Agenda

General Data Protection Regulation (GDPR)
• J. Sibenaller

Information Security Program Overview
• S. Malisch, J. Sibenaller

ITS Dashboard Pilot
• S. Malisch, B, Montes
Prior Work Completed

Where we left off in Feb

- GDPR Research
- Create Execution Framework
- Pre-Assessment of Risk
- Obtain Sponsorship & Support

Overall Risk Breakdown

<table>
<thead>
<tr>
<th></th>
<th>Overall Risk Score</th>
<th>Count</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>16</td>
<td>4</td>
<td>7%</td>
</tr>
<tr>
<td>High</td>
<td>12</td>
<td>8</td>
<td>41%</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>6</td>
<td>17</td>
<td>50%</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
<td>1</td>
<td>2%</td>
</tr>
</tbody>
</table>

5/25/2018

EU GDPR Countdown Clock

Day: 27  Hour: 01  Minute: 19  Second: 08
Recent Work Completed

- **Assembled GDPR Working Group**
  - Meet weekly to date
  - Expanded membership
    - JFRC – Marilyn Vitale
    - R&R – Kris Daggett
    - HSC Research – Cynthia Tom-Klebb
  - Standing General Counsel meetings

- **Distributed Personal Data Surveys**
  - ITS (8-10, 165 responses)
  - Department Head (90-100)

- **Completed Inventory Security Policies/Procedures**
  - Identified changes to be made

- **Drafted Privacy Policy & Notice**
  - Sent to GC for review, on Revision 5 of Notice, Revision 3 of Policy
In Progress & To Be Complete by 5/25

**GDPR Web Site**
- Site approved, waiting for “shell”
- Draft content being created

**Data Protection Impact Assessment**
- Action items identified & validated
- Formatting as final document

**Active With General Counsel**
- Draft Vendor Management Contracts/Policy
- Data Protection Officer Needs

**Dependent on Survey Results**
- Inventory Personal Data Survey Results
- Data Flow/Processing Analysis
- Develop Use Cases
- Determine Legal Basis
- Initial Privacy Policy & Notice(s) (already reviewed by GC)

**Dependent on Resources**
- Updates to Incident Response Plan
- Updates to Critical Policies & Procedures
Work Planned Beyond 5/25

**Future Tasks**

- Final Privacy Policy & Notice(s)
- Final Vendor Management Contracts/Policy
- Final Updates to Policies & Procedures
- Data Protection Policy
- Consent Pop-Ups
- Data Copy, Edit & Deletion Processes
- Remaining Risk Treatments Based on Gap Analysis
- GDPR Training Awareness
- Privacy Mgmt Activities
- Ongoing Risk Assessment & Process Validation
Where are we?

Validated that...
- Our plan is solid
- Ahead of most schools

EAB Asked – *What progress has been made on your campus towards GDPR compliance?*
GDPR Risks

Half-Empty

Unknowns
- How people will react?
- What will they ask for?
- No litigation history
- Regulation is “purposely ambiguous”

We have complex data
- Identify data sources and movements
- How do we track?
- Deletions will be difficult

Resources
- Can we handle requests?
- Compliance by Committee

Half-Full

Project
- We have a very good plan
- Ahead of others

Demonstrated due diligence
- Key deliverables will be complete
- Good documentation is “enough”

We are small compared to others
- Under the “radar”

Industry says...
- The sky is not falling
- Adjustments will be likely
GDPR Next Steps

1. Move plan forward
2. Be ready to respond to questions
3. Prepare to adjust after 5/25
4. Communicate progress
Agenda

General Data Protection Regulation (GDPR)
  • J. Sibenaller

Information Security Program Overview
  • S. Malisch, J. Sibenaller

ITS Dashboard Pilot
  • S. Malisch, B. Montes
Information Security Program Components

- Governance
- Cyber Threat Protection
- Awareness, Education & Training
- Data Identification, Analysis & Forensics
- Policies, Procedures & Guidelines
- Vulnerability Assessments
- Audit, Compliance & Regulations
- Secure Access
- Incident Response
- Risk Assessment Program
- Security Operations Center
- ERP Security Services
Information Security – A Layered Approach

Layered Security – Levels 1-5

Policy & Procedures
- Published, reviewed annually, governed by ISAC, cyber insurance

Awareness & Training
- Online sessions, social media, web site, videos, phish publishing

Firewalls
- Cisco ASA

Intrusion Prevention
- Trend Micro TippingPoint (RepDV, Geo-Filtering)

Web Security
- F5 Load Balancer, F5 Web Application Firewall

Layered Security – Levels 6-10

Email Security
- ProofPoint, MS Junk Filtering

End User Security
- MS Forefront, Bradford NAC, PulseSecure VPN, RSA-Risk Based Authentication

Data Loss Prevention
- Identify Finder (at rest data), data in motion (FY18)

Integrity Monitoring
- IBM AppScan (web application), Nessus (internal scanning), Logrhythm (SIEM), CimTrak (PCI file integrity), Trustwave (external scanning)

Data Encryption
- MS Bitlocker, Oracle native encryption
What has changed?

• Threat Landscape – 2017-2018
  • 92% increase in new cyber threat variants
  • 13% increase in reported vulnerabilities
  • 80% increase in new malware on Macs
  • 8500% increase in “coin miner” detections
  • Email has a spam rate of 55%, up 2% from 2017
  • Mobile malware up 54%
  • 46% increase in new ransomware variants, overall ransomware down 2%
  • 600% increase in attacks against Internet of Things (IoT) devices, 21% come from China

• Internet of Things - On average, each student has 4.5 devices they connect to Loyola’s network
  • Laptop or notebook computers
  • Smart watches
  • Tablets/Smartphones
  • Streaming Devices (AppleTV, SmartTV, Chromecast, Roku)
  • Gaming platforms
  • Printers

Sources – Verizon, Thales, Symantec, Cisco, Gartner
## Incident History

<table>
<thead>
<tr>
<th>Location/Dept.</th>
<th>Feb-2018</th>
<th>Law School</th>
<th>Nov-2017</th>
<th>Human Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of Incident</td>
<td>Direct mailing letter sent to prospective graduate student included the social security number in the address block</td>
<td></td>
<td>A completed form relating to a faculty member’s evidence of insurability was inadvertently packaged with other blank forms by Human Resources and distributed to 23 individuals completing open benefits enrollment.</td>
<td></td>
</tr>
<tr>
<td>Scope</td>
<td>1 Prospective Graduate Student</td>
<td>1 Faculty Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>• Established incident response team</td>
<td>• Established incident response team</td>
<td>• Communicated to affected party via letter</td>
<td>• Communicated to affected party via letter</td>
</tr>
<tr>
<td></td>
<td>• Communicated to affected parties via letter</td>
<td>• HR contacted all recipients to have them destroy the form</td>
<td>• Offered credit monitoring services (1 yr)</td>
<td>• Offered credit monitoring services (1 yr)</td>
</tr>
<tr>
<td>Credit Monitoring</td>
<td>• 100% enrolled</td>
<td>• 100% enrolled</td>
<td>• &lt; $50</td>
<td>• &lt; $50</td>
</tr>
<tr>
<td>Department Action</td>
<td>• Established a review process with vendor.</td>
<td></td>
<td>• Reviewed existing data security procedures with staff.</td>
<td></td>
</tr>
<tr>
<td>ITS Info. Security Action</td>
<td>Validated information handling policies are clear.</td>
<td></td>
<td>Validated information handling policies are clear.</td>
<td></td>
</tr>
<tr>
<td>Data Breach Validation</td>
<td>No fraudulent use of information reported</td>
<td></td>
<td>No fraudulent use of information reported</td>
<td></td>
</tr>
</tbody>
</table>

Cyber Security Concerns - Things to Watch

**People**
- Faculty/Staff – General complacency, risks to phishing
- Students – Over confident they are not vulnerable/untouchable

**Technology Advancements**
- Internet of Things – How to protect the explosion of device types
- Protecting Privacy – “leaky apps”, Alexa/Echo, phones, cameras, locations, phone numbers...

**Attacks & Threats**
- Creativity of Hackers – New attack variants come quickly, self-propagation
- Vulnerabilities/Out of Date Software – 10% of all known vulnerabilities get exploited
- Attacks on Computer Processors – Minimal defenses available
- Coin-Miner Attacks – Will continue with modified variants
- Mobile Devices – Threats occurring quicker than prevention methods
## Addressing Change – Strategic Projects

<table>
<thead>
<tr>
<th>Completed</th>
<th>Expanding</th>
<th>In Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next Generation Firewall Technology</strong></td>
<td><strong>New Web Application Firewall</strong></td>
<td><strong>Password Vault/Privileged Access</strong></td>
</tr>
<tr>
<td>+ Improves ability to identify and block more types of threats</td>
<td>+ Strengthened our web application protection</td>
<td>+ Implementation of an enterprise tool to improve password protection</td>
</tr>
<tr>
<td><strong>Updated SIEM Technology</strong></td>
<td><strong>Vulnerability Management Improvements</strong></td>
<td><strong>Multi-Factor Authentication</strong></td>
</tr>
<tr>
<td>+ Consolidation of network traffic logs that helps identify patterns of attacks and helps us improve our blocking techniques</td>
<td>+ Expanded program to repeated server scanning to identify vulnerabilities more quickly</td>
<td>+ Increases ability to verify identity of person</td>
</tr>
<tr>
<td>+ Logrhythm replaced IBM QRadar, improved functionality for less cost</td>
<td>+ Added administration tool for reporting and tracking efficiency</td>
<td>+ Researching campus wide use</td>
</tr>
<tr>
<td><strong>New Web Application Firewall</strong></td>
<td><strong>Data Loss Prevention</strong></td>
<td><strong>In Progress</strong></td>
</tr>
<tr>
<td>+ Blocking over 19,000 attacks a day (formerly 1,000/day)</td>
<td>+ Helps identify where and when protected data is being transmitted</td>
<td><strong>Technology recommendation approved, implementation in planning stages</strong></td>
</tr>
</tbody>
</table>
**Information Security – A Layered Approach**

### Layered Security – Levels 1-5

**Policy & Procedures**
- Published, reviewed annually, governed by ISAC, cyber insurance

**Awareness & Training**
- Online sessions, social media, web site, videos, phish publishing

**Firewalls**
- Palo Alto Next Generation Firewall

**Intrusion Prevention**
- Palo Alto Next Generation Firewall, Global Protect

**Web Security**
- F5 Load Balancer, F5 Web Application Firewall

### Layered Security – Levels 6-10

**Email Security**
- ProofPoint, MS Junk Filtering

**End User Security**
- MS Forefront, Bradford NAC, Global Protect VPN, Multi-Factor Authentication, LastPass Password Vault

**Data Loss Prevention**
- Identify Finder (at rest data), MS DLP (data in motion)

**Integrity Monitoring**
- IBM AppScan (web application), Nessus (internal scanning), Logrhythm (SIEM), CimTrak (PCI file integrity), Trustwave (external scanning)

**Data Encryption**
- MS Bitlocker, Oracle native encryption
## Beyond the Information Security Layers...

### GDPR Status Update (as of May 1st)

#### Work Completed
- GDPR Research
- Create Execution Framework
- Pre-Assessment of Risk
- Obtain Senior Leadership Sponsorship & Support
- Assemble GDPR Working Group
- Distribute Personal Data Surveys (Dept. Head & Technical)
- Inventory Security Policies/Procedures
- Draft Privacy Policy & Notice

#### In Progress & Complete by 5/25
- Inventory Personal Data Survey Results
- Data Flow/Processing Analysis
- Develop Use Cases
- Determine Legal Basis
- Initial Privacy Policy & Notice(s)
- GDPR Web Site
- Data Protection Impact Assessment
- Incident Response Plan
- Updates to Critical Policies & Procedures
- Data Protection Officer Needs
- Draft Vendor Management Contracts/Policy

#### Planned Beyond 5/25
- Final Privacy Policy & Notice(s)
- Final Vendor Management Contracts/Policy
- Final Updates to Policies & Procedures
- Data Protection Policy
- Consent Pop-Ups
- Data Copy, Edit & Deletion Processes
- Remaining Risk Treatments Based on Gap Analysis
- GDPR Training Awareness
- Privacy Mgmt Activities
- Ongoing Risk Assessment & Process Validation

---

January to May 2018

Beyond May 2018
Beyond the Information Security Layers...

• Physical Security – Security Cameras
  • 781 total cameras deployed, 65 new cameras deployed since 2017
  • 6 New Recording Servers Installed in 2016 with 20 TB of Storage each
  • Video Retention expanded in 2017 to 21 days from 14 days
  • High Definition/Infra-red/Night Vision functionality

High Definition Examples

Camera Replacement Program

Before

After
Beyond the Information Security Layers...

- Physical Security – Card Readers/Building Access
  - Loyola’s access management system, Maxxess, controls over 700 doors/gates.
  - Upgrade needed due to aging unsupportable card reader technology
    - Replacing Maxxess (proprietary) with Mercury (open architecture)
    - Supports multiple vendor applications and multiple access card types
    - Compatible with the Health Sciences system
    - Capital budget has been established
  - Upgrades have begun, 70+ doors completed
  - Remaining 630 doors/gates located in 64 buildings
  - 24-36 month timing to complete as coordinated with Campus Safety scheduling
Agenda

General Data Protection Regulation (GDPR)
• J. Sibenaller

Information Security Program Overview
• S. Malisch, J. Sibenaller

ITS Dashboard Pilot
• S. Malisch, B, Montes
2018 ITESC Schedule

February 6, 2018 - Tuesday, 1:00-3:00 PM
- BCDR – Program Restart
- General Data Protection Regulation
- Workday
- BI
- Student System Upgrade
- Technology Changes for Spring 2018

May 1, 2018 - Tuesday, 1:00-3:00 PM
- GDPR Project Update
- Information Security Program Overview
- ITS Dashboard Pilot

June 21, 2018 - Thursday, 10:00-12:00 PM
- BCDR Plan Update
- Project Portfolio Prioritization

August 23, 2018 - Tuesday, 1:00-3:00 PM
- 

September 18, 2018 - Tuesday, 1:00-3:00 PM
- 

October 25, 2018 - Tuesday, 1:00-3:00 PM
- 

December 11, 2018 - Tuesday, 1:00-3:00 PM
- Project Portfolio Prioritization