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

Brig Gen Charly Shugg, USAF, Retired

• Partner | Chief Operating Officer, Sylint Group
• Executive Director, Global Consortium for Counter Cyber Terrorism (GC³T)
• 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
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 “intelligence”

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
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)

“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
“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)

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
Has Your College or University Ever Had a Cyber Breach?

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

Case Study #1 (Website Attack / Data Compromise)

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies
Case Study #2 (Email Attack/Data Compromise)

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies

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

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies
Case Study #4 (Proxy / Mining & Exploitation)

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies

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

Attack Description / Impact / Ramifications

Lessons Learned / Mitigation Strategies
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

What is your responsibility?

AWARENESS

Proactive ↔ Reactive
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

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
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?

Cyber Security “Awareness”

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


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

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

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