



OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Office of CyberSecurity Response Capabilities

David Morris
CTO CyberSecurity



Relationships



Information Sharing, Education, Training



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Cyber Incident Analysis, Forensics



Monitoring, Alerting of Malicious Cyber Activity



OFFICE OF
CyberSecurity
STATE OF WASHINGTON

State Government

Local Government

Political Subdivisions

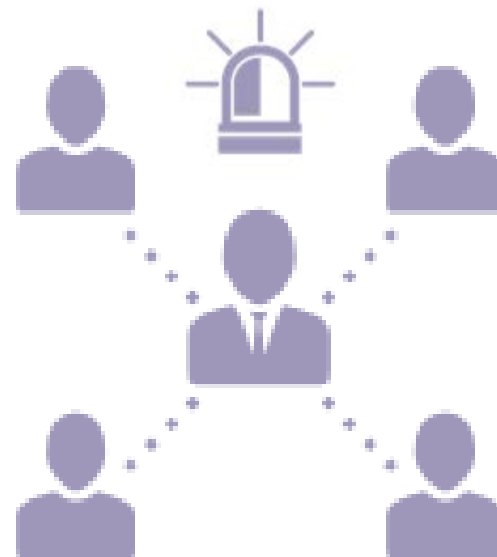
Critical Infrastructure

Tribal Government



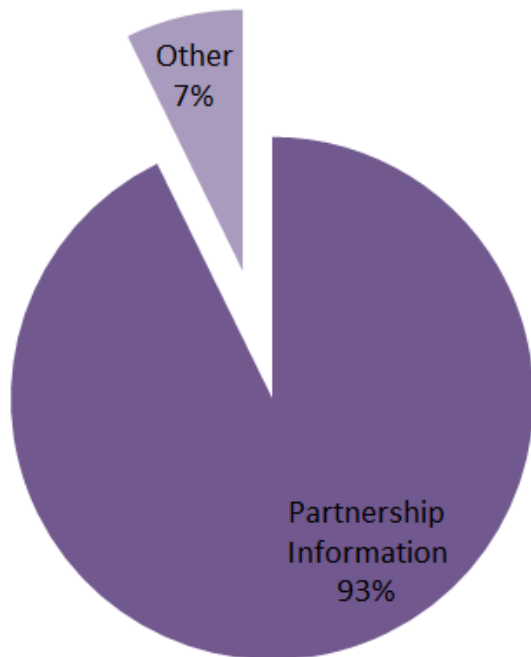
Building Trust

- ▶ Security is all about building trust relationships
- ▶ These relationships need to be in place before they are needed






Partnership Benefits

- ▶ Government advantage of information sharing



Categories

	 Personnel	 Systems	 Services
Solutions	<ul style="list-style-type: none">• Awareness materials• Training• Shared Knowledge	<ul style="list-style-type: none">• Threat Intelligence• Common Operational Picture	<ul style="list-style-type: none">• Network Monitoring• Malware Analysis• Digital Forensics

Framework



▶ **Security Operations Center (SOC)**



- Continuous Monitoring
- Event Correlation
- Packet Analysis

▶ **Computer Emergency Readiness Team (CERT)**

- Mitigation
- Forensics
- Incident Handling

Computer Emergency Readiness Team (CERT)

CERT personnel fill a role analogous to that of a firefighter

 Assessment	 Response
Proactive review Risk Identification Objective Custom modules	Remote Deployment Coordinated with Agency Resources Certified Experts Forensics Expertise

Computer Emergency Readiness Team (CERT)







Assessment Example

Security Assessment

Agency Name

August 11, 2015



TIP: AMBER

RECOMMENDATIONS

The following recommendations were created using a risk based approach. This risk based approach is built around reviewing the environment's threat, vulnerabilities, preexisting conditions, likelihood of occurrence, and potential impact.


Overview	Priority	Details
Upgrade end of life critical systems - Server	High	Replace near EOL Windows Server 2003 servers with a supported version of Windows Server. Windows Server 2003 systems will no longer be supported as of July 14th, 2015.
Upgrade end of life database systems - Server	High	Replace EOL Microsoft SQL 2005 with a supported version of Microsoft SQL. Near EOL Microsoft SQL 2005 will no longer be supported as of April 12th, 2016.
Central patch management solution - Server	High	Implementation of an enterprise level tool to manage operating system updates.
Application patch management	High	Review patch management program for 3rd party applications on servers and workstations. Verify deployed applications are covered in the program.
Implement security configurations - Server	Medium	Implement industry standard security configurations to harden server deployments. A target score of 70% or above is advised.
Implement security configurations - Database	Medium	Implement industry standard security configurations to harden database deployments. A target score of 85% or above is advised.
Implement security configurations - Workstation	Medium	Implement industry standard security configurations to harden workstation deployments. A target score of 70% or above is advised.
Vulnerability scanning	Medium	Implement routine scanning for vulnerabilities to verify configurations and patch management.
Disable unused or insecure services	Medium	Disabling unused or insecure services greatly diminishes the services or protocols an attacker can attempt to compromise.
Review and expand policies to OIGD Standard	Low	Review policies to verify they are up to date and expand sections to define policies for individual OIGD Standard items.
SSL expired certificates	Low	Review and document all SSL certificates and create a certificate management plan.
Disable unused and insecure services	Low	Disable any unused services such as port80 (HTTP) and 443 (HTTPS) for printers and networking devices. Disable rsh and configure SSH2 for secure management access. Disable ftp and use a secure file transfer method such as SCP or SFTP.
Continue security education and awareness training	Low	Cyber security is ever changing so providing users with regular security education and awareness training is key in defending the agency networks and services.

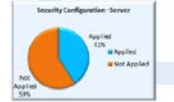
This report is exempt from disclosure under RCW 5A05.02.010 in the public interest. This report is only one element of a security risk assessment identifying specific system vulnerabilities in computer or telecommunication networks.

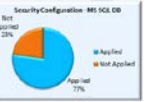



TIP: AMBER

DIS BENCHMARK








The DIS Benchmarks are a common standard industry standard practice for the security configuration of systems. Comparing systems to a benchmark allows the client to determine the extent to which the security of the system is in compliance.

SERVICE DISCOVERY


Top 5 Services



The above table represents the top 5 services that were discovered during the assessment. The results of the service discovery, based on the results of the scan, are used to identify the services that are running on the system. After identifying the services, the top 5 services are displayed in the table above. The results of the scan are used to identify the services that are running on the system. The results of the scan are used to identify the services that are running on the system.

HOST DISCOVERY

Systems/Devices Summary



This report is exempt from disclosure under RCW 5A05.02.010 in the public interest. This report is only one element of a security risk assessment identifying specific system vulnerabilities in computer or telecommunication networks.


Computer Emergency Readiness Team (CERT)



Response Example: Fish and Wildlife

- ▶ Petty criminal cyber actor: “MrHigh”
- ▶ Self reported
- ▶ Multiple states impacted: WA, OR, ID
 - ▶ WA: **2,435,452** records (Last 4 of SSN #)

03-27-2016, 03:24 AM

 **MrHigh**
wigga

Thanks (Given): 4
Thanks (Received): 89

Hack the Planet!

If I were in the process of pulling full information(full name, social security number, date of birth, drivers license, and other personal info) from a database in which I have found a security hole, and I have at least three to four more databases like it to pull information from, each containing anywhere from 500k to 1 million individuals personal information, in what way should I report the info after I have finished pulling the data?

My plan so far is to yank all of the data, and then on a special day that has some specific meaning(like 4-20, but that may be to soon due to myself finding more databases), report the security holes in detail to the administrators and at the same time, post a list of these websites on different forums so that others can take a stab at these websites themselves and possibly find the same security holes that I've found. This will give others a short time frame to find the same holes I've found and pull out some data for themselves.

What other ways of reporting these would make a big splash effect?

Tags: None

OCS Operational Picture

Week of January 15 – January 21

Security Operations Center

- 26 Alerts
 - Malicious Software (17)
 - Investigations (5)
 - Account Compromise (4)



Response Team

- 2 Response Incidents

Digital Forensics

- 2 Cases

Summary

- Security is empowered by relationships
- The Office of Cyber Security maintains two operational groups for detection and alerting
- The Computer Emergency Readiness Team responds to significant security incidents for State of Washington agencies, boards, and commissions
- The State of Washington is considered a leader amongst its peers

Questions?