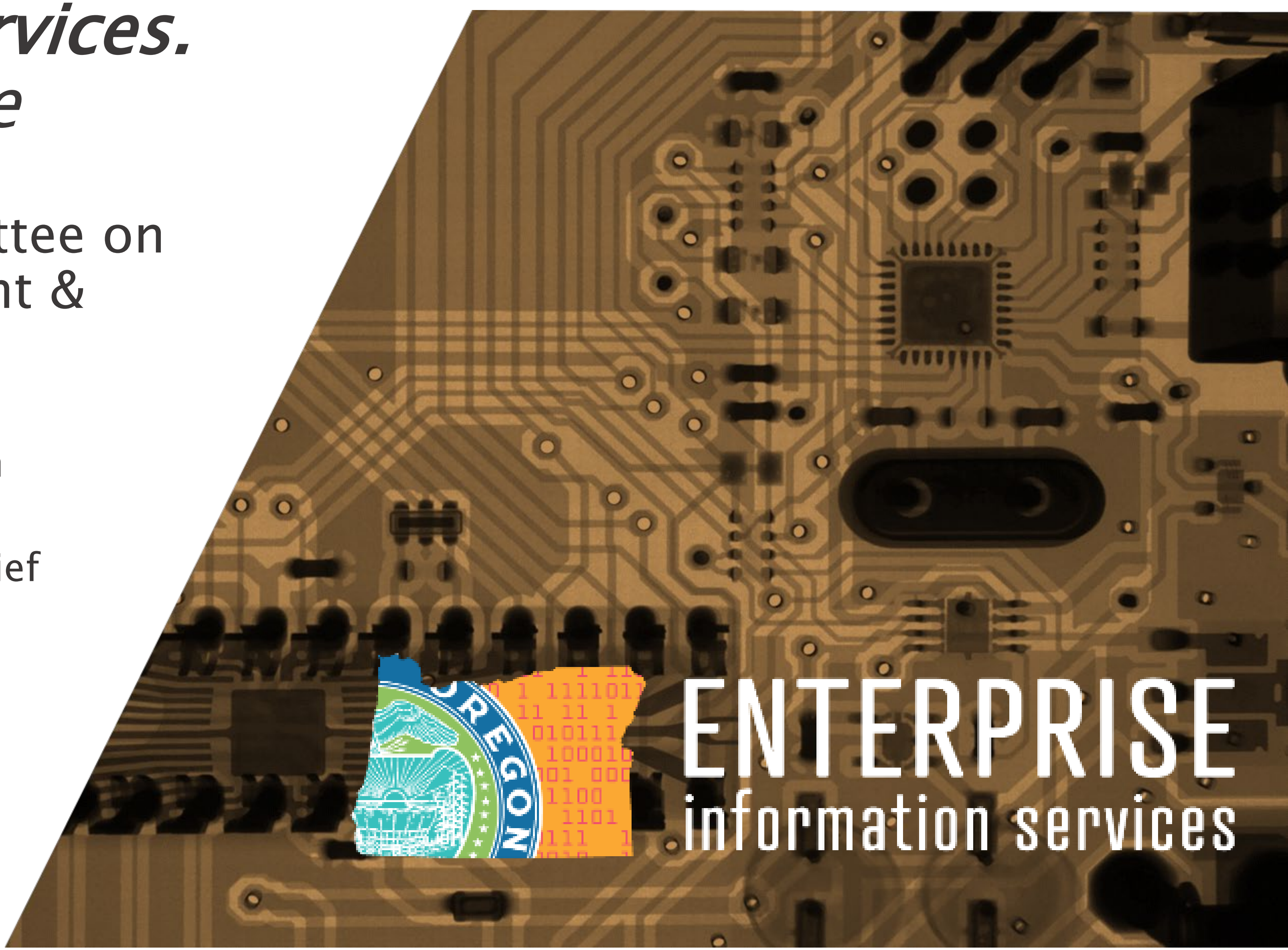
Cyber Security Services.
Unification Update

Joint Legislative Committee on Information Management & Technology

Gary Johnson, Chief Information Security Officer

Annalise Famiglietti, Deputy Chief Information Security Officer

2 June 2021



Cyber Security Unification

Cyber Security Services. *Overview*

GARY JOHNSON
Cyber Security Services

Chief Information Security Officer

Cyber Security Services brings together enterprise security - governance, policy, procedure and operations - under a single, accountable enterprise organization. This allows for end-to-end direction setting and execution for enterprise security.

ANNALISE FAMIGLIETTI
Cyber Security Services

Deputy Chief Information Security Officer

- **Policy.** Setting enterprise security policy and standards
- **Solutions.** Partnering with Strategy & Design to drive enterprise security architecture
- **Services**. Delivering on day-to-day enterprise security operations
- **Security Operations Center.** Providing dedicated, real-time security monitoring and response for enterprise operations
- **Consulting.** Provide cyber security consulting services to executive branch agencies

Cyber Security Services. *Unification*

- **Current State Assessments.** Engaged Deloitte, Gartner, and KPMG to gauge the culture of CSS and the overall IT security posture of the state
- **Firewall Replacement.** Deployed Next-Gen Firewall Capabilities
- **CSS Priorities.** Assessments informed the EIS Strategic Framework for 2020-2023

- **RACI + Service Catalog.** Used Gartner to facilitate agency engagement—clarifying IT security roles and responsibilities with a RACI Matrix and CSS Service catalog

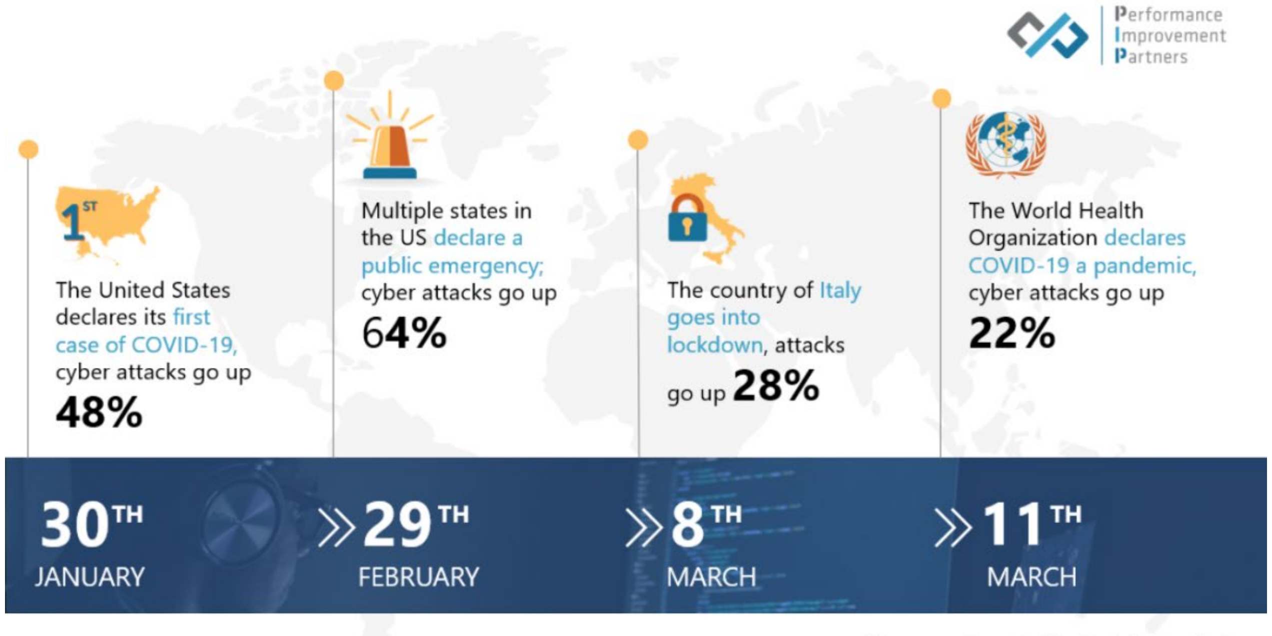
CSS Accomplishments

2019–21

ENTERPRISE
information services

CSS Highlights – Pandemic Response

- Increased VPN capacity for increased telework
- MFA rolled out statewide
  - VPN and M365
- Oregon Emergency Management Support
  - Participated in joint effort to improve Fusion/OEM cyber incident reporting procedures
  - Participated on the Statewide TIGER team to ensure 2020 election security
- 100% CSS staff working from home
- COVID drove exponential threat spike
  - And exploited new technology



30TH JANUARY: The United States declares its first case of COVID-19, cyber attacks go up 48%

29TH FEBRUARY: Multiple states in the US declare a public emergency; cyber attacks go up 64%

8TH MARCH: The country of Italy goes into lockdown, attacks go up 28%

11TH MARCH: The World Health Organization declares COVID-19 a pandemic, cyber attacks go up 22%

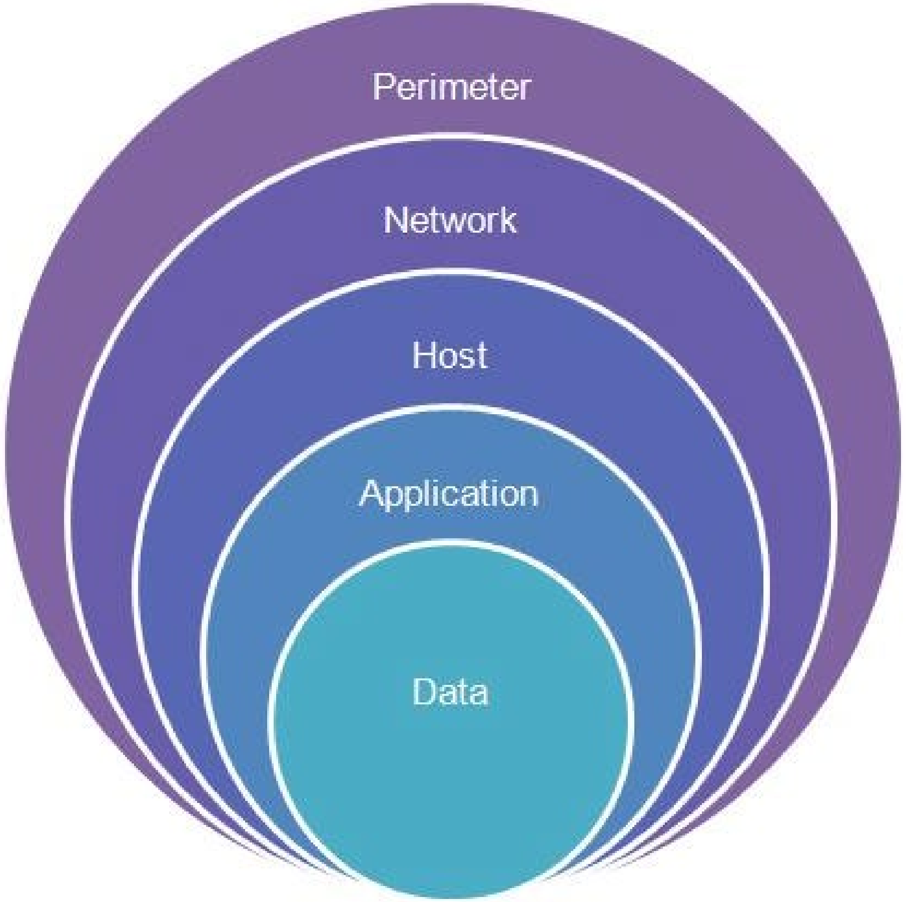
Data source: Computer Weekly via Carbon Black

CSS Highlights – Internal Focus

- Firewall lifecycle replacement
- Web Application Firewalls
- Security Information and Event Management
  - Migrated Integrated Eligibility SIEM from DHS|OHA to CSS
  - Added new capability for "Network Threat Detection”
  - Life cycle replacement upgrade
  - Health check of SIEM.
- Network Intrusion Prevention
- Network Performance Monitor Suite
- Network and Security Modernization Project
  - RFP in progress

CSS Highlights – External Focus

- Microsoft 365 effort
    - Developing roadmap for E5 Security Suite
        - Intune Mobile Device Management (MDM)
        - Advanced Threat Protection (ATP)
        - Security and Compliance Center/Secure Score
        - Data Loss Prevention
- CSS Service Catalog/RACI
- Critical\Compliance Infrastructure Logging
    - Scope determined
    - Business case completed
- Information Risk Management
    - RFP in process
    - Preparing to start contract negotiation with chosen vendor
- DNS Filtering
    - All DCS DNS customers
    - Adding non-DCS agencies
- Provided Albert sensors for all Oregon counties that chose to participate
    - All but 4



State of Oregon Albert Adoption By County

June 1, 2021

24x7x365 Network Monitoring Service

🟩 Albert Online

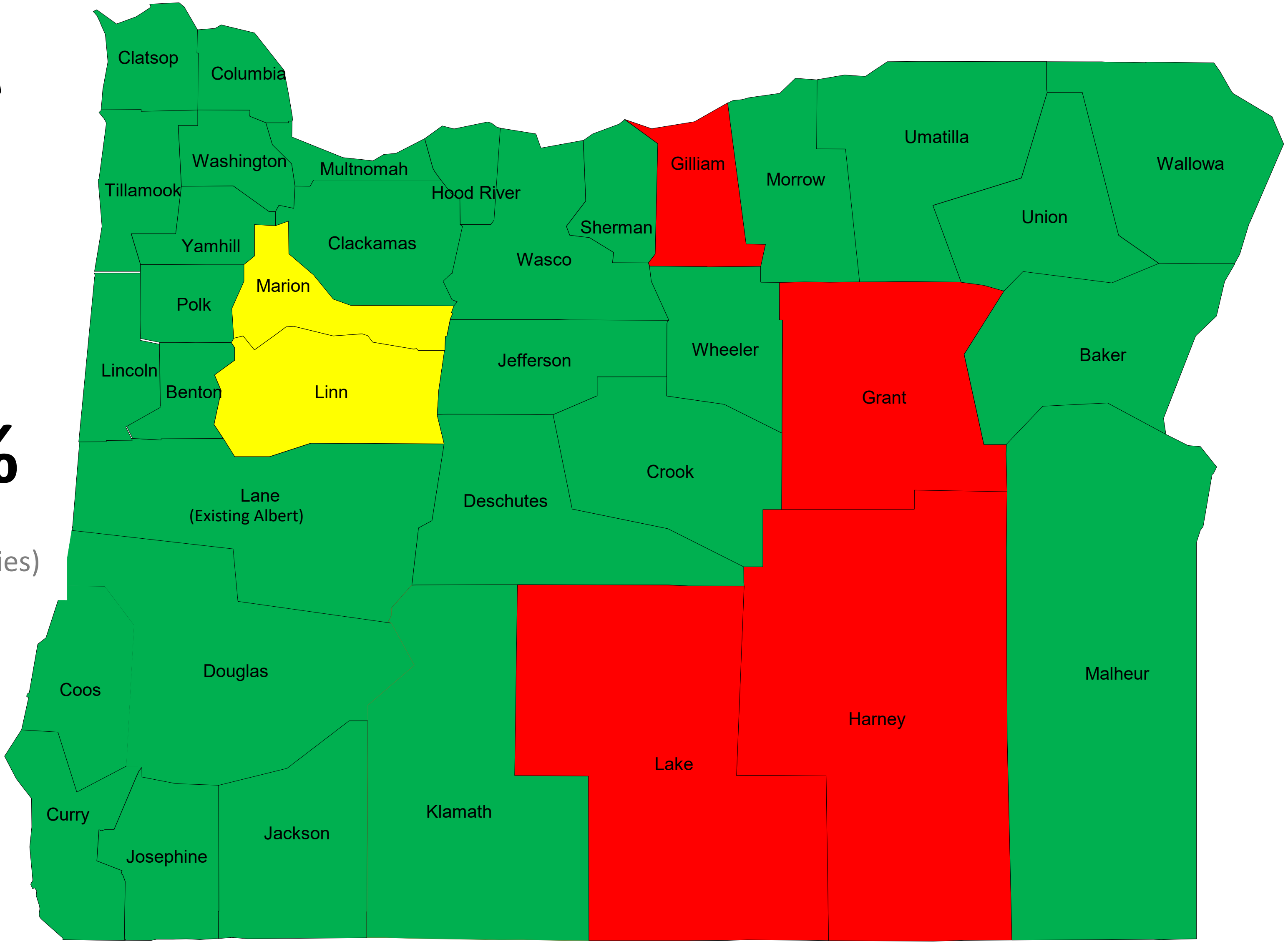
🟥 Declined Offer

🟨 Installation Pending

Coverage by Percentage of Population: **99.4%**

(includes Marion and Linn Counties)

Thirty (32) counties accepted the offer by Oregon state government to deploy a network security monitoring service offered by the Center for Internet Security (CIS) through the Multi-State Information Sharing and Analysis Center (MS-ISAC). This service is being provided/offered to all Oregon counties at no cost to them.

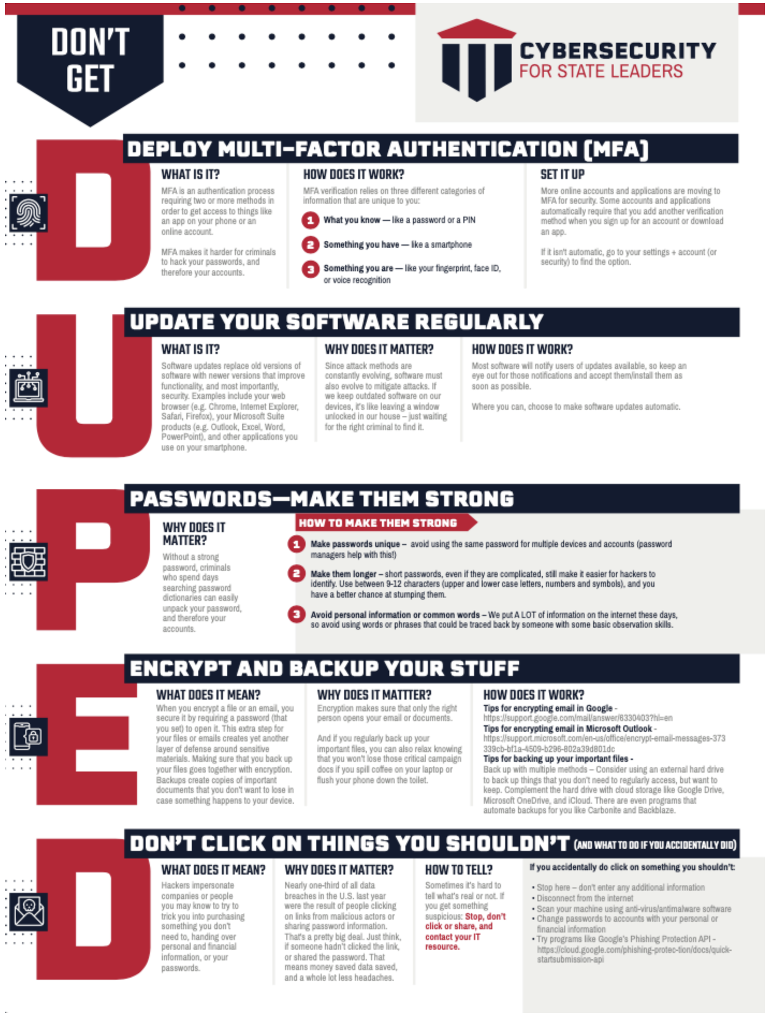


CSS Highlights – Education

- Awareness & Training:
  - Updated Awareness program for 2021 to include a security miniseries for the year
  - Ability to test out of the Annual Security training, this change was based on feedback from users and our workgroup
- Developed reusable SIEM training content for support staff with vendor.
- Entire Security Infrastructure team completed Certified Network Security Administrator firewall training
  - Staff are obtaining certification

CSS Highlights – Education: Cybersecurity for State Leaders

- Partnered on Cyber Security Training for State Leaders
- The ecosystem of cybersecurity
- How and why cyber attacks work
- Best practices on how to protect yourself against cyber threats, i.e. how to not get **D.U.P.E.D.**:
  - **D**eploy multi-factor authentication
  - **U**pdate software regularly
  - **P**asswords – make them strong!
  - **E**ncrypt files/folders, and backups
  - **D**on’t click on things you shouldn’t (and what to do if you accidentally do!)



DON'T GET

CYBERSECURITY FOR STATE LEADERS

DEPLOY MULTI-FACTOR AUTHENTICATION (MFA)

WHAT IS IT?

MFA is an authentication process requiring two or more methods in order to get access to things like an app on your phone or an online account.

MFA makes it harder for criminals to hack your passwords, and therefore your accounts.

HOW DOES IT WORK?

MFA verification relies on three different categories of information that are unique to you:

1. **What you know** — like a password or a PIN
2. **Something you have** — like a smartphone
3. **Something you are** — like your fingerprint, face ID, or voice recognition

SET IT UP

More online accounts and applications are moving to MFA for security. Some accounts and applications automatically require that you add another verification method when you sign up for an account or download an app.

If it isn't automatic, go to your settings + account (or security) to find the option.

UPDATE YOUR SOFTWARE REGULARLY

WHAT IS IT?

Software updates replace old versions of software with newer versions that improve functionality, and most importantly, security. Examples include your web browser (e.g. Chrome, Internet Explorer, Safari, Firefox), your Microsoft Suite products (e.g. Outlook, Excel, Word, PowerPoint), and other applications you use on your smartphone.

WHY DOES IT MATTER?

Since attack methods are constantly evolving, software must also evolve to mitigate attacks. If we keep outdated software on our devices, it's like leaving a window unlocked in our house – just waiting for the right criminal to find it.

HOW DOES IT WORK?

Most software will notify users of updates available, so keep an eye out for those notifications and accept them/install them as soon as possible.

Where you can, choose to make software updates automatic.

PASSWORDS—MAKE THEM STRONG

WHY DOES IT MATTER?

Without a strong password, criminals who spend days searching password dictionaries can easily unpack your password, and therefore your accounts.

HOW TO MAKE THEM STRONG

1. **Make passwords unique –** avoid using the same password for multiple devices and accounts (password managers help with this!)
2. **Make them longer –** short passwords, even if they are complicated, still make it easier for hackers to identify. Use between 9-12 characters (upper and lower case letters, numbers and symbols), and you have a better chance at stumping them.
3. **Avoid personal information or common words –** We put A LOT of information on the internet these days, so avoid using words or phrases that could be traced back by someone with some basic observation skills.

ENCRYPT AND BACKUP YOUR STUFF

WHAT DOES IT MEAN?

When you encrypt a file or an email, you secure it by requiring a password (that you set) to open it. This extra step for your files or emails creates yet another layer of defense around sensitive materials. Making sure that you back up your files goes together with encryption. Backups create copies of important documents that you don't want to lose in case something happens to your device.

WHY DOES IT MATTTER?

Encryption makes sure that only the right person opens your email or documents.

And if you regularly back up your important files, you can also relax knowing that you won't lose those critical campaign docs if you spill coffee on your laptop or flush your phone down the toilet.

HOW DOES IT WORK?

Tips for encrypting email in Google - https://support.google.com/mail/answer/6330403?hl=en
Tips for encrypting email in Microsoft Outlook - https://support.microsoft.com/en-us/office/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc
Tips for backing up your important files - Back up with multiple methods – Consider using an external hard drive to back up things that you don't need to regularly access, but want to keep. Complement the hard drive with cloud storage like Google Drive, Microsoft OneDrive, and iCloud. There are even programs that automate backups for you like Carbonite and Backblaze.

DON’T CLICK ON THINGS YOU SHOULDN’T (AND WHAT TO DO IF YOU ACCIDENTALLY DID)

WHAT DOES IT MEAN?

Hackers impersonate companies or people you may know to try to trick you into purchasing something you don't need to, handing over personal and financial information, or your passwords.

WHY DOES IT MATTER?

Nearly one-third of all data breaches in the U.S. last year were the result of people clicking on links from malicious actors or sharing password information. That's a pretty big deal. Just think, if someone hadn't clicked the link, or shared the password. That means money saved data saved, and a whole lot less headaches.

HOW TO TELL?

Sometimes it's hard to tell what's real or not. If you get something suspicious: **Stop, don't click or share, and contact your IT resource.**

If you accidentally do click on something you shouldn't:

- Stop here – don't enter any additional information
- Disconnect from the internet
- Scan your machine using anti-virus/antimalware software
- Change passwords to accounts with your personal or financial information
- Try programs like Google's Phishing Protection API - https://cloud.google.com/phishing-protec-tion/docs/quick-startsubmission-api

CSS Maturity Assessment

a work in progress…

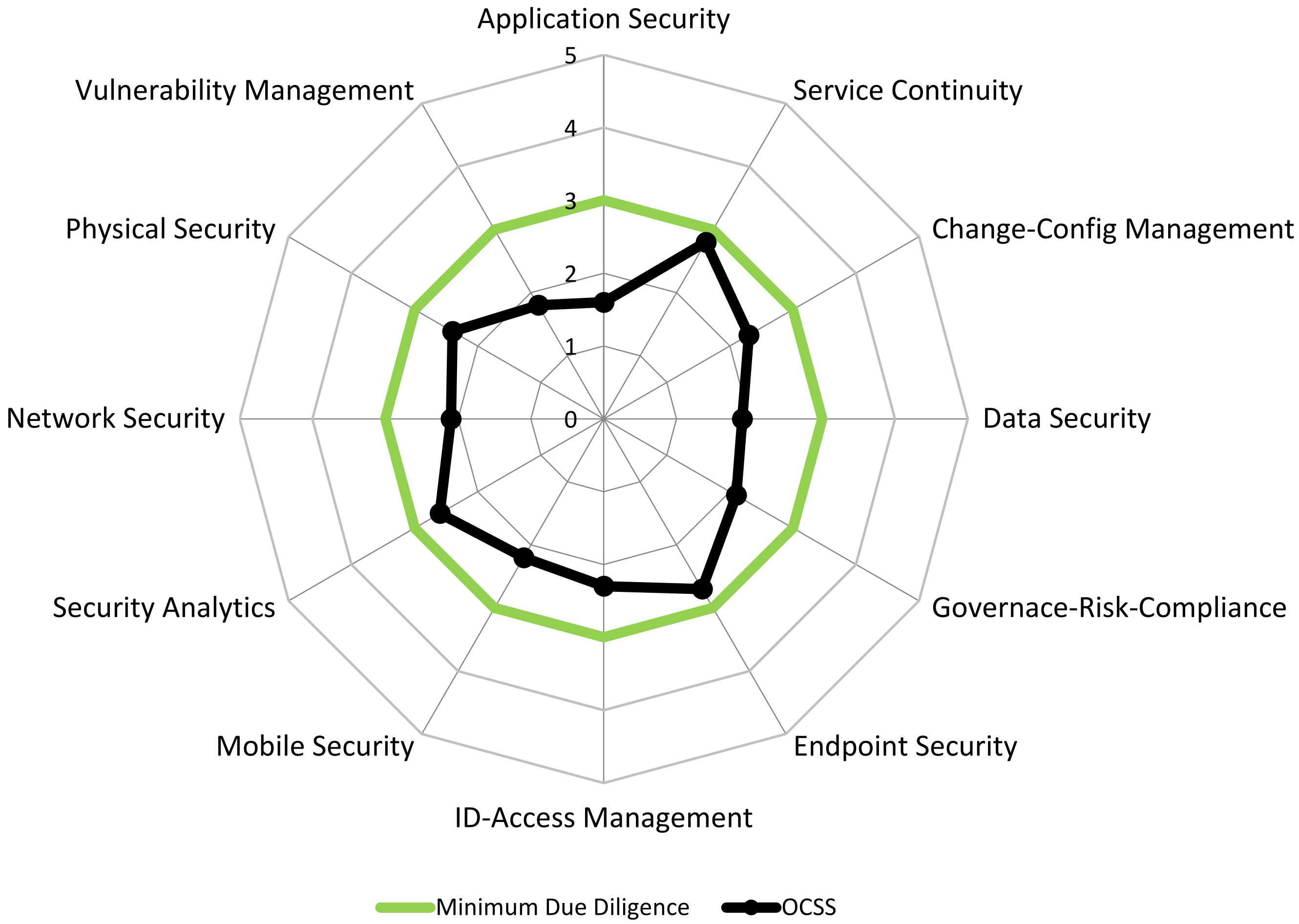
ENTERPRISE
information services

Security Maturity. *CSS Current State**

Maturity :	Weak/Ad Hoc	Reactive	Proactive	Managed	Optimized

1 → 5

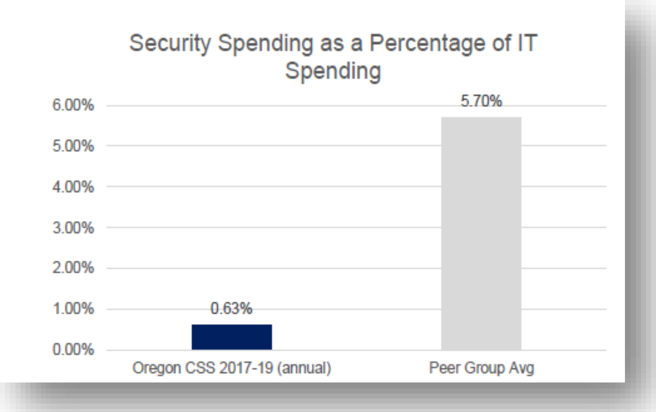
Security Maturity is a measure of an organization's ability to protect itself and it's services in the current threat landscape

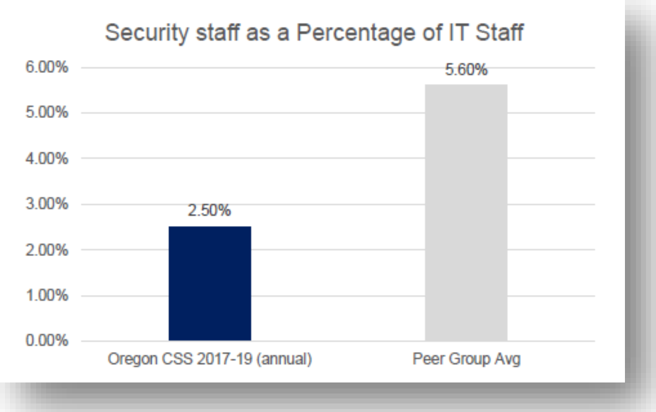


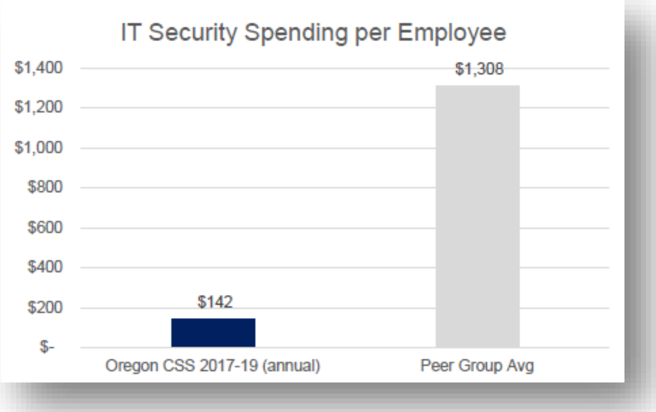
Application	1.6
Continuity	2.8
Change	2.3
Data	1.9
Governance	2.1
Endpoint	2.7
IAM	2.3
Mobile	2.2
Analytics	2.6
Network	2.1
Physical	2.4
Vulnerability	1.8

Developed in partnership with* **Gartner

CSS in Context. *State + Local Government Peers**







- **Security as a % of Overall IT Spending.** *"CSS spending on security operations* ***[0.63%]*** *as a percentage of the overall IT budget is* ***significantly lower*** *than other State and Local Government Organizations* ***[5.7%]****"*

- **Security Staff as a % of IT Staff.** *"CSS's proportion of security staff* ***[2.5%]*** *as a percentage of total IT employees is* ***lower*** *than peers* ***[5.6%]****"*

- **Security Spending per Employee.** *"CSS security spending per employee* ***[$142]*** *is* ***significantly lower*** *than the peer group average* ***[$1,308]****"*

Developed in partnership with* **Gartner; *source: Gartner IT Key Metrics Data 2020: IT Security Measures - Analysis*

ENTERPRISE information services

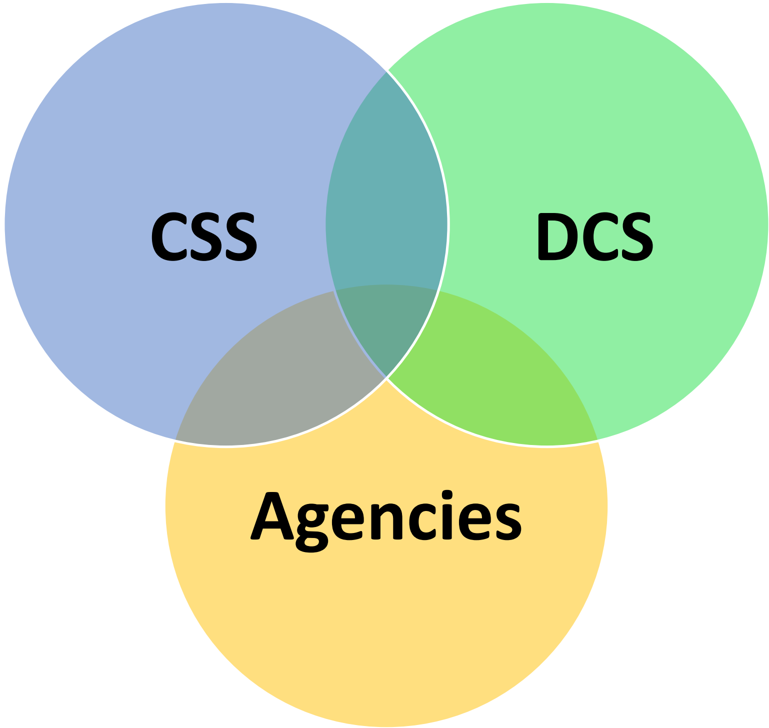
RACI

recommended security roles and responsibilities

IT Security. *Current State Responsibilities**

Cyber Security Services (CSS)

- Enterprise security policy
- Security monitoring of the state network
- Managing perimeter and border firewalls
- Enterprise incident response
- Enterprise security architecture
- Dissemination of security training
- Policy
- Security best practices across state government



Data Center Services (DCS)

- Local Network Connectivity
- Statewide Network Connectivity
- Storage Management
- Computer Hosting
- Secure Connections
- Enterprise Email

Agencies

- Agencies are ostensibly responsible for everything that DCS and CSS don't handle
- All executive branch agencies are expected to follow CSS guidance.

* Developed in partnership with **Gartner**

RACI. *Determining the Future-state of CSS**

Security Capabilities

- Program Management
- Governance, Risk and Compliance (GRC)
- Security Architecture (standards)
- Infrastructure and Data Protection
- Identity and Access Management (IAM)
- Security Operations Center
- Security Administration
- Systems Integration
- Vendor Management
- Security Consulting

R Responsible

Those who do the work to achieve the task. There is typically one role with a participation type of Responsible, although others can be delegated to assist in the work required.

A Accountable

Approver or final approving authority accountable for reviewing, approving and taking ownership of the deliverable/activity.

C Consulted

Those whose opinions are sought; and with whom there is two-way communication.

I Informed

Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

* Developed in partnership with **Gartner**

CSS Security Catalog

recommended service offerings

ENTERPRISE
information services

CSS Catalog – Future-state Capabilities and Services*

37 centralized service offerings across 10 primary programmatic capabilities

Program Management

- Security Policy-Setting + Advisory
- Statewide Security Management Plan
- Security Program and Resource Management

Identity and Access Management (IAM)

- Identity Lifecycle Management + Advisory

Governance Risk & Compliance (GRC)

- Working Group(s) Sponsorship
- CISO Roadshow
- Requirements-setting + Advisory
- General Security Awareness Training

Security Administration

- Release Management Requirements + Advisory
- Change Management Requirements + Advisory

Security Architecture

- Standards-setting

Systems Integration

- Secure Technology Transformation Guidance

Vendor Management

- Vendor Contract Review
- Vendor Security Evaluation + Advisory

Security Consulting

- Security Risk Assessment
- Business Enablement + Advisory
- Business Case Security Consulting
- SOC Advisory (reference SOC capabilities)
- Configuration and Security Review

Data and Infrastructure and Operations (I&O)

- Endpoint Security Baseline Guidance
- SDLC Process Framework + Advisory
- Data Protection Configuration Guidance
- Network Operations Consulting

Security Operations Center (SOC)

- NIDS Monitoring
- Firewall Log Monitoring
- Platform Log Monitoring
- Security Advisories
- Incident Recording
- Incident Consulting
- Incident Response
- IT Forensics
- Internal Vulnerability Scanning
- External Vulnerability Scanning
- Penetration Testing
- Threat Hunting
- Red/Blue Teaming

* Developed in partnership with **Gartner**

Summary – Key Benchmark Takeaways*

Security Maturity

1. Security program is in a ***reactive posture***
2. Overall security posture is ***25% lower*** than peer group
3. 50% of security program capabilities appear to be ***critical risk exposures***
4. Spending on security operations is significantly lower than other state governments: ***0.6% versus 5.7%***

RACI

1. Accountability and execution across the 10 primary programmatic security capabilities
2. Recommended initiatives include enhanced ***agency support***, ***communications***, ***coordination*** and ***governance***
3. CSS is primarily accountable for ***governance*** and overall ***security program deployment*** and ***management***
4. Agencies primarily responsible for ***execution*** of ***security capabilities*** as defined by CSS

Security Catalog

1. 37 centralized service offerings across the 10 primary programmatic capabilities
2. Catalog offerings are strongly focused around ***monitoring*** and ***incident response***, ***standards*** and ***governance***, ***vulnerability management*** and ***awareness***, ***identity lifecycles*** and ***change management***

* Developed in partnership with **Gartner**

Plans

next biennium

Future State – RACI Overview*

Capability	CSS				DCS	Shared Services	Strategy & Design	Data Governance and Transparency	Agencies
	CISO	GRC*	SOC	Operations					
Program Management (policy)	A, R, C	I	I	I	C, I	C, I	C, I	C, I	C, I
Governance, Risk, Compliance (requirements, guidelines, awareness)	A, C	I	I	I	R, C	R, C	C, I	C, I	A, R, C
Security Architecture (standards)	A, C	I	I	I	R, C	R, C	C, I	C, I	R, C
Infrastructure and Data Protection (includes platforms, applications, data, vulnerability management)	A, C	R	C	R, I	R, C	R, C	C, I	C, I	R, C
Identity and Access Management	A, C	R	C	I	R, C	R, C	C, I	C, I	R, C
Security Operations Center (including incident response and vulnerability assessment)	A*	I	R	C, I	C, I	C, I	I	I	C, I
Security Administration (patching, system admin., change management, operational user provisioning)	C	R	C	R	R, C	R, C	I	I	A, R, C
Systems Integration	C	R	I	C, I	R, C	R, C	C, I	I	A, R, C
Vendor Management	C	R	I	I	R, C	R, C	I	I	A, R, C
Security Consulting	A	R	R	R	R, C	R, C	C, I	C, I	I

* Developed in partnership with **Gartner**

Next Steps

- Mature agencies connection into CSS (POP 126)
- Cybersecurity Assessments: Finalized the 2021 assessment schedule
- END POINT \ MDM
- Expand Web Application Firewalls across the enterprise
- Re-establish the scope of scanning
- Enable Risk-Based Vulnerability Management
- Enable Web Application Scanning
- Security Network Planning and Architecture

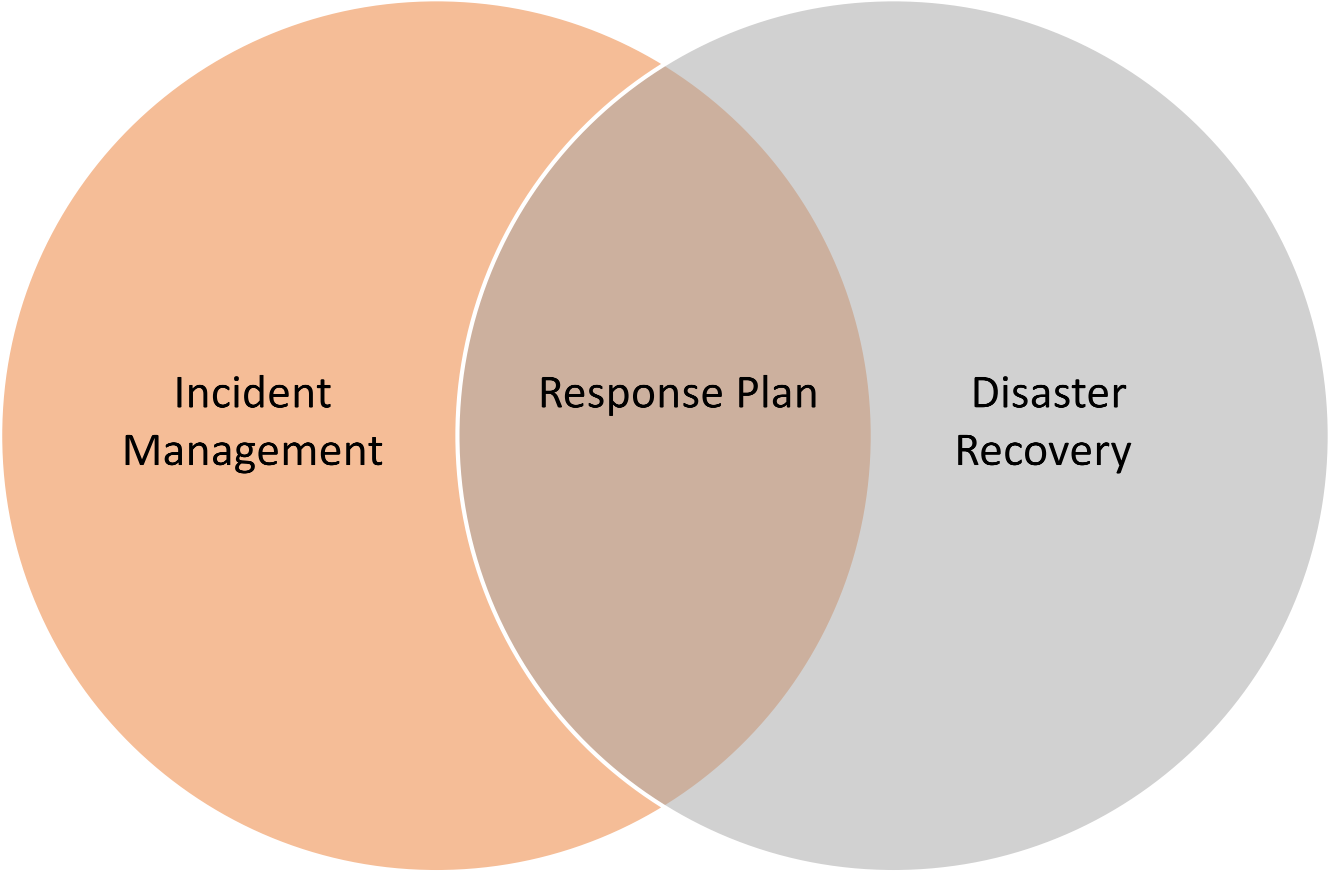
THE CYBERSECURITY BALANCE
RISK TOLERANCE
CONTINUOUS IMPROVEMENT
AFFORDABILITY

Incident Response

mitigating the impact

ENTERPRISE
information services

Cybersecurity Mitigation Methodology



Incident Response (IR). *Why is an IR plan important?*

An effective incident response plan helps ensure that

- the ***right people***,
- with the ***right skills***,
- ***experience***, and
- ***decision authority***,

know what procedures to follow to contain and remediate an information security incident

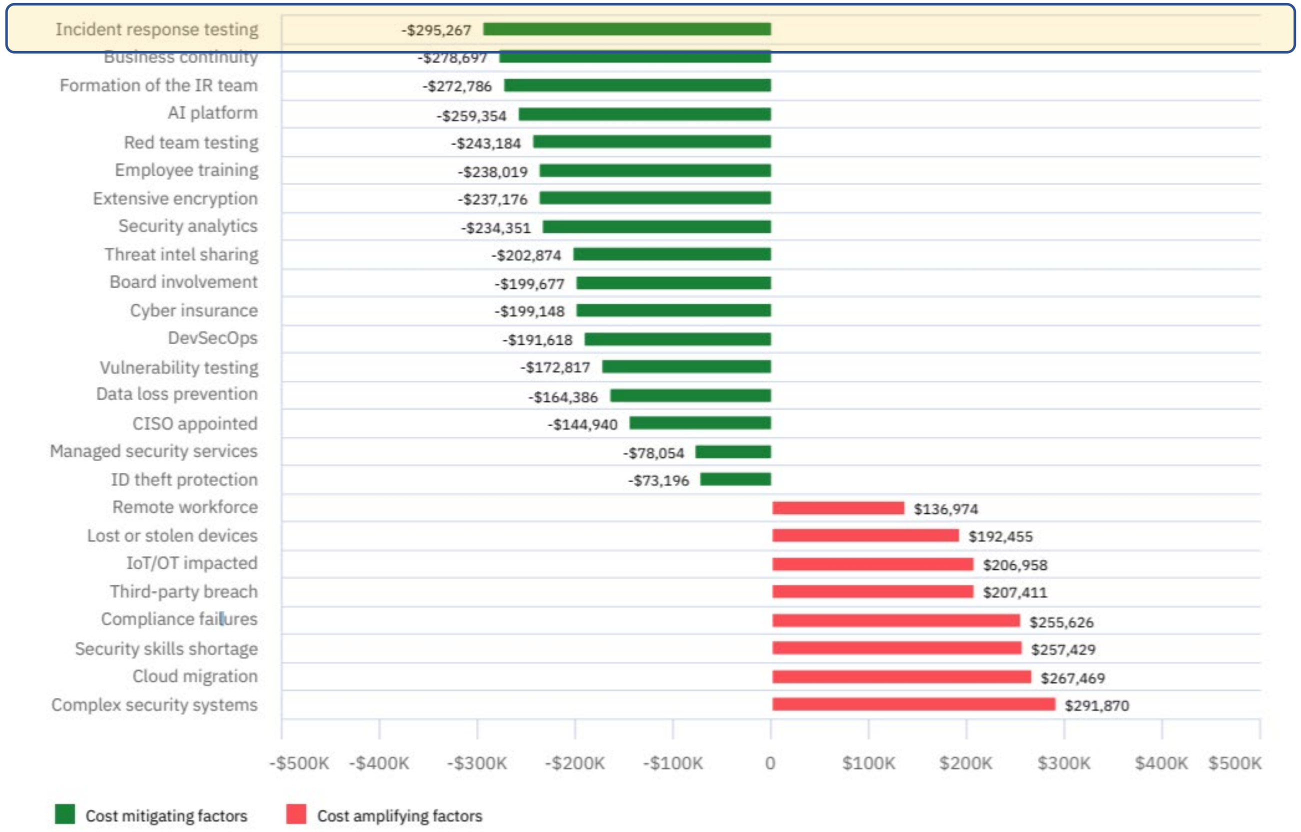
Benefits of an IR Plan

- Rapid detection and response
- Effective communications
- Mitigation of reputational, financial, and business impacts

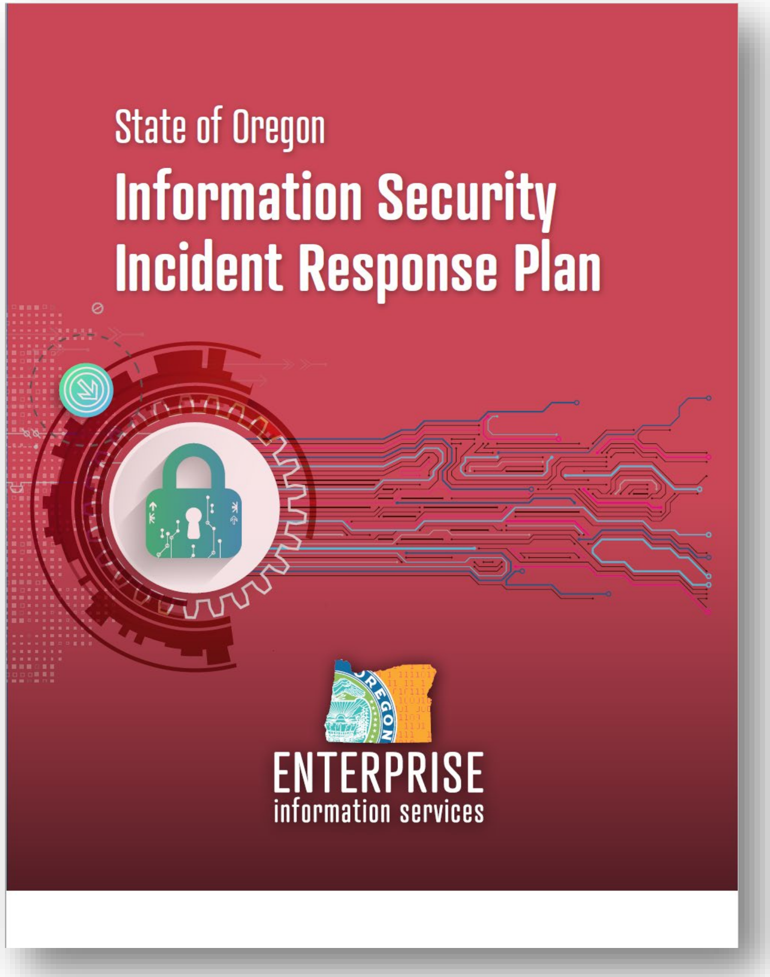
Figure 26

Impact of 25 key factors on the average total cost of a data breach

Change in US$ from average total cost of $3.86 million



State IR Plan. *What has changed?*



State of Oregon

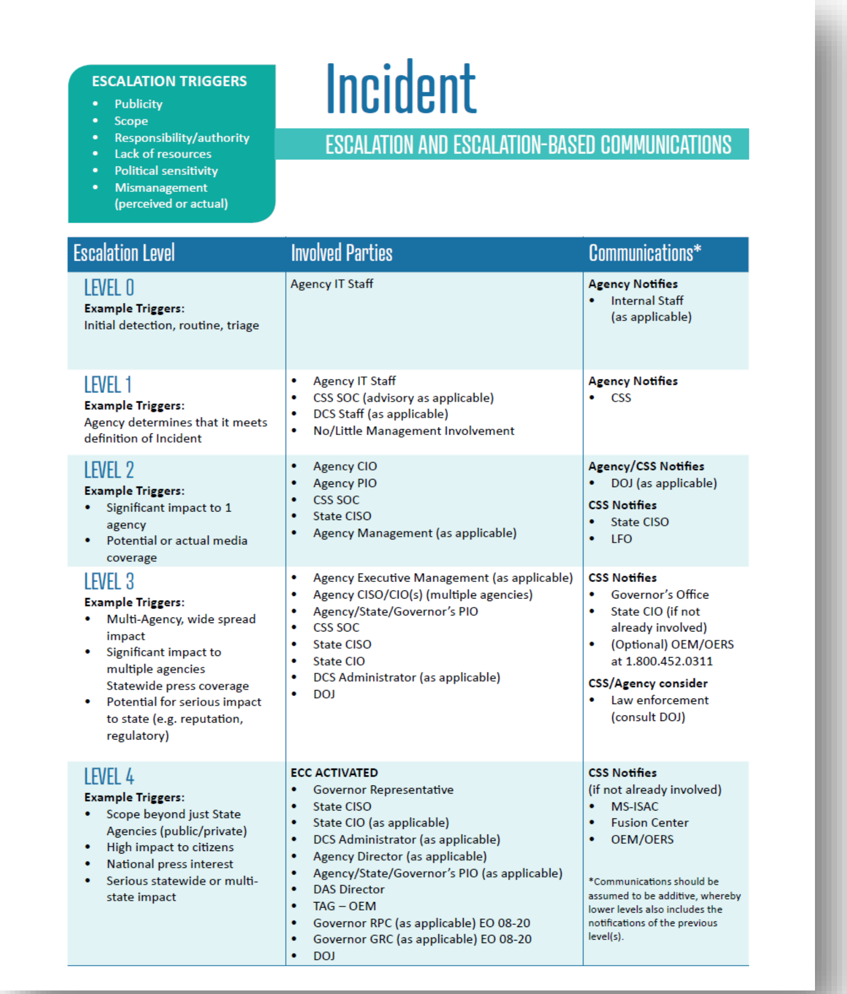
Information Security Incident Response Plan

ENTERPRISE information services

- **Layout and Readability.** Improved format and fewer security-related terms and acronyms
- **Housekeeping.** Updated to reflect current ORS and Statewide Security Policies
- **NIST-Aligned.** Aligned to NIST's Cybersecurity Framework
- **Roles and Responsibilities.** Updated to reflect working relationships between Cyber Security Services and its partner agencies

State IR Plan. *Response Processes and Escalation*

- **Preparation.** *Exercises, training, and security awareness*
- **Identification.** *Detection, alerting and initial fact finding*
- **Scoping and Classification.** *Triage, preliminary forensics, business impact analysis, incident escalation, CSS resources engaged, and activation of command structure*
- **Containment.** *Limiting incident impacts and ensuring communications control*
- **Eradication and Recovery.** *Elimination of threats and vulnerabilities and restoration of services*
- **Post-Incident Activity.** *Lessons learned and continuous improvement*



ESCALATION TRIGGERS

- Publicity
- Scope
- Responsibility/authority
- Lack of resources
- Political sensitivity
- Mismanagement (perceived or actual)

Incident

ESCALATION AND ESCALATION-BASED COMMUNICATIONS

Escalation Level	Involved Parties	Communications*
LEVEL 0 **Example Triggers:** Initial detection, routine, triage	Agency IT Staff	**Agency Notifies** • Internal Staff (as applicable)
LEVEL 1 **Example Triggers:** Agency determines that it meets definition of Incident	• Agency IT Staff • CSS SOC (advisory as applicable) • DCS Staff (as applicable) • No/Little Management Involvement	**Agency Notifies** • CSS
LEVEL 2 **Example Triggers:** • Significant impact to 1 agency • Potential or actual media coverage	• Agency CIO • Agency PIO • CSS SOC • State CISO • Agency Management (as applicable)	**Agency/CSS Notifies** • DOJ (as applicable) **CSS Notifies** • State CISO • LFO
LEVEL 3 **Example Triggers:** • Multi-Agency, wide spread impact • Significant impact to multiple agencies Statewide press coverage • Potential for serious impact to state (e.g. reputation, regulatory)	• Agency Executive Management (as applicable) • Agency CISO/CIO(s) (multiple agencies) • Agency/State/Governor's PIO • CSS SOC • State CISO • State CIO • DCS Administrator (as applicable) • DOJ	**CSS Notifies** • Governor's Office • State CIO (if not already involved) • (Optional) OEM/OERS at 1.800.452.0311 **CSS/Agency consider** • Law enforcement (consult DOJ)
LEVEL 4 **Example Triggers:** • Scope beyond just State Agencies (public/private) • High impact to citizens • National press interest • Serious statewide or multi-state impact	**ECC ACTIVATED** • Governor Representative • State CISO • State CIO (as applicable) • DCS Administrator (as applicable) • Agency Director (as applicable) • Agency/State/Governor's PIO (as applicable) • DAS Director • TAG – OEM • Governor RPC (as applicable) EO 08-20 • Governor GRC (as applicable) EO 08-20 • DOJ	**CSS Notifies** (if not already involved) • MS-ISAC • Fusion Center • OEM/OERS

*Communications should be assumed to be additive, whereby lower levels also includes the notifications of the previous level(s).

Cyber Disruption Plan

- The National Governor's Association (NGA) supported Oregon in establishing a "Whole Community" Cyber Disruption Plan.
- Engaged participants from State Agencies, Cities and Counties in Oregon as well as our Federal partners to develop the plan
- The plan covers Roles and Responsibilities, Resources and Services, Principles, Plan Training and Exercise and Plan Maintenance. Appendixes cover services available: State and Federal; Templates; How to prepare for a Cyber Disruption and various references.
- Next steps include socializing the plan to across the state; establishing a website for the plan and related materials