SecureState®

Your Security Team

State of Oregon, 9-1-1 Program - Quarterly Meeting

6/9/2011

Agenda

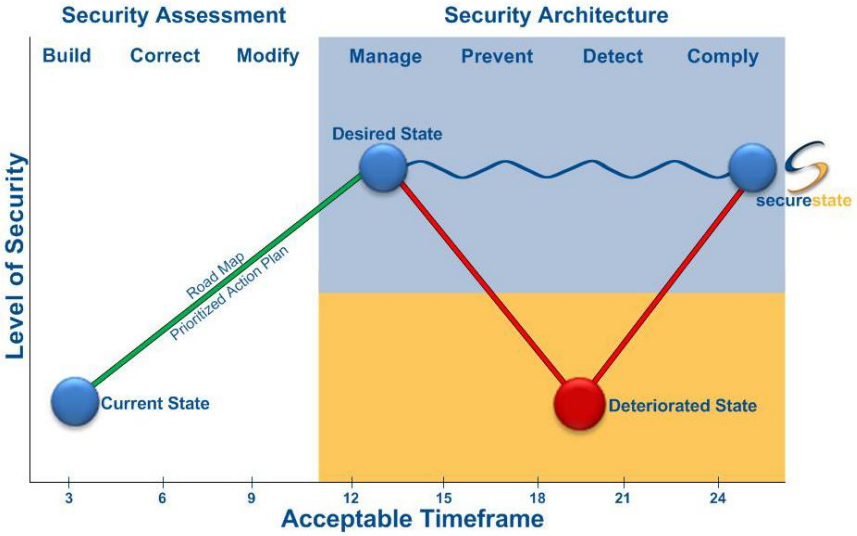
- Who am I?
- Why am I here?
- Project Recap
- State of the Security Playbook
- How this affects PSAPs, 9-1-1 vendors, and OEM
- Q & A

Who am I?

SecureState Overview

A Management Consulting Firm Specializing in Information Security

- Founded in September 2001
- Payment Card Industry Certified (PCI)
- Qualified Security Assessor (QSA)
- Approved Scanning Vendor (ASV)
- Largest dedicated security company in the Great Lakes
- Practices include:
  - Advisory Services
  - Audit & Compliance
  - Business Preservation
  - Profiling & Penetration
  - Risk Management



The Company We Keep

Key Industries: Retail , Financial Services, Healthcare, Critical Infrastructure, Professional Services, Service Providers, Education, Food Service, Entertainment and Government

Vera Bradley
DICK'S
NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
MEDICAL MUTUAL
ThirdFederal SAVINGS & LOAN
GRACO
Vita-Mix
PARK PLACE INTERNATIONAL
FORESTCITY ENTERPRISES
EXPRESS
SHEETZ FRESH FOOD MADE TO ORDER
CAMPMOR.COM
STEP 2
OhioHealth
Bob Evans
GFS gordon food service
Darice
QVC QUALITY. VALUE. CONVENIENCE.
KITCHEN COLLECTION
Baker Hostetler Counsel to Market Leaders
FEDERAL RESERVE BANK of CLEVELAND
University Hospitals
CINTAS THE SERVICE PROFESSIONALS
GIANT EAGLE
Domino's Pizza
STERLING JEWELERS INC.
AKRON GENERAL MEDICAL CENTER
CASE WESTERN RESERVE UNIVERSITY EST. 1826 think beyond the possible
PSG Phoenix Systems Group, Inc.
PEPBOYS AUTO Parts, Service and So Much More
Kinetico water systems
windstream communications
Dollar Bank Since 1855
SAFEAUTO
HYLAND SOFTWARE
LINCOLN ELECTRIC
FirstEnergy
NorthShore University HealthSystem
HIGHMARK Blue Cross Blue Shield
KeyBank
OEMA
NASA NATONAL AERONAUTICS AND SPACE ADMINISTRATION
MTD For A Growing World.
heinen's fine foods
Akron Children's Hospital
IGS ENERGY Your Natural Gas Choice.
dots
JO-ANN
THE OHIO STATE UNIVERSITY
FIRST PLACE Financial Corp.
Arizona State RETIREMENT SYSTEM
RITE AID
SQUIRE SANDERS
DP&L
NCFTA
expedient ONE INCREDIBLE NETWORK.
PROGRESSIVE
PACER Making Your World Run Smoother
M&T Bank
MidwestISO Energizing the Heartland
AMERICAN HOME BANK We help build your future.
corbis
JONES DAY

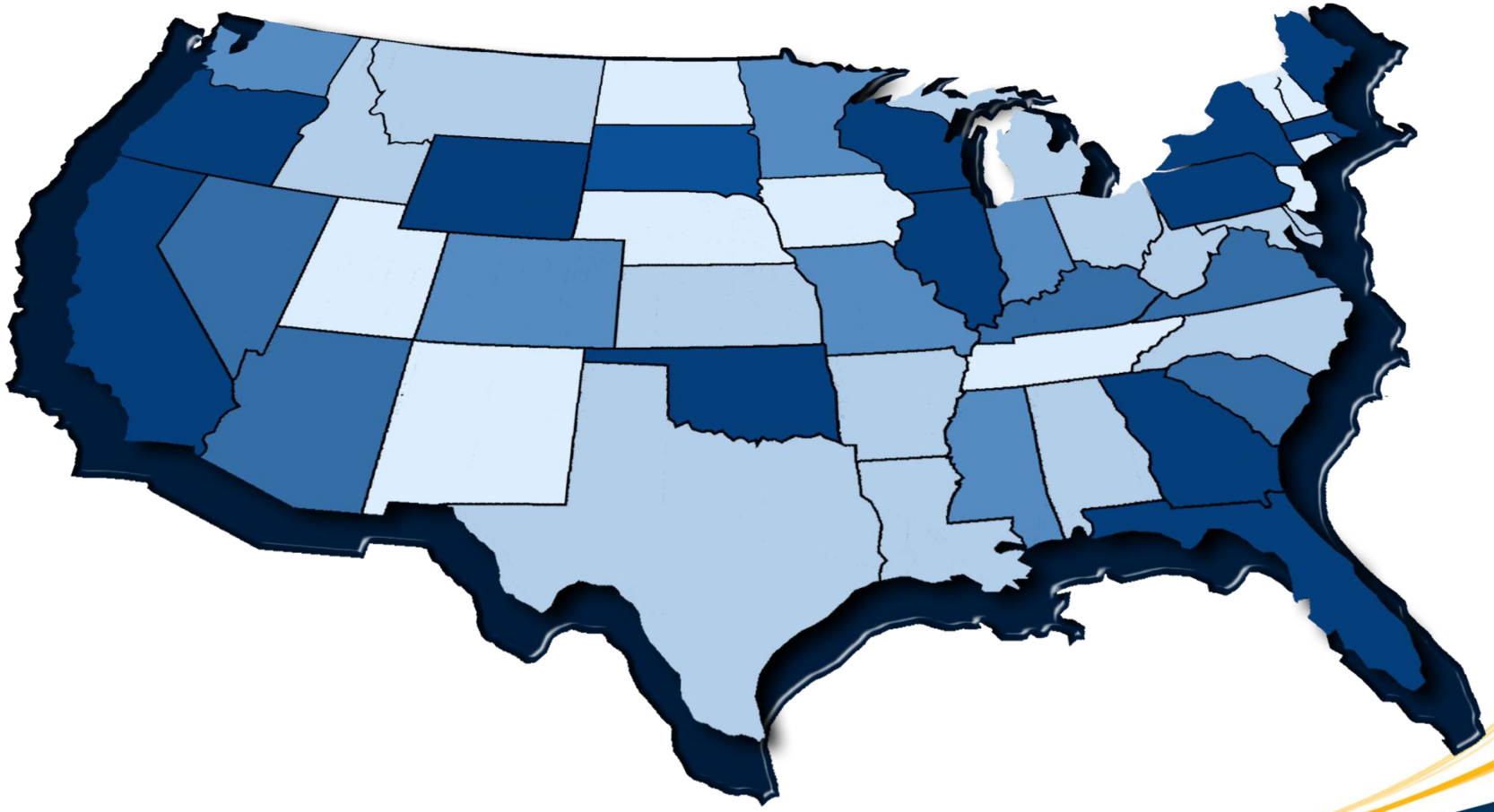
About your presenter…

- Chris Clymer
  - Senior Consultant, Advisory Services Practice
  - Acting Chief Security Officer for 6 organizations of various sizes within public sector, retail, manufacturing, & technology
  - 13 Years of experience in Information Security & Technology, including multiple security roles with one of the five largest U.S. banks
  - Certifications: CISSP, CISA, GPEN, GWAPT

Security Program Development

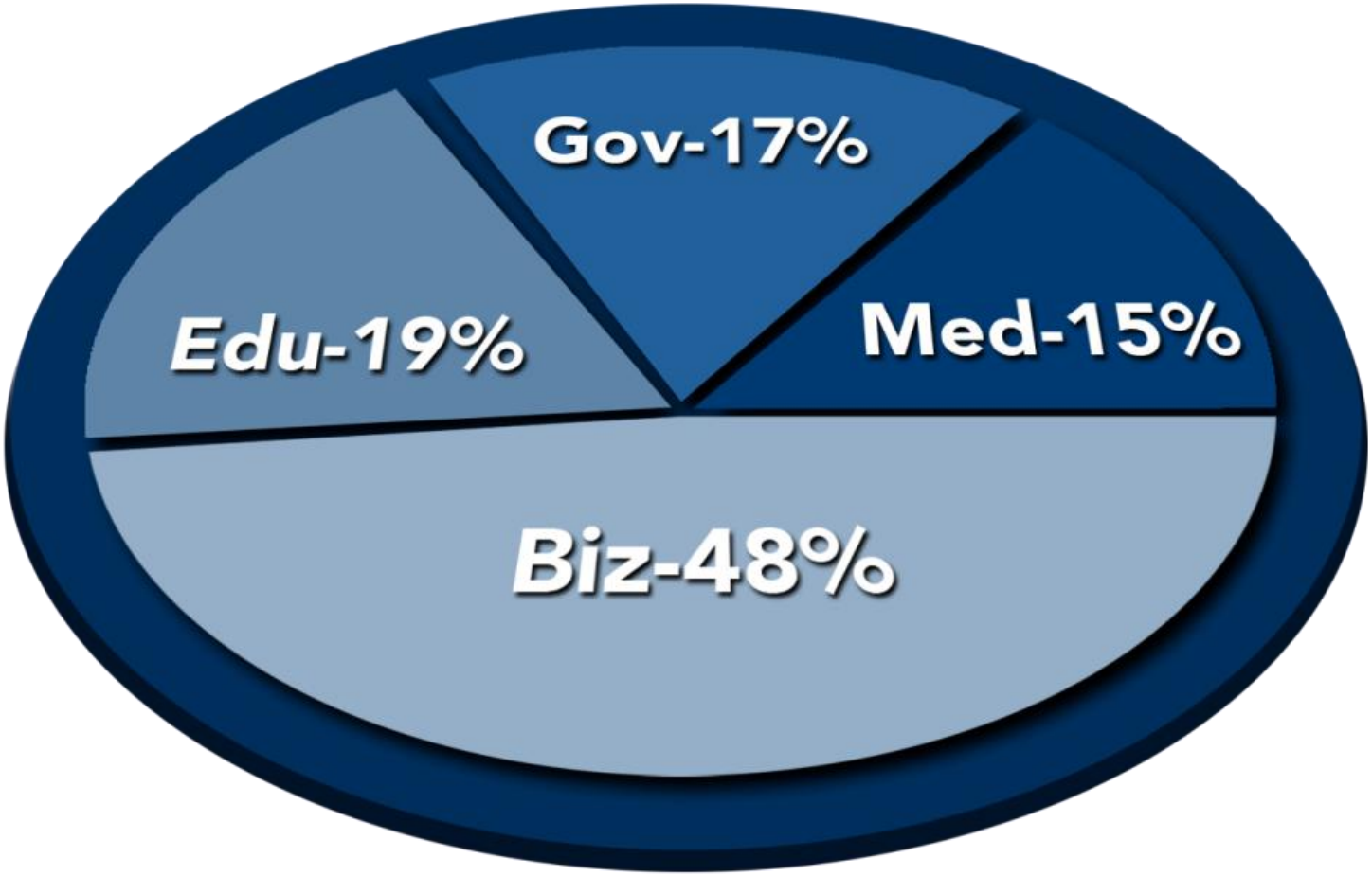
Why am I here?

Data Breaches by State



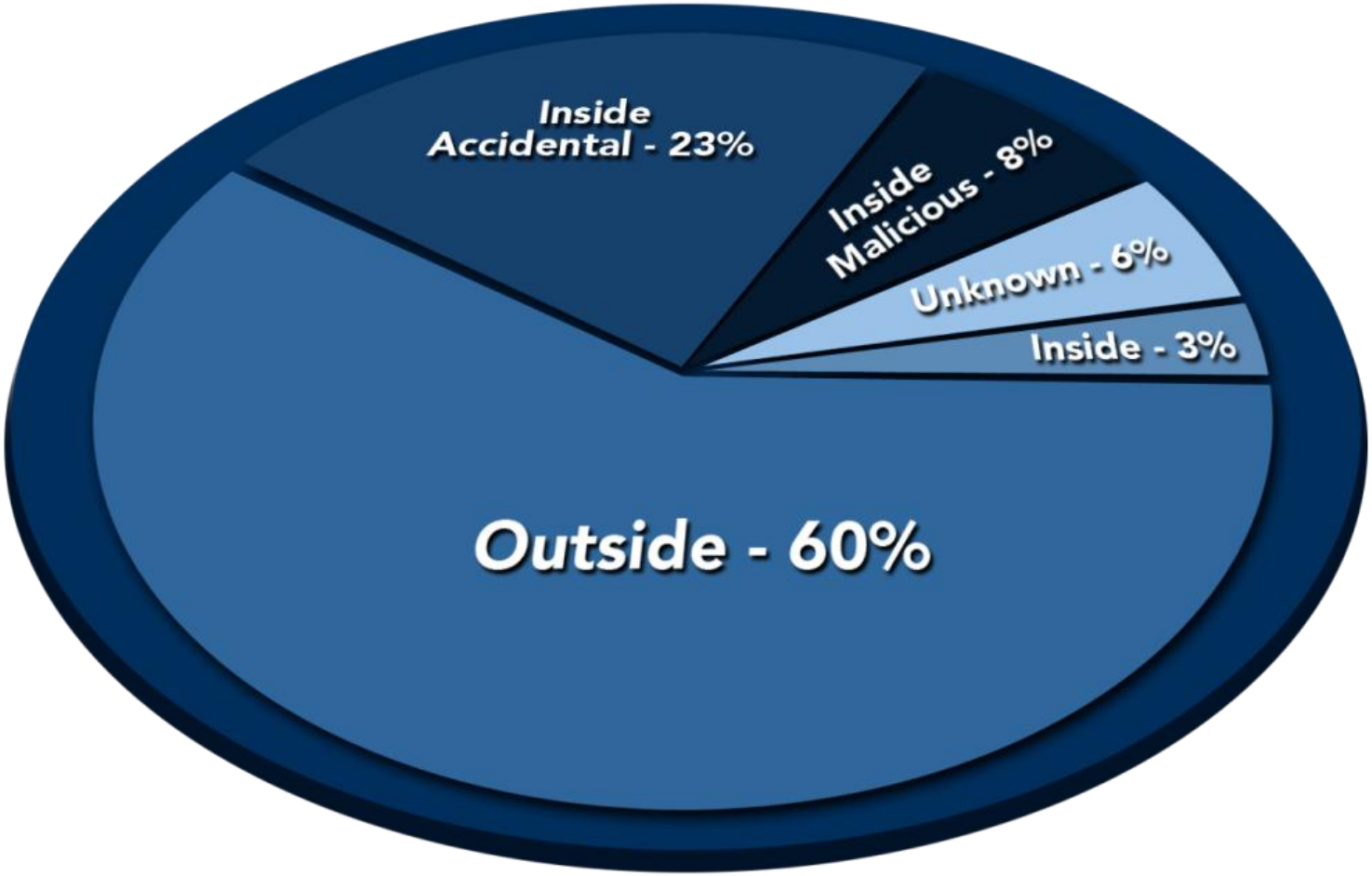
Source: Data Loss Database, http://datalossdb.com

Incidents By Business Type



Source: Data Loss Database, http://datalossdb.com

Incidents By Vector



Source: Data Loss Database, http://datalossdb.com

Oregon Gov Breaches

- Oregon Community Credit Union
  - **Incidents:** 1 **Records:** 200
  - **Headquarters Location:** Eugene OR
- Oregon Department of Revenue
  - **Incidents:** 1 **Records:** 2,200
  - **Headquarters Location:** Albany OR
- Coos County Oregon
  - **Incidents:** 1 **Records:** 500
  - **Headquarters Location:** Coquille OR
- Oregon State University
  - **Incidents:** 1 **Records:** 4,700
  - **Headquarters Location:** Corvallis OR
- Deschutes County, Oregon
  - **Incidents:** 1 **Records:** 3,400
  - **Headquarters Location:** OR, US
- Southwestern Oregon Community College
  - **Incidents:** 1 **Records:** 200
  - **Headquarters Location:** Coos Bay OR
- City of Oakridge Oregon
  - **Incidents:** 1 **Records:** 0
  - **Headquarters Location:** Oakridge OR
- Oregon National Guard
  - **Incidents:** 1 **Records:** 3,500
  - **Headquarters Location:** OR
- Oregon Health & Science University
  - **Incidents:** 3 **Records:** 5,890
  - **Headquarters Location:** Portland OR
- Oregon Department of Corrections
  - **Incidents:** 1 **Records:** 550
  - **Headquarters Location:** Salem OR
- Oregon Department of Human Services
  - **Incidents:** 1 **Records:** 45
  - **Headquarters Location:** Coos Bay OR
- Oregon Housing and Community Services
  - **Incidents:** 1 **Records:** 0
  - **Headquarters Location:** Salem OR
- Oregon Parks and Recreation Department
  - **Incidents:** 1 **Records:** 0
  - **Headquarters Location:** Salem OR
- University of Oregon Youth Transition Program
  - **Incidents:** 1 **Records:** 2,000
  - **Headquarters Location:** Eugene OR

Source: Data Loss Database, http://datalossdb.com

Project Recap

Recap

- In early 2010 SecureState performed a penetration test on the 9-1-1 frame network
  - *Multiple vulnerabilities were found across the network, at PSAPs, and at OEM*
- In June of 2010 SecureState was contracted to develop a "Security Playbook" to provide guidance on securing the 9-1-1 networks
  - *This was developed with an eye on Next Generation 9-1-1*

Recap

- In August of 2010 SecureState performed on-site assessment of OEM itself
- In October of 2010 SecureState visited 11 PSAPs to conduct brief on-site assessments
- In December, January, and February of 2010/2011 SecureState conducted assessments of network vendors (Qwest, CenturyLink, Frontier) via phone
- In April of 2011 SecureState delivered the draft Security Playbook to OEM
- This draft is under review, and will be finalized by July

Playbook Status

Security Playbook Status

- **Draft Delivered!**

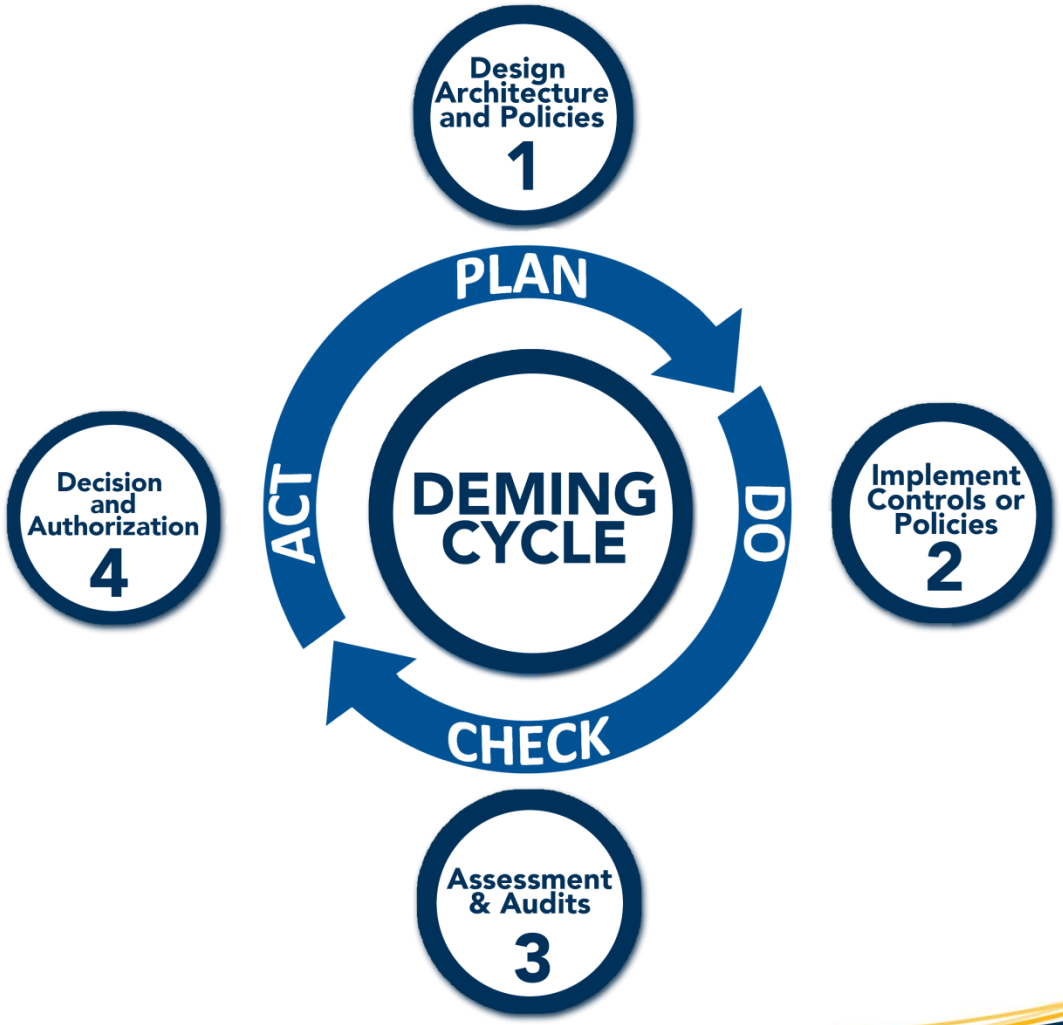
Security Playbook Status

- Draft playbook delivered to OEM on 4/30
- SecureState and OEM have been reviewing, and making changes where appropriate
- On 6/30 the playbook is finalized, and implementation begins

9-1-1 SECURITY CONTROLS **15**

NIST CONTROL MAPPING 15
9-1-1 NETWORK 16
(A) Access Control 16
(B) Security Awareness and Training 17
(C) Audit and Accountability 17
(D) Security Assessment 17
(E) Configuration Management 19
(F) Continuity Planning 21
(G) Identification and Authentication 23
(H) Incident Response 25
(I) Maintenance 26
(J) Media Protection 27
(K) Physical and Environmental Protection 28
(L) Personnel Security 32
(M) System and Service Acquisition 33
(N) System and Communication Protection 34
(O) System and Information Integrity 35
9-1-1 Network diagram *36*
9-1-1 ENDPOINTS 37
Control Areas *37*
(A) Access Control 37
(B) Awareness and Training 40
(C) Audit and Accountability 41

Plan – Do – Check - Act



Phase 1: Plan

- Develop security plan (the playbook)
- Review previous year's plan
- Perform assessments
- Adjust plan where necessary

Phase 2: Do

- Implement the plan developed in phase 1
- This is where security tasks actually happen

Phase 3: Check

- Check validates that things are going as expected
  - Review vulnerability assessment results
  - Follow-up discussions with 9-1-1 participants if necessary

Phase 4: Act

- Make adjustments based on results of “Check” phase
- If any component seems to have drifted significantly from the original plan, we adjust it here and get back on track

PDCA

- After “Act” the cycle begins again
- Annul assessments are performed
- Plans for the next year are made

Vulnerability Assessment

- This is performed through network scanning
- Performed on a quarterly basis
- OEM will perform these on the 9-1-1 network
- Any PSAPs performing these actions themselves are encouraged to share results

Penetration Testing

- This is a manual, simulated attack performed by an experienced assessor
- Meant to simulate a real-world attack by a hacker
- Will be performed by OEM, on the 9-1-1 networks

Risk Assessment

- Risk Assessment will include two questionnaires:
  - Questions for vendors on the 9-1-1 networks
  - Questions for each PSAP
- This will also include an asset inventory, provided by PSAPs
- OEM will collect, review, and rate the results
- This will give OEM a view of the current state of security across the 9-1-1 networks
- It will also allow OEM to prioritize actions related to security

How does this affect you?

How does this affect vendors?

- Expect more engagement from OEM on security of your products, and of their deployment
- Expect more questions about how security is considered in the development and implementation of your products and/or services
- Be prepared to answer a brief questionnaire which includes some of these questions

Vendor Name	Date	Product or Service	Contact	

Vendor Assessment Questionaire

Control Area	Control	Question	Response	Detail
Access Control	A1, E1, G3	Do you have security standards for your 9-1-1 Products?	yes	We perform our own hardening of 9-1-1 devices based on internal standards
Security Assessment	D1	Do you have any policy preventing OEM from performing security assessments of your products?	yes	We do not allow assessments of our products
Security Assessment	D2, D3, D4	Do you perform security assessments of your own products? (These include penetration tests, vulnerability assessments, and web application assessments)	no	We do not perform this testing
Configuration Management	E2	Do you have a change management process for 9-1-1 equipment that you manage?	yes	
Configuration Management	E2	Do you utilize any centralized authentication system, such as Active Directory, for your equipment?	yes	Our equipment is deployed with its own domain
Media Protection	J3	Do you have secure destruction processes to eliminate 9-1-1 data from hard drives and other media utilized on 9-1-1 networks?	yes	
Personnel Security	L2	Do you perform background checks on employees who have access to 9-1-1 equipment?	yes	
Personnel Security	L3	Do you restrict 9-1-1 equipment access to only employees whose job role requires it?	yes	
Personnel Security	L4	Do you allow any other 3rd party access to 9-1-1 equipment?	yes	
System & Service Acquisition	M1	Do you maintain network diagrams for any 9-1-1 equipment which you maintain?	no	
System & Communication Protection	N1	Do you utilize firewalls to isolate any 9-1-1 equipment you maintain from non 9-1-1 equipment?	yes	

How does this affect PSAPs?

- Expect more engagement from OEM on security of your 9-1-1 equipment and facilities, specifically anything connected to 9-1-1 networks
- Expect OEM to perform periodic security tests of the 9-1-1 networks
- Be prepared to answer a brief questionnaire once each year about security of 9-1-1 equipment
- Be prepared to provide OEM with an inventory of your 9-1-1 assets on an annual basis
- Be prepared for comparison to other PSAPs, and anyone else connecting to the 9-1-1 networks

PSAP Location	Date	PSAP Contact		

PSAP Self Assessment Questionaire				
Control Area	**Control**	**Question**	**Control Met?**	**Description**
Access Control	A1, C1, E1, G3	Do you have security standards for your 9-1-1 equipment?	yes	The vendor dictates any security settings, we do not alter in any way
Access Control	A2	Do you isolate 9-1-1 equipment from other parts of your network?	yes	9-1-1 equipment does not connect to other equipment
Access Control	A3, C3, E3, G1, I2	Do you utilize centralized account management, such as Active Directory?	no	systems on the 9-1-1 network are managed as standalone servers
Security Awareness	B1	Do you have a Security Awareness Program?	no	
Audit & Accountability	C2, H1, O1	Do you utilize centralized network monitoring, such as a SIEM?	no	
Security Assessment	D1	Do you have a policy permitting security assessments such as vulnerability scans and penetration tests on your networks?	yes	we have no policy disallowing or requiring this
Security Assessment	D2	Do you perform vulnerability assessments of your networks?	yes	The only activities we are aware of like this were performed by OEM
Security Assessment	D3	Are there any internet-facing 9-1-1 applications?	yes	there are no internet facing 9-1-1 applications
Security Assessment	D3	Have you performed web application assessments of internet-facing applications (if they exist)?	yes	

(K3) Monitoring

Methods should be in place to help to detect unauthorized access to 9-1-1 facilities. This should include detection on the facility perimeter, as well as the datacenter housing 9-1-1 equipment.

Detective controls which can be used for monitoring include:

- **Cameras which are continuously monitored**
- **Cameras which can play back events as-needed**
- **Cameras which record and alert based on motion**
- **Motion sensors, with alerting**
- **Door and window sensors, with alerting**
- **Employees who visually monitor building and datacenter ingress/egress points**
- **Access control system logs, with alerting**

At least one of these methods should be used for monitoring building ingress/egress points, as well as any ingress/egress points to the datacenter. Which method is most appropriate will vary between 9-1-1 facilities. Additionally, if resources allow a 9-1-1 facility to implement more than one of these methods, they are encouraged to do so.

Control Mapping

NIST 800-53 Control	NIST 800-53 Control Name
PE-6	Monitoring Physical Access
PE-8	Access Records

PSAP Location	Date	PSAP Contact	

PSAP Asset Inventory			
Asset	Value	Owner	Description
Call processing server	(A)		
Mapping Server	(B)		
PSAP Datacenter	(A)		
Voice recording	(C)		

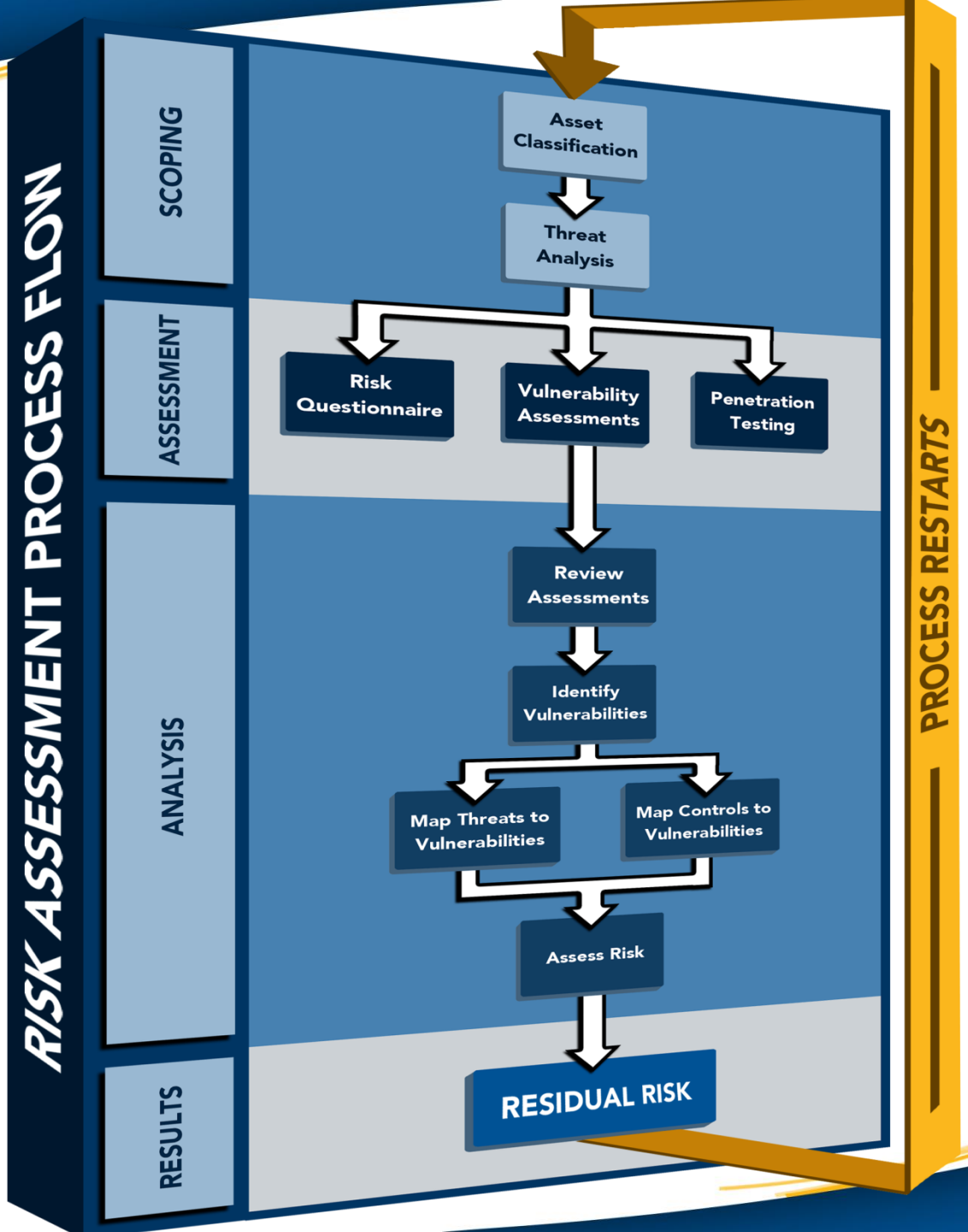
How does this affect OEM?

- OEM will be performing annual assessments of security on the 9-1-1 networks
- These results will be reviewed, and used to set security priorities across the 9-1-1 networks
- Priorities will be based on risk
- OEM will be investing significant effort into the ongoing management of security on Oregon's 9-1-1 networks

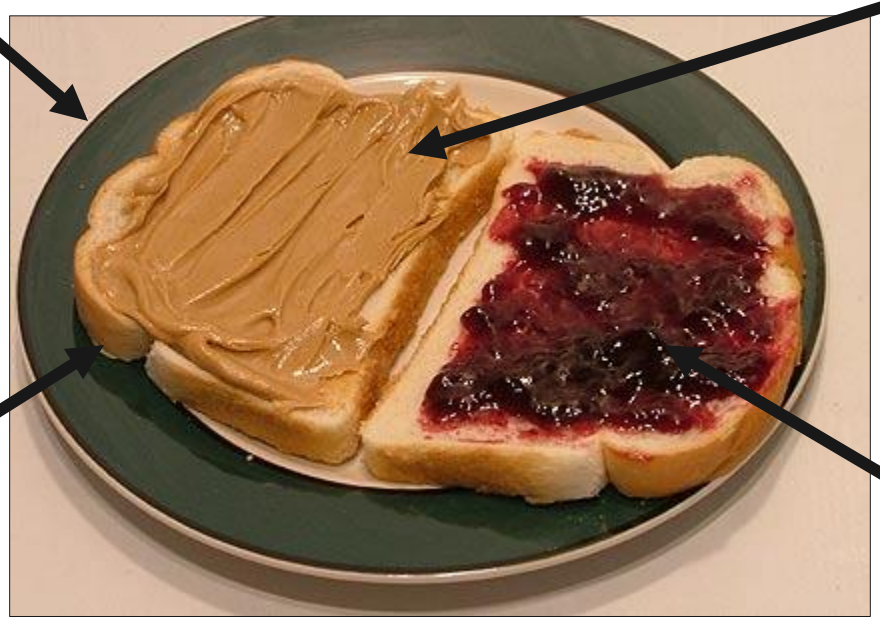
Date	Assessor Name
6.6.2011	Chris

Risk Assessment Worksheet

Assets	Asset Value	Associated Threats	Threat Likelihood	Threat Impact	Identified Vulnerability	Vulnerability Rating	Compensating Controls?	Control Description	Control Effectiveness	Residual Risk
PSAP Phone System	3	Outside Attacker (hacker)	2	3	PBX Accessible from Frame	3	Yes	Network segmentation and firewall	3	6
PSAP datacenter	3	Physical Intruder	1	3	Many individuals with physical access to datacenter	1	Yes	Physical access control	4	0
OEM Mapping Server	2	Malware	3	2	Windows OS susceptible to	2	Yes	Antivirus installed and updated	3	1
PSAP Datacenter	3	Earthquake	1	3	PSAP facility is not built to resist	3	No	None	1	9

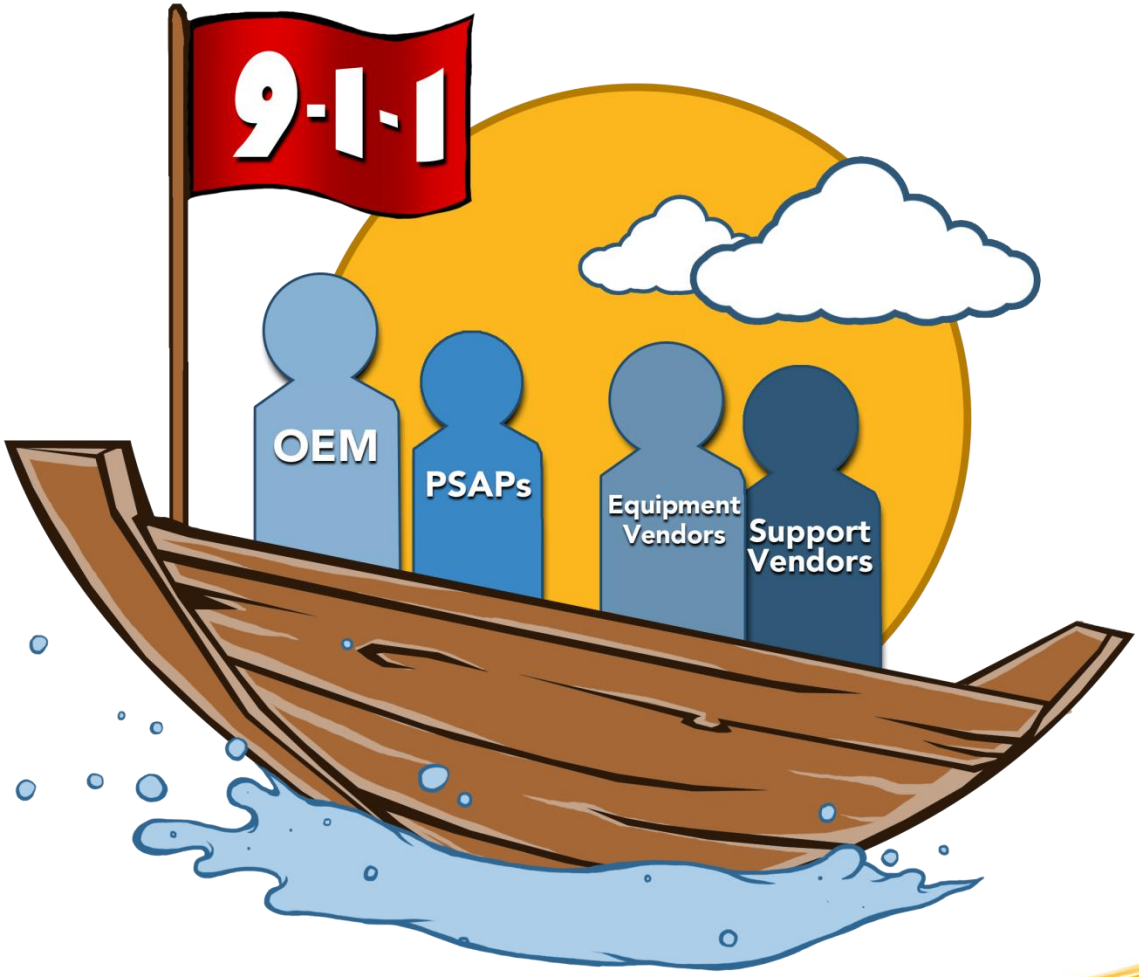

RISK ASSESSMENT PROCESS FLOW
SCOPING
ASSESSMENT
ANALYSIS
RESULTS
Asset Classification
Threat Analysis
Risk Questionnaire
Vulnerability Assessments
Penetration Testing
Review Assessments
Identify Vulnerabilities
Map Threats to Vulnerabilities
Map Controls to Vulnerabilities
Assess Risk
RESIDUAL RISK
PROCESS RESTARTS

How It Fits Together



The Playbook in Action

We're All In This Together



Thank you for your time!

Chris Clymer
Senior Consultant, Advisory Services
cclymer@securestate.com