CACUBO Higher Education Accounting Workshop
Top 10 Cyber Security Issues for Higher Education Business Managers

May 2017
“Phun with Phishing”
### Breach Report(s)

<table>
<thead>
<tr>
<th>Category</th>
<th>Breaches</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking/Financial</td>
<td>43</td>
<td>71,912</td>
</tr>
<tr>
<td>Business</td>
<td>432</td>
<td>5,649,046</td>
</tr>
<tr>
<td>Educational</td>
<td>84</td>
<td>1,015,813</td>
</tr>
<tr>
<td>Government/Military</td>
<td>66</td>
<td>13,070,531</td>
</tr>
<tr>
<td>Medical/Healthcare</td>
<td>355</td>
<td>15,426,015</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td><strong>980</strong></td>
<td><strong>35,233,317</strong></td>
</tr>
</tbody>
</table>

*Identity Theft Resource Center (ITRC)*

2016 Data Breach Category Summary (12/31/2016)
Agenda – Top Security Issues for Business Managers

- Cyber Threats & Attackers
- Compliance
- Risk Management
- Security Framework
- Actions
Cyber Threats & Actors
“Big 3” Cyber Threats Now

“Security Hygiene”
- Assess
- Design
- Operate
- Implement

Third Parties

People
High Profile Breaches from the “Big 3”

- Fraud & Extortion
- Intelligence Gathering
- Massively Successful

City of El Paso duped out of $3.3 million in phishing scam

By: Brenda De Anda-Swann

City of El Paso duped out of $3.3 million in phishing scam

IRS, States and Tax Industry Renew Alert about Form W-2 Scam Targeting Payroll, Human Resource Departments

WASHINGTON – The Internal Revenue Service, state tax agencies and the tax industry today renewed their warning about an email scam that uses a corporate officer’s name to request employee Forms W-2 from company payroll or human resources departments.

This week, the IRS already has received new notifications that the email scam is making its way across the nation for a second time. The IRS urges company payroll officials to double check any executive-level or unusual requests for lists of Forms W-2 or Social Security number.

The W-2 scam first appeared last year. Cybercriminals tricked payroll and human resource officials into disclosing employee names, SSNs and income information. The thieves then attempted to file fraudulent tax returns for tax refunds.
# Cyber Actors, Means & Motivation

<table>
<thead>
<tr>
<th>Actor</th>
<th>Means</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional</td>
<td>Technical</td>
<td>Challenge &amp; Fame</td>
</tr>
<tr>
<td>Security Researchers</td>
<td>Technical</td>
<td>Reputation</td>
</tr>
<tr>
<td>Activists/Hacktavists</td>
<td>Social and Technical</td>
<td>Discredit / Expose Target</td>
</tr>
<tr>
<td>Criminals</td>
<td><strong>Social and Technical</strong></td>
<td>$$$$</td>
</tr>
<tr>
<td>Terrorists</td>
<td>Technical</td>
<td>Damage / Disrupt Target</td>
</tr>
<tr>
<td>Nation States</td>
<td>Social and Technical</td>
<td>I.P. and Intelligence</td>
</tr>
<tr>
<td>Insiders</td>
<td>Privileged Access</td>
<td>$$$$ or Exposure</td>
</tr>
</tbody>
</table>
Cyber Attacks – Path of Attack

- Services in the Cloud
- Customers / Clients
- 3rd Parties
- Employees
- Web App
- Firewall
- Remote Access
Cyber Attacks – Anatomy of a Breach

- Discovery
- Capture
- Internal Attacks
- Exfiltration

Web App
Firewall
Remote Access
Cyber Compliance
Compliance

- Student Information Protection (FERPA)
- Credit Cards (PCI DSS)
- Healthcare Information (HIPAA)
- Student Financial Information (GLBA)
- Others (DFARS, export control, etc.)
High awareness of FERPA requirements

Good controls for protecting information

Greatest threat is from the “Big 3”

Additional considerations:
- Data Flow (especially non-application storage)
- Application Security
Compliance – Credit Cards (PCI DSS)

- Large variations in handling compliance
- Multiple Self Assessment Questionnaires?
- Confusing, Technical, Detailed, and Vague
- Additional considerations:
  - Coordinated Program Approach
  - Negotiate with your Bank
Compliance – Healthcare Information

- Understand Who/Where/How
- Healthcare services vs. Healthcare data
- Encryption?
- Additional considerations:
  - Data Flow Analysis
  - Segmentation & Restriction
Compliance – Student Financial Aid Information

- Gramm-Leach-Bliley Act (GLBA)
- Annual Risk Assessment
- Vendor Risk Assessments
- Additional considerations:
  - NIST SP 800-171
  - EDUCAUSE HEISC Tool (modified) approach
Compliance – But wait, there’s more!

- Defense Finance Acquisition Regulation Supplement (DFARS)
- Export Controls
- Breach Laws
- General Data Protection Regulation (GDPR)
- And....
Risk Management
Risk Management

- Risk Assessments: Annual + Changes
- Insurance: Cyber Security
- Insurance: Appropriate for Institution
- Additional Considerations:
  - Regular Reports and Updates
  - Spot / Detailed Assessments for High Risk Areas
What Can We Do?
What can we do?!?

- Understand Our Environment
  - Strengths & Limitations

- Design Better Security
  - Requirements, Resources

- Address Key Areas
  - Top 10 Areas to Address
  - To Cover Risk Areas

*Mantra: Prevent what you can, Detect what you cannot and Prepare for the worst*
Perform Risk Assessments

- Risk Assessments
  - Annual
  - As part of any major changes
  - Use NIST 800 series as a guide (NIST SP 800-171)

- New Solutions & Vendors
  - Software/Hardware Products
  - Vendors
  - Pre-implementation and Annual
Understand Our Environment – Risk
What we can do – Security Hygiene

- Security Risk Assessments
- Vulnerability Testing
- Penetration Testing
- Application Testing
- Security Hardening
- Security Patch Updates
- Processes
Design Better Security

Drivers & Requirements
▪ Confidentiality
▪ Integrity
▪ Availability

Assess

Resources & Capabilities
▪ People
▪ Process
▪ Technology

Cyber Security Program

GOVERNANCE & POLICIES

CYBER SECURITY FUNCTIONS

ASSESS
- Risk Assessments
- New Solutions
- Vulnerability Management
- Compliance

PROTECT
- Network
- Systems
- Applications
- People

DETECT
- Threats
- Attacks
- Incidents
- Breach

TRAIN
- Awareness
- Compliance
- Technical
- Executive

MONITOR

RESPOND & RECOVER

INDEPENDENT ASSESSMENTS & REPORTING

CYBERSECURITY INSURANCE
What we can do – Vet your Third Parties
YOU ARE A TARGET

Username & Passwords
Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:
- Your bank or financial accounts, where they can steal or transfer your money.
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.
- Your Amazon, Walmart, or other online shopping accounts where they can purchase goods in your name.
- Your UPS or FedEx accounts, where they ship stolen goods in your name.

Email Harvesting
Once hacked, cyber criminals can read your email for information they can sell to others, such as:
- All the names, email addresses and phone numbers from your contact list.
- All of your personal or work email.

Virtual Goods
Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:
- Your online gaming characters, gaming goods or gaming currencies.
- Any software licenses, operating system license keys, or gaming licenses.

Botnet
Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:
- Sending out spam to millions of people.
- Launching Denial of Service attacks.

Identity Hijacking
Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:
- Your Facebook, Twitter or LinkedIn account.
- Your email accounts.
- Your Skype or other IM accounts.

Web Server
Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:
- Hosting phishing websites to steal other people’s usernames and passwords.
- Hosting attacking tools that will hack people’s computers.
- Distributing child pornography, pirated videos or stolen music.

Financial
Once hacked, cyber criminals can scan your system looking for valuable information, such as:
- Your credit card information.
- Your tax records and past filings.
- Your financial investments and retirement plans.

Extortion
Once hacked, cyber criminals can take over your computer and demand money. They do this by:
- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.
- Encrypting all the data on your computer and demanding payment to decrypt it.
- Tracking all websites you visit and threatening to publish them.

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com
What we can do – People

- **Training** – **DON’T CLICK!**

  ![Stop.Think.Connect.](image)

- **Culture** – Reporting & Response

  I *may* have clicked on something....

- **Technical Controls** – designed in to the process

  Use the capabilities included in your technology.

- **Internal Controls** – use your people & processes

  Processes designed to support proper controls and approvals.
Key Take-Aways & Action Items

- Get started!
- Perform a cyber risk assessment
  - What sensitive/protected data is in the environment?
  - Where is it transmitted, processed and stored (data flow)?
  - Who has access to the data?
  - What improvements do we need to make?
  - What are my compliance requirements?
- Vendor Risk Management
- Cyber Security Insurance?
Questions

Rob Rudloff, CISSP-ISSMP, PMP
303.590.8770
rob.rudloff@rubinbrown.com

Brent Stevens, CPA
314.290.3428
brent.stevens@rubinbrown.com