State of Alaska
Department of Administration

State of Alaska Cyber Security
Presentation to (S) Finance Committee
Bill Smith, Office of Information Technology
4/26/2022

Agenda

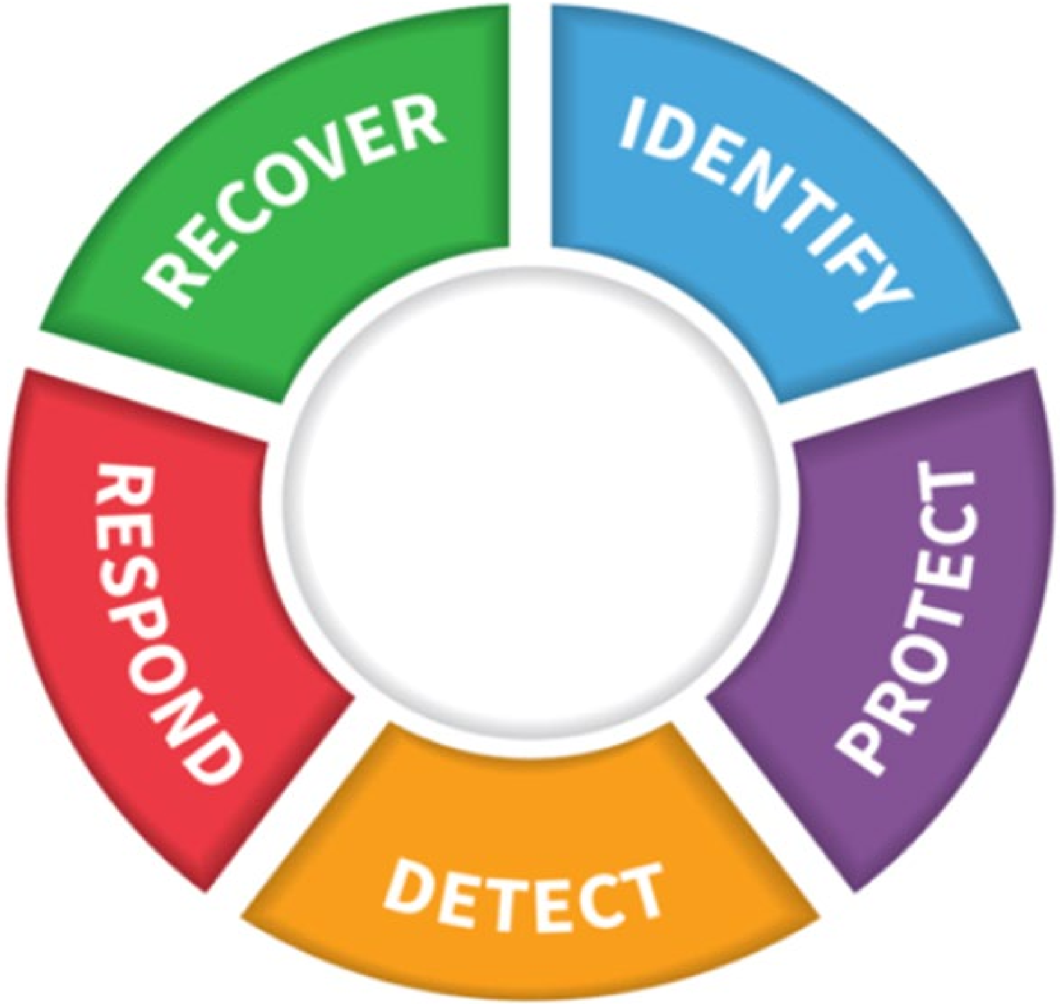
Cyber Threat Landscape

Cyber Security Incident Cost

FY23 Cyber Security Requests

Cyber Security Ecosystem
- **People**
- **Technology**
- **Processes**

Questions



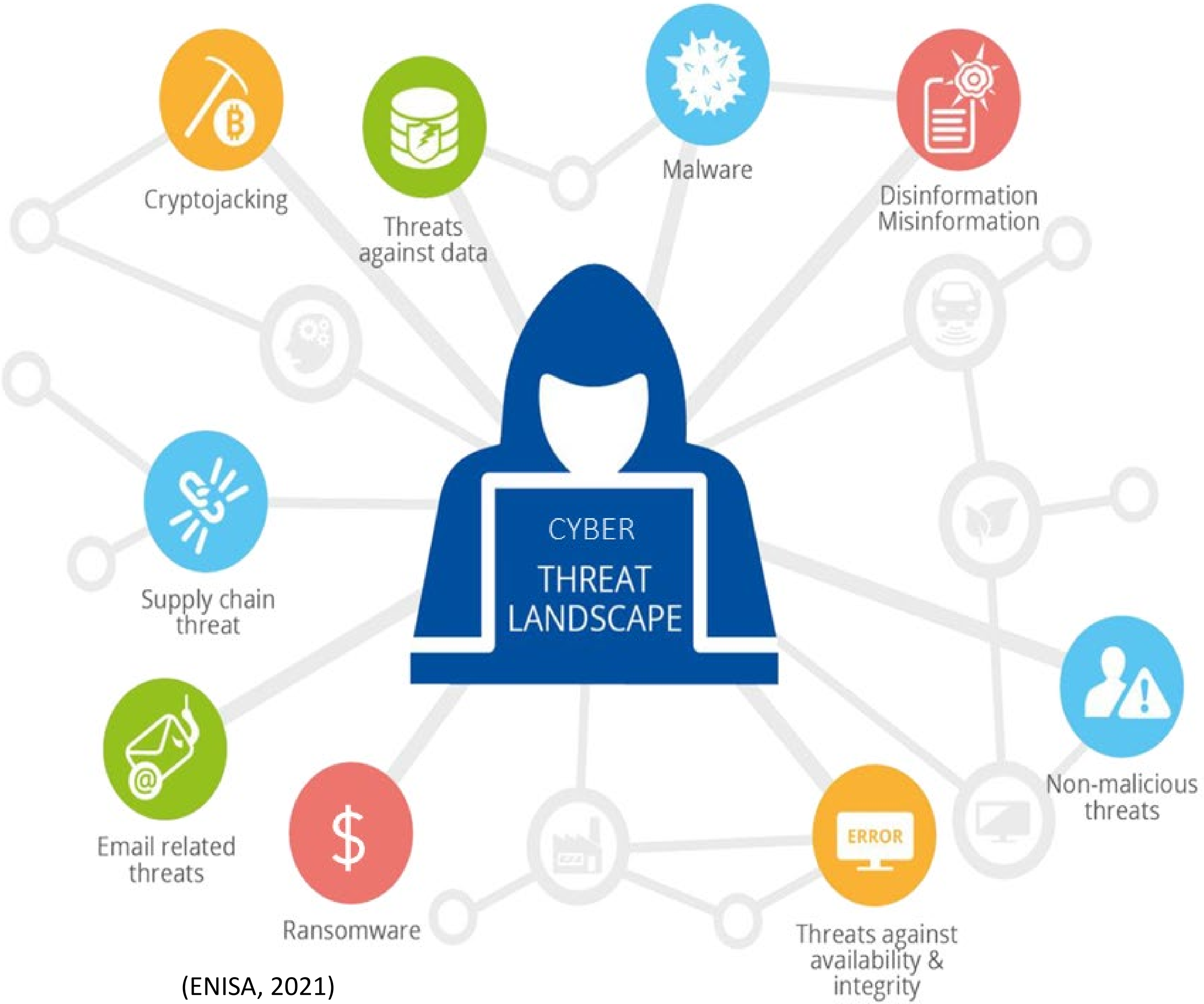
(NIST, 2018)

Cyber Threat Landscape

Threat activity drivers:

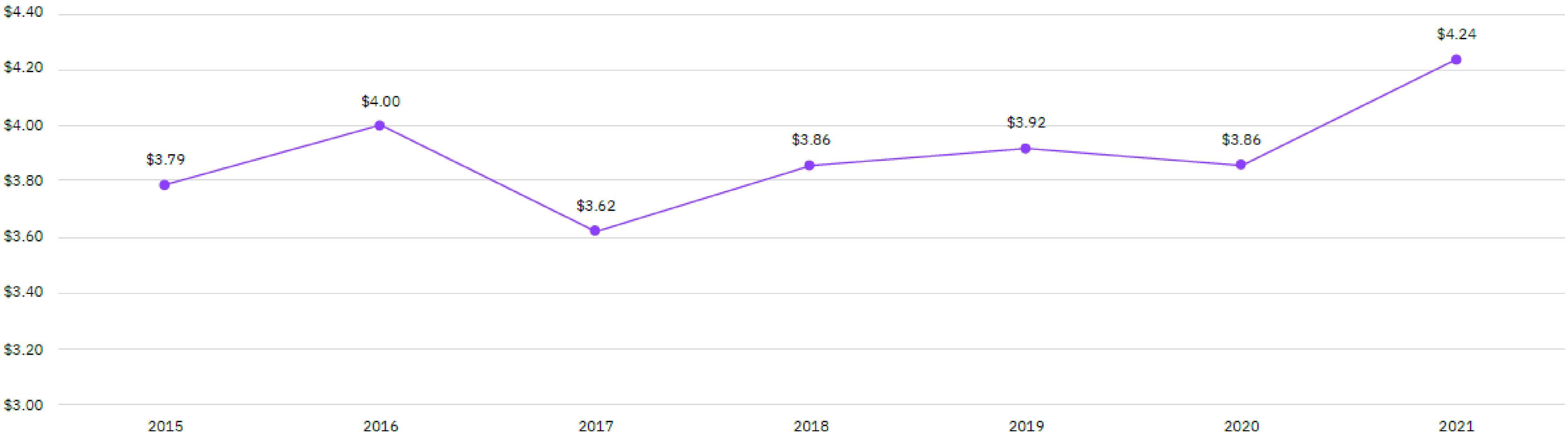
- Cybercrime is a $6 trillion annual industry (Security Magazine, 2021)
- Industrialization and automation of cyberattack capabilities
- Nation state threats
- Supply chain activity
- Pre-existing vulnerabilities

Breaches are no longer just a technical problem...threat awareness is the responsibility of the whole organization.(Gartner, 2021)



(ENISA, 2021)

Cyber Security Incident Cost



Average total cost of a data breach

Measured in US$ millions

The average total cost of a data breach increased by the largest margin in seven years.

Data breach costs increased significantly year-over year from the 2020 report to the 2021 report, increasing from $3.86 million in 2020 to $4.24 million in 2021.

The increase of $0.38 million ($380,000) represents a 9.8% increase. This compares to a decrease of 1.5% from the 2019 to 2020 report year. The cost of a data breach has increased by 11.9% since 2015.

(Ponemon Institute, IBM Security 2021)

FY23 Budget Cyber Security Requests

- **DOA Azure Adoption to Assist with Cloud Migration – $23,116.0** – Obtain professional assistance with State of Alaska migration to the Cloud.

- **DOA Microsoft Security Upgrade – $1,149.0** – Complete implementation of upgraded State Microsoft licensing to better protect employee accounts and data, reduce security expenditures, and allow the State of Alaska to meet common compliance standards.

- **DOA Initiate a 24/7 Security Monitoring Center and Improve Threat Hunting Capabilities – $1,700.0** – Obtain managed 24/7 Security Operations Center (SOC) coverage for a period of 24 months, evaluate SOC requirements for the State to determine enduring requirements and best path forward, and implement internal and/or external capabilities to meet documented cybersecurity requirements.

- **DMVA Homeland Security State and Local Cybersecurity Grant Program - IIJA Division J, Title VI - $2,404.4**

- **DOH Information Technology Security Program Assessment - $1,900.0**

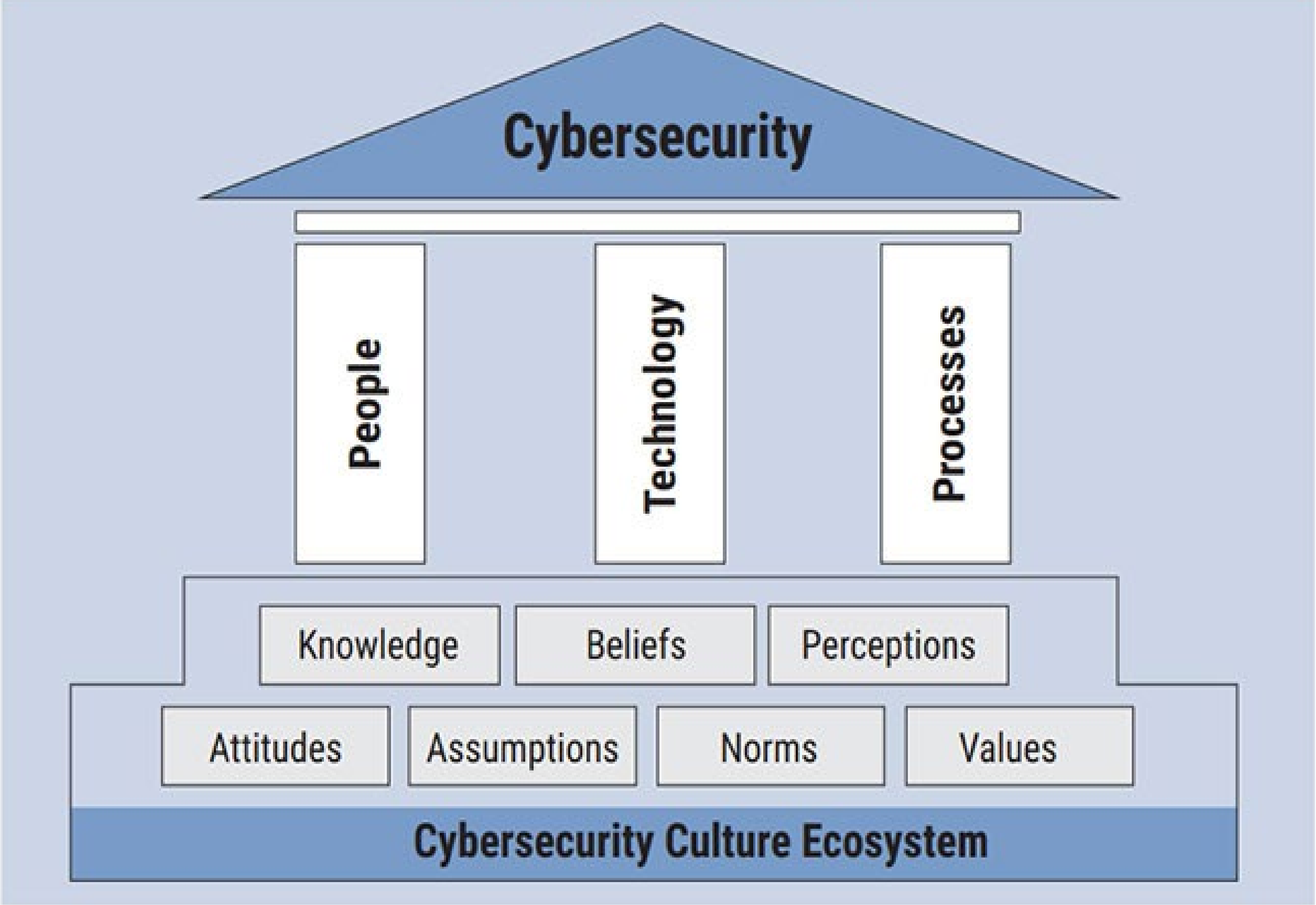
Cyber Security Ecosystem

Cyber security throughout the Information Technology environment:

- **People** - Staff training that creates a culture of security awareness (Annual cyber training)

- **Technology**
  - Network architecture (Cloud Migration)
  - Constantly evolving systems (Security Projects)

- **Processes** - Organization to support compliance and incident response (IT Consolidation)

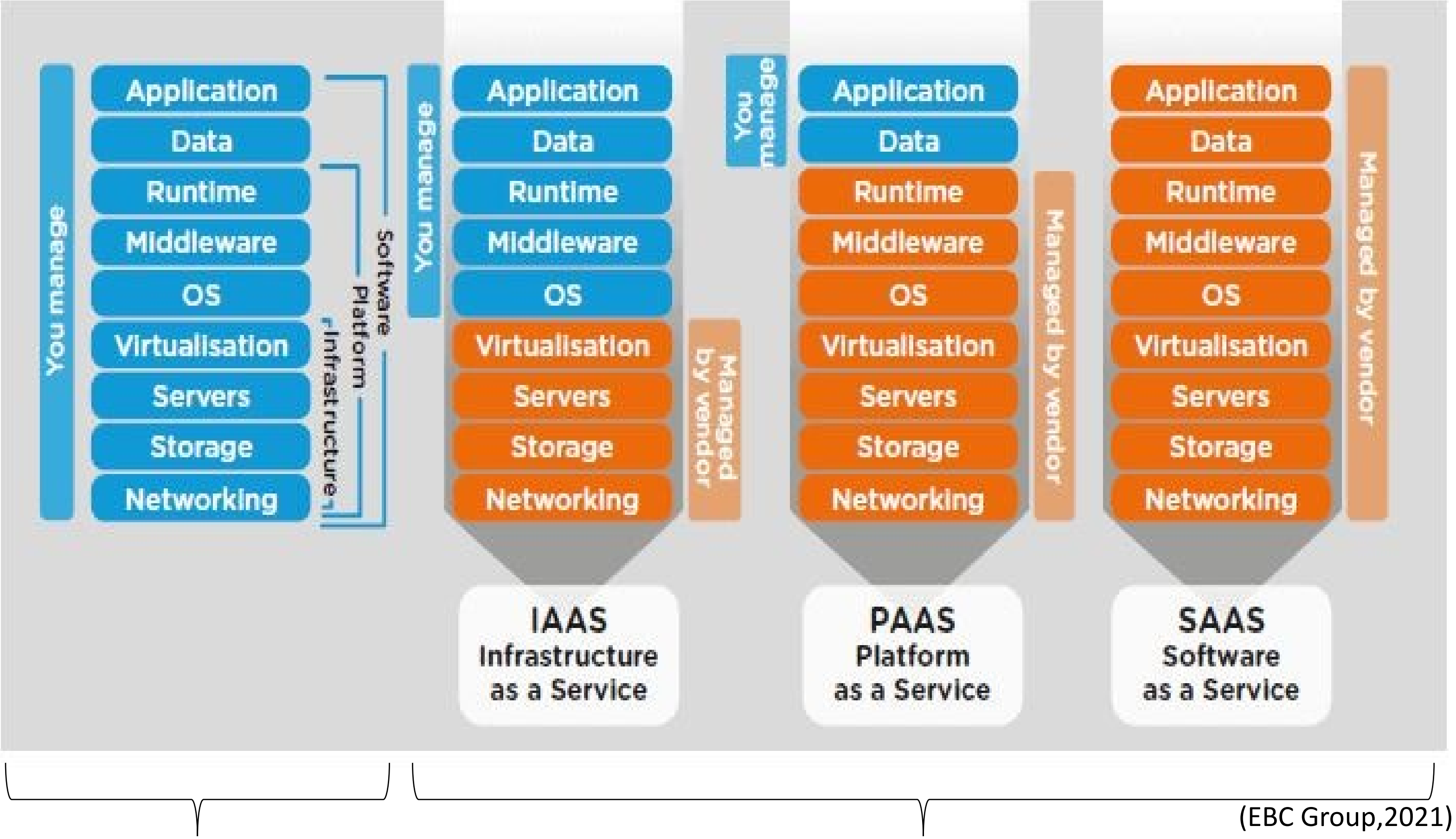


(ISACA, 2019)

Technology - Cloud Migration

Cyber security benefits of cloud migration:

- **Shared Security**
  - Provider secures infrastructure
  - We focus on account and access security
- **Secure Foundation**
  - Modern, continuously updated infrastructure
  - Distributed Denial of Service (DDoS) resistant
- **Built-in security controls**
  - Managed identity and access
  - Always on encryption (data at rest/in transit)
- **Global threat intelligence**



(EBC Group,2021)

'On Premise'

'In the Cloud'

Technology - Cloud Migration

Capital Supplemental Request - $23,116.0 (HB284/SB165)

Project scope

Assess and migrate ~3000 executive branch servers located throughout the state.

- Discovery, development of SOW/timeline, migration services
- Phased large-scale lift-and-shift approach to achieve significant cloud benefit in shortest amount of time
- Complex modernizations deferred until after migration
- Disaster Recovery, Cloud Storage and Operational costs
- Network costs specific to cloud operations

ROI Implications

- **Experience to date:** 93 servers in SOA Azure, with an average cost per server of $1,812/year (25% less than current chargeback rates to departments).
- Industry trends indicate total cost of ownership ROI in 4 to 5 years with an average 21% savings (Gartner, 2021)
- Complexity (1,800+ applications across 60+ locations) and cloud-based options adds significant variability

On Premise alternative

~$39 M over 5 years + Migration Services

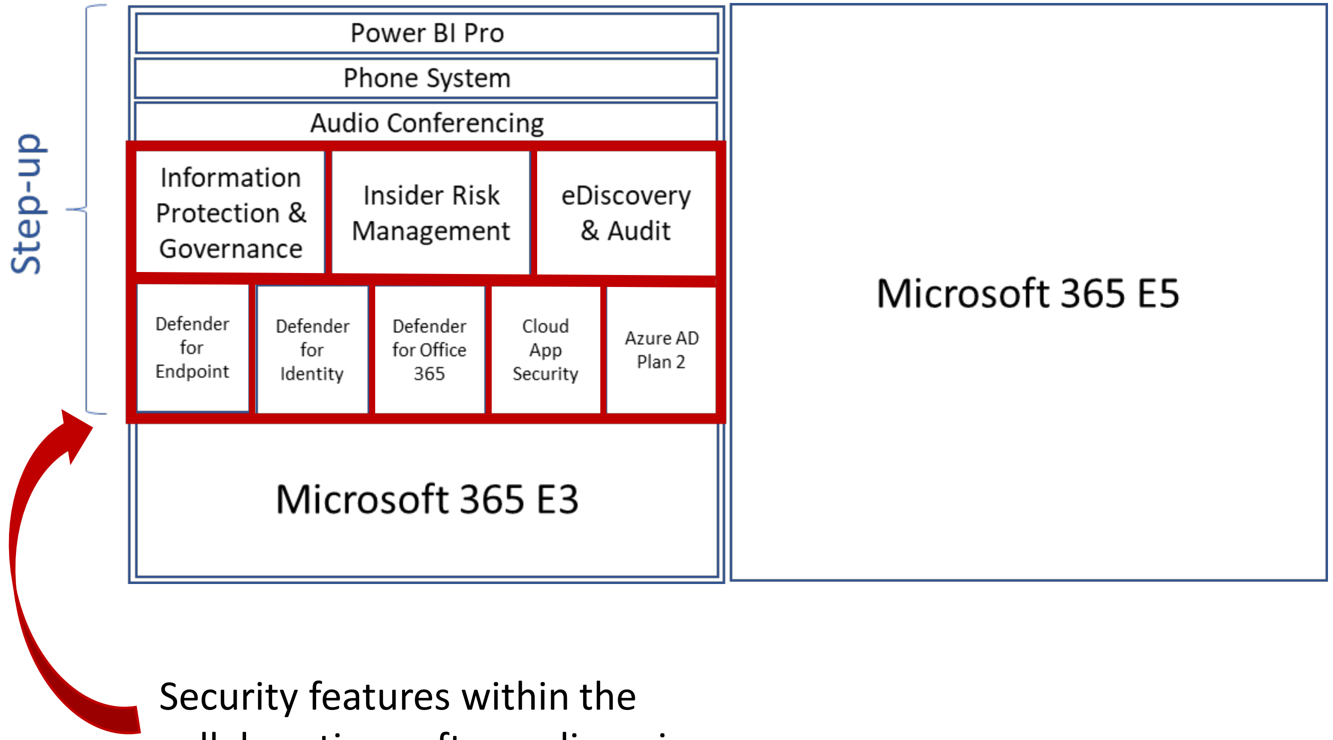
- Consolidate remaining servers (~50%) into primary datacenters
- Update aged infrastructure (expand primary datacenters)
- Procure security systems similar to those offered in cloud environment
- **Does not provide all cloud-based security benefits (DDoS, shared responsibility, etc.)**

Technology – Enterprise Systems

Cyber security benefits of enterprise systems:

- **Microsoft Licensing**
  - Multi-factor Authentication & Conditional Access
  - Endpoint/Mobile Device Management and patching
  - Defender Suite (desktop, email, identity)
  - Identity management

- **Managed Security Operations integration**
  - Common system avoids one off solutions
  - Fully integrated suite of products informed by worldwide intelligence
  - Creates capacity within SOA security professionals



Step-up

Power BI Pro

Phone System

Audio Conferencing

Information Protection & Governance

Insider Risk Management

eDiscovery & Audit

Defender for Endpoint

Defender for Identity

Defender for Office 365

Cloud App Security

Azure AD Plan 2

Microsoft 365 E3

Microsoft 365 E5

Security features within the collaboration software licensing bundle

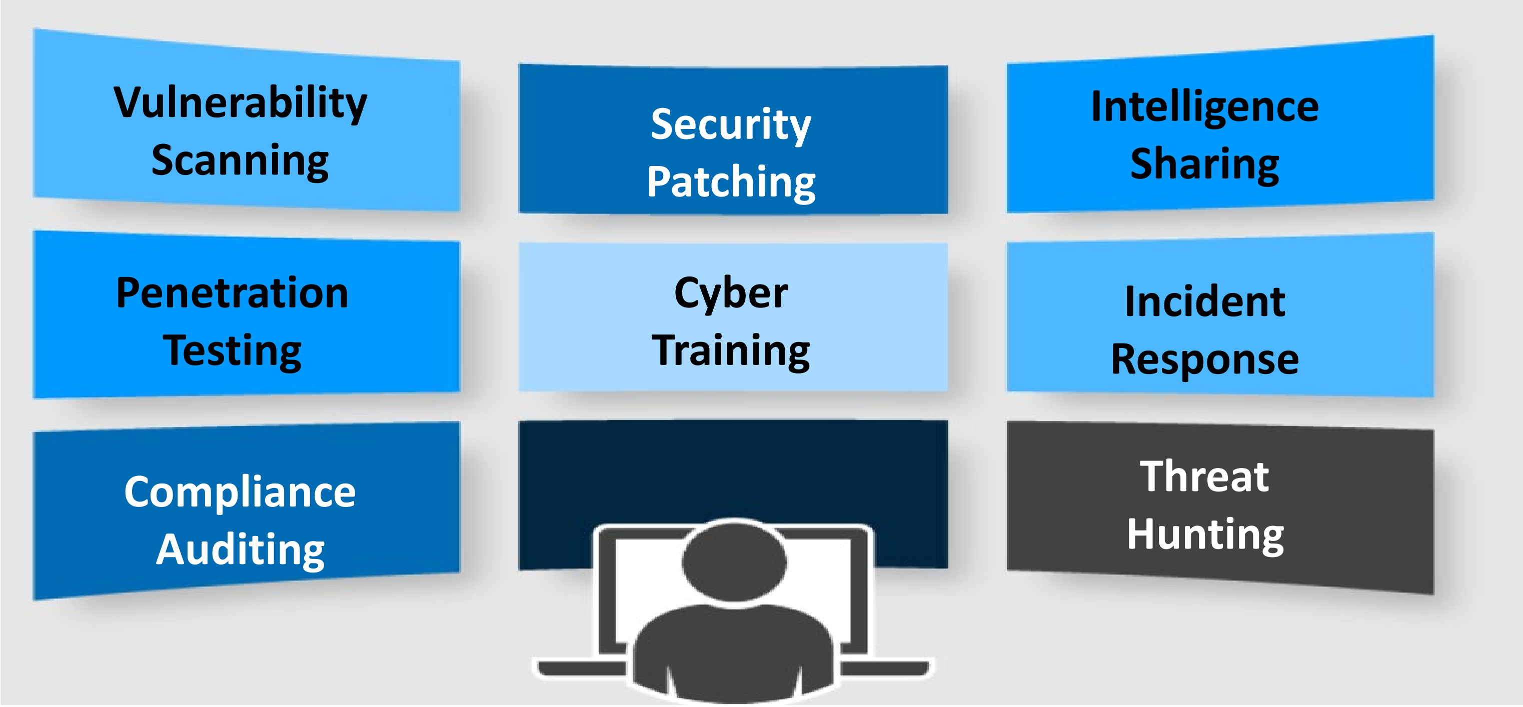
Infrastructure Bill Requests:

- Security tool implementation - $1,149.0
- Managed Security Operation Center - $1,700.0

Processes – IT Consolidation

Single, focused approach to cyber security

- **Execute basic protocols well**
  - Practice good cyber hygiene
  - Ensure Compliance
  - Enhance response capabilities
  - Immediate threat hunting against security threats
- **Simplify the enterprise security environment**
  - Speed and efficiency of incident response
  - Integrated systems avoid gaps in coverage
- **Continue the path to Zero Trust**
  - Assume breach
  - Verify explicitly
  - Least privileged access



(EfficentIP,2020)

Most states indicate that a **centralized** operating model can best reduce cybersecurity risk (Deloitte & NASCIO,2020)

Questions

Department of Administration

Championing improvement in the State’s performance and results.

For more information, please contact Ken Truitt at ken.truitt@alaska.gov

Background Slides

References

1. NIST Cybersecurity Framework, The Five Functions of the Cybersecurity framework. NIST.,2018.

2. Security Magazine. The new threat economy: A guide to cybercrime’s transformation – and how to respond, Brown, L., 2021

3. Gartner, The Urgency to Treat Cybersecurity as a Business Decision, Proctor, P., 2021.

4. ENISA, Threat Landscape 2021, ENISA,2021

5. Ponemon Institute, IBM Security” IBM Security – Cost of a Data Breach“, 2021

6. ISACA, Implementing a Cybersecurity Culture. ISACA, 2019.

6. EBC Group, On Premises vs Cloud, EBC Group, 2021.

7. EfficientIP. IPAM For Microsoft DNS and DHCP servers Simple, Secure And Unified Management. EfficientIP, 2020

8. Deloitte & NASCIO, “2020 Deloitte–NASCIO Cybersecurity Study States at risk: The cybersecurity imperative in uncertain times”, 2020.