Cyber Security Overview

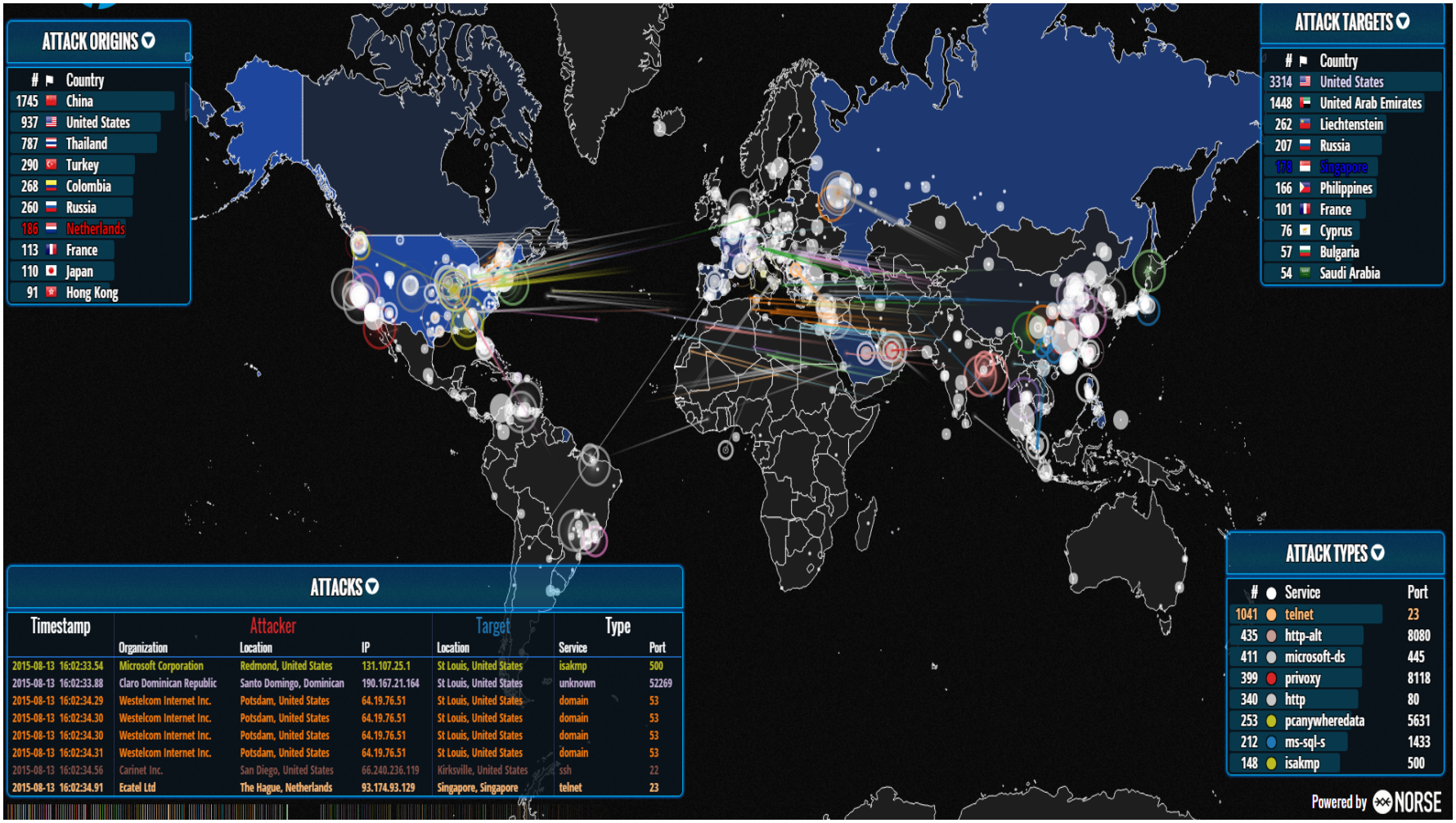
Prepare for the worst so that we can be at our best.

IT Security
Dennis Tomlin

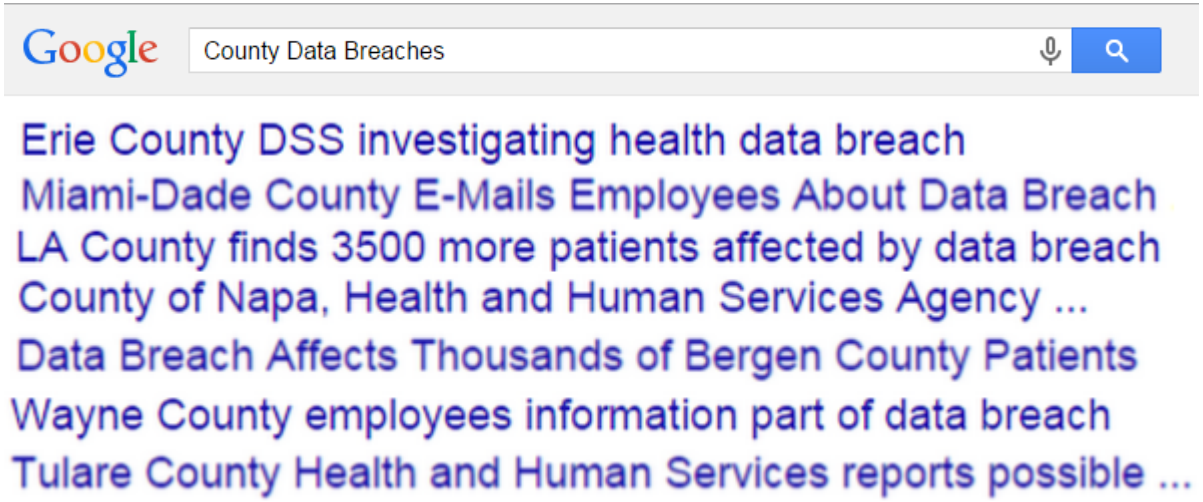
In this presentation you will learn:

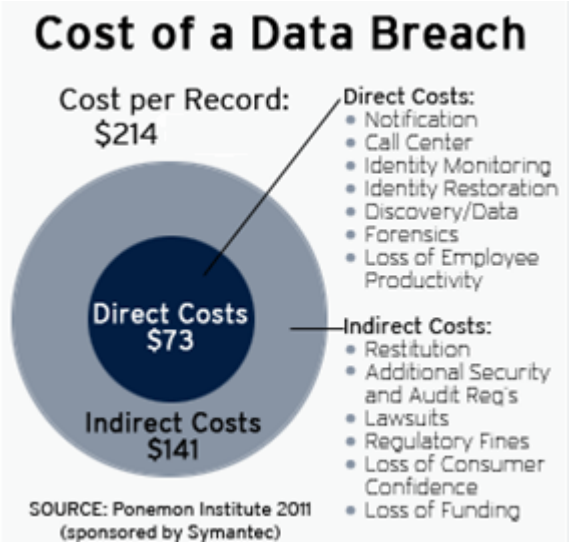
- Cyber threats are real
- The stakes are high
- Who are the “Bad Actors” that we are concerned about?
- What do they do with the data that they steal?
- How does an intrusion occur?
- How do we respond?
- What is our strategy?
- Where are our gaps?
- What are we doing to bridge the gaps?
- What can you do as a member of our organization?

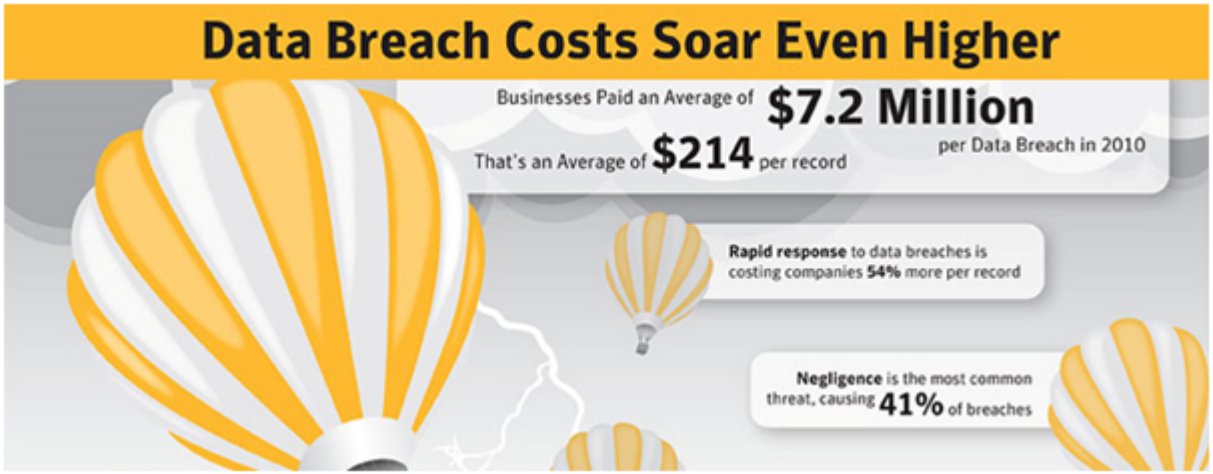
The Threat Is Real



And The Stakes Are High







Virus
Malware
Targeted Attacks
Phishing
Java
Removable Media
Social Engineering
Social Networking
Employee Carelessness

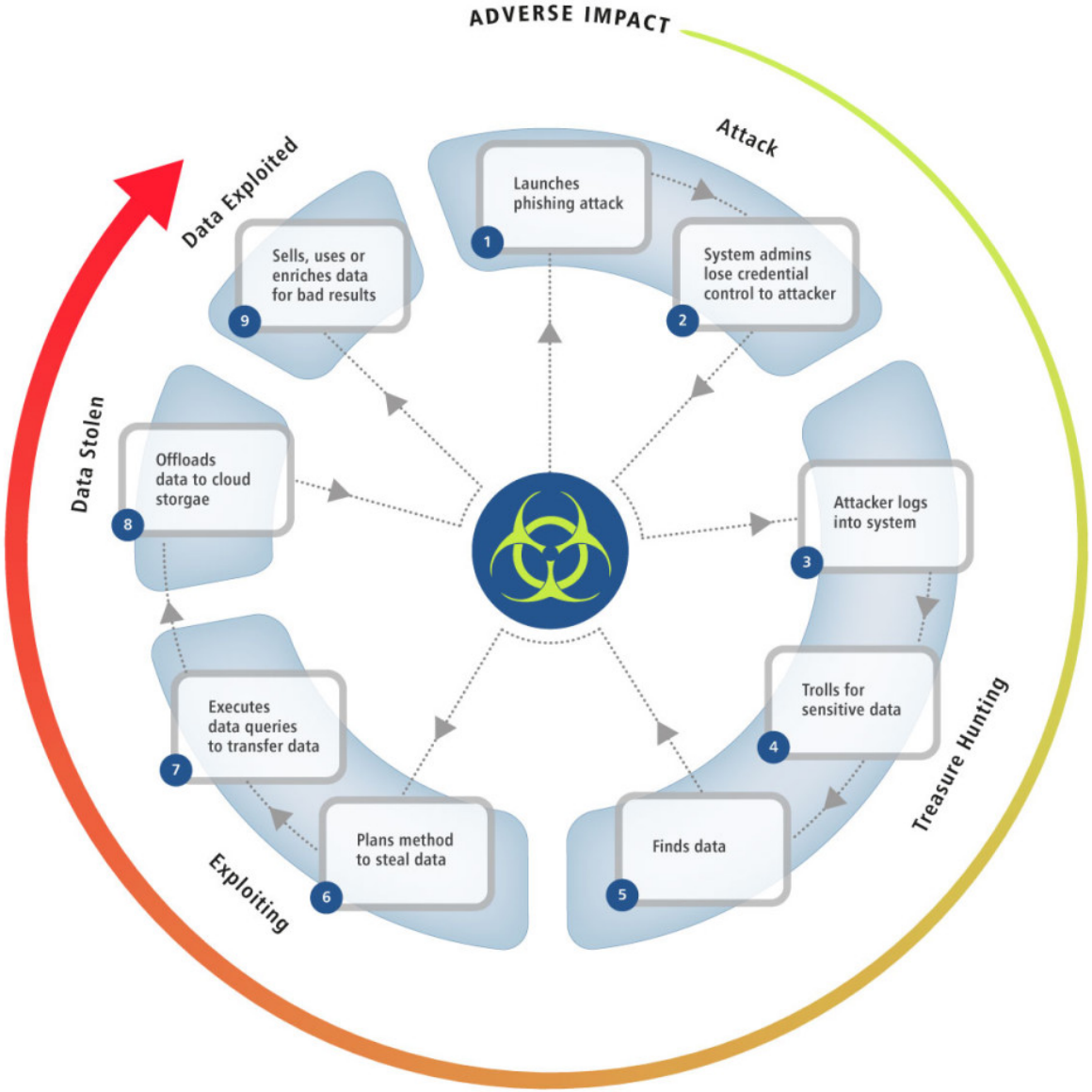
GROUP: Script Kiddies
TARGETS: Individuals, Opportunistic, Not Targeted
MOTIVE: Bragging Rights, Attention of Peers, Mischief, Identity Theft
METHODS: Scanning for vulnerabilities, pre-made scripts and tools that are widely available

GROUP: Hacktivist / Social Activist
TARGETS: Government Agencies, Corporations
MOTIVE: Bring Awareness to social causes / Damage Reputation, Disrupt Service, Intelligence
METHODS: Targeted Web Defacements, Denial of Service Attacks, Leakage of Sensitive Data used to expose or embarass

GROUP: State Sponsored Hackers
TARGETS: Government Agencies, Corporations, Utilities
MOTIVE: Espionage (Political and Industrial), Terrorism (Financial Damage, Instill Fear and Doubt)
METHODS: Targeted Attacks, Known Target Data, Advanced Persistent Threats

GROUP: Organized Cyber Criminals
TARGETS: Retail, Banking, Government Agencies
MOTIVE: Monetization of Stolen Digital Assets, Cyber Extortion, Fraud, Identity Theft, Bank Transfers
METHODS: Targeted Entities, Opportunistic, Data Exfiltration of PII


BINs:
Country:
Bank: (+$1)
Code: (+$1.5)
Level: (+$1)
Credit/Debit:
Type:
Base:
Any (4350
Any (4350
Any (43507)
Any (43507)
Any (43507)
Any
usa b2 t1
Search
Reset
USA
SPAIN
UK
TURKEY
NEW ZEALAND
NETHERLANDS
LUXEMBURG
DENMARK
BELGIUM
GERMANY
FINLAND
CANADA
NORWAY
ITALY
NIGERIA
BRAZIL
HONG KONG
SWEDEN
MALDIVES
CZECH REPUBLIC
RUSSIA
FRANCE
22
COUNTRIES
THE FAKE DATA TRAVELLED TO
22 DIFFERENT COUNTRIES AND
5 OF THE WORLD'S 7 CONTINENTS



Most Intrusions Are Caused By Human Error

Most Attacks Are Opportunistic

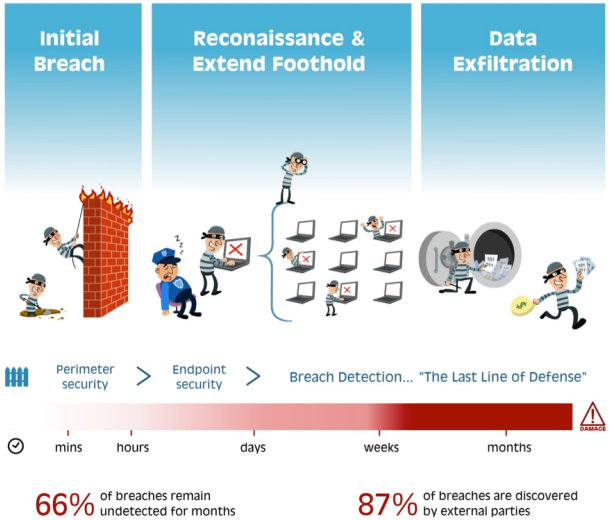
Bad Actors Are Patient

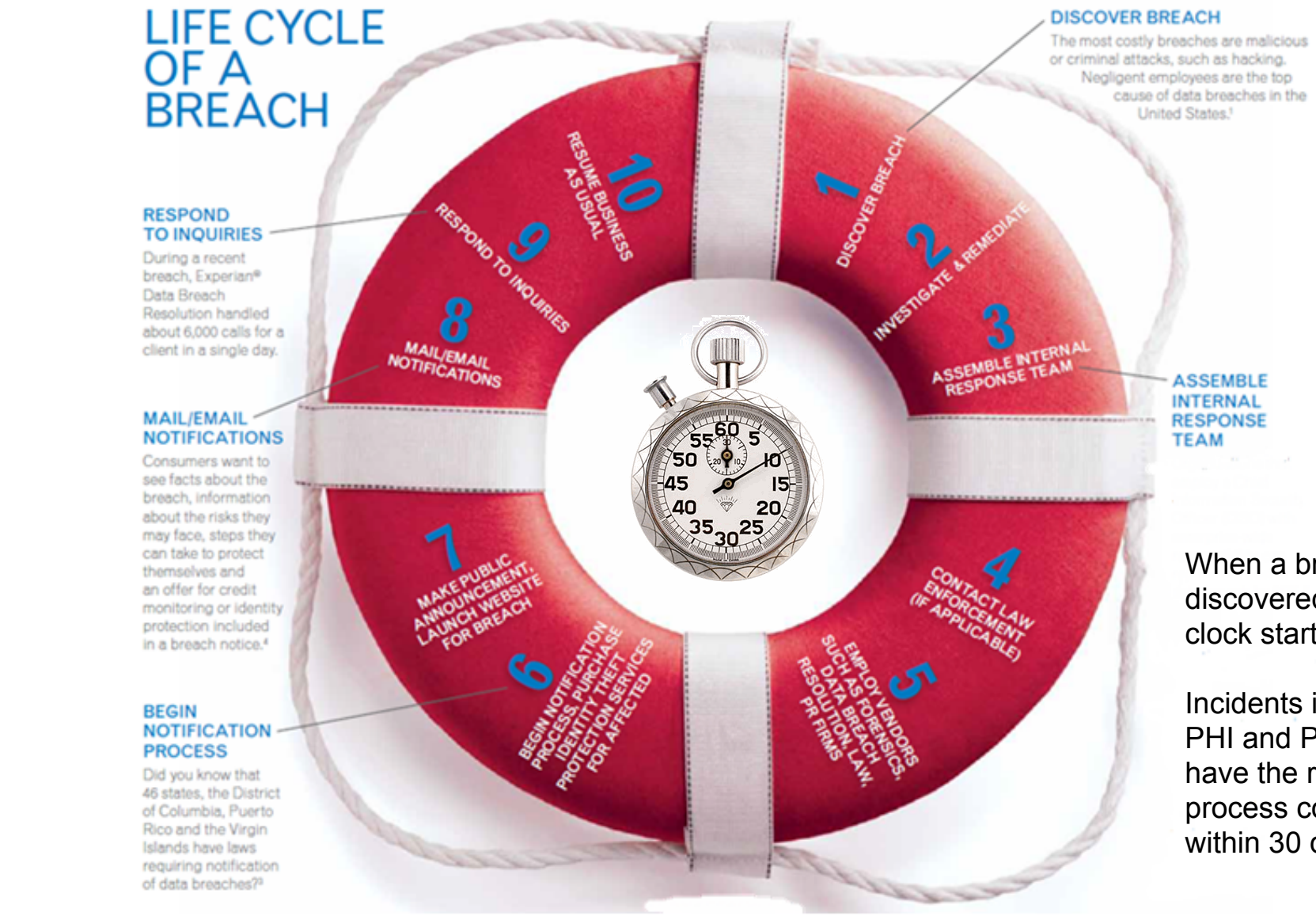
Bad Actors Are Smart and Well Funded

Average Time To Detection

243 DAYS

(Ponemon Institute)





When a breach is discovered, the clock starts ticking.

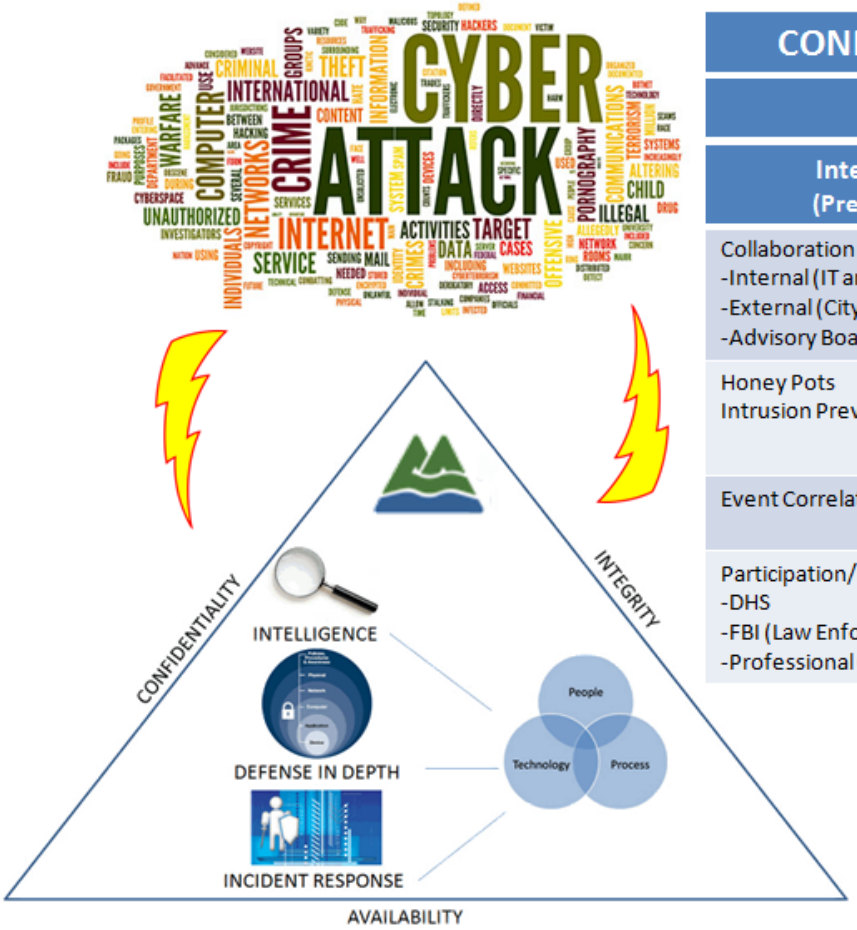
Incidents involving PHI and PII need to have the response process completed within 30 days.

VISION

"Become one of the most secure local governments in the U.S."

MISSION

To use a **3x3x3** Strategy of considering **People, Process** and **Technology** in our model of **Intelligence** (Prevention), **Defense in Depth** (Detection) and **Incident Response** (Remediation) while protecting **Confidentiality** (Privacy), **Integrity** (Data Protection) and **Availability** (Performance).



CONFIDENTIALITY-INTEGRITY-AVAILABILITY		
PEOPLE-PROCESS-TECHNOLOGY		
Intelligence (Prevention)	**Defense in Depth (Detection)**	**Incident Response (Remediation)**
Collaboration -Internal (IT and Others) -External (City, State, Industry) -Advisory Board	Technology -Perimeter -Endpoint	Elevate Team -Increase Skills -More Tier 1 Involvement
Honey Pots Intrusion Prevention	Human Firewall -Education -Awareness	Training Exercises -Table Top -War Room
Event Correlation	Multiple Layers Vendor Diversity	Mature Response Plan Proactive Response
Participation/Partnership -DHS -FBI (Law Enforcement) -Professional Organizations	Proactive Monitoring Early Detection	Quick Resolution RPO-RTO Lessons Learned

MULTNOMAH COUNTY
CYBER SECURITY

Applying Our Strategy And Roadmap To An Established Framework Will Deliver Results

IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

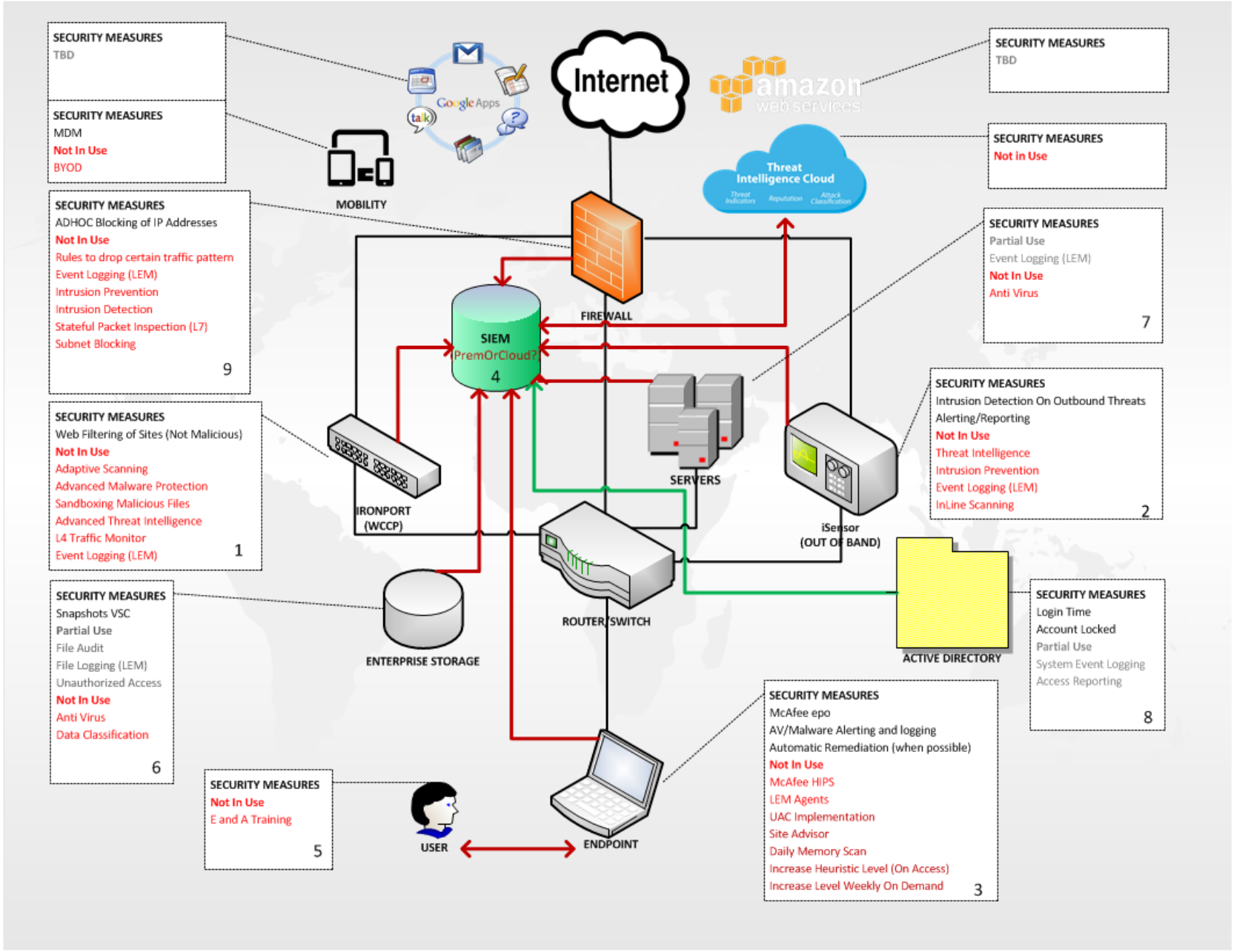
RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery planning
- Improvements
- Communications

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


SECURITY MEASURES
TBD
SECURITY MEASURES
MDM
Not In Use
BYOD
MOBILITY
Google Apps
Internet
amazon web services
SECURITY MEASURES
TBD
Threat Intelligence Cloud
SECURITY MEASURES
Not In Use
SECURITY MEASURES
ADHOC Blocking of IP Addresses
Not In Use
Rules to drop certain traffic pattern
Event Logging (LEM)
Intrusion Prevention
Intrusion Detection
Stateful Packet Inspection (L7)
Subnet Blocking
9
FIREWALL
SIEM
(PremOrCloud?)
4
SECURITY MEASURES
Partial Use
Event Logging (LEM)
Not In Use
Anti Virus
7
SECURITY MEASURES
Web Filtering of Sites (Not Malicious)
Not In Use
Adaptive Scanning
Advanced Malware Protection
Sandboxing Malicious Files
Advanced Threat Intelligence
L4 Traffic Monitor
Event Logging (LEM)
1
IRONPORT
(WCCP)
SERVERS
SECURITY MEASURES
Intrusion Detection On Outbound Threats
Alerting/Reporting
Not In Use
Threat Intelligence
Intrusion Prevention
Event Logging (LEM)
InLine Scanning
2
iSensor
(OUT OF BAND)
ROUTER/SWITCH
SECURITY MEASURES
Snapshots VSC
Partial Use
File Audit
File Logging (LEM)
Unauthorized Access
Not In Use
Anti Virus
Data Classification
6
ENTERPRISE STORAGE
ACTIVE DIRECTORY
SECURITY MEASURES
Login Time
Account Locked
Partial Use
System Event Logging
Access Reporting
8
SECURITY MEASURES
Not In Use
E and A Training
5
USER
ENDPOINT
SECURITY MEASURES
McAfee epo
AV/Malware Alerting and logging
Automatic Remediation (when possible)
Not In Use
McAfee HIPS
LEM Agents
UAC Implementation
Site Advisor
Daily Memory Scan
Increase Heuristic Level (On Access)
Increase Level Weekly On Demand
3

Efforts For FY16

Area	What Have We Done	Next Steps FY16
End Point Protection	* Increased Heuristics (Detection) for Scanning * Increased Detection Level for Weekly Scans * Implemented Daily Memory Scan	* Hardware Intrusion Detection
Web Filtering	* Added Advanced Malware Protection to scan files transferred * Added Participation in the Threat Intelligence Cloud	* Safer Web Browsing Technology
End User Awareness	* Began Conducting Random Phishing Training Program * Consistent Cadence of Wednesday Wire Articles * Security Presentations to Groups Outside of IT * Planning Events for Cyber-Security Awareness Monty	* Mandatory Awareness Training for All Couty Employees * Increased Routine Phishing Education * Increased Communication through Relevant Web Presence * Development of Clear Standards for Development and Deployment
Firewall	* Beginnng the Process of Defining Requirements For Next Gen Firewalls * Manual Blocking of Known Malicious IP Addresses	* Next Generation Firewalls with Threat Intelligence * Correlation of Log Files with Events from Other Devices
Mobile Device Management	* Participation in BYOD Project	* Anti-Virus and Malware Protection on County Phones
Cloud Application	* Manual Upload of Known Spam and Phishing Sites into Google Deny List	* Extra Layer of Protection Above Google Apps * Mandatory Security Reviews of Cloud Services * Automatic Threat Intelligence Feeds to Screen Email * Compliance Control in Google Docs
Servers	* Started the Process of Installing Anti-Virus on County Servers	
Intrusion Prevention	* Installed Technology that Blocks Intrusion Attempts and Known Malicious Traffic	* Additional Intrusion Prevention on the Firewall
Intrusion Detection	* Installed Technology that Provides RealTime Alerts of Intrusion Attempts and Malicious Traffic	* Additional Intrusion Detection on the Firewall
Active Directory	* Federated Login Services for most Major Services	* Data Classification * Role Based Authentication
SAP Security	* Audit of Access Roles and Removal of Unneeded Access	* Continue to Audit Roles, Access and Data-Dei-dentification

WHAT'S MISSING?

THE HUMAN FIREWALL IS CRITICAL

STOP … THINK … CONNECT

BE SUSPICIOUS OF EMAILS FROM UNKNOWN SOURCES

NEVER SHARE YOUR PASSWORDS

REPORT ALL SUSPICIOUS CYBER ACTIVITY TO THE HELPDESK

DON'T CLICK ON LINKS IN EMAILS OR OPEN SUSPICIOUS ATTACHMENTS

SPREAD THE WORD / CREATE A CULTURE OF AWARENESS !

USE SECURE OR ENCRYPTED EMAIL WHEN SENDING CONFIDENTIAL INFORMATION

This Presentation Can Be Tailored To Your Organization.

If you would like IT Security to make a presentation to your group please contact: it.security@multco.us

CYBER SECURITY IS OUR SHARED RESPONSIBILITY

Thank You

MULTNOMAH COUNTY
CYBER SECURITY