Cyber Security – Case Studies

- Ransomware – Hospitals and Health Care Agencies
- Higher Education – Research, Financial, Personal
- Phishing – W2 breaches
- Financial Trojans (banking, credit cards)
St. Joseph's Healthcare System falls victim to phishing scam

More than 5,000 employees of St. Joseph's Healthcare System facilities in Paterson, Wayne and Cedar Grove may be victims of identity theft as the result of a sophisticated email phishing scheme.

On February 2, 2015, staff at Holy Name Medical Center discovered that personal data was compromised by an email phishing attack. The attackers sent emails that appeared to be legitimate internal communications to Holy Name's employees and clinic staff, urging them to click on a link and enter their user name and password. The email contained a legitimate user name and password, but no further directions. The attackers used access to the email to gain access to the email address book for internal communications, which is a common technique for identity theft.

The attack was reported to the Federal Bureau of Investigation (FBI) and the U.S. Secret Service, which are investigating the matter. The company has implemented additional security measures to prevent future attacks. The company's employees have been notified and encouraged to change their passwords and be vigilant for any unusual activity on their accounts.

The company's chief information officer, Karina H. Morris Jr., said the company was working with the FBI and the Secret Service to determine the extent of the damage and to ensure the security of its systems.

The company has also been working with the FBI and the Secret Service to determine the extent of the damage and to ensure the security of its systems.
WASHINGTON (AP) — FBI investigating computer virus causing major outages at large hospital chain MedStar Health.

Hospital Declares ‘Internal State of Emergency’ After Ransomware Infection

A Kentucky hospital says it is operating in an “internal state of emergency” after a ransomware attack paralyzed its networks, encrypting files on computer systems and holding the data on them hostage unless and until the hospital pays up.
Cyberattacks on the rise in higher education

Foreign governments and organized crime targeting institutions’ most sensitive information.

By Matt Zalaznick — University Business, October 2013

The lone-wolf hacker creating nuisance viruses in a basement has been replaced by sophisticated foreign governments and organized crime rings as the top cybersecurity threat to colleges and universities.

Today’s hackers are now being deployed around the clock to steal intellectual property, sensitive research, and personal information, potentially costing colleges and universities millions of dollars and badly damaging their reputations.
FBI: $2.3 Billion Lost to CEO Email Scams

April 16

The U.S. Federal Bureau of Investigation (FBI) this week warned about a "dramatic" increase in so-called "CEO fraud," e-mail scams in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters. FBI estimates these scams have cost organizations more than $2.3 billion in losses over the past three years.

In an alert posted to its site, the FBI said that since January 2015, the agency has seen a 37 percent increase in identified victims and exposed losses from CEO scams. The alert states that law enforcement globally has received complaints from victims in every U.S. state and in at least 79 countries.

Thieves Phish Moneytree Employee Tax Data

March 16

Payday lending firm Moneytree is the latest company to alert current and former employees that their tax data -- including Social Security numbers, salary and address information -- was accidentally handed over directly to scam artists.

Seattle-based Moneytree sent an email to employees on March 4 stating that "one of our team members fell victim to a phishing scam and revealed payroll information to an external source."

"Moneytree was apparently targeted by a scam in which the scammer impersonated me and asked for an email copy of certain information about the Company's payroll including Team Member names, home addresses, social security numbers, birthdates and W2 information," Moneytree co-founder Dennis Bassford wrote to employees.

The message continued:

"Unfortunately, this request was not recognized as a scam, and the information about current and former Team Members who worked in the US at Moneytree in 2015 or were hired in early 2016 was disclosed. The good news is that our servers and security systems were not breached, and our millions of customer records were not affected. The bad news is that our Team Members' information has been compromised."
• UC Cyber Risk Governance
• Actions taken to date and impact
• Current action plan
Charter for the Cyber Risk Governance Committee (CRGC)

- Enhanced governance structure
- Enhanced risk management
- Adoption of modern technology
- Hardened security environment
- System wide culture change
Technical Actions (Current Focus)

- Two Factor Authentication
- Minimum Security Standards
- Scanning Systems
- Network Access Control
Cyber Security – 2016 Actions Taken To-Date

- Proactive removal of phishing attempts – January 16th
- Web Security and Advanced Malware Protection – January 25th (HS)
- Secure (encrypted) Email – March 1st
- Monthly Cyber Security Awareness Alerts – March 15th
- Full Disk Encryption – March 24th (HS)
- Multi-factor Authentication – April 1st
- Data Loss Prevention (DLP) – Requirements gathering (POC for Health targeted for 4/15/2016 start)
## Cyber Security – Actions/Impact

### Cybersecurity Protection Impact

<table>
<thead>
<tr>
<th></th>
<th>Jan-16</th>
<th>Feb-16</th>
<th>Mar-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Bad Content Blocks</td>
<td>2,000</td>
<td>14,700</td>
<td>56,900</td>
</tr>
<tr>
<td>Phishing Messages Proactively Removed</td>
<td>2,358</td>
<td>5,799</td>
<td>9,916</td>
</tr>
<tr>
<td>Bad Executable Blocks</td>
<td>-</td>
<td>139</td>
<td>876</td>
</tr>
<tr>
<td>Encrypted Messages Sent</td>
<td>-</td>
<td>-</td>
<td>1,537</td>
</tr>
</tbody>
</table>
Cyber Security – Actions/Impact

Information Technology Services & Health Systems IT

Number of Bad Content Blocked and Phishing Messages Removed

- No. Messages Removed
- Known Bad Content Block
- Bad Executables Block
- No. Encrypted Messages

Bad ExecutablesBlocked, Encrypted Message Sent

No. Messages Removed | Known Bad Content Block | Bad Executables Block | No. Encrypted Messages
--- | --- | --- | ---
Jan '16 | 2,000 | 2,358 | 0
Feb '16 | 14,700 | 5,799 | 139
Mar '16 | 56,900 | 1,537 | 876

UC San Diego
Cyber Security – Action Plan

- Updated Governance
- Enhanced Risk Management
- Adoption of Modern Technology
- Hardened Security Environment
- System-wide Culture Change
Cyber Security – Governance

• Security Governance Structure
• Security Governance Committee
• Update Security Policies and Standards
Cyber Security – Enhanced Risk Management

• Security Risk Assessment
• Targeted Vulnerability Scanning
Cyber Security – Adoption of Modern Technology

- Efforts within the UC system to standardize on specific technologies, share data and expertise and leverage the purchasing power of the entire system.
- Each location will also have certain efforts that are unique.
<table>
<thead>
<tr>
<th>Action</th>
<th>Scope</th>
<th>Target Date</th>
<th>Status/Notes</th>
<th>Financial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Scanning Systems</td>
<td>Campus &amp; Health Sciences</td>
<td>In place</td>
<td>Ongoing host scanning.</td>
<td>$ - &lt;$50K</td>
</tr>
<tr>
<td>Network Access Control (NAC)</td>
<td>Campus &amp; Health Sciences</td>
<td>In place</td>
<td>Currently ResNet only. Expansion of NAC is very difficult in research environments.</td>
<td>$ - Annual</td>
</tr>
<tr>
<td>Intrusion Detection Systems</td>
<td>Campus &amp; Health Sciences</td>
<td>In place</td>
<td>Ongoing Suricota open source service.</td>
<td>$ - Annual</td>
</tr>
<tr>
<td>Remove known phishing messages from email</td>
<td>Campus &amp; Health Sciences</td>
<td>1/16/2016</td>
<td>Process Implemented by IT Services (ITS)</td>
<td>$ - Initial</td>
</tr>
<tr>
<td>Web Security and Advance Malware Protection</td>
<td>Health Sciences</td>
<td>1/29/2016</td>
<td>Completed 1/25</td>
<td>$ - Initial</td>
</tr>
<tr>
<td>Encrypted Email Solution*</td>
<td>Campus &amp; Health Sciences</td>
<td>4/1/2016</td>
<td>rolled out to all HS on 3/1 Available for campus departments ITS working with campus IT resources.</td>
<td>$ - Initial</td>
</tr>
<tr>
<td>Monthly Cyber Security Awareness Alerts</td>
<td>Campus &amp; Health Sciences</td>
<td>3/15/2016</td>
<td>Communication plan has been developed. Initial monthly communication sent 3/15/2016. Subsequent communications are targeted for the 15th of each month.</td>
<td>$ - Initial</td>
</tr>
<tr>
<td>Multi-factor Authentication*</td>
<td>Campus &amp; Health Sciences</td>
<td>PII - 4/1/2016</td>
<td>Phase I: IT Srv/Ntwrk PII - 5/1/2016 Phase II: Citrix VPN/SharePoint. Phase III: Email</td>
<td>$ - Annual</td>
</tr>
<tr>
<td>Data Loss Prevention (DLP) Solution for Network/Email, EndPoint and Discovery*</td>
<td>Campus &amp; Health Sciences</td>
<td>4/25/2022</td>
<td>Email integration design underway. POC for Health Sciences targeted 4/15 Requirements for campus use-cases are being documented.</td>
<td>$ - Initial</td>
</tr>
<tr>
<td>Require encrypted USB attached storage</td>
<td>Health Sciences</td>
<td>5/1/2016</td>
<td>Under development.</td>
<td>TBD</td>
</tr>
<tr>
<td>DNS Sinkhole (phishing protection)</td>
<td>Campus &amp; Health Sciences</td>
<td>10/1/2016</td>
<td>Budgeted for FY 16-17.</td>
<td>$ - Annual</td>
</tr>
<tr>
<td>Mobile Device Management (MDM) for BYOD</td>
<td>Health Sciences</td>
<td>4/1/2016</td>
<td>MDM being deployed with TigerText. BYOD testing underway, review draft BYOD policy</td>
<td>$ - Annual</td>
</tr>
<tr>
<td>Intrusion Prevention Solution (IPS)</td>
<td>Health Sciences</td>
<td>7/1/2016</td>
<td>Solution identified – pending review of req UC Security Monitoring (TDI) for overlap</td>
<td>$ - Initial</td>
</tr>
<tr>
<td>Threat Intelligence and Analytics</td>
<td>Campus &amp; Health Sciences</td>
<td>7/1/2016</td>
<td>Advanced threat scanning, analytics and coordinated security operations center for the UC system.</td>
<td>$AAA$ - Annual</td>
</tr>
<tr>
<td>Security Risk Assessment</td>
<td>Campus &amp; Health Sciences</td>
<td>9/1/2016</td>
<td>Software licensing in place. Services TBD in cooperation with system wide CISO committee</td>
<td>$AAA$ - Initial</td>
</tr>
<tr>
<td>HIPAA-compliant cloud-based research infrastructure</td>
<td>Health Sciences</td>
<td>12/31/2016</td>
<td>Under development.</td>
<td>TBD</td>
</tr>
</tbody>
</table>
Cyber Security – Hardened Security Environment

- Threat Detection and Analytics
- Targeted Vulnerability Scanning
- Minimum Security Standards
Cyber Security – System wide Culture Change

- Communication Plan
- Training
- Comprehensive Security Staffing Plan
Campus Engagement

- UC Training – 58% participation
- CARE Committee ✔️
- Health Sciences Executive and Governing bodies ✔️
- Cabinet – Feb 3 ✔️
- Senate Administrative Council – Mar 8 ✔️
- Monthly campus notice – Mar 15 ✔️
- Academic Senate – April 12 ✔️
Cyber Security @ UC San Diego

• Questions?