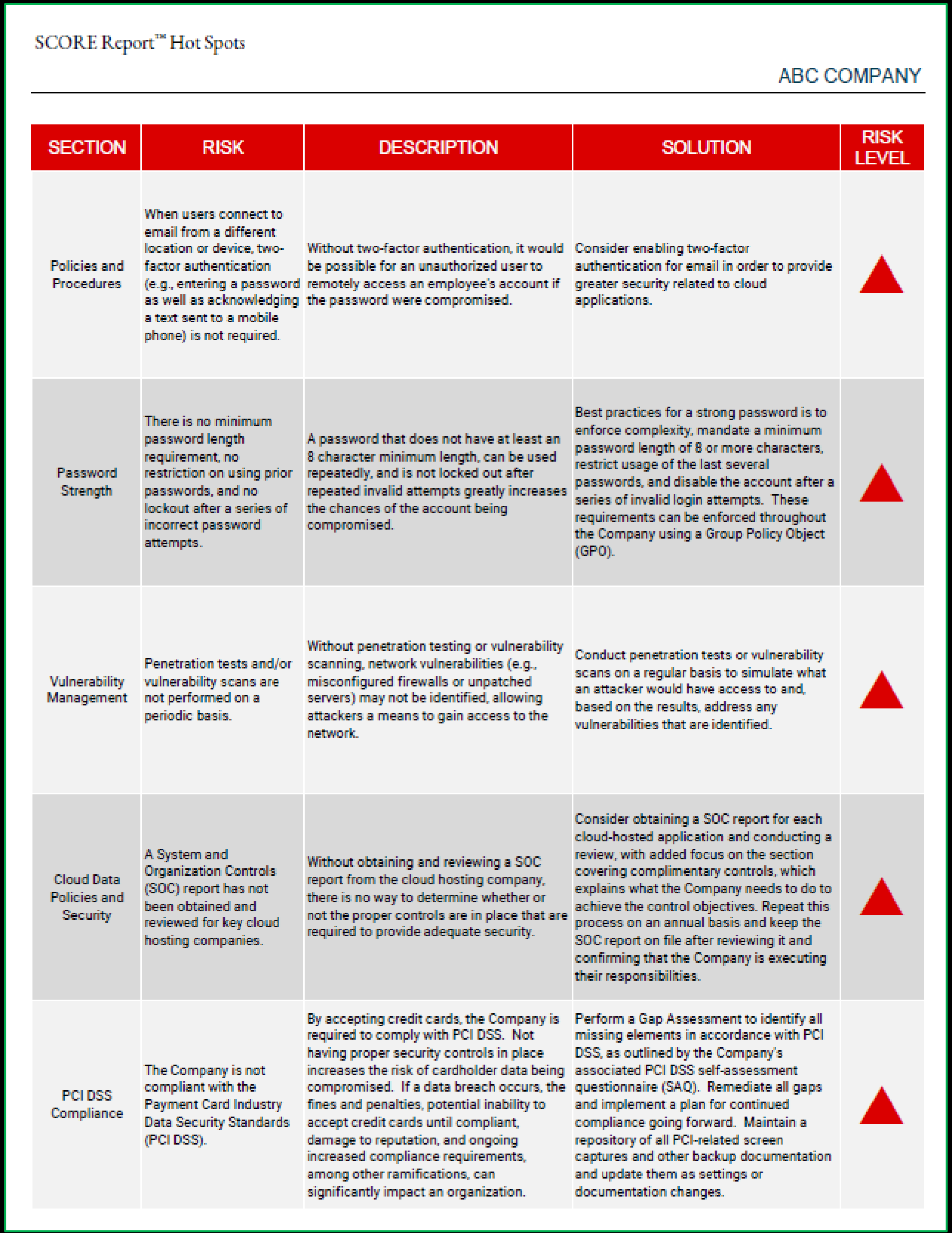
Overall SCORE:

76.9%

	YOUR SCORE	AVERAGE SCORE	DIFFERENCE	
IT Operations	62.5%	67.4%	-4.90%	▲
Physical Security	83.3%	75.8%	+7.53%	▼
Logical Security	78.6%	77.2%	+1.37%	▼
Mobile Devices	100.0%	66.9%	+33.10%	▼
Resilience	95.0%	77.8%	+17.20%	▼
Network Security	60.0%	78.0%	-18.00%	▲
Online Security	60.0%	69.3%	-9.30%	▲
Data Privacy and Security Compliance	41.7%	35.7%	+5.97%	▼
System and Hardware Controls	94.4%	76.0%	+18.44%	▼

This communication is intended solely 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 these specified parties. The observations contained in the SCORE Report were the result of limited inquiries performed during our 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 observations noted herein.

THE SCORE REPORT

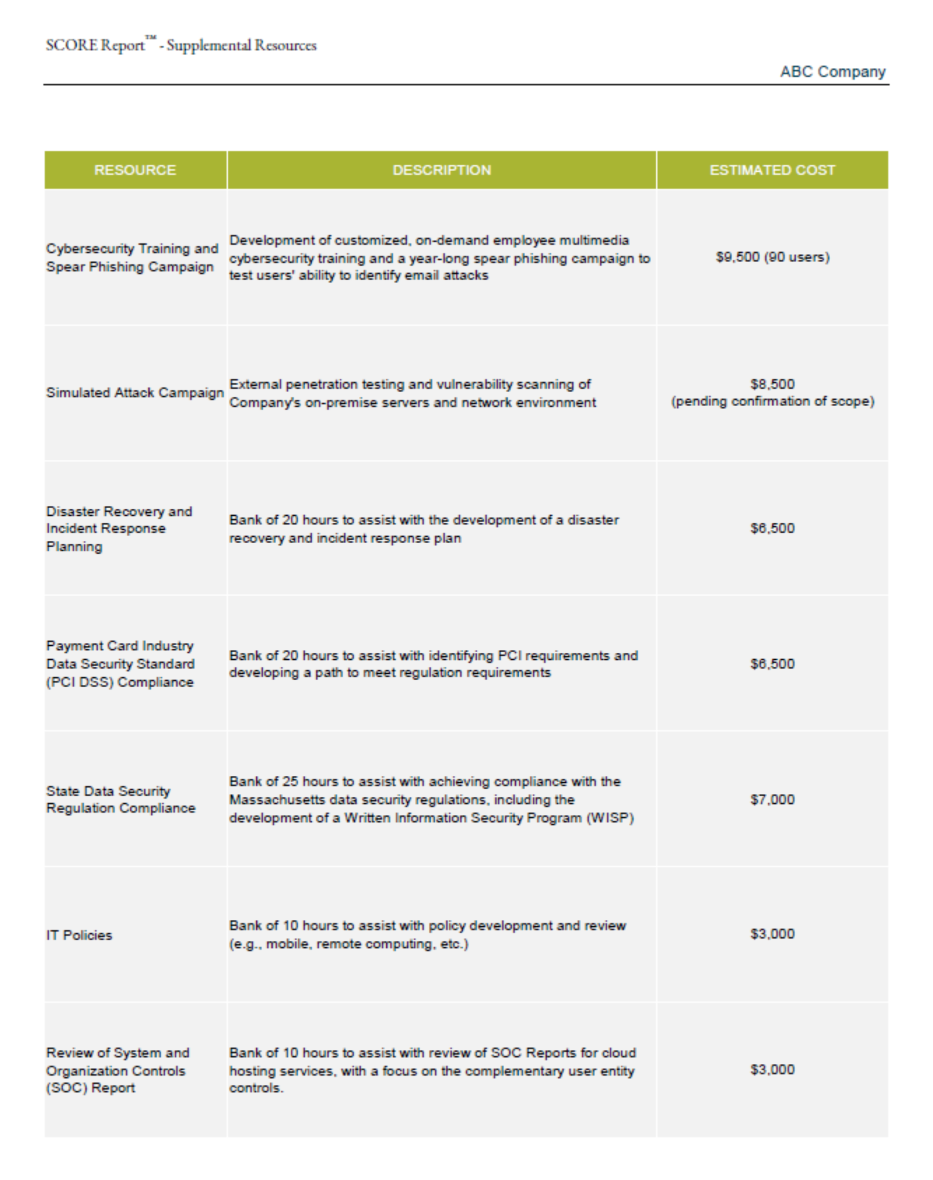


SCORE Report™ Hot Spots

ABC COMPANY

SECTION	RISK	DESCRIPTION	SOLUTION	RISK LEVEL
Policies and Procedures	When users connect to email from a different location or device, two-factor authentication (e.g., entering a password as well as acknowledging a text sent to a mobile phone) is not required.	Without two-factor authentication, it would be possible for an unauthorized user to remotely access an employee's account if the password were compromised.	Consider enabling two-factor authentication for email in order to provide greater security related to cloud applications.	▲
Password Strength	There is no minimum password length requirement, no restriction on using prior passwords, and no lockout after a series of incorrect password attempts.	A password that 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 a Group Policy Object (GPO).	▲
Vulnerability Management	Penetration tests and/or vulnerability scans are not performed on a periodic basis.	Without penetration testing or vulnerability scanning, network vulnerabilities (e.g., misconfigured firewalls or unpatched servers) may not be identified, allowing attackers a means to gain access to the network.	Conduct penetration tests or vulnerability scans on a regular basis to simulate what an attacker would have access to and, based on the results, address any vulnerabilities that are identified.	▲
Cloud Data Policies and Security	A System and Organization Controls (SOC) report has not been obtained and reviewed for key cloud hosting companies.	Without obtaining and reviewing a SOC report from the cloud hosting company, there is no way to determine whether or not the proper controls are in place that are required to provide adequate security.	Consider obtaining a SOC report for each cloud-hosted application and conducting a review, with added focus on the section covering complimentary controls, which explains what the Company needs to do to achieve the control objectives. Repeat this process on an annual basis and keep the SOC report on file after reviewing it and confirming that the Company is executing their responsibilities.	▲
PCI DSS Compliance	The Company is not compliant with the Payment Card Industry Data Security Standards (PCI DSS).	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.	▲

THE SCORE REPORT



SCORE Report™ - Supplemental Resources

ABC Company

RESOURCE	DESCRIPTION	ESTIMATED COST
Cybersecurity Training and Spear Phishing Campaign	Development of customized, on-demand employee multimedia cybersecurity training and a year-long spear phishing campaign to test users' ability to identify email attacks	$9,500 (90 users)
Simulated Attack Campaign	External penetration testing and vulnerability scanning of Company's on-premise servers and network environment	$8,500 (pending confirmation of scope)
Disaster Recovery and Incident Response Planning	Bank of 20 hours to assist with the development of a disaster recovery and incident response plan	$6,500
Payment Card Industry Data Security Standard (PCI DSS) Compliance	Bank of 20 hours to assist with identifying PCI requirements and developing a path to meet regulation requirements	$6,500
State Data Security Regulation Compliance	Bank of 25 hours to assist with achieving compliance with the Massachusetts data security regulations, including the development of a Written Information Security Program (WISP)	$7,000
IT Policies	Bank of 10 hours to assist with policy development and review (e.g., mobile, remote computing, etc.)	$3,000
Review of System and Organization Controls (SOC) Report	Bank of 10 hours to assist with review of SOC Reports for cloud hosting services, with a focus on the complementary user entity controls.	$3,000

60 Second Cyber Assessment

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

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

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

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

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

6. Are key IT procedures and credentials documented and accessible by trusted and authorized members of the Company?

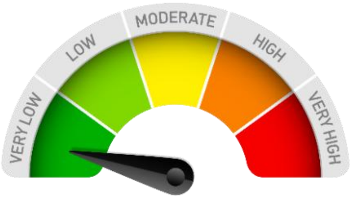
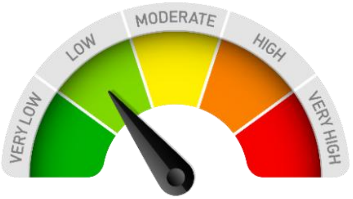
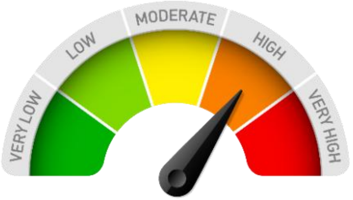
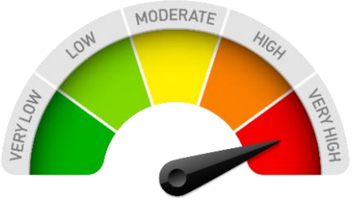
7. Do you have a third-party risk management system to evaluate your vendor's cybersecurity efforts?

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

9. Are your servers and workstations running operating systems that are supported by the vendor (e.g., Server 2008 or Windows 10)?

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

60 Second Cyber Assessment

Number of "YES" Answers	Risk Level
10	
7 - 9	
4 - 6	
0 - 3	

CITRIN COOPERMAN

Questions?

KEVIN RICCI, CISM, CISA, CRISC, MCSE, QSA
kricci@citrincooperman.com
https://www.linkedin.com/in/kevinricci/
401-421-4800

CITRINCOOPERMAN®

Contact Us

Partner

Kevin Ricci,

CISM, CISA, CRISC, MCSE, QSA

kricci@citrincooperm.com

Partner, Franchise Practice Leader

Michael Iannuzzi

miannuzzi@citrincooperman.com

CITRINCOOPERMAN®
FOCUS ON WHAT COUNTS

Thank You