INFORMATION SECURITY

Presentation to the Institutional Research and Planning Committee

David A. Bowers

March 15, 2016

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

WHAT IS INFORMATION SECURITY ?

*Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability**

*Source: “Glossary of Key Information Security Terms”, NIST IR 7298

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

EDUCAUSE
TOP 10 IT ISSUES OF 2016

Number 1 = **Information Security***

Developing a holistic, agile approach to information security to create a secure network, develop security policies, and reduce institutional exposure to information security threats

**Source: "Top 10 IT Issues for 2016: Divest, Reinvest and Differentiate", Educause Review, January/February 2016*

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

SUNY SYSTEM HIGH RISK AREAS

Number 1 = **Information Security***

*As reported to SUBOA in February 2016 by SUNY ERMP Manager and University Controller

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

DATA BREACH TOTALS IN 2015

- From January – December 2015, a total of 781 breaches were reported affecting 169,068,506 records
  - *Medical/Healthcare and Education combined accounted for 42.9% of the total breaches and 67.1% of the total number of records affected**

NOTE: These are only the data breaches reported

*Source: Identity Theft Resource Center (ITRC) Data Breach Reports

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

TOP INFORMATION SECURITY DATA BREACHES – 2015

- Anthem
  - Personal information about more than 80 million people, from Social Security numbers to birth dates and addresses
- Premera BlueCross BlueShield
  - Names, dates of birth, addresses, telephone numbers, email addresses, Social Security numbers, member identification numbers, medical claims information and financial information for 11 million customers
- Vtech
  - 4.8 million records, as well as a database of first names, genders and birthdays of more than 200,000 kids

TOP INFORMATION SECURITY DATA BREACHES – 2015

- UCLA Health
  - 4.5 million records, including Social Security numbers and medical data
- Experian/T-Mobile
  - 15 million people's records
- Ashley Madison
  - 37 million clientele records
- U.S. Office of Personnel Management
  - Personnel records on 21-25 million current and former federal employees

TOP INFORMATION SECURITY DATA BREACHES – 2015

- Internal Revenue Service
  - Using personal information gained from third-party sources to circumvent authentication protections, hackers breached as many as 724,000 accounts (updated in Feb 2016; IRS originally reported 100,000 in May 2015) of taxpayers who had used the IRS's "Get Transcript" application
- Hollywood Presbyterian Medical Center (2016)
  - A *ransomware* program (malware that encrypts the data stored on infected machines) shut down the entire hospital's computer systems for more than a week until the hospital finally agreed to pay its attackers 40 bitcoins (currently worth about $17,000)

COSTS OF A DATA BREACH

- Average total cost of a breach is $3.8 million*
  - 23% increase since 2013
- Average cost per record breached is $154*
  - 12% increase in per capita cost since 2013

*Source: “2015 Cost of Data Breach Study: Global Analysis”, IBM

COSTS OF A DATA BREACH

BUT…

COSTS OF A DATA BREACH

- Average cost per record breached for healthcare organizations is $363*
- Average cost per record breached in education is $300*

*Source: “2015 Cost of Data Breach Study: Global Analysis”, IBM

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

COSTS OF A DATA BREACH

In addition to a potentially devastating financial cost is……

- **Reputational Cost**
  - This is a loss that may never be fully recovered by the impacted organization.

"If you lose money for the firm, I will be understanding. If you lose reputation, I will be ruthless." - Warren Buffet

WHO IS RESPONSIBLE FOR INFORMATION SECURITY?

- Everyone who uses a computer needs to know how to keep his or her computer and data secure to ensure a safe working environment, and
- Everyone who accesses the College/UEC information assets, whether electronic or on paper.

INFORMATION SECURITY IS EVERYONE'S RESPONSIBILITY!

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

INFORMATION SECURITY – LAWS AND REGULATIONS

- Relevant Laws, Guidelines, Regulations and Policies
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Family Educational Rights and Privacy Act (FERPA)
  - Gramm-Leach-Bliley Act (GLB-Act)
  - Red Flag Rules (Identity Theft)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Cybersecurity Information Sharing Act

INFORMATION SECURITY – LAWS AND REGULATIONS

- Relevant Laws, Guidelines, Regulations and Policies
  - NYS Information Security Breach and Notification Act
  - NYS Personal Privacy Protection Law
  - NYS Freedom of Information Act (FOIL)
  - New York State Governmental Accountability, Audit and Internal Control Act
  - NYS Business and Technology Law
  - NYS Information Security Policy
  - NYS Disposal of Personal Records Law
  - SUNY Information Security Guidelines (6608)

WHAT'S HAPPENING HERE?

Sentinel Intrusion Prevention/Detection System

Time period: January 1 to March 1, 2016

Total Alerts: 82,122

Severity Levels:

Level 1 – 34,434 (scans/probes)

Level 2 – 44,237 (information gathering)

Level 3 - 3,451 (targeted attacks)

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

- SUNY Information Security Guidelines, Document # 6608, February 1, 2008
  A. Establish Program Organization
  B. Declare Campus Policy and Standards
  C. Create and Maintain Risk-Oriented Inventories
  D. Conduct Analysis of Risk, Practices and Protections
  E. Improve and Maintain Practices and Protections

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

A. Establish Program Organization
   - Responsible, Authorized Experts
   - Executive Oversight
   - Comprehensive Scope
   - Documentation and Compliance Reporting

B. Declare Campus Policy and Standards
   - Declaration of Sensitivity Categories
   - Campus Policy and Standards

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

C. Create and Maintain Risk-Oriented Inventories
- Asset Inventory
- Workforce Inventory

D. Conduct Analysis of Risk, Practices and Protections
- Risk Analysis
- Analysis of Practices and Protections

E. Improve and Maintain Practices and Protections
- Improved Practices and Protections
- Learning
- Readiness

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

A. Establish Program Organization

- "Tone at the Top"
  - President Heath signs Information Security Program Authorization
- Governance
  - Senior Executive
  - Information Security Officer
  - Information Security Committee
- Information Security Program
  - Including Risk Management and Confidentiality Agreement

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

B. Declare Campus Policy and Standards

- Information Security Policies and Procedures
  - Institutional Issues Computing Policy
  - Acceptable Use Policy: Public Access Facilities and E-Mail
  - Information Security Policy
  - Data/Information Confidentiality, Security and Integrity Policy
  - Internet Privacy Policy
  - Information Security Breach And Notification Procedures
  - Password Policy
  - Disposal Of Computer Equipment Procedures
  - Electronic Media Sanitization Policy
- UEC Policies and Procedures related to HIPAA/Information Security
- Other campus policies related to Information Security

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

C. Create and Maintain Risk-Oriented Inventories

- Asset Inventory
  - Information system assets that contain Protected Identifiable Information (PII)
  - Including SSN, credit card numbers, and other sensitive and private information
- Workforce Inventory
  - Users authorized to have access to information system assets containing PII
  - Information access restrictions in accordance with access control policies

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

D. Conduct Analysis of Risk, Practices and Protections

- SAQ: IT Security Controls and Security Management
- SUNY Information Security Audits conducted in 2008 and 2013 (Overall and HIPAA)
- Information security tools to protect the network and end-point devices, including:
  - Strong password complexity requirements
  - Intrusion Prevention/Detection System (IPS/IDS)
  - Firewall
  - Anti-virus
  - Anti-SPAM

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

E. Improve and Maintain Practices and Protections

- Information Security Awareness Education and Training
  - For students, faculty and staff
  - Comprehensive
  - Provides tips and best practices to minimize risk
- Incident Response Team
  - Assess, detect, respond and recover from information security incidents
  - Includes IT, Legal, Public Relations, Law Enforcement and others as needed

CURRENT INFORMATION SECURITY TOOLS/STRATEGIES

- Participation in the SUNY Security Operations Center (SOC)

  Base Membership service offering includes:

  - Vulnerability Scanning (Nexpose or Trustwave)
  - Penetration Testing (Metasploit)
  - Outline/Template for Annual Information Awareness Training
  - Development of and Assistance with Campus Information Security Self-Assessments (SUNY SAQ, PCI, etc.)

  Future a-la-carte services may include:

  - Information Security As A Service
  - Third Party Risk Assessment
  - Campus Breach Simulation Exercise

WHAT'S NEXT IN INFORMATION SECURITY PLANNING

- Enterprise Risk Management Program (SUNY)
- Cybersecurity Breach Insurance
- Expand information security awareness education and training
- Consider SUNY SOC a-la-carte offerings
- Whole Disk Encryption for portable devices
- Continue to assess/review/recommend next-generation information security tools and technologies to respond to evolving threats

Questions

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

Information Security

- Background Information…..

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

- Created in 1996, HIPAA protects the privacy and security of Protected Health Information (PHI)
- Gives patients more control over their health records
- Sets limits on the accessibility and disclosure of patient health information
- Includes breach notification rules

FAMILY EDUCATION RIGHTS AND PRIVACY ACT (FERPA)

- AKA The Buckley Amendment
- Created in 1974, FERPA protects the confidentiality of student educational records and governs
  - the release of educational records maintained by the university, and
  - access to these records

GRAMM-LEACH-BLILEY ACT (GLB-ACT)/RED FLAGS RULES

- AKA The Financial Modernization Act of 1999
- Created in 1999, The GLB-Act protects the security and confidentiality of a consumer's personal financial records held by financial institutions
- GLB-Act include the Safeguards Rule: financial institutions must implement security programs
- Red Flags Rules requires organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

- Formed in 2004, PCI DSS defines controls around use of cardholder data to reduce credit card fraud via its exposure
- Requires the following:
  - Build and maintain a secure network
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

INFORMATION SECURITY – POTENTIAL THREATS

- Malicious Software (viruses, worms, trojan horses, spyware or other malicious code)
- SPAM/SPIM
- Social Engineering
- Phishing
- Pharming
- Identity Theft
- Physical Threats

POTENTIAL THREATS - MALICIOUS SOFTWARE

Malicious software (also known as malware) is a serious threat. These are programs that can "infect" other programs, damage hard drives, erase critical information, take critical systems off-line, and forward your data to external sites without your knowledge.

Malware includes:

- Viruses
- Worms
- Trojan Horse programs
- Spyware
- Programs which accidentally harm any system or data

POTENTIAL THREATS – SIGNS OF MALWARE

- Unusual items appearing on the screen (graphics, odd messages or system error messages)
- Corrupted or inaccessible program or data files
- Programs taking longer to start up, running more slowly than usual or not running at all
- Increased number of pop-up advertisements
- Changed system settings that can't be changed back to the way they were
- Web browser contains additional components that you don't remember downloading

If you suspect your computer has malware, stop using your computer and contact the IT Help Desk - x5730 immediately

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

POTENTIAL THREATS – SPAM/SPIM

- SPAM
  - Junk email
- SPIM - SPAM in Instant Messaging
  - Uncontrolled viewing (pop-up windows)
  - Bot generated (software that runs automated tasks over the Internet)

If you suspect your received SPAM or SPIM, contact the IT Help Desk - x5730 or *helpdesk@sunyopt.edu* immediately

POTENTIAL THREATS – SOCIAL ENGINEERING

Social Engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud or access computer systems.

- Non-technical or low-technology means, such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems
- Can occur in-person, over the phone, in emails or fake web pages

POTENTIAL THREATS – PHISHING

A type of Social Engineering. The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

- 'Trustworthy entity' asks via e-mail for sensitive information such as SSN, credit card numbers, login IDs or passwords.

POTENTIAL THREATS – PHARMING

Another type of Social Engineering. A user's session is redirected to a masquerading website. At the fake website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real site and conduct transactions using the credentials of a valid user on that website.

- The link provided in the e-mail leads to a fake webpage which collects important information and submits it to the owner
- The fake web page looks like the real thing

POTENTIAL THREATS – IDENTITY THEFT

Identity theft is the unauthorized collection and use of your personal information for criminal purposes. This information can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, and even secure employment. If this happens, you could be left with the bills, charges, bad checks, and taxes.

POTENTIAL THREATS – SIGNS OF IDENTITY THEFT

- Unexplained bank statements, charges on phone, credit cards or other consumer accounts
- Being denied a loan you qualify for
- Unexplained changes in your bank access codes
- Missing credit card bills or other mail
- Unusual calls regarding your personal or financial information

POTENTIAL THREATS – IDENTITY THEFT: WHAT TO DO

If you suspect that you may be a victim of Identity Theft, you should immediate take the following steps:

- Place an initial fraud alert to each of the credit bureaus
- Order Credit Reports (initiating an initial fraud alert entitles you to a free credit report from each of the credit bureaus)
- Create an Identity Theft Report to deal with credit reporting companies, debt collectors and businesses that opened accounts in your name

INFORMATION SECURITY – EMERGING THREATS

- Wireless
- Portable Devices

STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY

EMERGING THREATS – WIRELESS

- Common Attacks
  - Wired Equivalent Privacy (WEP) cracking
  - Sniffing (software/hardware that can intercept and log traffic passing over a network)
  - Fake wireless access points
- Best Practices
  - Use Wi-Fi Protected Access (WPA/WPA2) wireless encryption protocol
  - Use Virtual Private Network (VPN) where applicable

EMERGING THREATS – PORTABLE DEVICES

- Includes phones, laptops, tablets, portable/flash drives
- Common Concerns
  - Easy to lose, easy to steal
  - Sometimes carry confidential information
  - Usually very valuable; the physical device and the information being stored
- Best Practices
  - Always keep within sight, or lock away when not in use
  - Use strong passwords
  - Require the device to lock after a period of inactivity
  - Use encryption
  - Always cleanly wipe portable devices before disposal

INFORMATION SECURITY – PHYSICAL SECURITY THREATS

- Theft
  - Documents
  - Backup tapes
  - Money
  - Equipment
  - Resources
- Dumpster Diving
- Piggybacking/Tailgating
- Shoulder Surfing

PHYSICAL SECURITY THREATS – ONE MAN'S TRASH…

Dumpster diving is the act of sorting through garbage to find documents and information that has been improperly discarded, including:

- Customer information
- Internal records/reports
- Memorandums
- Applications

PHYSICAL SECURITY THREATS – PIGGYBACKING/TAILGATING

Piggybacking or *tailgating* occurs when one user follows closely behind another user without using valid credentials, i.e. using smart cards or proximity cards to gain access to secure areas. Ideally each person would use his/her access card and the door would close behind them. When piggybacking, when that one person uses his/her card, others follow behind without using their access card.

PHYSICAL SECURITY THREATS – SHOULDER SURFING

Shoulder surfing refers to the act of obtaining personal or private information through direct observation. Shoulder surfing involves looking over a person's shoulder to gather pertinent information while the victim is oblivious. This is especially effective in crowded places where a person uses a computer, smartphone or ATM. Binoculars, video cameras and vision-enhancing devices also are used, depending on location and situation.

INFORMATION SECURITY BEST PRACTICES - PASSWORDS

- Passwords
  - Never share your password with anyone
  - Don’t write your password down and store them
  - Don’t reveal your password in an email message
  - Don’t use simple dictionary words
    - including family name, sports name or pet name
  - Don’t use a sequence of letters and numbers
    - i.e., 123456, abcdef, 111111

INFORMATION SECURITY BEST PRACTICES - PASSWORDS

- Recommendation – Utilize strong password attributes
  - use phrases or misspelled words with embedded numbers and special characters
  - minimum 8 characters, at least one capitalized, one number, one special character (i.e., ^!$@(?>, etc.)

Sample Passwords - Business – Biz!ne2z
Thank God Its Friday - Tg1Fr!da
New York Giants - nYJ1@nTz

INFORMATION SECURITY BEST PRACTICES – MISC.

- Lock (Ctrl-Alt-Del) or log off your computer when leaving your work area
- Don’t leave any files unattended that may contain confidential information
  - Lock information in filing cabinets
  - Clean desk policy
- Maintain current software and updates

INFORMATION SECURITY BEST PRACTICES – MISC. (cont.)

- Dispose of all confidential paper data properly
  - Place in provided shred bins for disposal
  - Shred it yourself if you have access to a personal shredder
  - Cross-cut only – Straight-cut is easy to re-assemble
- Frequently backup important files
- Report suspicious activity or persons immediately

INFORMATION SECURITY BEST PRACTICES – MISC. (cont.)

- Use of strong passwords
- Beware of unknown email, attachments and untrusted links
- Use security software
  - anti-virus, firewall, anti-spyware
- Protect any and all sensitive information that you handle, including your own