A Journey Down the Road of College & University Breaches

"A Review of Recent University & College Case Studies, Lessons Learned, and How to Mitigate Being a Victim"

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

SCCE Society of Corporate Compliance and Ethics

Sylint

1

Brig Gen Charly Shugg, USAF, Retired

- Partner | Chief Operating Officer, Sylint Group
- Executive Director, Global Consortium for Counter Cyber Terrorism (GC^3T)
- Last USAF position, key to establishing Air Force Cyber Command and United States Cyber Command
- Graduate United States Air Force Academy with three advanced degrees including Master of Science in National Security Strategy

SCCE Society of Corporate Compliance and Ethics

Sylint

2

Question of the Day

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

- **Sylint** (sī-lənt): 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

3

Sylint Group, Inc

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

- Clients - Fortune 500, Gov't, Public, Private, Regional, LEO
  - ***Includes large State University Systems & smaller Private Colleges***

Unique Corporate Qualifications/Insight

- 1 of 10 Companies Authorized to Investigate Card Breaches (PCI) in USA for VISA, MasterCard, AMEX: PCI Forensic Investigators (PFI)
- 1 of 16 Companies Accredited by National Security Agency (NSA) and NSCAP for Cyber Incident Response Assistance (CIRA)
- National Security Agency, DoD, FBI – Intelligence/Investigative Methodologies

SCCE Society of Corporate Compliance and Ethics

Sylint

4

Insight from National Security Viewpoint

"Know your enemy and know yourself and you can fight a hundred battles without disaster…" Sun Tzu

- "Know your enemy…" = **Intent**
- "…know yourself…" = **Concept of Operations** (Open Environment of Academia - free exchange of ideas, sharing and collaboration around data) & **Valuable Assets** (Crown Jewels)

SCCE Society of Corporate Compliance and Ethics

Sylint

5

"Know your Enemy" Bottom Line

Universities and Colleges are Very Lucrative Targets for Nation State Actors, Organized Crime and Activists!

#2 Target for Cyber Attacks

SCCE Society of Corporate Compliance and Ethics

Sylint

6

“Know Yourself”

Dynamic Group of Users (Small Cities)

- Incoming freshmen
- Outgoing seniors
- Additional Alumni
- Visiting professors

Multi-role Users (many “personas”)

- Multi-role faculty
- Graduate Assistants

Fascination with Leading Technology

- Cloud based data repositories
- Mobile devices
- WiFi (public and unprotected wireless access points)

SCCE Society of Corporate Compliance and Ethics

Sylint

7

“Know Yourself”

Repository of Sensitive Information

- Access to thousands of individual’s SSN, bank accounts, credit cards, health information, financial data
- Personal and biographical information
- Valuable research projects for government or private sector

Siloed Multiple networks and Systems

- In-house developed systems possibly outdated

Lack of community security awareness

- Shared passwords
- Not protecting credentials

SCCE Society of Corporate Compliance and Ethics

Sylint

8

Has Your College or University Ever Had a Cyber Breach?

Yes	**A**
No	**B**
Do Not Know	**C**
Do Not Want to Say	**D**

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Society of Corporate Compliance and Ethics

9

Case Study #1 (Website Attack / Data Compromise)

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies

SCCE Society of Corporate Compliance and Ethics

Sylint

10

Case Study #2 (Email Attack/Data Compromise)

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies

SCCE Society of Corporate Compliance and Ethics

Sylint

11

Case Study #3 (3rd Party Vendor Access Attack)

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies

SCCE Society of Corporate Compliance and Ethics

Sylint

12

Case Study #4 (Proxy / Mining & Exploitation)

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies

SCCE Society of Corporate Compliance and Ethics

Sylint

13

Case Study #5 (Denial of Services Attack/Extorsion)

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies

SCCE Society of Corporate Compliance and Ethics

Sylint

14

How Does Your Institution's Senior Staff Rate the Importance of Cyber Security Awareness

Top Issue - Discussed Regularly

Minor Issue - Rarely Discussed

Reactive Issue Only - Discussed When Impacted

Not an Issue - Never Discussed

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

SCCE Society of Corporate Compliance and Ethics

Sylint

15

What is your responsibility?

AWARENESS

Proactive ⟷ *Reactive*

SCCE Society of Corporate Compliance and Ethics

Sylint

16

Proactive

KPI Monitoring/Communication - (Make it a "Team" Risk Issue)

Establish a communications pathway for early identification of potential risks

- What gets measured and communicated gets attention
- Facilitates awareness, collaboration and cooperation outside of IT

Methodology to regularly verify & communicate status

- Critical System(s) status
- Basic hygiene control & monitoring standards

SCCE Society of Corporate Compliance and Ethics

Sylint

17

Do You Think Your Senior Staff Would Be Interested In Qtr/Semi-Annual Cyber Security KPI results?

Yes - Interested and Demonstrates Due Diligence

Maybe - Would be a New Concept

No - Either No Interest or Lack of Understanding with Issue

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

SCCE Society of Corporate Compliance and Ethics

Sylint

18

Reactive
"Equifax Example"

Timeline of Events

Could have it been avoided?

Who was at fault?

Does your organization have a "fire alarm" and if so, who can pull it?

SCCE Society of Corporate Compliance and Ethics

Sylint

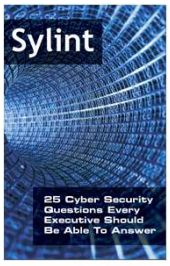
19

Cyber Security "Awareness"

From the Top…Due Diligence is the requirement & is expected:

Knowledge of Operations/Cyber Security Measures versus Cyber Security Threat/Impact

For a free hard copy of this pamphlet, please email me at cshugg@usinfosec.com with your name, title and physical mailing address.



SCCE Society of Corporate Compliance and Ethics

Sylint

20

Reality

Universities and Colleges are Very Difficult to Protect…but it Can be Done!

SCCE Society of Corporate Compliance and Ethics

Sylint

21

Where Does Your University / College 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

22