HANDLING A CYBERSECURITY INVESTIGATION
An Interactive Tabletop Exercise

THE BRIEFEST OF INTRODUCTIONS

SHAMOIL SHIPCHANDLER
Regional Director
SEC Fort Worth, Texas
817.978.3821
shipchandlers@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

COMMON THREATS
REGULATORY LANDSCAPE
TABLETOP EXERCISE

OUTLINE: HANDLING A CYBERSECURITY INVESTIGATION
### Common Threats

<table>
<thead>
<tr>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Brute Force Attacks</td>
</tr>
<tr>
<td>Lost Laptops, Backup Tapes</td>
<td>Denial-of-Service (“DDoS”)</td>
</tr>
<tr>
<td>Fraudulent Wire Transfers</td>
<td>Ransomware</td>
</tr>
<tr>
<td>Advanced Persistent Threats</td>
<td>Phishing</td>
</tr>
<tr>
<td>Industrial Espionage</td>
<td>Spyware &amp; Other Invasive Software</td>
</tr>
<tr>
<td>Third-Party Vulnerabilities</td>
<td>Insider Threats</td>
</tr>
</tbody>
</table>

### 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:

```
Oops, your files have been encrypted!
What Happened to My Computer?
Your computer files were encrypted using a powerful new ransomware virus that can't be removed without paying! To recover your files, you will have to pay a ransom in “Bitcoin.” 

How Much You Need to Pay:

Send $20,000 worth of bitcoin to this address:

[Bitcoin Address]

Payment will be raised on
DAY 02 – 5:00pm

Your files will be lost on
DAY 03 – 12:00am
```

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.
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

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.
DAY 03

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

SHAMOIL SHIPCHANDLER
Regional Director
SEC
Fort Worth, Texas
817.978.3821
shipchandlers@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