Cyber Security Due Diligence:

Will You Be the One to Save Your Company & CEO From Disaster

Charly Shugg, Brig Gen, USAF, Retired
Partner | Chief Operating Officer, Sylint Group Incorporated

SCCE Society of Corporate Compliance and Ethics

Sylint

1

The Question of the Day

How did we come up with the company name **"Sylint"** and what does it mean?

- Sylint (si-lent): from the Greek variant "**Syl**-" meaning "together" and the suffix "-**int**" comes from the variant meaning "information", usually associated with secret information regarding the enemy or about hostile activities, or "**int**elligence"

SCCE Society of Corporate Compliance and Ethics

Sylint

2

Sylint Group, Inc

Incident Response, Cyber Security, Digital Data Forensics (SRQ 1999)

- Clients - Fortune 500, Gov't, Public, Private, High Profile, LEO
- 1 of 16 Companies Accredited by National Security Agency (NSA) and NSCAP for Cyber Incident Response Assistance (CIRA)
- 1 of 11 Companies Authorized to Investigate Card Breaches (PCI) in USA for VISA, MasterCard, AMEX: PCI Forensic Investigators (PFI)
- NSA, DoD/Air Force – Intelligence Centric Methodologies
- DHS Industrial Control System (ICS) Joint Working Group Member

SCCE Society of Corporate Compliance and Ethics

Sylint

3

What is Your Position?

CCEO / General Counsel	**A**
C&E Staff	**B**
Other Senior Management	**C**
Techical / Security Staff	**D**
Other	**E**

Start the presentation to see live content. Still no live content? Install the app or get help at **PollEv.com/app**

SCCE Society of Corporate Compliance and Ethics

Sylint

4

Have Senior Executives Been Held Responsible For Data Breaches in the Past?

Target
- CEO (Fired); CIO (Fired)

Yahoo
- General Counsel (Fired)

FACC (Austrian Aerospace Company)
- CEO (Fired); CFO (Fired)

UBER
- Founder / CEO (Fired)
- CSO and Legal Director of Security and Law Enforcement (Fired)

SONY
- CEO (Fired)

Equifax
- CEO (Retired)
- CSO (Retired)
- CIO (Retired)

SCCE Society of Corporate Compliance and Ethics

Sylint

5

Any Trends or Reports on This Issue?

Kaspersky Lab (Sep '18)

- *In North America, reports that 32% of breaches led to a member of the C-suite losing his or her job.*

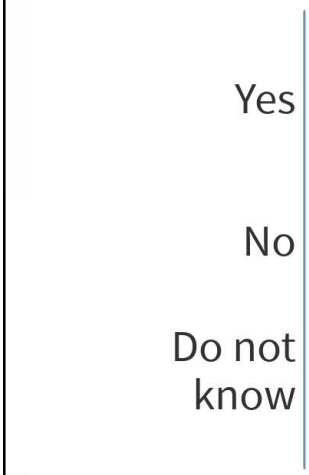
- *Nearly 30% of SMBs and 27% of large enterprises fired senior, non-IT personnel*
  - Highlights how protecting data is a team sport
  - If done poorly, will often result in non-IT stakeholders leaving the building

SCCE Society of Corporate Compliance and Ethics

Sylint

6

Has Your Company Experienced a Cyber Security Incident?



Start the presentation to see live content. Still no live content? Install the app or get help at PollEv.com/app

Society of Corporate Compliance and Ethics

Sylint

7

Results of Public Outcry - Legislation

4/3/2019: Senator Elizabeth Warren (D-Massachusetts) announced that she was proposing legislation to ***ensure CEOs whose companies are involved in massive data breaches be held accountable "in ways not seen before"***

SCCE Society of Corporate Compliance and Ethics

Sylint

8

Results of Public Outcry - Legislation

Data Breach Prevention and Compensation Act of 2019 (Sponsored by Senators Warren and Warner and Representatives Cummings and Krishnamoorthi), would impose jail time for violations:

- Violations would be defined as those who "negligently permit or fail to prevent" (**read as lack of due diligence**) a "violation of the law" (**read as a malicious cyber breach**), that "affects the health, safety, finances or personal data" of 1% of the population of any state.
- Recommends up to a one (1) year in prison for the CEO if it is their first offense with repeat offenders getting as much as three (3) years
- Penalty has constraints as it would only apply to companies that generate more than $1 billion in annual revenue ***(for perspective, Equifax generated $3.4 billion in revenues in 2017)***
- To appease those who think this prospective legislation might be too harsh, the authors added a clause that a company would also have to be either convicted of violating a law or have settled a claim with a state or federal regulator ***(Equifax signed a consent decree with state regulators in 2018)***

SCCE Society of Corporate Compliance and Ethics

Sylint

9

Results of Public Outcry - Legislation

And there is more…

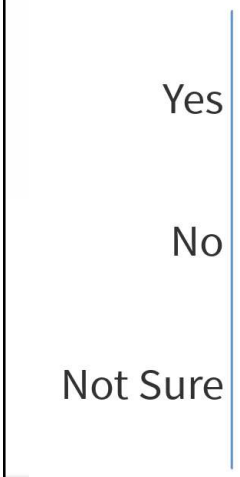
Senator Ron Wyden (D-Oregon) is proposing an even harsher legislative bill regarding data privacy that would recommend up to twenty (20) years of prison for corporate executives who violate their customer's privacy

SCCE Society of Corporate Compliance and Ethics

Sylint

10

Do You Agree with the Proposed Legislation?



Start the presentation to see live content. Still no live content? Install the app or get help at PollEv.com/app

SCCE Society of Corporate Compliance and Ethics

Sylint

11

Is It Really That Bad Out There with Regard to Senior Executive Oversight?

Let's Look at Equifax through the lens of Senior Executive Oversight

SCCE Society of Corporate Compliance and Ethics

Sylint

12

Equifax Incident Response Review*

3/8	US-CERT sends Equifax an alert to patch Apache Struts software
3/9	Equifax GTVM team disseminates notification requesting to apply the critical patch within 48 hours
3/15	Equifax Security team runs scan to ensure patch compliance
5/13	**Attackers enter network** via Apache Struts vulnerability (9K queries)
7/29	Renew expired security certificate for monitoring device (19 months)
7/30	Equifax takes ACIS application offline; CIO informed of incident
7/31	Equifax staff determines PII may have been exfiltrated with intrusion

*US House of Representatives, Committee on Oversight and Government Reform, Dec 2018

SCCE Society of Corporate Compliance and Ethics

Sylint

13

Equifax Incident Response Review*

7/31 (Mon)	CIO informs CEO of security incident
8/2 (Wed)	Law firm and cybersecurity company engaged; FBI informed
8/11	Security experts suspect threat accessed large amount of PII data
8/17 (Thurs)	Equifax holds senior leadership team meeting
8/24-25	Volume of PII confirmed; CEO holds telephonic BoD meeting
9/1	Board meeting convened to discuss investigation & another senior leadership team meeting
9/7	Equifax makes public announcement of breach

*US House of Representatives, Committee on Oversight and Government Reform, Dec 2018

SCCE Society of Corporate Compliance and Ethics

Sylint

14

Equifax Incident Response Review*

Public Announcement Issues:

Website Notification

- New website that was totally separate from corporate website
- Equifaxsecurity2017.com provided customers with incomplete or incorrect information
- ***Equifax Twitter account directed customers to phishing website for nearly two (2) weeks***

Call Center Notification

- Grossly inadequate preparations weeks prior to announcement (Onboard, train and set up support for 1,500 call center agents)
- Immediately overwhelmed with volume as ***representatives were understaffed and untrained***
- Individuals unable to find out if personal information was compromised or failed to reach an actual person to talk with

Credit Monitoring

- Advised people to sign up for credit monitoring service but…forced consumers to agree to terms of use with a mandatory arbitration clause (preventing right to sue)
- Eventually, Equifax agreed that the arbitration clause would not apply to claims arising from the breach

Public outreach after the breach "haphazard," ill-conceived," and a "dumpster fire." Brian Krebs

*US House of Representatives, Committee on Oversight and Government Reform, Dec 2018

Equifax Incident Response Review*

9/14	Congressional Committee launches investigation
9/15	**CIO David Webb and CSO Susan Mauldin announce retirement**
9/26	**CEO Richard Smith announces retirement**
9/27	**Interim CEO Paulino de Regos Barros Jr. publishes public apology**
10/2	**2.5 Million more victims announced**
3/1/2018	**2.4 Million additional victims announced**
3/28	**Equifax names Mark Begor as CEO**

*US House of Representatives, Committee on Oversight and Government Reform, Dec 2018

Do These Facts Make a Difference?*

Did You Know?

- In 2015 Experian disclosed a breach of approx. 15 Million PII on individuals (risk to industry)
- In 2016, Equifax was assigned at rating of "Zero out of Ten" regarding their data security efforts
- In 2017, the rating remained unchanged….both reports included:

  "…The company's data and privacy policies are limited in scope and Equifax shows no evidence of data breach plans or regular audits of its information security policies and systems."
- Equifax never disclosed any cybersecurity risks or incidents in SEC filings prior to their 2017 data breach

*US House of Representatives, Committee on Oversight and Government Reform, Dec 2018

SCCE Society of Corporate Compliance and Ethics

Sylint

17

Do You Think Equifax Senior Executives Demonstrated Appropriate Due Diligence?

Yes

NO

Do not know--Not a Lawyer

Start the presentation to see live content. Still no live content? Install the app or get help at PollEv.com/app

SCCE Society of Corporate Compliance and Ethics

Sylint

18

Do You Now Agree with the Proposed Legislation Regarding Cyber Security and Senior Executives?

Yes

No

Still not sure and more confused

SCCE Society of Corporate Compliance and Ethics

19

Emerging Issue

General Data Protection Regulation (GDPR)

British Airways (2019) – UK (*GDPR Fine* = **$230M**)

BRITISH AIRWAYS

Marriot (2019) - UK (*GDPR Fine* = **$123M**)

Marriott

MARRIOTT

SCCE Society of Corporate Compliance and Ethics

Sylint

20

What Can Compliance & Ethics Officers Do?

SCCE Society of Corporate Compliance and Ethics

Sylint

21

What is "Reasonable" Cyber Security

SCCE Society of Corporate Compliance and Ethics

Sylint

22

“Reasonable” Cyber Security Due Diligence

Pre-Incident Awareness/Oversight

- Operational Security Procedures and Processes
- Incident Response Plans and Testing
- Senior and Middle Management Communication Flow

Post-Incident Actions

- Senior and Middle Management Involvement
- Public Facing Communication

SCCE Society of Corporate Compliance and Ethics

Sylint

23

Pre & Post Incident Due Diligence Commonalities

Timely, Relevant and Accurate Information Flow

Checks and Balances

Plans & Testing/Exercises

SCCE Society of Corporate Compliance and Ethics

Sylint

24

Cyber Security Communications Flow
(For Non-Security People)

Key Performance Indicators (KPI) Metrics

- Identify Status of "Show Stoppers" in Timely Manner
- Different Levels of "Indicators" for Levels of Management

SCCE Society of Corporate Compliance and Ethics

Sylint

25

Cyber Security Checks and Balances

Communication Flow (KPI)

Internal IT Department (Tasks Accomplished)

- Patch Management / External and Internal Scans / Password Audit / Monitoring

Middle Management (Task Resolved)

- Inter-departmental Issues (Non-compliance with security processes/procedures)

Senior Management (Overall Awareness)

- Process Issues (see above)
- Compliance & Resource Issues
- Cyber Security Assessment (Internal & 3rd Party Venders/Business Associates)

SCCE Society of Corporate Compliance and Ethics

Sylint

26

Plans and Testing/Exercises

Business Continuity Plans

Cyber Security Incident Plan / Exercises

- *Internal IT Department* – Technical focus ("Systems Owner")
- *Middle Management* – Operational concerns focus ("Business Owner")
- *Senior Management* – Strategic focus / Public facing

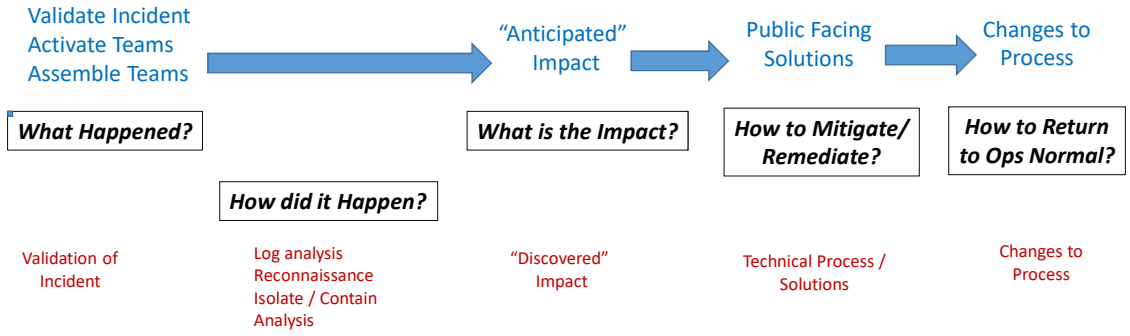
SCCE Society of Corporate Compliance and Ethics

Sylint

27

Division of Responsibilities

Senior Incident Response Team



Internal Technical / External Incident Response Team

SCCE Society of Corporate Compliance and Ethics

Sylint

28

Major Points to Ponder From Equifax

Pre-Incident

- Follow up/awareness of cyber security posture review discrepancies *(at least they did one annually)*
- Ensuring policies and procedures are synchronized *(at least they had policies)*
  "…we had the notifications, but we didn't notify the people…we had scanning, but it didn't scan all the things…" *Mark Begor, new Equifax CEO*
- Credible Senior Executive feedback on current cyber security posture *(at least it was on BoD agenda)*

Post-Incident

- "Who & When to pull the fire alarm" (push as low as possible)
- Well thought out (discussed/exercised) potential cyber security scenarios/plans of action (internal & public facing)

SCCE Society of Corporate Compliance and Ethics

Sylint

29

Where Does Your Company / Organization Stand Regarding Cyber Security Due Diligence?

Charly Shugg, Brig Gen, USAF, Retired
Partner | Chief Operating Officer, Sylint Group Incorporated
cshugg@usinfosec.com

SCCE Society of Corporate Compliance and Ethics

Sylint

30