



**SERS Retirement Board
Technology Committee Agenda
Regular Meeting
May 26, 2021
12:30 P.M.**

Click to join the Zoom meeting:

<https://ohsers.zoom.us/j/93678902339?pwd=Yk0xK09rdmhLQkhwbIhoYUd6dmZ6UT09>

Meeting ID: 936 7890 2339

Password: 633902

To join by phone, dial: (301) 715-8592 and enter the meeting ID: **936 7890 2339** and password: **633902** when prompted.

1. Roll Call
2. Technology Committee's Purpose & Role
3. SERS Technology Delivery Footprint
 - Information Technology Overview
 - SMART Overview
 - Information Security Overview
4. Upcoming Technology Committee Meetings
 - Calendar Dates for Future Committee Meetings
 - Continued or New Business
 - Information Requests and Follow-up Items from May 26, 2021 Meeting
 - Future Topics
5. Adjournment (R)



Technology Committee

05/26/2021

Agenda - May 26, 2021

- Technology Committee's Purpose & Role
- SERS Information Technology Delivery Footprint
 - Information Technology Overview
 - SMART Overview
 - Information Security Overview
- Upcoming Technology Committee Meetings



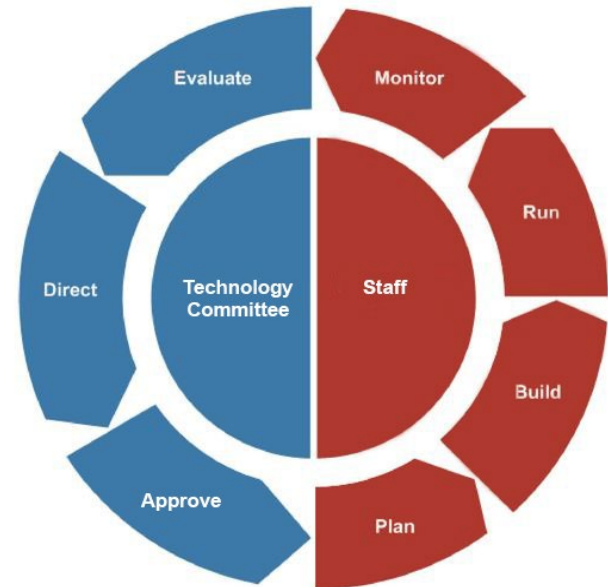
Technology Committee Strategic Intent

..So that Board has over-all business and technology strategy alignment, deeper awareness and understanding of technology direction, integration with information security and insight into long-term investment plan to sustain and evolve technology program at SERS.



Technology Committee Role

- Provide a platform for staff to engage and collaborate with board members on information technology and security topics
- Oversight and approval of information technology and security strategy and direction that aligns with SERS' vision
- Awareness of technology and information security trends, challenges, cost and risks
- Guidance on multi-year technology investment capital plan
- Advocate and champion information technology and security strategy, and investment (budget) to full Pension Board



IT Mission and Core Values



Information Technology Mission

To fulfill the mission of SERS, we in the Information Technology Department ensure:

- A department that values teamwork with a passion for building an environment of integrity and trust.
- Effective and efficient delivery of technical programs and services for our Business Partners who support our membership on a daily basis.
- Identification, evaluation and selection of technology should be consistent and compatible with current and future business needs and technology advances.

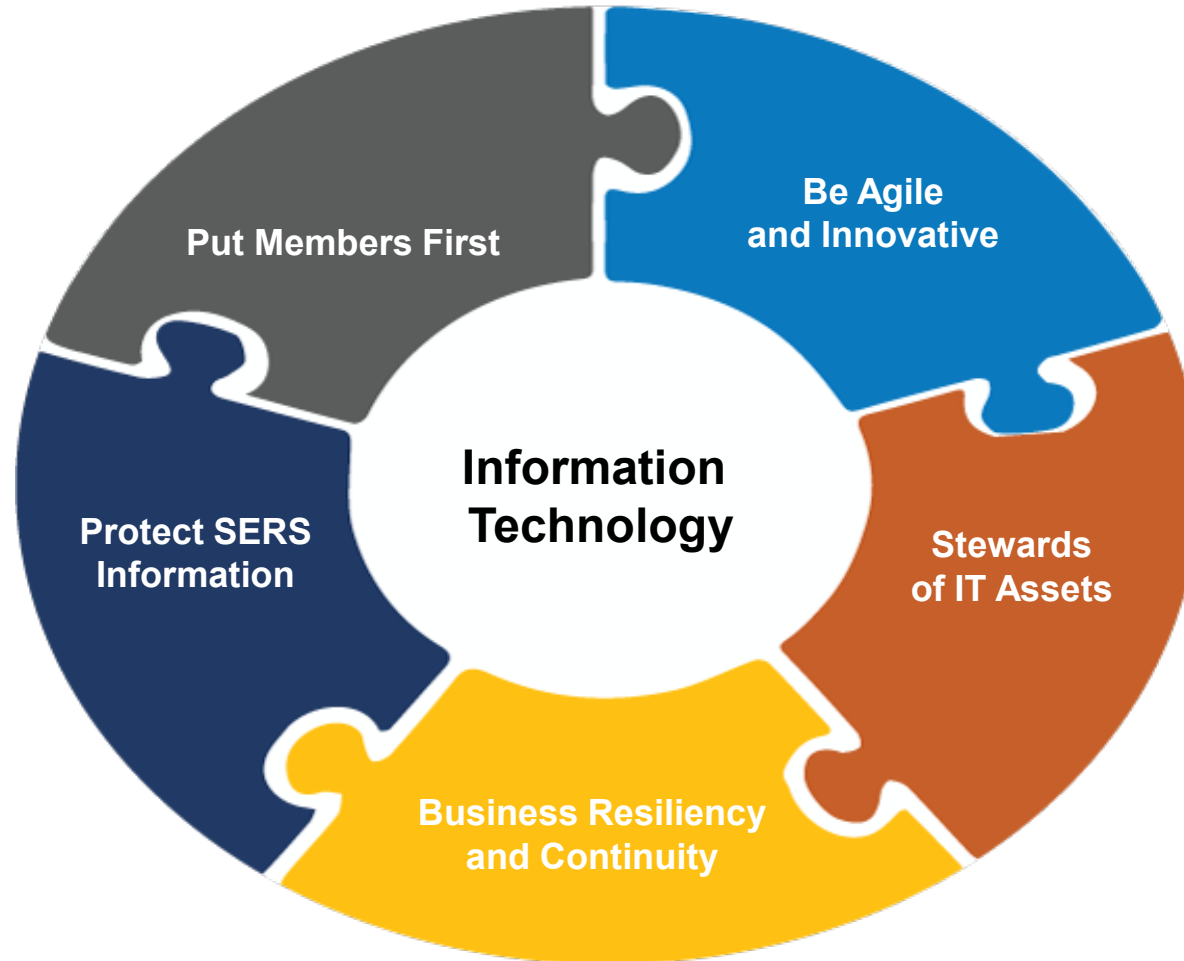
IT Core Values

Responsive / Creative / Dependable / Efficient



IT – Guiding Principles

...In harmony with the SERS 5 Year Strategic Plan



“The greatest danger in times of turbulence is not the turbulence; it is to act with yesterday’s logic,”
as management guru Peter Drucker previously warned enterprise leaders.

IT Operating Model

Leadership || Governance || Strategy



PLAN



- Strategic Planning
- Business Analysis
- Quality Assurance
- SMART Release Planning



BUILD



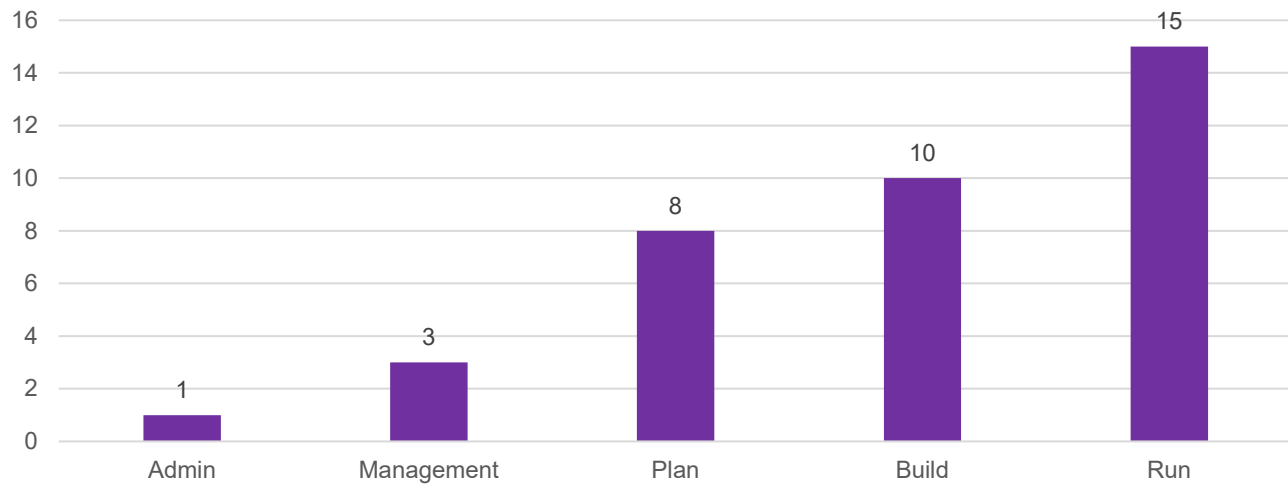
- SMART Design & Development
- SMART Release Deployment
- Boulevard Development



RUN

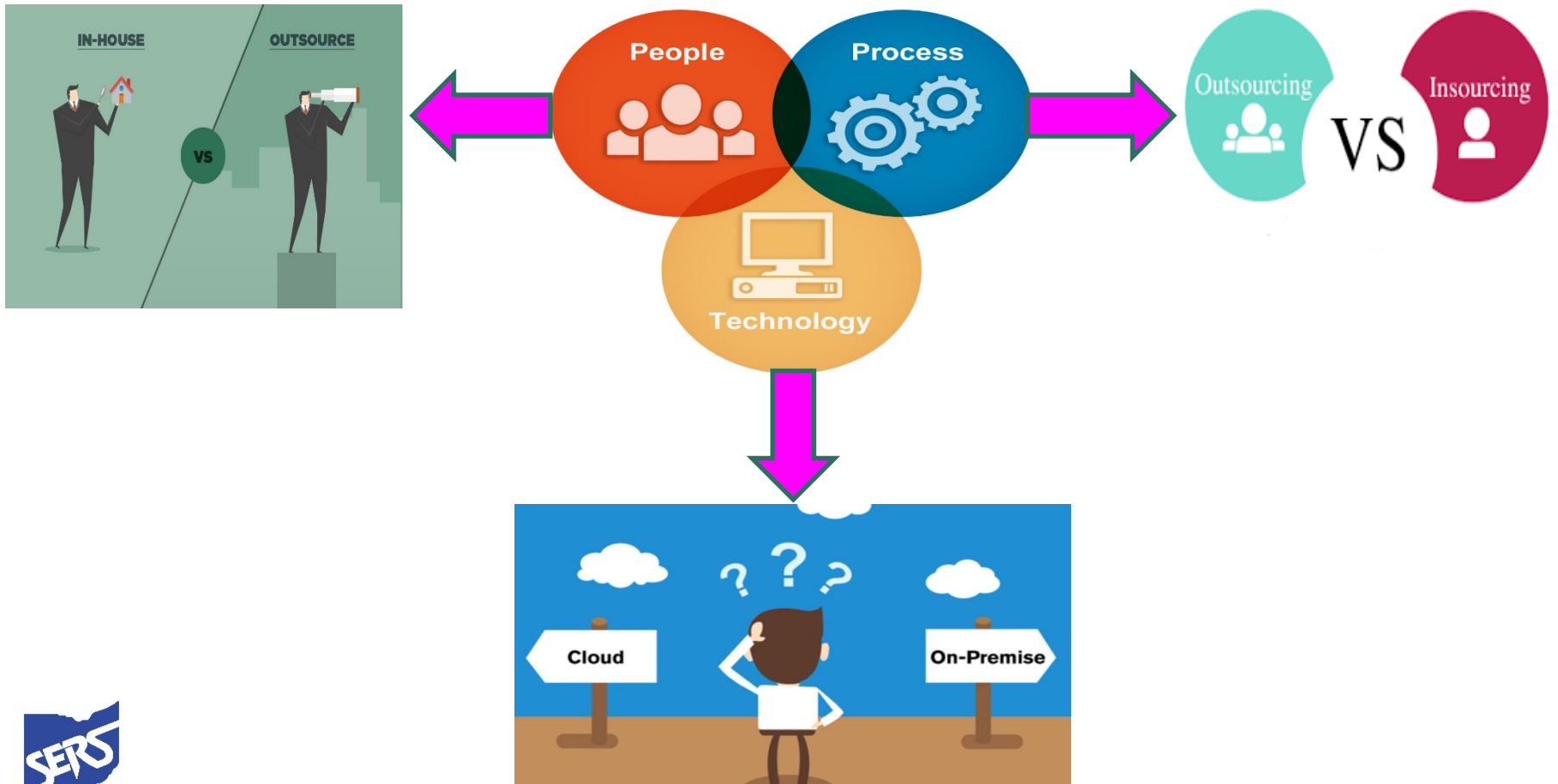


- Service Desk
- Project Management
- Infrastructure Management
- Information Security
- Telecommunication Management



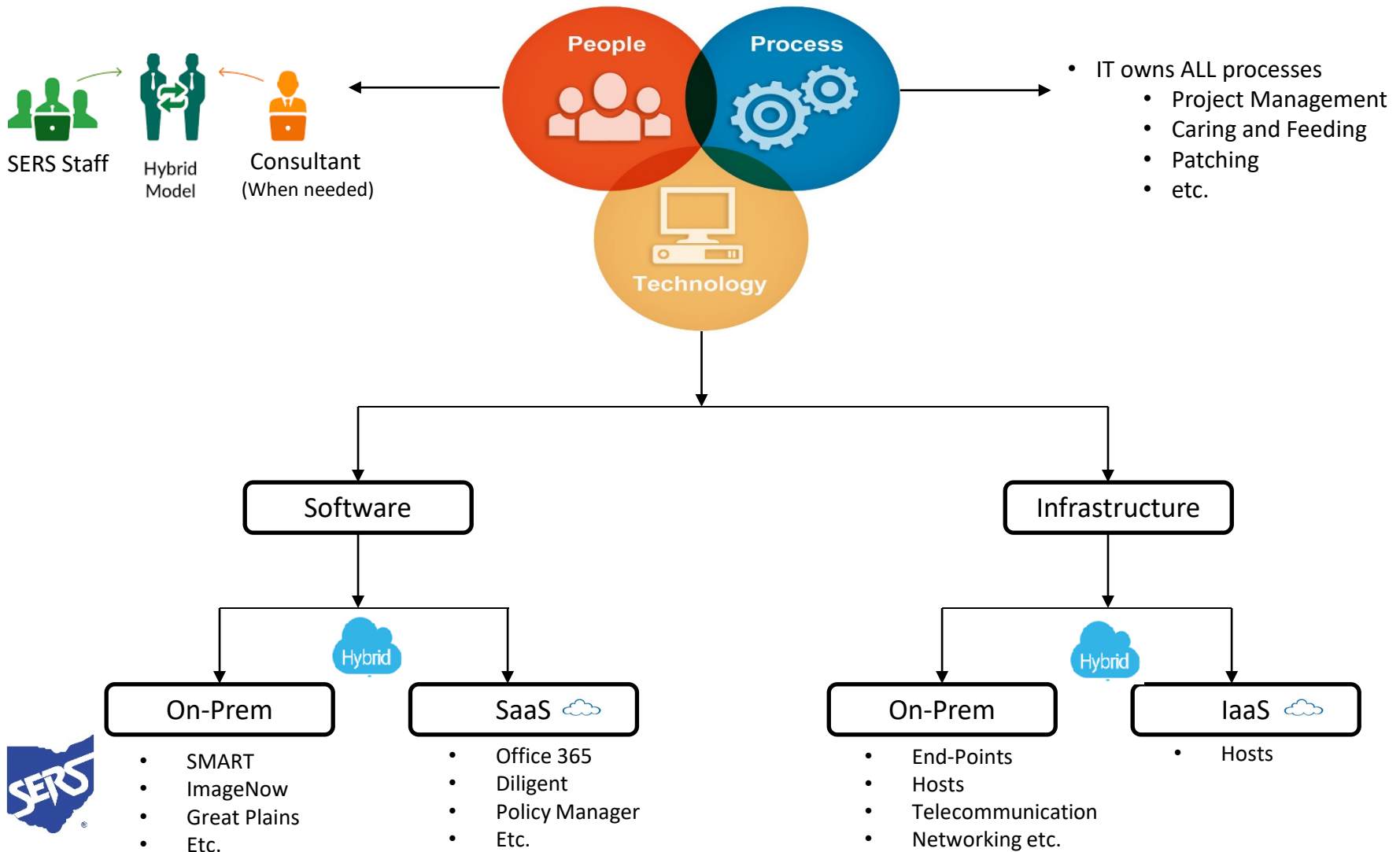
IT Service Delivery

Traditionally, IT delivers services through the combination of – People, Process and Technology
This delivery model is enabled by various options.



IT Service Delivery @ SERS

@ SERS, IT delivers services through the appropriate balance of People, Process and Technology.



IT – Infrastructure (Bits and Bytes)

End User

250 End-Points



80 Laptops



30 VOIP



Primary Data Center (HQ)

27 Hosts



~320 TB Storage



5 Firewalls



~480 Virtual Machines (VM)



28 Networking Gear



4 Load Balancers



Software

45
Products



ISP

Verizon
100 MB

Spectrum
500 MB

Voice

CenturyLink
Avaya Call
Center

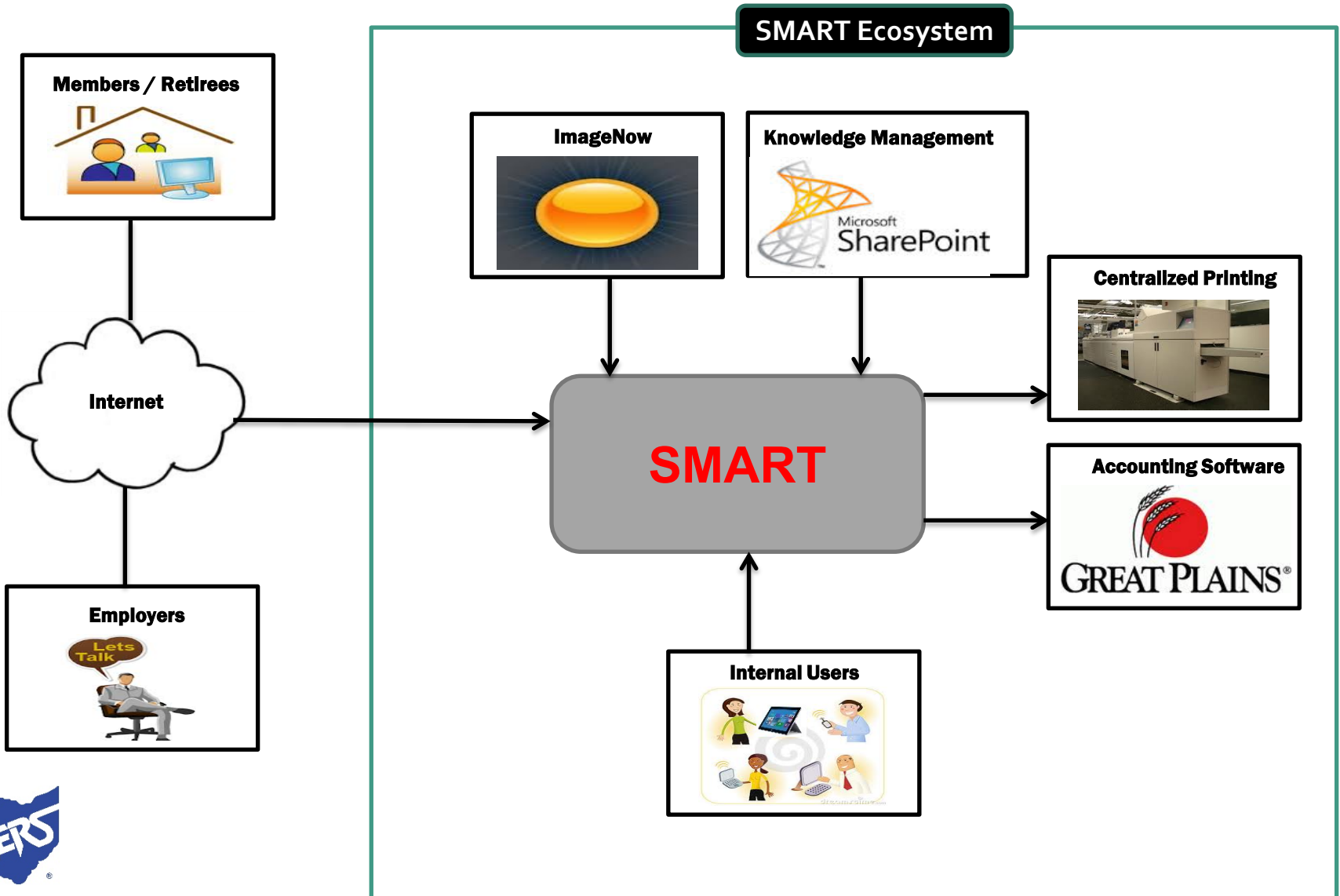


SMART

- MARS- Member and Retiree System
 - 13+ years old
 - Reaching end of life
 - Limited Self-Service capabilities
- Decision in late 2010 to replace system
 - Off the shelf customizable solution
 - Meet the needs of today and the future (online, self-serve, etc.)
 - Understand this is a major and complex SERS wide project
 - Awareness of on-going investment to sustain and enhance system
- SMART in production – February of 2017
 - Sagitec (vendor) partnered with SERS on a fixed bid project
 - SERS IT caring and feeding for SMART since March 2018
 - Core functionality very solid with on-going new capabilities added



SMART Eco-System



SMART + Infrastructure = Harmony



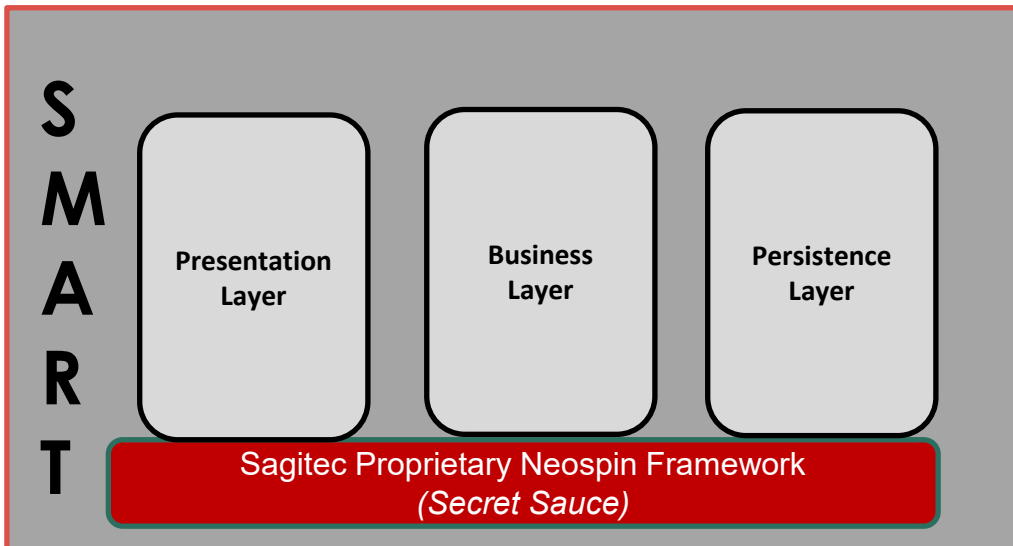
MSS User



eSERS User



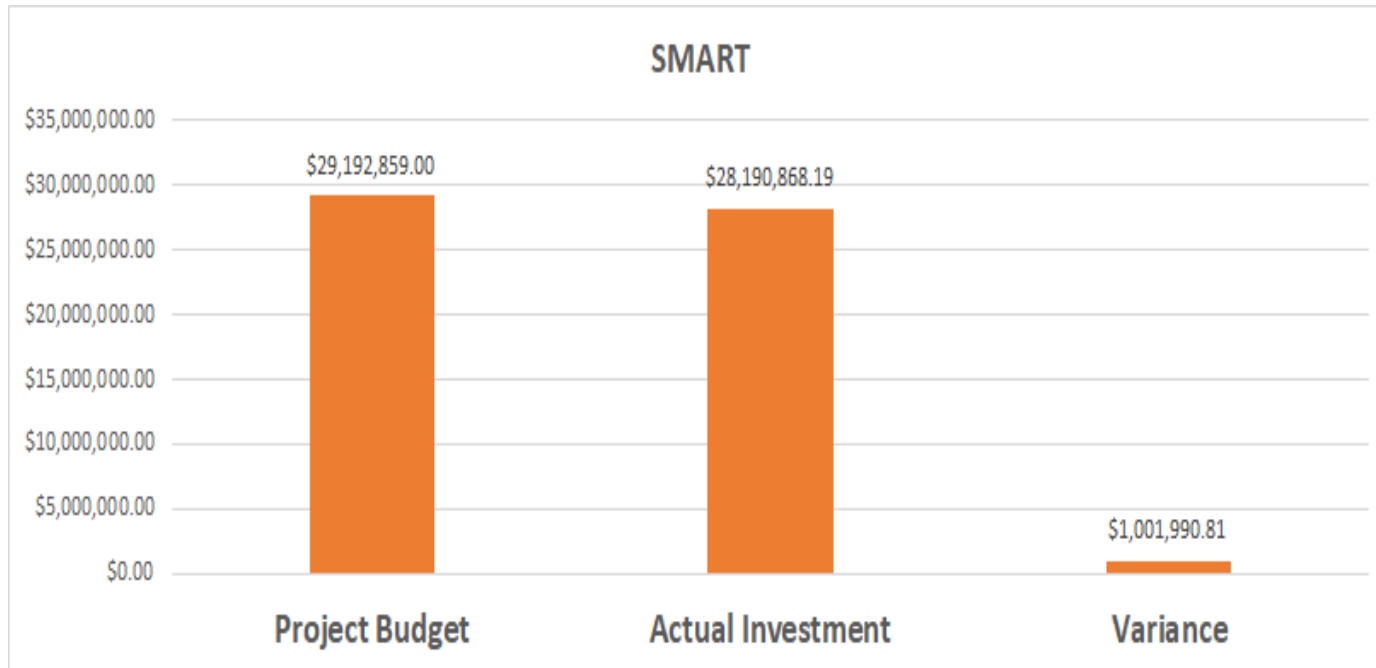
Internal User



SMART By the Numbers..

- Lines of Code – 269,241
- # of Images – 31 Million
- Size of the Database – 500GB
- # of Screens – 980
- # of Correspondences – 687
- # of Database Tables – 665
- # of Reports – 283
- # of Batch Jobs – 243
- # of Workflows – 174
- # of Outgoing Files - 80
- # Incoming Files – 27

SMART Project Financials



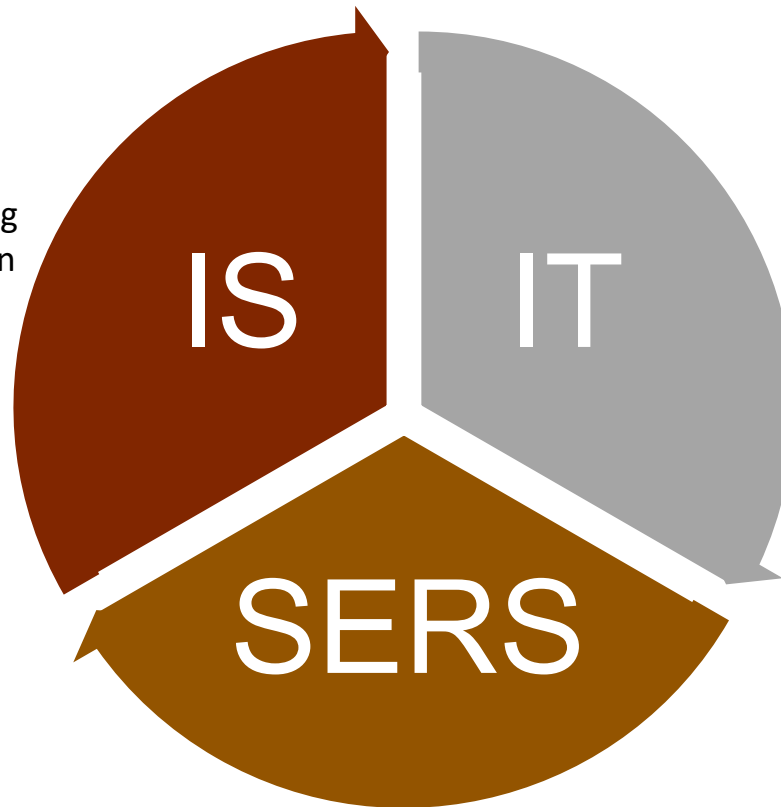
- SMART capital project has been closed.
- Expenditures were less than capital plan. However, deployment timeline was extended.
- Project required extended internal resource commitment to deploy SMART to production.



IS and IT Collaboration

Senior Leadership Oversight (Karen, Joe B. and Jay)

- Security Strategy
- Security Awareness Training
- Control Testing & Validation
- Security Policies
- Security Best Practices
- Incident Management



- Security Architecture
- Security Controls
- Alerts and Monitoring
- Permission Management
- Incident Management
- Security Best Practices

- Security Aware Culture
- Security Awareness Training



Risk Management - Information Security

Mission:

Safeguard confidentiality, integrity, and availability of SERS' information systems, identity, and data assets.

Key Objectives:

- Align activities with business strategy to support SERS objectives
- Foster culture of security awareness and compliance
- Provide proactive security expertise and identify top cyber risks
- Monitor threat landscape and implement risk management measures
- Identify and manage advanced capabilities to protect / detect cyber attacks
- Plan and manage incident response and BC/DR resiliency
- Monitor and report on information security processes and risks



Risk Management – Leadership

Risk Management

Information Security

Enterprise Risk Management

Investment Compliance



Information Security, Phil Grim

- Over 20 years of progressive information security leadership roles within a Fortune 500 electric company and accomplished military security roles
- Led global enterprise and product security program, developed and implemented crisis management plan, centralized security operations, created strategic plan, implemented risk management reporting, vendor management compliance to best practices, develop data protection compliance program
- Business MBA with information systems concentration; numerous training and certifications as a Certified Information Systems Security Professional, data security, advanced smartphone forensics & incident management



ERM Officer, Susan Bradley

- Over 20 years private sector experience within insurance and health care industries with experience concentrated in enterprise risk management, project management, organization change management & software development testing
- Led major projects and programs involving quality, enterprise risk management, incident response, disaster recovery, and business continuity; excellent knowledge and use of risk tools, such as business impact analysis, risk registers, risk assessments and incident tracking analysis
- MBA with multiple certifications as a Risk and Information Systems Control (CRISC), Business Continuity Professional (CBCP), Six Sigma Black Belt (CSSBB) & Software Testing Engineer (CSTE)



Investing in experienced & qualified staff helps SERS establish sustainable programs that add value and systematically address key risks

Information Security – NIST Cybersecurity Approach



IDENTIFY

- ▶ Asset management
- ▶ Business environment
- ▶ Governance
- ▶ Risk assessment
- ▶ Risk management strategy

PROTECT

- ▶ Access control
- ▶ Awareness and training
- ▶ Data security
- ▶ Information protection and procedures
- ▶ Maintenance
- ▶ Protective technology

DETECT

- ▶ Anomalies and events
- ▶ Security continuous monitoring
- ▶ Detection process

RESPOND

- ▶ Response planning
- ▶ Communications
- ▶ Analysis
- ▶ Mitigation
- ▶ Improvements

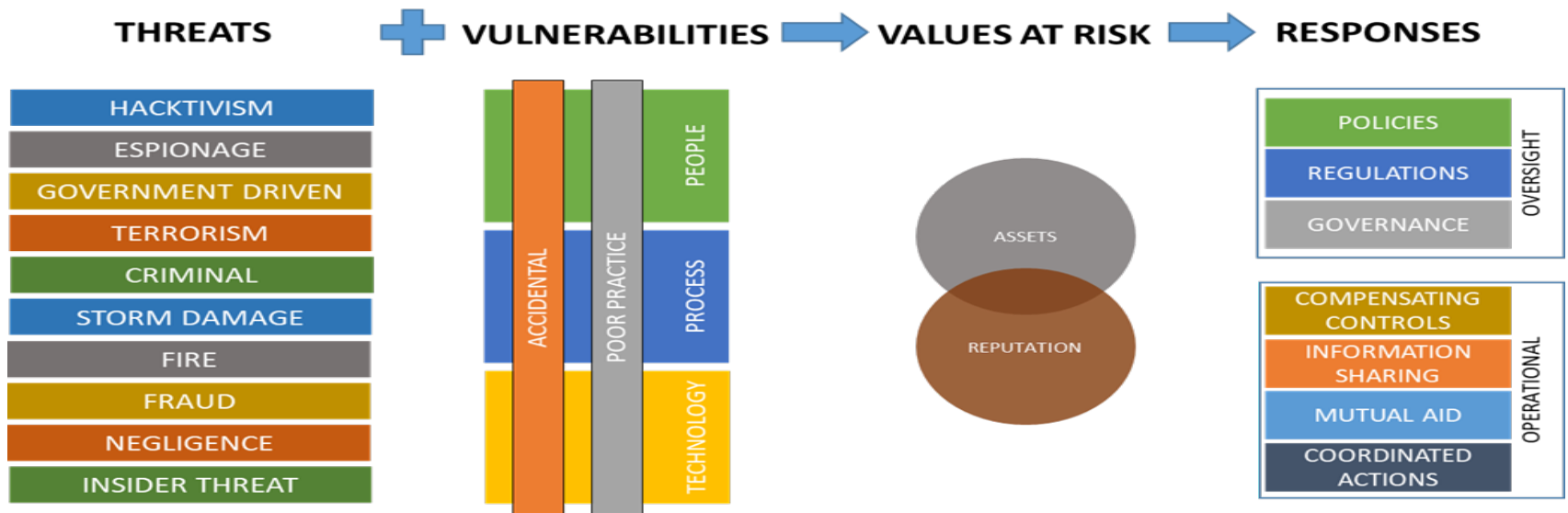
RECOVER

- ▶ Recover planning
- ▶ Improvements
- ▶ Communications

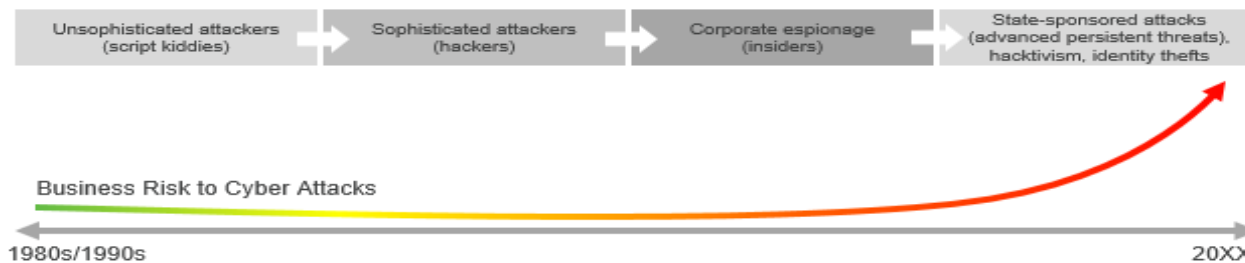


Understanding Cyber Risks (SERS=100%, Threats=1x)

➤ Focus on threats impacting confidentiality, integrity, or availability of SERS data & systems



➤ SERS is defending itself against well-funded and highly capable threat actors.



Cyber risks continue to increase as response times decrease

Information Security & ERM – Core Responsibilities



Awareness and Education



Policy Management



Security Governance



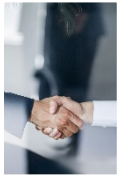
Identity and Access Management



Risk Assessment



Vulnerability Management



Vendor Management



Regulatory Compliance



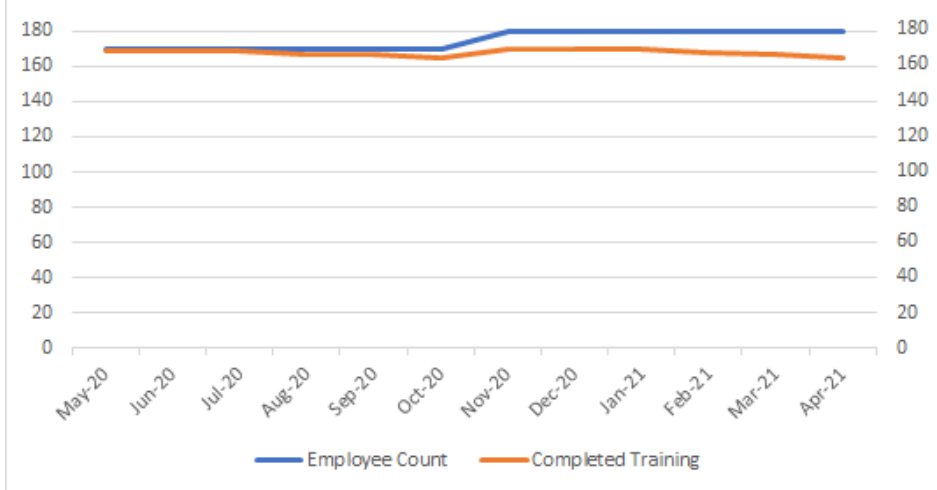
Incident Response



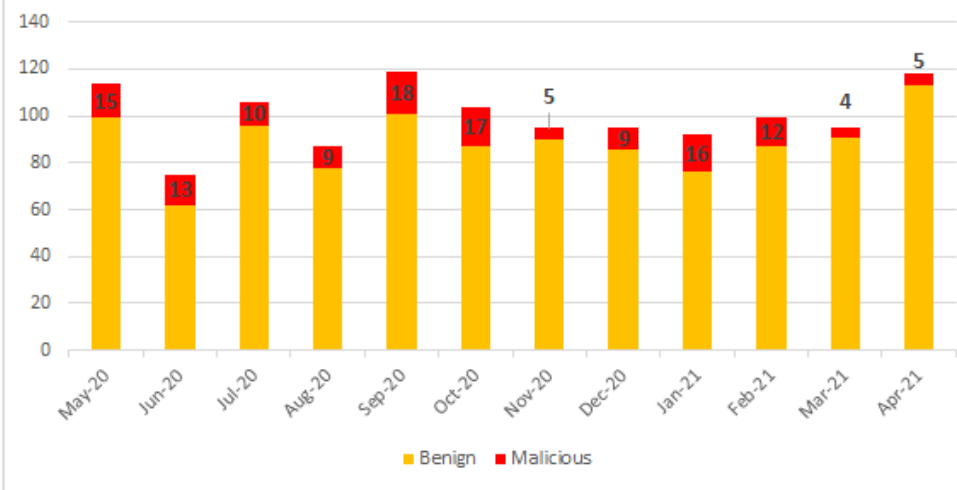
Business Continuity and Disaster Recovery Management

Information Security – Metrics & Measures

Monthly InfoSec Training Participation



Phish Reporter



Dashboard - All Web Applications

Viewing: Wed 21 Apr 2021 - Fri 21 May 2021

All Web Applications | Last 30 days

Total Alerts: **70.4K** (HIGH: 39.4K, MED: 2.19K, LOW: 28.8K)

Activity Timeline

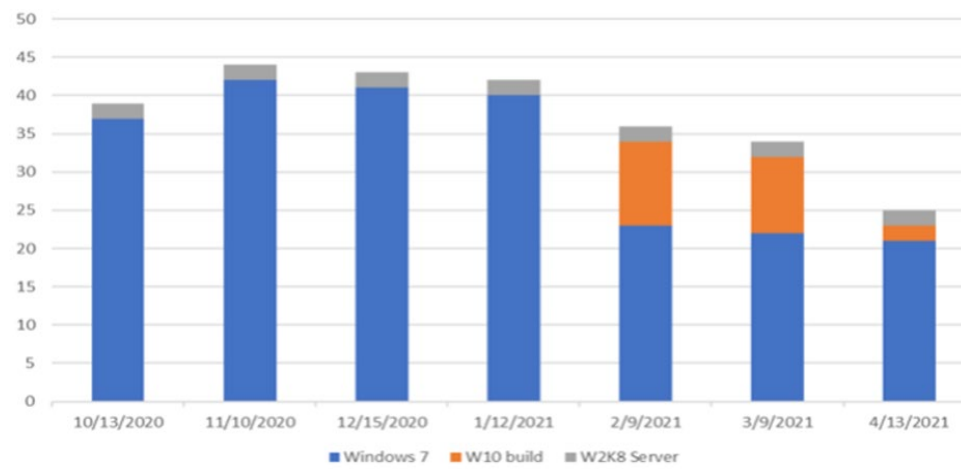
Web Application Statistics

- Hits: **1.87M**
- Blocked Events: **41.1K**
- Client Bandwidth: **8.3 GB**

Event Summary

Top Events Traffic Origins

End of Life OS



Cybersecurity measurement and monitoring will continue to improve to help identify trends and better direct resources

3-Year Information Security Plan



Improving existing processes

- ❖ Awareness & Training - monthly videos, quarterly phishing, frequent articles
- ❖ Implementing Metrics & Monitoring

FY2021 Key Activities

- ❖ Procured and implemented organizational digital signature solution and bulk email security enhancements
- ❖ Vulnerability security scans (applications and hardware) to identify, monitor and report on resolution
- ❖ Improved security with tools for password management, data and system access, device monitoring, financial data exchange, disability HIPAA data transfer, denial of service attacks, OHSERS website
- ❖ Partner with IT on Microsoft Office 365 security framework design review and security enhancements addressing November 2019 system outage
- ❖ Implement a micro-segmentation tool to help prevent data loss
- ❖ Plan security services provider for 24/7 event monitoring and escalation



IS closely aligns with IT staff and leadership - enables security to be positioned at the forefront of new initiatives and emerging risks



QUESTIONS