VALENCIA

Valencia College
Office of Information Technology

Office of Information Technology

Information Security Update

District Board of Trustees

July 22, 2020

Office of Information Technology

Project Management Office

Enterprise Application Services

Campus Technology Services

Technology Infrastructure & Security Services

Commitment to Information Security

The Office of Information Technology is committed to dedicating time and resources to continuously identify, assess, and mitigate threats to Valencia College's information technology systems and data.

As we work through COVID-19, our efforts have not wavered. We continue to address our threats with the same, if not greater diligence. Our threat has changed during these times and we are changing our tactics to ensure we mitigate these changing risks.

VALENCIA

Valencia College
Office of Information Technology

Challenges

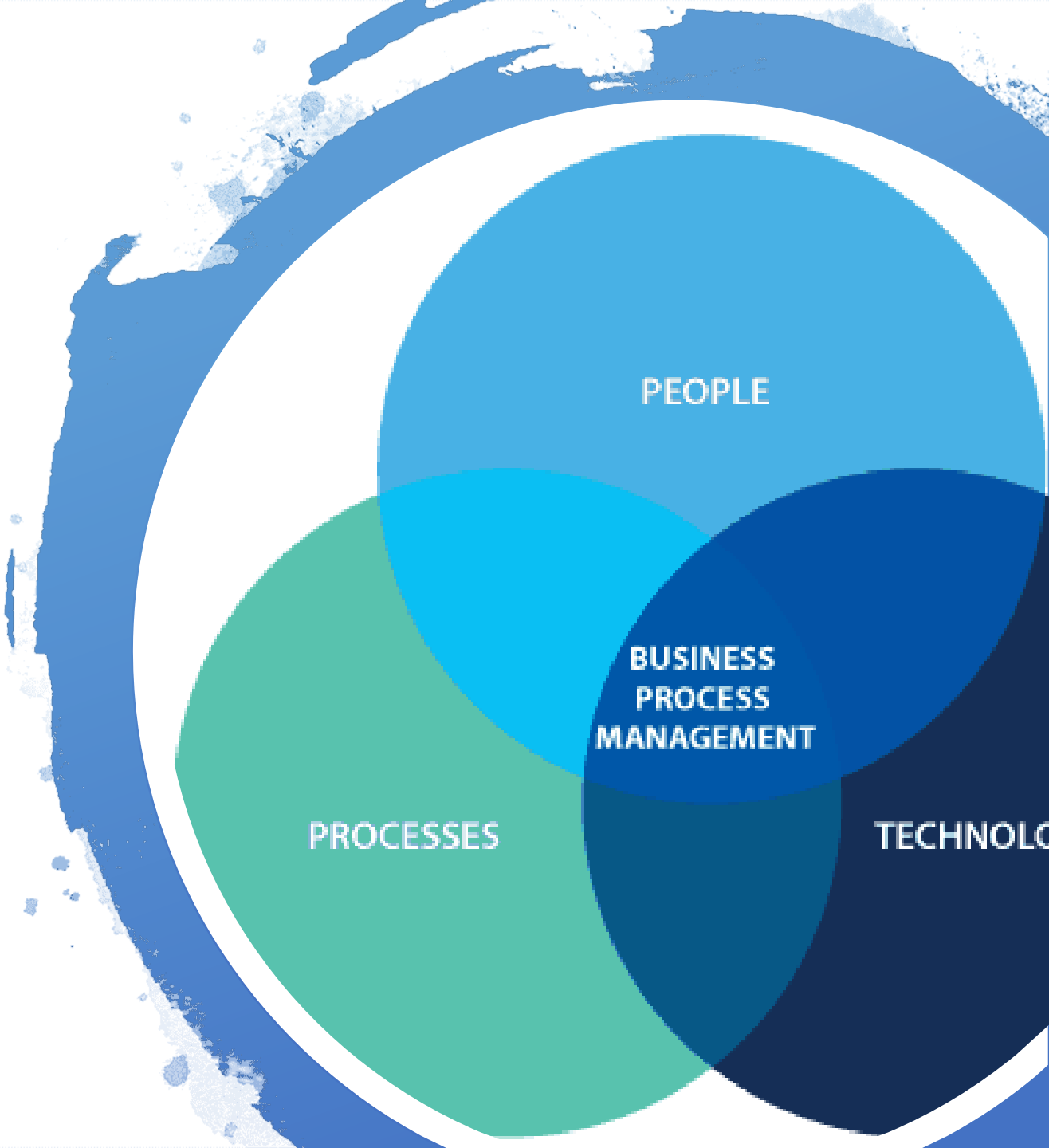
- People
  - Social Engineering
  - The “Human Firewall”
  - User education
- Process
  - Within Information Technology
  - College-wide
- Technology
  - Phishing
  - Ransomware
  - Hacking
  - Mobile device management

People

- Improved security personnel talent
  - Application Security Administrator (Banner)
- Enhanced partnerships
  - FBI on Cyber Security – Trends, Tips, Best Practices
  - Florida College System guidelines & strategies
  - Local law enforcement
  - With industry leaders such as Educause and Gartner
- Trend awareness (conferences, webinars, trade-journals)
- Information Security training

Process

- Adopted National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Improved change management
- Partnered with internal contracts administrator for software/hardware related purchases
- Diligence in reviewing and revising access controls and information security components of all IT related processes

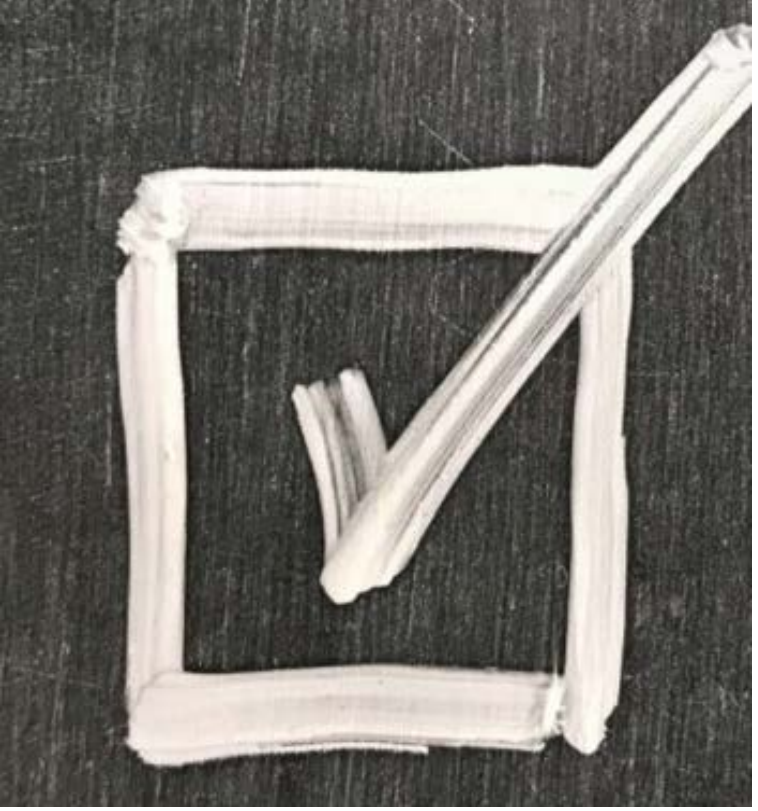


Technology

- Implemented numerous software tools:
  - Security Information & Event Management (SIEM)
  - New firewall
  - Vulnerability management
  - Endpoint protection (ransomware & malware)
  - Payment Card Industry (PCI) Chip & PIN credit card readers
- Improved email controls
  - Email migration to Office 365
  - External email notification
  - “Report Message” functionality
  - Multi-factor authentication for Office 365

Technology

- Microsoft Advanced Threat Protection
  - ✓Validating email links
  - ✓Blocking malicious email
  - ✓Automatic response to suspicious sign in activity
- Developed and maintain new system baseline configurations
- Homeland Security Vulnerability Scanning



Action Items

People

- Engagement with Homeland Security / risk assessment
- Engage managed service security provider
- Multi-factor authentication for students
- Hire Director, Information Security Operations
- Enhance engagement across college raising awareness

Process

- Update Information Technology policies
- Continue improvements of Information Security Plan

Technology

- Implement additional technology to firewall
- Expand cloud security capabilities
- Move Banner to Cloud to limit local physical vulnerabilities

Summary

- We don’t control the threat, but we do control the organization's readiness.
- Our readiness is good, but we must beware of a false sense of security.
- There is no such thing as perfect protection…we are seeking a balance between protection and achieving the desired outcomes of the college.
- Understand the connection between IT dependency and critical business processes to guide prioritization, investment and defensibility.

Gartner