

HANDLING A CYBERSECURITY INVESTIGATION

An Interactive Tabletop Exercise

THE BRIEFEST OF INTRODUCTIONS



**SCOTT
MASCIANICA**
Assistant Director
SEC
Fort Worth, Texas
817.978.3821
MascianicaS@sec.gov



**CHAD
PINSON**
Executive Managing Director
Stroz Friedberg
Dallas, Texas
214.377.4553
cpinson@strozfriedberg.com



**JAY
JOHNSON**
Partner
Jones Day
Dallas, Texas
214.969.3788
jjohnson@jonesday.com

OUTLINE: HANDLING A CYBERSECURITY INVESTIGATION

**COMMON
THREATS**

**REGULATORY
LANDSCAPE**

**TABLETOP
EXERCISE**

Common Threats

Malware	Brute Force Attacks
Lost Laptops, Backup Tapes	Denial-of-Service (“DDoS”)
Fraudulent Wire Transfers	Ransomware
Advanced Persistent Threats	Phishing
Industrial Espionage	Spyware & Other Invasive Software
Third-Party Vulnerabilities	Insider Threats

□ □ □

REGULATORY LANDSCAPE

FTC

SEC

States

DOJ



HYPOTHETICAL INCIDENT

SCCE, Inc.

*A provider of compliance-related
educational services.*

*Regulated by the National Compliance
Education Agency (NCEA)*



DAY 01

- Karl works at SCCE and reports to IT that his laptop is “locked on a scary screen” and is asking for “a bunch of bitcoins or something.”
- Others report that SCCE’s files containing forward-looking financial information and HR data are no longer accessible.
- Karl’s computer is locked on the following screen:



DAY 02

- IT quickly reviews available network logs and detects unusual network activity.
- IT identifies a malicious email that was sent to Karl on DAY 00.

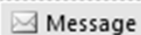


USPS Delivery Error No#2487

Your FedEx <customer-services@fedex.com>

Sent: DAY 00, 4:30pm

To: karl@corporatecompliance.org



Message



FedEx_Invoice.zip (42 KB)

Dear Customer,

Your package has been returned to the FedEx office.

The reason of the return is - Incorrect delivery address of the package.

Please print out the invoice copy attached and collect the package at our office.

FedEx Logistics Services.

DAY 03

- A well-known blogger blogged.
- An anonymous tweeter tweeted.



Johnson Speaks – You Listen

Thoughts from a well-known blogger.



Compliance-Related Education Providers Attacked

DAY 03, 2:30pm

Compliance-related education service providers are being targeted in a phishing and ransomware campaign. The phishing emails carry ransomware and malware known as Compliance.exe, capable of exfiltrating HR, finance, and other data. Sources confirm that SCCE has been targeted.

ABA SciTech Retweeted



Anon Tweeter

@AnonTweeter · DAY 03

@SCCE failed to protect data! Was distracted by #ransomware. Hey @NCEA, check this out! #databreach #IamChadPinson

DAY 04

- FBI contacts SCCE to arrange an immediate “conversation” about confirmed data loss. FBI requests all written information concerning the incident.
- SCCE’s forensics firm confirms that the phishing email to Karl led to the ransomware attack, and that the email also included the malware Compliance.exe. The firm confirms data loss.

DAY 35 (Post Incident Notification)

- Access Letter from NCEA requests “documents sufficient to identify the cause of the security incident” and “documents evidencing SCCE’s software patching process.”
- NCEA requests interviews with Karl and other key SCCE employees and executives.

□ □ □

DAY 60

- NCEA issues Civil Investigative Demand (CID) requesting all information related to the security incident.

□ □ □

DAY 90

- NCEA files a complaint against SCCE for inadequate data protection practices.



QUESTIONS?



**SCOTT
MASCIANICA**
Assistant Director
SEC
Fort Worth, Texas
817.978.3821
MascianicaS@sec.gov



**CHAD
PINSON**
Executive Managing Director
Stroz Friedberg
Dallas, Texas
214.377.4553
cpinson@strozfriedberg.com



**JAY
JOHNSON**
Partner
Jones Day
Dallas, Texas
214.969.3788
jjohnson@jonesday.com