Cyber Security and Your School

New York Association Of Independent Schools
November 6th, 2015
Session Objectives

- Raise awareness, not trying to scare you
- Gain a basic understanding of cyber security concepts
- Discuss the unique information security challenges in an academic environment
- Discuss methods for minimizing your risk of a security incident and data breach
Agenda

- Part 1: Introduction to Cyber Security
- Part 2: Today’s Information Security Reality
- Part 3: Interactive Exercise
- Part 4: Unique Academic Challenges
- Part 5: How Can I Protect My School’s Data?
Part 1:
Introduction to Cyber Security
Part 1 Agenda

✦ Common Terminology
✦ Anatomy of a Data Breach
✦ Data Breach Statistics
✦ What Does it Mean to My School?
Common Terminology

- **Information Security**: practice of defending information from unauthorized access, use, disclosure, disruption, modification, or destruction.

- **Security Incident**: any event that compromises the confidentiality, integrity, or availability of an information asset.

- **Data Breach**: an incident that resulted in confirmed disclosure to an unauthorized party.

Cyber Security Lexicon can be found at 
http://go.northstargroupllc.com/CSL
Common Terminology

- **Vulnerability**: an unintended flaw in software code or a system that leaves it open to the potential for exploitation in the form of unauthorized access or malicious behavior such as viruses, worms, Trojan horses and other forms of malware.

- **Defense in Depth**: the approach of using multiple layers of security to guard against failure of a single security component.

Cyber Security Lexicon can be found at http://go.northstargroupllc.com/CSL
Relevant Regulatory Terms

- **PII**: Personally Identifiable Information
- **PHI**: Protected Health Information
- **FERPA**: Family Educational Rights and Privacy Act
- **HIPAA**: Health Insurance Portability and Accountability Act
- 47 states and 3 territories have unique breach notification laws
Today’s Threat Actors

- Criminal Hacker
- Ignorant Insider
- Malicious Insider
- Cloud/3rd Party Compromise
- Nation States
- Script Kiddies
- Hacktivist
Anatomy of a Data Breach

- **Step 1: Research** - The cybercriminal looks for a weakness in the target's people, systems, or networks. This may include conducting research on the organization’s employees, internal network, web site, social media, etc.

- **Step 2: Attack** - The cybercriminal makes initial contact with the target through either a network vulnerability or social attack.
Anatomy of a Data Breach

- **Step 3: Exfiltration** - The cybercriminal extracts and transmits data back to themselves. Data could include:
  - Student health records
  - Donor records
  - Family financial records
  - Confidential information such as budget, strategic plan, etc.

- **Step 4: Use of Exposed Data** - The cybercriminal uses the stolen data for financial gain or to perpetuate a higher level attack.
Social Engineering/Phishing

- Nearly identical email address (JohnHill vs. JohnHilll)
- Place she had visited from Facebook
- Name of a local bank
- Home address including phone number
2015 Verizon Data Breach Report

In 2014 there were:

- 79,790 security incidents
- 2,122 confirmed data breaches
- Education was #12 of top 20 industries based on # of security incidents
- Approximately 85% of threat actors were external
2015 Verizon Data Breach Report

- Phishing and spear phishing increasingly successful
- Software vulnerabilities continue to be a big problem (some were identified in 1999)
- Smart phones saw minimal targeting
2015 Secunia Vulnerability Review

- 15,435 vulnerabilities across 3,870 applications
  - Examples – Google Chrome, Adobe Reader, Windows 7
- 18% increase from 2013 to 2014
- 11.3% rated as either Extremely Critical or Highly Critical
How Could My School be Affected?

- Common data possessed by a school:
  - PII and PHI
  - Parent financial records
  - Donor/development office records
  - Sensitive information (budget, enrollment numbers, strategic plans, etc.)

- What would be the impact if your website was defaced?

- What would be the impact if you were the victim of ransomware?
Hacking by Students

Long Island students busted for allegedly hacking into high school’s computer system, changing grades and schedules in Ferris Bueller-style scheme

By Edgar Sandoval, Thomas Tracy / New York Daily News / Updated Wednesday, October 21, 2015, 11:40 AM

Three Long Island teens were arrested Tuesday for committing a Ferris Bueller-style hack into their high school’s computer system, where they pumped up their grades and altered the schedules for 300 students, officials said.

One of Commack, is accused of slipping into Commack High School after hours and connecting a device known as a key log to the keyboard of a classroom computer on May 28. He did it again in June, authorities said.

The small gizmo records all the keystrokes made on the computer, according to Detective Sgt. John Best, of the Suffolk County Police Department Computer

Emblem Health

What care feels like.

CLICK HERE
Unencrypted USB

York school admits data breach after unprotected memory stick is lost
Stolen Laptop

HealthITSecurity ➤ Latest Health Data Breaches

**OU Health Data Breach from Stolen Laptop Affects Over 9,000**

By Sara Heath on October 15, 2015

Although healthcare providers often report taking mobile device security seriously, health data breaches due to lost or stolen laptops still do occur. Such was the case at the University of Oklahoma Department of Urology, according to a recent hospital statement.

According to OU Medicine, a laptop potentially storing a spreadsheet containing limited patient information was stolen from a former OU physician between July 16 and 17. The spreadsheet contained limited information for approximately 9,300 pediatric patients between 1990 and 2000, according to the Department of Health and Human Services' (HHS's) Office for Civil Rights database.

Health information that may have been breached includes patient name, diagnosis, treatment code, date of treatment, date of birth, description of urologic medical treatment or procedure, medical record number, and physician name. According to OU Medicine, no addresses, Social Security numbers, or other billing information was included.

Although OU Medicine reported not knowing whether the spreadsheet containing the patient information was indeed on the laptop, the hospital reportedly wanted to take precautions by notifying the 9,300 potentially affected patients.
Part 2: Today’s Information Security Reality
Today’s Information Security Reality

✦ Organizations are not focusing on the basics
✦ Most organizations don’t practice good IT security hygiene
✦ Employees are the weakest link
✦ Organizations tend to focus on technology and neglect the people and policy side
✦ IT personnel are:
  ✦ Not security experts
  ✦ Stretched thin in most organizations
  ✦ Unable to afford most cyber security related tools
What Is Your Password?
The Password Minder
Part 3: Interactive Exercise
Interactive Exercise

Question - What are the things you do to protect sensitive information at your residence or in your organization?

Example would be to lock your doors
## Interactive Exercise - Technology

<table>
<thead>
<tr>
<th>Your Residence</th>
<th>Your Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locks on doors</td>
<td>Passwords, 2 factor authentication</td>
</tr>
<tr>
<td>Monitored alarm system</td>
<td>Firewall, antivirus, security monitoring</td>
</tr>
<tr>
<td>Signage</td>
<td>Group policies</td>
</tr>
<tr>
<td>Safe for valuables</td>
<td>Network segmentation, encryption</td>
</tr>
<tr>
<td>Dog</td>
<td>Firewall, intrusion detection system, network alarms</td>
</tr>
<tr>
<td>Video cameras</td>
<td>Security incident &amp; event monitoring (SIEM)</td>
</tr>
<tr>
<td>Security guard(s)</td>
<td>Security consultants</td>
</tr>
<tr>
<td>Police activity reports</td>
<td>Threat intelligence</td>
</tr>
</tbody>
</table>
Interactive Exercise – People/Policy

<table>
<thead>
<tr>
<th>Your Residence</th>
<th>Your Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual keys</td>
<td>Password management; privileged access; access control policy</td>
</tr>
<tr>
<td>Alarm system code(s)</td>
<td>Role based access; password management</td>
</tr>
<tr>
<td>Stranger danger awareness</td>
<td>Security awareness training</td>
</tr>
<tr>
<td>Check who is at door before opening</td>
<td>Role based access (guest/faculty); awareness training</td>
</tr>
<tr>
<td>Annual fire drill exercises</td>
<td>Phishing exercises, incident response plan</td>
</tr>
</tbody>
</table>
Part 4: Unique Academic Challenges
Unique Academic Challenges

- Balancing functionality and security
- Protecting data while not inhibiting the learning process
  - Segment network and data storage
  - Security awareness training tailored to the user audience
  - Tailor security policies and applications to environment
- Providing faculty with the technology they need to support the learning experience
  - Cross-functional vetting process for new applications
  - Formal communication process to organization
- High # of visitors and guests who may require access to your network
  - Segment network and create separate production and guest networks
Unique Academic Challenges

- Limited budgets and minimal IT staff
  - Use assessments to identify highest value actions to protect data
  - Leverage cost effective external services such as security monitoring

- Policies need to accommodate the open learning environment
  - Develop a cross-functional vetting process for new applications and systems

- High usage of social media by students
  - Provide frequent social media awareness training and information

- Majority of mobile devices are personally owned
  - Establish minimum security settings for mobile devices
Part 5: How Can I Protect My School’s Data?
Information Security Ecosystem

- Disaster Recovery
- Threat Intelligence
- Project Management
- Employee Training
- IT Security Assessment
- Technology
- Data Management
- Business Continuity
- Supply Chain Management
- Enterprise Risk Management
- Remote Security Monitoring
- Crisis Management
- Insurance
- Data Breach/Privacy Insurance
- Policies and Procedures
- Cyber Security Ecosystem
- Compliance/Validation
- Penetration Testing
- Intrusion Detection
- Threat Assessment and Mitigation
- Information Assurance
- Policy Analysis
Defense in Depth

- Policies, Procedures, & Awareness
- Physical
- Perimeter
- Internal Network
- Computer (Host)
- Application
- Data
Three Pillars of Cyber Security

1. People
   A. **Every** member of an organization has a role
   B. Humans are the weakest link

2. Policies and procedures
   A. Organization specific rules and guidelines
   B. Absence of official guidance forces students, faculty and administration to “guess” at the organization’s position

3. Technology
   A. Should support the organization’s policies
   B. Provide defense in depth (segmentation, firewalls, access control, anti-virus, etc.)
How Do I Do This?

The “right” solution is unique to each organization
- Take a building block approach

Start with the basics and build from there
- Objective IT security assessments and data classification are key to developing the right roadmap

Initially focus on:
- Cataloging your data
- Conducting an IT security audit and assessment
- Leveraging existing technology
- Educating your organization
- Security monitoring
- Incident response planning
Best Practices

People and Processes

▫ Adopt policies that formally communicate how the institution stores, works with, transmits, and destroys sensitive data
▫ Perform annual policy review to address new technologies
▫ Make Students and Faculty an integral part of the information security program
▫ Develop a crisis management strategy and define roles
  ▫ Start simple and build from there
▫ Incorporate security related education into daily life
  ▫ Newsletters, fun fact at staff meetings, etc.
  ▫ Include in parent and alumni correspondence
▫ Provide students and parents with tips for safe browsing and social media at home
Best Practices

**Technology**
- Design and implement a segmented network
- Do not charge mobile devices via laptop and USB
- Perform an annual independent IT security assessment
- Limit employee use of public Wi-Fi when accessing school data
- Examine the use of cloud storage for highly sensitive data
- Continuously monitor all inbound/outbound traffic on all networks
- Continuously update software to close potential vulnerabilities
- Encrypt portable devices (laptops, smartphones, USB)
- Ensure that shared resources such as wireless printers are secure
- Use two-factor authentication on privileged accounts
- Minimize 3rd party access to sensitive data and network assets (Ex. HVAC vendor)
Potential Pitfalls

- Applicable data breach notification law(s) tied to residency
- Use of mobile device as an access point to bypass company filters on work computer
- Assuming that in-house IT personnel have security expertise
- Cyber insurance exclusions (ex. mobile device encryption)
- Single, shared admin usernames and passwords
- Lack of system monitoring and logging
  - Bad actors are working 24x7x365
  - Makes forensic analysis more difficult and expensive
- Cloud storage contracts terms of use and privacy policy
- Inappropriate application permission requests
  - Ex. keyboard app that requested to record every key stroke
Key Takeaways

- Data breaches can happen to organizations of all sizes and industries
- Most organizations have been breached and don’t know it
- Organizations need to perform regular assessments
- An organization’s security posture can be improved with some simple and cost effective measures
- Breaches will occur and the focus should be on minimizing the damage
- Be proactive!
Contact Information

Robert (Bob) Olsen

Chief Executive Officer, MBA, MS, CISSP

rolsen@tnsgllc.com

410-340-3560

LinkedIn: @rolsen3

Twitter: @rlolsen3
Reference Sources

- Verizon 2015 Data Breach Report
- Secunia 2015 Vulnerability Review
- (ISC)$^2$ [www.isc2.org]