Oregon Department of Justice

Ellen F. Rosenblum, Attorney General

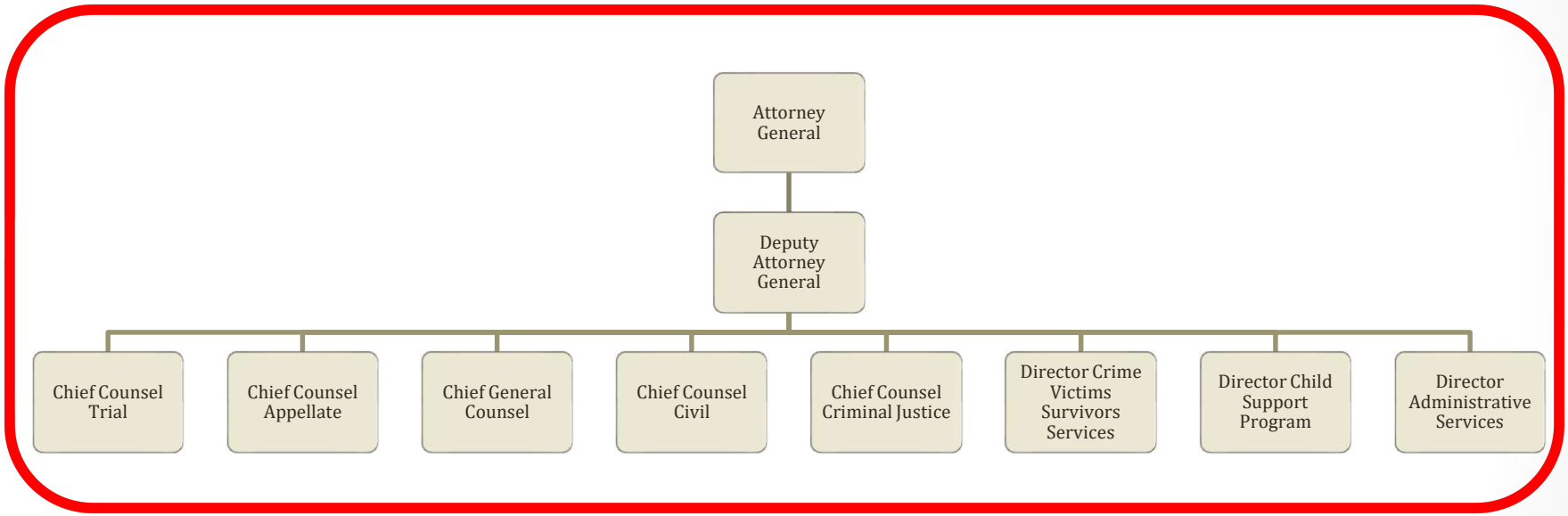
Information Security Report

2021 Joint Legislative Committee on Information Management and Technology

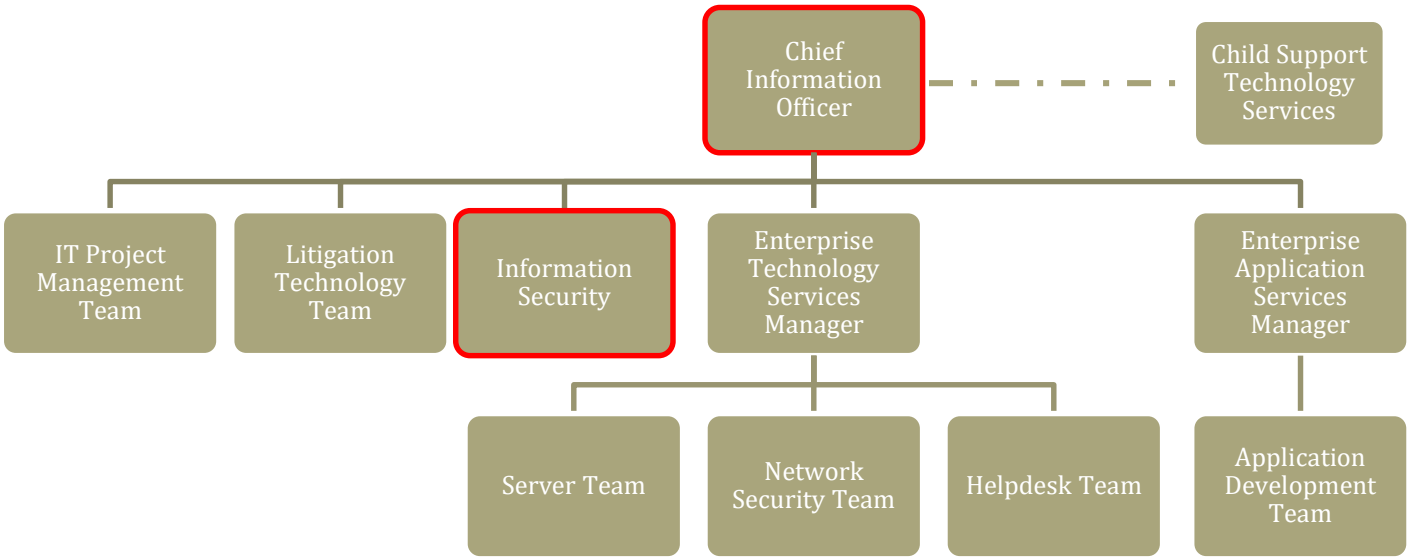
June 2, 2021

Richard Rylander, Chief Information Officer
Anthony Mingus, Information Security Officer

DOJ Security Oversight



DOJ IT Organization



FTE: 45 DOJ IS with 25.5% able to retire within 5 years

FTE: 22 Child Support with 29.4% able to retire within 5 years

Information Security Program

- ✓ Information Security Policy and Procedures
- ✓ Information Security Solutions
- ✓ Vulnerability/Penetration Assessments & Testing
- ✓ Regulatory Audit Management
- ✓ Regulated Data Compliance
- ✓ Security Incident Response Management
- ✓ Security Awareness Training
- ✓ State-wide Information Security Collaboration

1 Dedicated Information Security Officer with overall responsibility for the Information Security Program

44 Staff providing technology support and solutions for the business that comply with regulatory requirements and information security best practices

DOJ Security Layers

People

- First Line of Defense
- Security Awareness
- Role Based Access

Computers

- Patching
- Data Loss Prevention
- Security Policy
- Encryption

Network

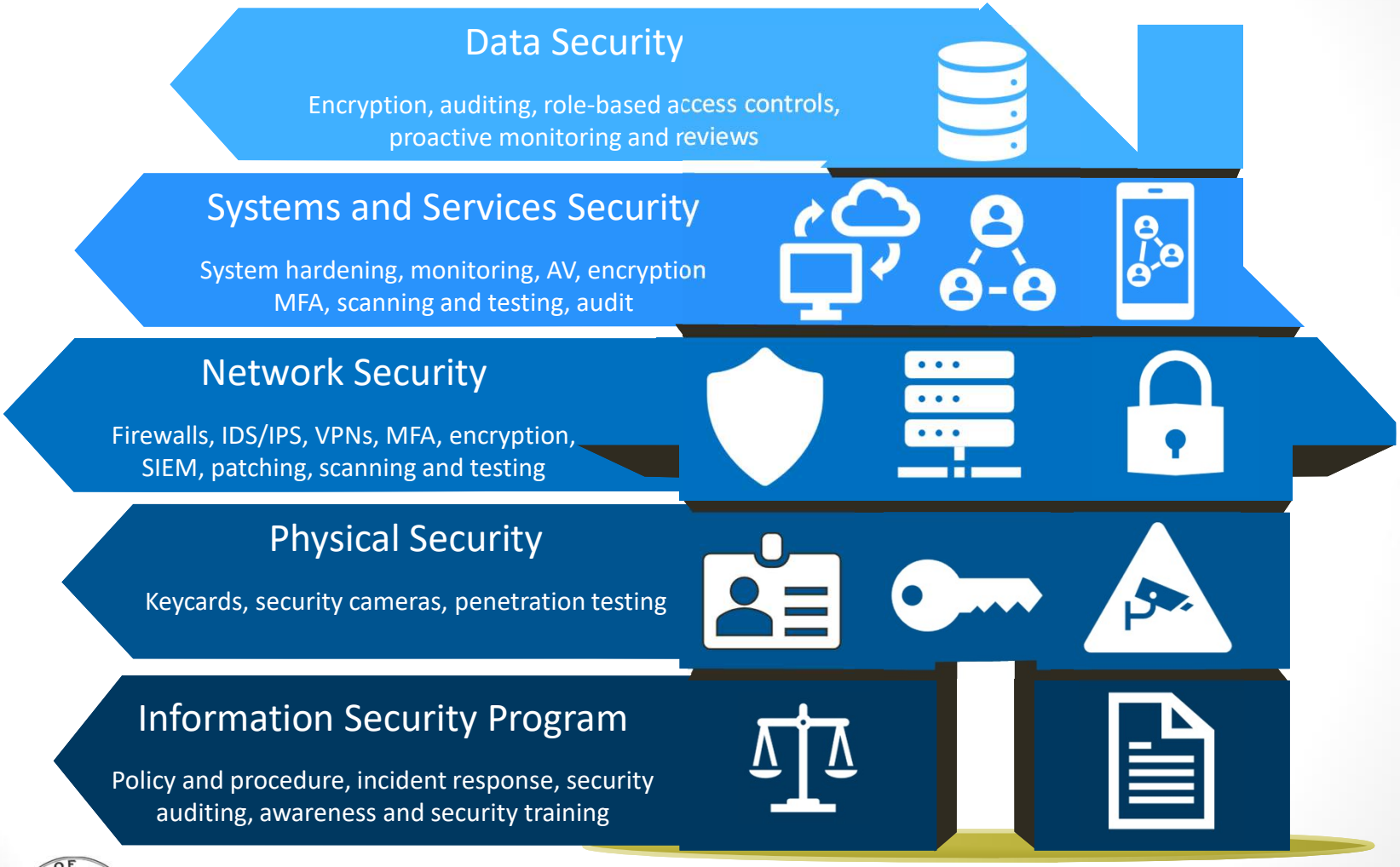
- Patching
- Identity Service
- Partner Access
- IDS/IPS
- Encryption

Servers

- Patching
- Data Access
- Data Security
- Security Policy
- Encryption

End-to-End Multifactor Authentication

DOJ Defense in Depth



COVID-19 Security Statistics

Security Border Stats

- ✓1.5 Billion dropped attacks
- ✓1,090 Network malware attacks blocked
- ✓1,692 Relevant attacks
  - ✓Privilege escalation
  - ✓Protocol subversion
  - ✓Network trojan
  - ✓Spyware/adware
  - ✓Admin account attacks

Internal Security Systems

- ✓16,471 Alerts
  - ✓10,324 malware objects blocked
  - ✓6,147 behavior-based action blocks
- ✓ 6,500 quarantined files
- ✓ 5,962 cleaned files
- ✓ 4,005 false positives (after review)
- ✓4 files deletions

Mail Security

- ✓1.2 Million blocked phishing attacks
- ✓8,600+ Blocked virus/malware attacks
- ✓300+ Blocked zero-day attacks
- ✓2.2 Million emails encrypted

Top Attacks

- ✓Phishing/Spear Phishing
- ✓Privilege Escalation/Exploits
- ✓Password Stealers (Trojans)
- ✓Code Injection
- ✓Brute Force

Cost of a Data Breach

- The average cost of a data breach is $3.86 million. Healthcare breaches average $7.13 million. (IBM/Poneman 2020)
- The most expensive component of a cyber attack is information theft, which represents 43 percent of costs. (Accenture)
- Cybercrime to cost the world $10.5 trillion annually by 2025. (CyberSecurity Ventures 2021)
- The 2017 Equifax breach cost the company over $1.4 billion plus legal fees. (WABE)
- The most expensive breach was Epsilon in 2011 costing the email communications firm $4 billion. (Firmex)
- Malware and web-based attacks are the two most costly attack types — companies spent an average of US $3.7 million in defense ($2700 per employee). (Accenture 2021)

DOJ IT Security Accomplishments 19-21

- ✓ **Independent 3rd Party Security Assessment**
  - ✓ DOJ External Web Systems
  - ✓ DOJ Origin System
  - ✓ DOJ Multifactor Authentication System
  - ✓ DOJ SolarWinds
  - ✓ DOJ Email System

- ✓ **Enhanced audit and log management**
  - ✓ Security Information Event Management System
    - ✓ Increase security visibility
    - ✓ Automate security alerts

- ✓ **Data and secure data sharing with agencies and partners**

DOJ IT Security Accomplishments 19-21

- ✓ **Security awareness**
  - ✓ Implemented Phishing Awareness Program
  - ✓ Continue awareness campaign and staff security training
- ✓ **Implemented and Validated DOJ's Multifactor Security and Federated Identity** on all DOJ external authentication sites for DOJ staff including Outlook Web Access, SharePoint, and third-party solutions such as Smartsheet and KnowBe4
  - ✓ 3rd party assessment performed on DOJ's end-to-end multifactor authentication solution
  - ✓ This is in addition to ALL DOJ computers requiring multifactor authentication to access the DOJ network
- ✓ **Continued US DHS external monitoring of DOJ external systems**
  - ✓ At no cost to the State of Oregon

DOJ IT Security Accomplishments 19-21

- ✓ **Implemented Advanced Posture Checking** on DOJ VPN connections supporting remote work for DOJ, District Attorney Child Support, and Partner staff
- ✓ **Implemented Automated Security and Patch Management Assessments** of all DOJ servers, laptops, network hardware, and computers
- ✓ **Implemented Quarterly Phishing** assessments and training through KnowBe4
- ✓ **Enhanced End to End Vulnerability and Patch Management** scanning of all DOJ workstations, laptops, servers, and network devices through Qualys.

DOJ IT Security Strategy 21-23

- ✓ Homeland Security 24/7 vulnerability assessment
  - ✓ External systems tested 24/7 – At no cost to the State of Oregon
- ✓ Add ShadowServer external assessments
  - ✓ 24/7 external vulnerability scanning - At no cost to the State of Oregon
- ✓ Independent 3rd party security assessment
  - ✓ End-to-End Penetration Test of DOJ network
- ✓ Research micro-segmentation for zero trust implementation
  - ✓ Servers, network, desktops, laptops, applications, and printers

DOJ IT Security Strategy 21-23

- ✓ Security Awareness Program
  - ✓ Using KnowBe4 security trainings
  - ✓ Continue Quarterly Phishing Tests using KnowBe4
- ✓ CIS Secure Suite Third Party Audit
  - ✓ CIS Top 20 Security Controls
  - ✓ CIS Benchmarks for security control application
- ✓ IT staff information security and skill training (ongoing)

DOJ Security Posture

- **To protect critical data and to maintain a strong security posture:**
  - ✓ **We must continuously** enhance our Defense In Depth**.**
  - ✓ **Information Security must** encompass and wrap around everything we do.
  - ✓ **Information Security Governance is** held at the highest level of DOJ with our Executive Team.
  - ✓ **Information Security is** built into our core values, and we invest in it.

With the increasing levels of sophistication in cyber attacks, coupled with employees who have ready access to agency data, it is no longer a question of ***if*** but ***when*** a data breach will occur. *In spite of all the preventative measures we have in place, being prepared for the inevitable with an incident response plan is perhaps the most important component of all.*

Data Breaches Are Not IF but WHEN

Questions?