Managing Cyber Risk in Higher Education

Gerry Kane – Cybersecurity Segment Director, Schaumburg, IL USA

Midwestern Higher Education Compact - 20th Annual Master Property Program Loss Control Workshop

March 8, 2018
Managing Cyber Risk in Higher Education

Agenda

- Setting the Stage
- Higher Education as a Target
- Cyber Risk Management Strategy
- Key Takeaways
- Q&A
Setting the Stage

Definitions

• **Cyber** – Having to do with a computer or computing system

• **Threat** – Any circumstance or event with the potential to cause harm to an information system.
  • **Threat Actor** – Bad guy
  • **Threat Vector** – Modus Operandi

• **Vulnerability** - Any condition that creates susceptibility of the information system to a threat

• **Exploit** - The successful execution of a threat via a present vulnerability.

• **Risk** - A relative measure based on the likelihood of an exploit (combination of threat and vulnerability) and the resulting impact of that adverse event on the organization.
## Breach History – All Industries

<table>
<thead>
<tr>
<th>Year</th>
<th>Records</th>
<th>Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>55,101,241</td>
<td>136</td>
</tr>
<tr>
<td>2006</td>
<td>68,580,749</td>
<td>482</td>
</tr>
<tr>
<td>2007</td>
<td>140,683,184</td>
<td>453</td>
</tr>
<tr>
<td>2008</td>
<td>130,782,100</td>
<td>355</td>
</tr>
<tr>
<td>2009</td>
<td>251,576,624</td>
<td>271</td>
</tr>
<tr>
<td>2010</td>
<td>140,920,913</td>
<td>802</td>
</tr>
<tr>
<td>2011</td>
<td>447,910,188</td>
<td>789</td>
</tr>
<tr>
<td>2012</td>
<td>298,559,924</td>
<td>882</td>
</tr>
<tr>
<td>2013</td>
<td>155,398,160</td>
<td>852</td>
</tr>
<tr>
<td>2014</td>
<td>1,308,560,110</td>
<td>878</td>
</tr>
<tr>
<td>2015</td>
<td>510,284,542</td>
<td>542</td>
</tr>
<tr>
<td>2016</td>
<td>4,619,627,058</td>
<td>812</td>
</tr>
<tr>
<td>2017</td>
<td>1,931,414,997</td>
<td>572</td>
</tr>
<tr>
<td></td>
<td>10,059,399,790</td>
<td>7,826</td>
</tr>
</tbody>
</table>

Source: www.privacyrights.org
## Breach History – All Industries

<table>
<thead>
<tr>
<th>Type</th>
<th>Industry</th>
<th>Records</th>
<th>Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSR</td>
<td>Retail/Merchant</td>
<td>483,239,922</td>
<td>559</td>
</tr>
<tr>
<td>BSF</td>
<td>Financial/Insurance</td>
<td>632,997,191</td>
<td>712</td>
</tr>
<tr>
<td>GOV</td>
<td>Gov't/Military</td>
<td>227,109,668</td>
<td>765</td>
</tr>
<tr>
<td>MED</td>
<td>Healthcare</td>
<td>227,352,060</td>
<td>3857</td>
</tr>
<tr>
<td>BSO</td>
<td>Business-Other</td>
<td>8,458,712,051</td>
<td>1018</td>
</tr>
<tr>
<td>EDU</td>
<td>Educational</td>
<td>25,078,033</td>
<td>803</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Profit</td>
<td>4,910,865</td>
<td>112</td>
</tr>
</tbody>
</table>

|               |                  | 10,059,399,790 | 7826    |

Source: www.privacyrights.org
Breach History – Education

Source: www.privacyrights.org
## Breach History – Education

It isn’t only about PII theft

<table>
<thead>
<tr>
<th>Frequency</th>
<th>455 incidents, 73 with confirmed data disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 3 Patterns</td>
<td><strong>Cyber Espionage</strong>, Miscellaneous Errors and Everything Else represent 67% of all data breaches within Education</td>
</tr>
<tr>
<td>Threat Actors</td>
<td>71% External, 30% Internal, 3% Partner</td>
</tr>
<tr>
<td>Actor Motives</td>
<td>45% Financial, 43% Espionage, 9% Fun</td>
</tr>
<tr>
<td>Data Compromised</td>
<td>56% Personal, 27% Secrets, 8% Credentials</td>
</tr>
<tr>
<td>Summary</td>
<td>This section will focus on confirmed data breaches, but <em>Education remains a consistent target of Denial of Service (DoS) attacks also</em>. 2016 results reflect a substantial increase in the number of espionage-related breaches.</td>
</tr>
</tbody>
</table>

A Practical Cyber Risk Management Framework

- Based on the NIST* “Framework for Improving Critical Infrastructure Cybersecurity”
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

*NIST – National Institute of Standards and Technology (US)
A Practical Cyber Risk Management Framework
The NIST* Cybersecurity Framework (CSF)

- **IDENTIFY** - *Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.*

*What needs to be protected?*

- Is there an Information Asset Inventory
  - Data, classified
  - Business Processes
  - Hardware
  - Software
  - Operating Systems
    - Versions
    - Patch Levels
- Has risk assessment been done for each asset or class of assets?
- Is there appropriate governance

*National Institute of Standards and Technology*
A Practical Cyber Risk Management Framework
The NIST* Cybersecurity Framework (CSF)

- **PROTECT** – *Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.*

_How are the identified assets protected?_

- **At the Network Perimeter**
  - Firewalls
  - Intrusion detection/prevention
- **At the Endpoints**
  - Hardened, standard configurations
  - Controlled local admin access
  - Full disk encryption for mobile devices
  - Application whitelisting
  - Segmentation
Simple Enterprise Network

Internet

Firewall

DMZ

email

Web apps

Router

Switch

Servers

INTERNAL USE ONLY
Enterprise Network with Segmentation

Internet

DMZ
- Email
- Web apps

Secure Segment

Router

Switch

IDS/IPS

Internet

Switch
PROTECT (continued)

- Protect the data
  - Eliminate it
  - Encrypt it
    - At rest
    - In transit
  - On backups
  - On removable devices
- Restrict access to it
  - User access
  - Privileged access
  - Third party access
  - Require strong, multifactor authentication
- Educate the users
A Practical Cyber Risk Management Framework
The NIST* Cybersecurity Framework (CSF)

- **DETECT** — *Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.*

How are security events discovered?
A Practical Cyber Risk Management Framework
The NIST* Cybersecurity Framework (CSF)

- **RESPOND** - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

When monitoring indicates a problem, are we prepared to respond?

- Document a plan
  - Assign roles and responsibilities
  - Include all levels
  - Have “Playbooks”
  - Have arrangements with breach service providers
  - Practice, practice, practice
A Practical Cyber Risk Management Framework
The NIST* Cybersecurity Framework (CSF)

• **RECOVER** - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

If systems are damaged or unavailable, are there alternative arrangements to keep the business operating?

– Document plans for Disaster Recovery and Business Continuity
  – Prioritize systems and applications
  – Have Recovery Time Objectives
  – Have Recovery Point Objectives
  – Have Alternate Datacenter Facilities
  – Have Manual Workarounds
  – Practice, Practice, Practice
Key Take-Aways

• The Basics
  – Identify
  – Protect
  – Detect
  – Respond
  – Recover

• The “Musts”
  – Know your information assets (asset inventory)
  – Segmentation (isolation)
  – Encryption!
  – Strong Authentication
    – For privileged users
    – For remote users
    – For connected devices
  – Monitoring - Prevention is ideal, but detection is a must
  – Be Prepared, Be Resilient
The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute advice (particularly not legal advice). Accordingly, persons requiring advice should consult independent advisors when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. We undertake no obligation to publicly update or revise any of this information, whether to reflect new information, future developments, events or circumstances or otherwise. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.

©2018 Zurich American Insurance Company