ITS Executive Steering Committee (ITESC)

Agenda and Materials – May 1, 2018

Technology@Loyola
INFORMATION TECHNOLOGY AND SERVICES
LOYOLA UNIVERSITY CHICAGO

Agenda

General Data Protection Regulation (GDPR)

- J. Sibenaller

Information Security Program Overview

- S. Malisch, J. Sibenaller

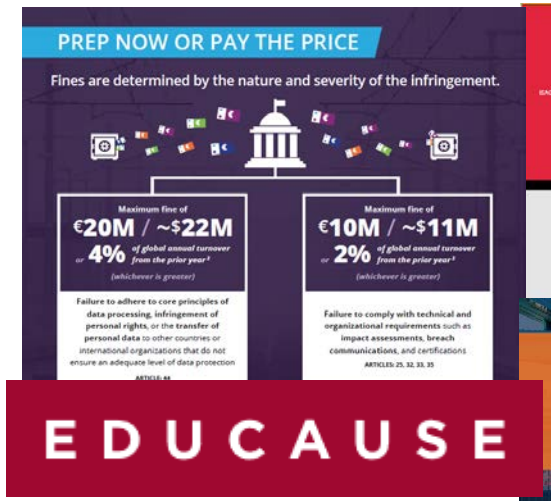
ITS Dashboard Pilot

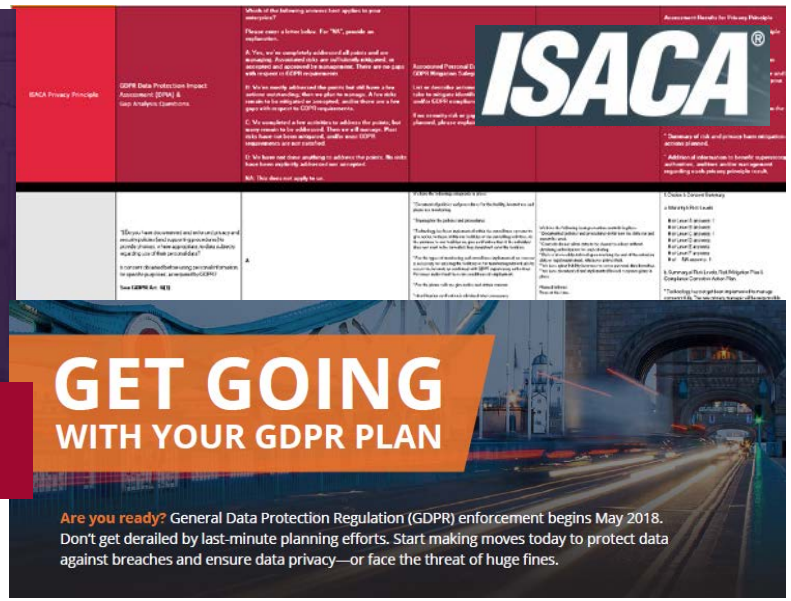
- S. Malisch, B, Montes

Prior Work Completed

Where we left off in Feb

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





Overall Risk Breakdown

	Overall Risk Score	Count	Count
Critical	16	4	7%
High	12	8	41%
	9	13	
	8	2	
Medium	6	17	50%
	4	11	
Low	2	1	2%
		56	100%

5/25/2018

LOYOLA UNIVERSITY CHICAGO
1870
AD · MAJOREM · DEI · GLORIAM

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

LOYOLA UNIVERSITY CHICAGO

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?*

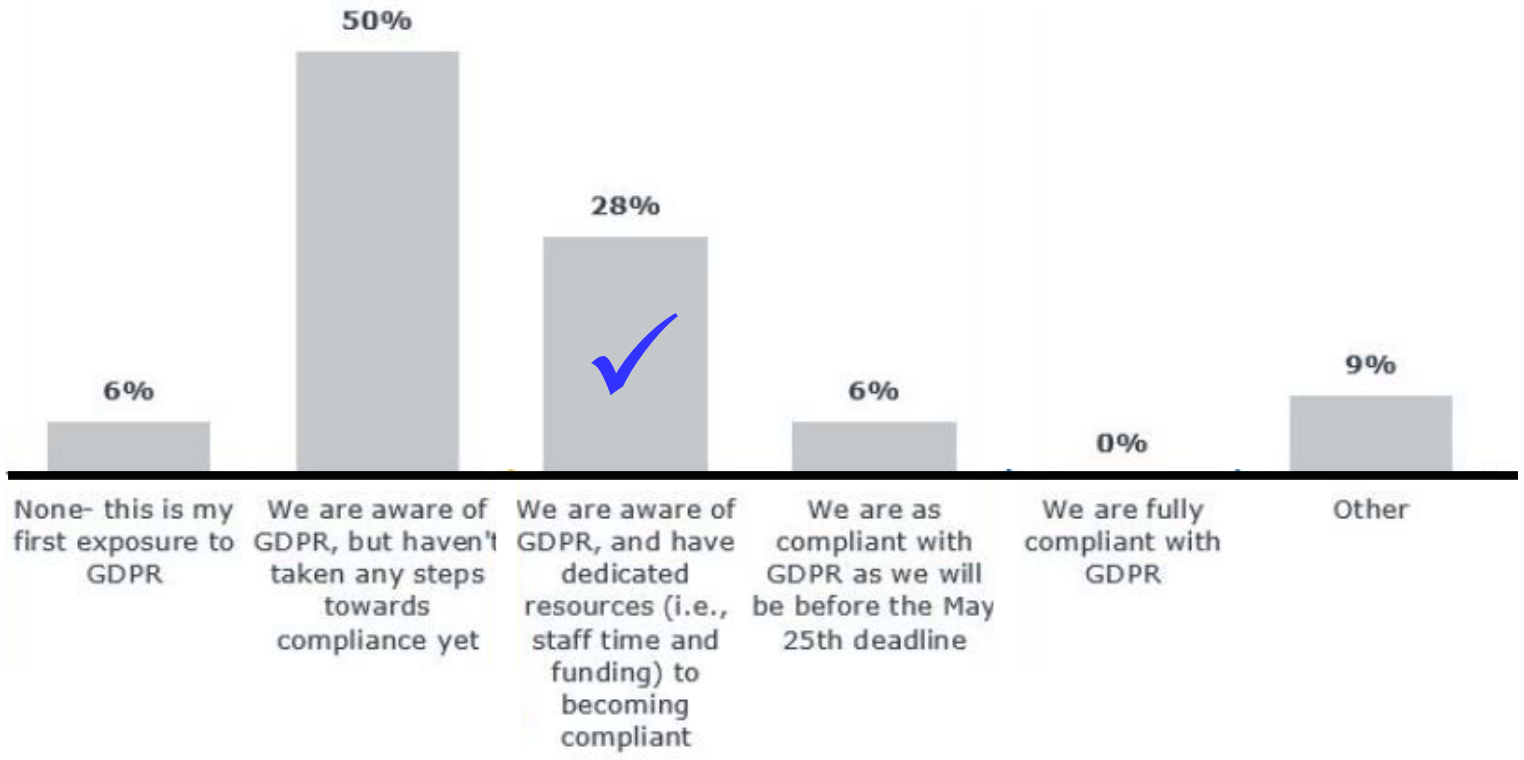


Chart Sources – EAB-Education Advisory Board

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

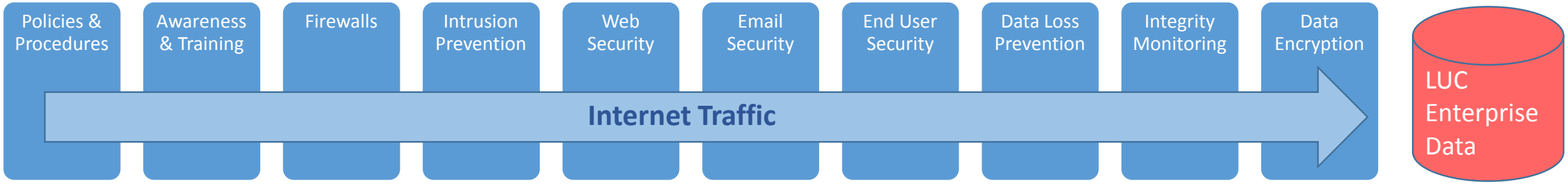
ITS Dashboard Pilot

- 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

	Feb-2018	Nov-2017
Location/Dept.	**Law School**	**Human Resources**
Description of Incident	Direct mailing letter sent to prospective graduate student included the social security number in the address block	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.
Scope	1 Prospective Graduate Student	1 Faculty Member
Incident Response	• Established incident response team • Communicated to affected parties via letter • Offered credit monitoring services (1 yr)	• Established incident response team • Communicated to affected party via letter • HR contacted all recipients to have them destroy the form • Offered credit monitoring services (1 yr)
Credit Monitoring	• 100% enrolled • < $50	• 100% enrolled • < $50
Department Action	• Established a review process with vendor.	• Reviewed existing data security procedures with staff.
ITS Info. Security Action	Validated information handling policies are clear.	Validated information handling policies are clear.
Data Breach Validation	No fraudulent use of information reported	No fraudulent use of information reported
Policy/Process	http://www.luc.edu/its/policies/incident_response_plan.shtml	

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

Completed

Next Generation Firewall Technology
- Improves ability to identify and block more types of threats

Updated SIEM Technology
- Consolidation of network traffic logs that helps identify patterns of attacks and helps us improve our blocking techniques
- Logrhythm replaced IBM QRadar, improved functionality for less cost

Expanding

New Web Application Firewall
- Strengthened our web application protection
- Blocking over 19,000 attacks a day (formerly 1,000/day)

Vulnerability Management Improvements
- Expanded program to repeated server scanning to identify vulnerabilities more quickly
- Added administration tool for reporting and tracking efficiency

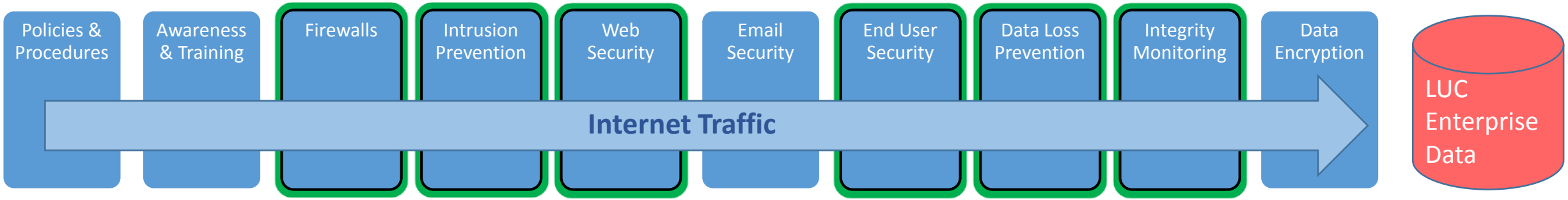
In Progress

Password Vault/Privileged Access
- Implementation of an enterprise tool to improve password protection

Multi-Factor Authentication
- Increases ability to verify identity of person
- Researching campus wide use

Data Loss Prevention
- Helps identify where and when protected data is being transmitted
- Technology recommendation approved, implementation in planning stages

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

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

Planned Beyond 5/25

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

Camera Replacement Program

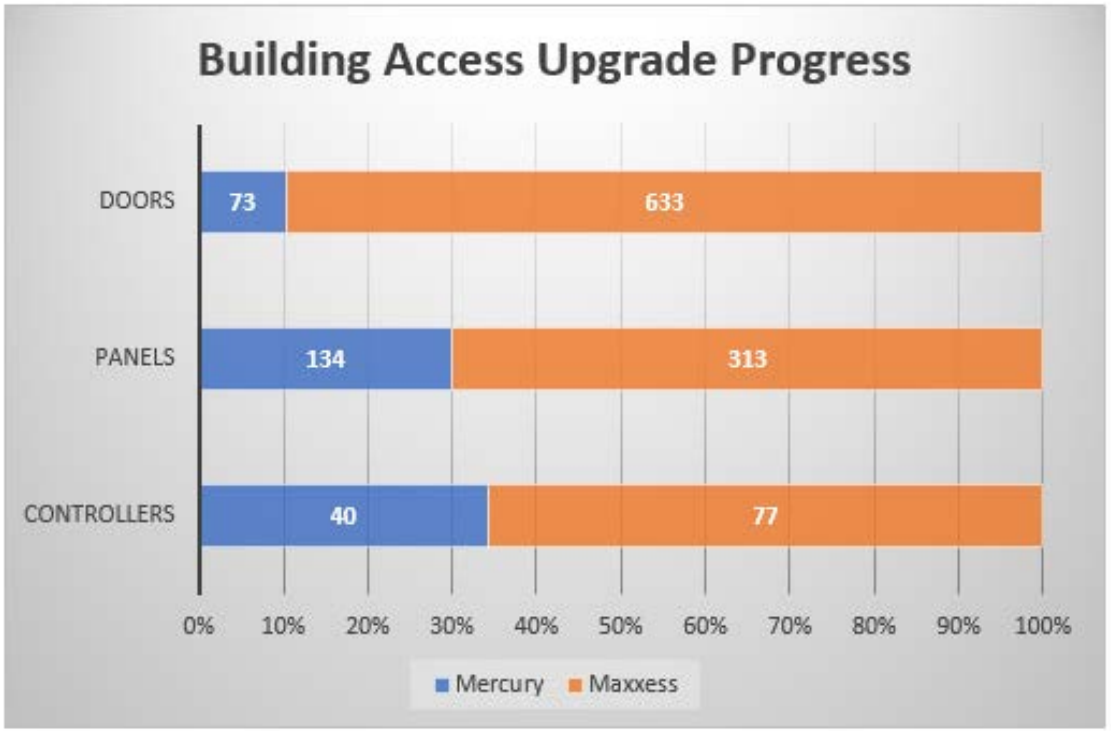
High Definition Examples

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

Current Reader

New Reader



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

-

December11, 2018 - Tuesday, 1:00-3:00 PM

- Project Portfolio Prioritization