



Cyber Security / Cyber Liability

Presented by

Doug Selix, MBA, CISSP, CISM, PMP
The Office of Risk Management

What is Cyber Security?

Cyber security is defined as:

“Measures taken to protect a computer or computer system (as on the Internet) *and the data they contain* against unauthorized access or attack.”

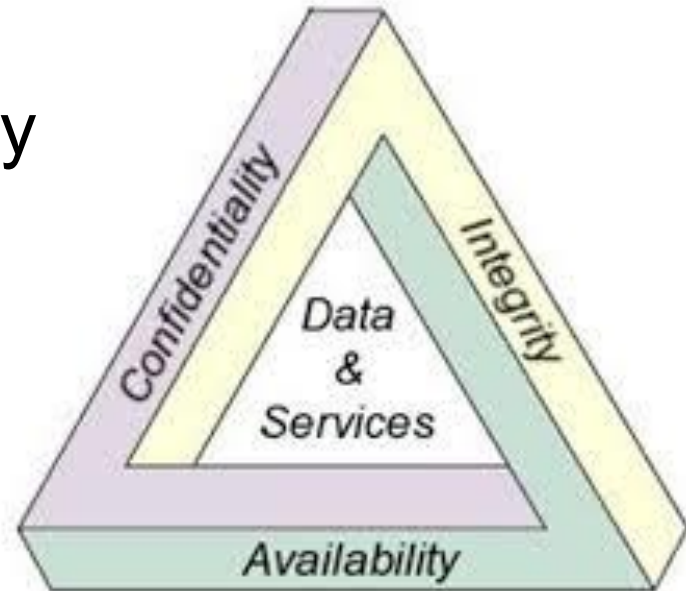
<http://www.merriam-webster.com/dictionary/cybersecurity>



Cyber Liability

IT Security Context

- A Security Incident that results in the:
 - Loss of “Data Confidentiality”
 - Loss of “Data Integrity”
 - Loss of “Data Availability”



The Big Picture – Breaches Happen

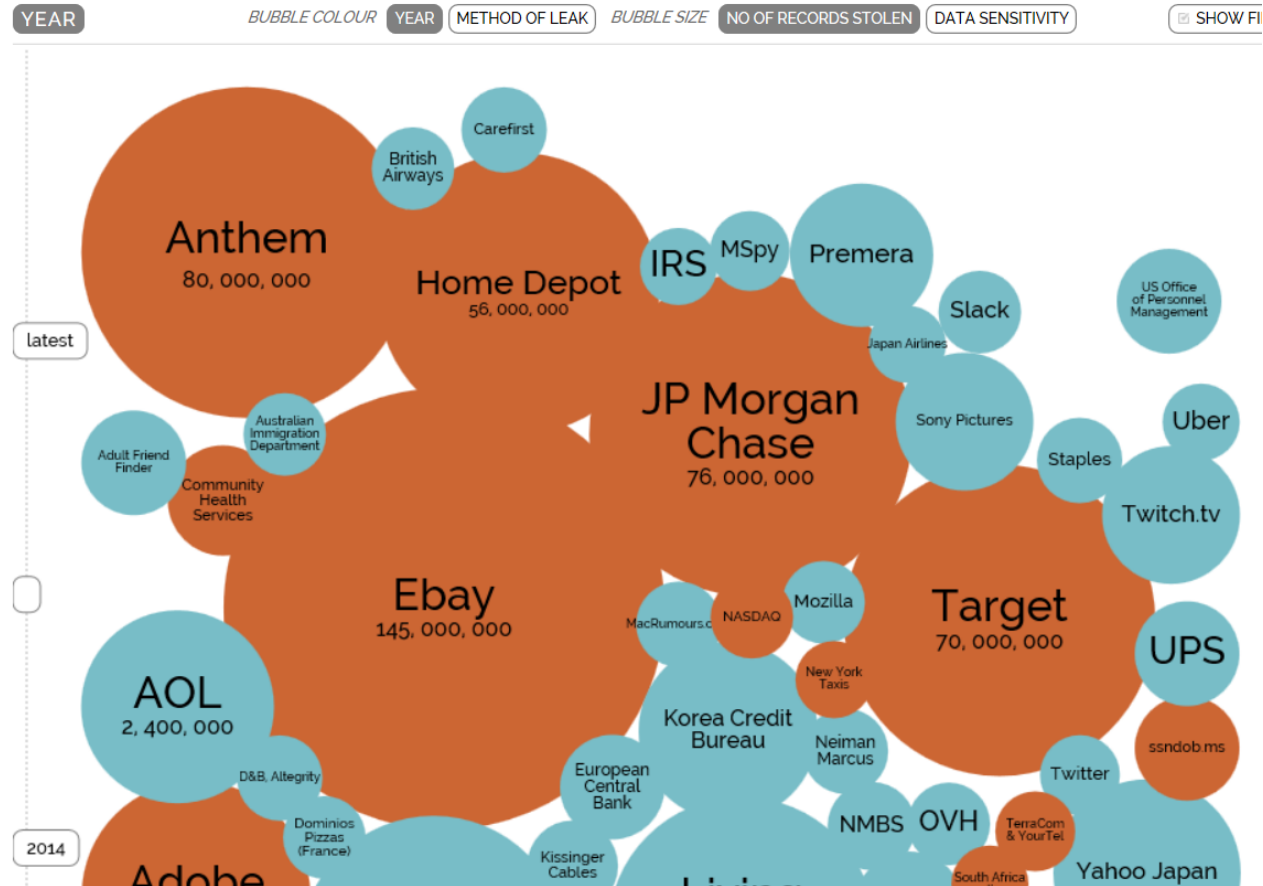
The Open Security Foundation's DataLossDB gathers information about events involving the loss, theft, or exposure of personally identifiable information (PII).



World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 6th June 2015)

interesting story



Source: www.InformationisBeautiful.com



Think About This

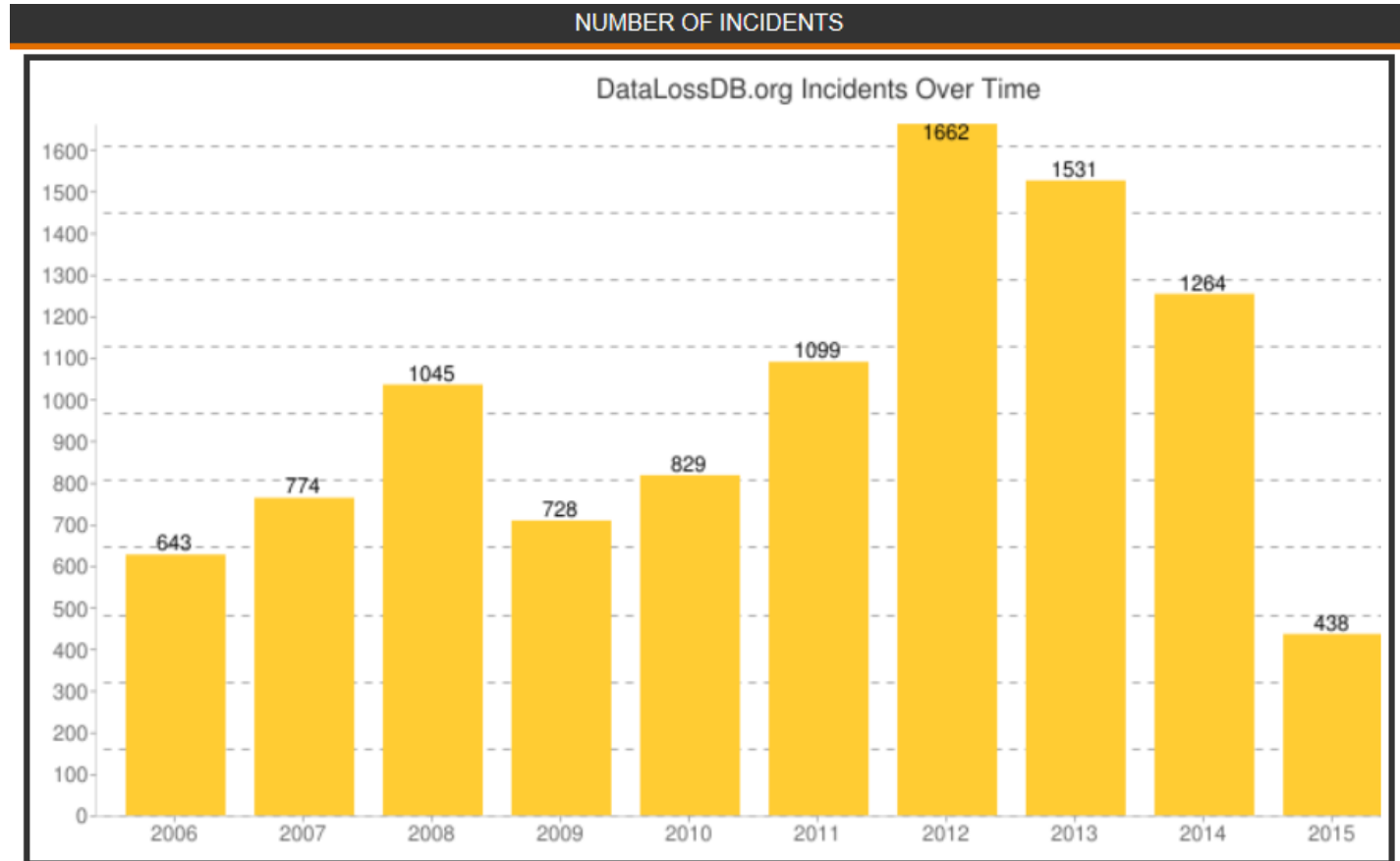
- **Most Breaches Are Avoidable**
 - 92% of attacks are not highly difficult
 - 83% of victims were targets of opportunity
 - 92% stemmed from external agents
 - 17% implicated insiders
 - 96% of breaches were avoidable through simple or intermediate controls

Source: Verizon Data Breach Investigations Reports (2011-2015)



Probabilities are Low, Impacts High

The Open Security Foundation's DataLossDB gathers information about events involving the loss, theft, or exposure of personally identifiable information (PII).



What Data Are We Talking About?

- Data that can cause financial harm to your agency “if” it is not kept secure
 - Personally identifiable information (RCW 42.56.590)
 - Electronic personal health information (HIPAA Security Rule)
 - Credit card information (PCI Data Security Standard)
 - Bank account information used to process electronic fund transfers or payments
 - IRS tax information (IRS 1075)
 - Student education information (FERPA)
 - Data protected by attorney client privilege
 - Criminal justice information (FBI CJIS standards)
 - Proprietary information (agreement, contract, or license)



Why Are We Focused On These?

Data Breaches Cost Money We Don't Have!

Data Types with Liability Risk	Sources of Data Breach Cost							Loss of Reputation
	Breach Response, Analysis, and Forensics	Breach Notification	Regulatory Fines	Pre-Claim Loss Control	Significant 3rd Party Cost Claims	Post-Claim Litigation	Cyber Extortion	
Credit card information	X	X		X	X	X	X	X
Electronic personal health Information	X	X	X			X	X	X
Bank account information	X	X	X	X	X	X	X	X
Personally identifiable information	X	X		X		X	X	X
IRS tax information	X	X	X		X	X	X	X
Student education information	X	X	X			X	X	X
Data protected by attorney-client privilege	X	X			X	X	X	X
Criminal justice information	X	X	X			X	X	X
Proprietary information	X	X			X	X	X	X

- ✓ \$3/Record – EWU 2009 actual cost
- ✓ \$172/Record ([Ponemon Institute 2014 US Cost of a Data Security Breach Report](#))
- ✓ \$73/Record ([Ponemon Institute 2015 US Cost of a Data Security Breach Report](#))



Do You Know How Much Cyber Liability Risk You Have Today?

- Quantify Your Confidential Data
- Compute Cyber Liability Risk Exposure
- Worksheet used by DES ORM

Sample - Data Breach Risk Exposure Worksheet																							
Type of Data	Unique Records	Data Source	Data Location	Data Shared With	Applicable Data Security Regulation	Data Breach Impact						Cost of a Data Breach Estimate						Funding Source					
						Notification	Root Cause Investigation	Regulatory Fines	Credit Monitoring for 3rd Parties	Legal Defense	Damages to 3rd Parties	Cost per Record to Notify	2014 Public Sector Market Cost per Record (Note 1)	Regulatory Fine Cost (Note 2)	Min Cost Estimate	Max Cost Estimate	Most Likely Cost for full notification and credit services	Notice Cost Limit (RCW 42.56.590.7c) (Note 3)	Regulatory Fines	Most Likely Cost (Net)	Agency Budget	PEPIP Cyber Liability Insurance	Cyber Liability Insurance AIG Layer
System 1 (PII)	0				RCW 42.56.590	Yes	Yes	No	No	No	No	\$3	\$107	0	\$0	\$0	\$0	\$250,000	\$0	\$250,000	\$100,000	\$150,000	\$0
System 2 (HIPAA)	0				HIPAA	Yes	Yes	Yes	No	No	No	\$3	\$107	1,000,000	\$1,000,000	\$1,000,000	\$1,000,000	\$0	\$1,000,000	\$1,000,000	\$100,000	\$900,000	\$0
System 3(Credit Card)	0				PCI	Yes	Yes	Yes	Yes	Yes	Yes	\$3	\$107	0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
System 4 (Bank Accounts)	0				RCW 42.56.590	Yes	Yes	No	No	No	No	\$3	\$107	0	\$0	\$0	\$0	\$250,000	\$0	\$250,000	\$100,000	\$150,000	\$0
System 5 (IRS Pub 1075)	0				IRS Publication 1075	Yes	Yes	Yes	No	No	No	\$3	\$107	0	\$0	\$0	\$0	\$250,000	\$0	\$250,000	\$100,000	\$150,000	\$0
System 6 (FERPA)	0				FERPA	Yes	Yes	No	No	No	No	\$3	\$107	0	\$0	\$0	\$0	\$250,000	\$0	\$250,000	\$100,000	\$150,000	\$0
Maximum Data Breach Risk Exposure	0														\$1,000,000	\$1,000,000	\$1,000,000	\$250,000		\$1,000,000			\$0
NOTES -->						NOTE -1 The high estimate is based on \$172 per record cost for the Public Sector that comes from the 2014 Ponemon Institute Cost of a Data Breach Study. That study also breaks down the elements of this cost. One element they include is "Lost Customer Business". We have removed this from the estimate above because the State is a monopoly. If we have a breach we will not loose business. Our planning number is \$107.						NOTE -2 a) IRS Fine based on \$25/record b) HIPAA Fine - Arbitrary estimate based on HHS/OCR cases						NOTE -3 RCW 42.56.590 allows agencies to use mass media for notification if cost is over \$250,000 or the number of notices exceed 5000,000. Estimate assumes we would use this provision in the event of a breach					
												Security Breach Risk Exposure if Agency is NOT in the Master Property Insurance Program						Uninsured Risk Exposure if Agency is in the Master Property Insurance Program					



Thoughts on Compliance

- PII Data – Rules are Changing
 - [RCW 42.56.590](#) - Breach Notice Context
 - [House Bill 1078](#) – 45 days to give notice
 - Substitute notice may be available
- Some of you have HIPAA Data
 - HIPAA - Breach Notice Context
 - Must send notice to all individuals
 - 60 days to complete notice
 - Risk of regulatory penalties



How Most Breaches Happen - Short Answer

- Requires a trusted person to do something the bad guys want you to do
 - Mistakes / Poor Judgement
 - Phishing and spear phishing attacks
- Requires your computer to be poorly defended
 - Missing or out-of-date anti-virus protection
 - Missing patches
 - Local administrator privilege



WA Local Government Cyber Liability Incidents

- City of Burlington WA – 2012
 - \$400K stolen from city bank account
- Skagit County Transit – 2012
 - \$300K failed attack on bank account
- Chelan County Hospital District - 2013
 - \$1 million stolen from bank account
- Skagit County – 2014
 - \$215K HIPAA violation federal fine



Data Breach

Incident Example – Deeper Dive

Idaho State University – August 2011

- **Direct Costs:**
 - \$52,500 - Cost to notify (~\$3/Name)
 - \$36,750 - Cost to offer credit monitoring (~\$14/Name, 15% opt in)
2,625 @ \$14/Ea. = \$36,750
 - \$400,000 - HIPAA Fine
- **Indirect Costs:**
 - Effort to respond to the incident
 - ISU Worked with DHH/OCR for over a year
 - Effort to gain compliance
 - Effort to correct underlying security problems that lead to the breach
- **Root cause: Human Error**
 - System administrator turned off the firewall protecting a university server storing the ePHI.



Contributing Risk Factors

- Cyber security is a “business problem,” not an IT problem. It is about acceptable risk – apply ERM Principles
- The bad guys are really good
- Public agencies are resource constrained – can’t do it all
- Prevailing denial – won’t happen to us
- Good IT security is complex – not free
- IT security is rarely complete – technology can only go so far (No firewall for stupid)
- Cyber risks are not well understood or well managed
- Probabilities of a cyber incident are low, impacts can be huge



Contributing Risk Factors

Seven Worst Security Mistakes Senior Executives Make

1. Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job.
2. Failing to understand the relationship of information security to the business problem-they understand physical security but do not see the consequences of poor information security.
3. Failing to deal with the operational aspects of security: making a few fixes and then not allowing the follow through necessary to ensure the problems stay fixed
4. Relying primarily on a firewall.
5. Failing to realize how much money their information and organizational reputations are worth.
6. Authorizing reactive, short-term fixes so problems re-emerge rapidly.
7. Pretending the problem will go away if they ignore it.



The Bottom Line: Cyber Risks Are Increasing

- State and local government organizations are targets and are not well defended
 - Traditional defenses are no longer effective
 - Probability of successful attack increasing
 - IT security is not well managed in most organizations
 - Workstations are the front line of this battle space
 - IT security mistakes are happening too often
 - We have too much old insecure technology in use
 - IT Management not incentivized to be secure
 - We do not understand our Cyber Liability Risks
 - Etc.





“Good” Security Covers the Basics

- Make sure you have “Minimum Security”
- Minimum Security = SANS 20 Critical Controls

<http://www.sans.org/critical-security-controls/>

- [1: Inventory of Authorized and Unauthorized Devices](#)
- [2: Inventory of Authorized and Unauthorized Software](#)
- [3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers](#)
- [4: Continuous Vulnerability Assessment and Remediation](#)
- [5: Malware Defenses](#)
- [6: Application Software Security](#)
- [7: Wireless Device Control](#)
- [8: Data Recovery Capability](#)
- [9: Security Skills Assessment and Appropriate Training to Fill Gaps](#)
- [10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches](#)
- [11: Limitation and Control of Network Ports, Protocols, and Services](#)
- [12: Controlled Use of Administrative Privileges](#)
- [13: Boundary Defense](#)
- [14: Maintenance, Monitoring, and Analysis of Audit Logs](#)
- [15: Controlled Access Based on the Need to Know](#)
- [16: Account Monitoring and Control](#)
- [17: Data Loss Prevention](#)
- [18: Incident Response and Management](#)
- [19: Secure Network Engineering](#)
- [20: Penetration Tests and Red Team Exercises](#)

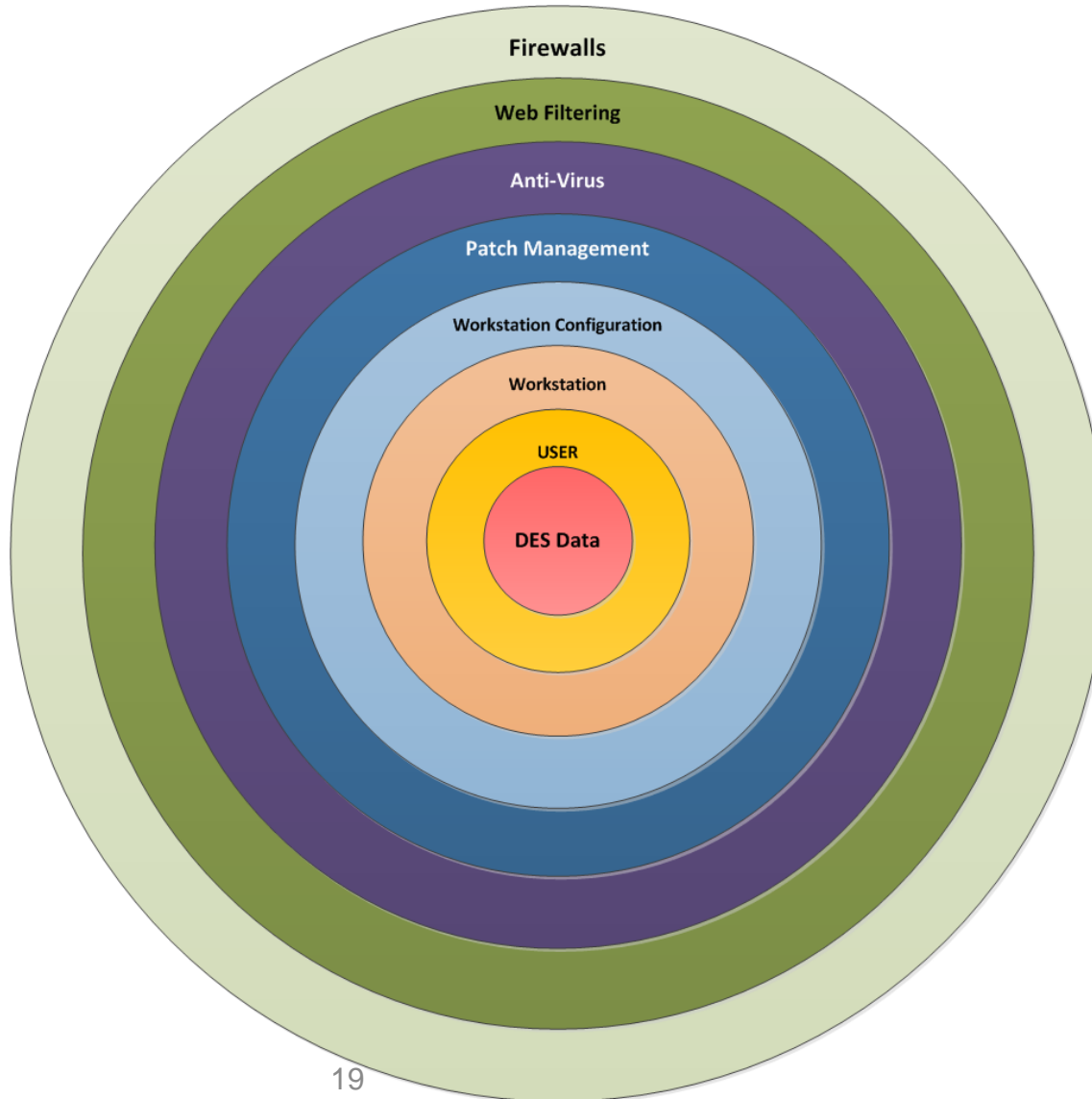


IT Security is an Investment

- **Cyber Defense needs an Investment Plan**
 - Understand what problem you are trying to fix
 - Treat it like any other capital investment
 - Based on a Business Case and ROI
 - IT Security has a lifecycle (acquire, maintain, monitor, upgrade)
 - Manage change
 - Manage the risks
 - Hold IT accountable
 - Transfer risk when you can, finance it when you can't



Our Goal – Defense in Depth



The Finance Officer - Challenge

- **Big Questions:**

1. How do you measure Cyber Liability Risk?
2. How much residual Cyber Liability Risk is appropriate for your agency?
3. If a data breach happens to your agency, how are you going to pay for it? And who is going to do the work?
4. How much security spend is enough?

- **Lead from Where You are:**

You can influence getting the right things done, before and after a security incident?





Switch Gears



What Happens if “it” Happens?

Security Event Incident Response



Working Analogy

- **Think of an IT security incident like a house fire:**
 - Call 911 and ask for help
 - Fire department puts out the flame
 - Property owner cleans up the mess
 - If insured then there is help provided by the insurance company
 - Resources to clean-up and reconstruct
 - Funds to pay out of pocket costs over the deductible up to the policy limit
 - If not, the property owner pays all costs.



Follow Your Incident Response Plan, Right?



**Incident Response
Team Follows the Plan**



Who's Got The Plan?



Or Maybe Not

- We can deal with whatever comes up.....



Most IT/IR Plans Stops Short



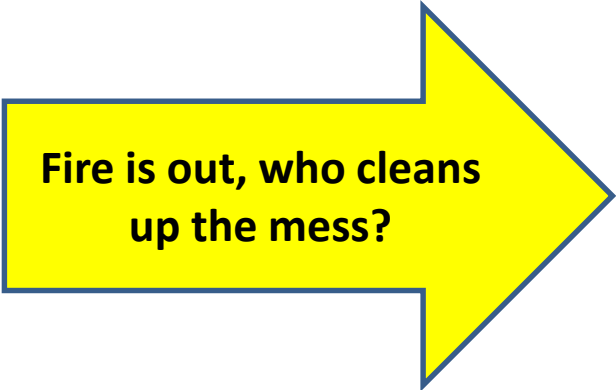
Focus tends to
be on putting out
the flame.

Was there a data
security breach?



Our Working Assumption:

- It is rare to find a Cyber Security Incident Response Plan that includes steps to be taken in the event of a data security breach. Most organizations wing it.....



**Fire is out, who cleans
up the mess?**





Switch Gears



Insurance as a tool to
Clean Up the Mess



Insurance Context

- Cyber Liability Insurance covers:
 - 1st Party Damages
 - 3rd Party Liabilities



Insurance Context

Cyber Liability Risks

- 1st Party Damages – Common Insurable Losses
 - Cost for forensic investigation to find the cause of the damage
 - Cost to figure out if/what data was breached
 - Cost to comply with Breach Notification Regulations (RCW, HIPAA, FERPA, etc.)
 - Cost for customer Risk Mitigation Services



Insurance Context

Cyber Liability Risks

- 1st Party Damages – Continued
 - Expert Legal Advice
 - Expert Public Relations Advice
 - Expert Crisis Management Advice
 - Cyber Extortion Payments
 - Cost to Restore Data Integrity or Availability
 - Lost Income and Extra Operating Cost due to network interruption



Insurance Context

Cyber Liability Risks

- 3rd Party Liability
 - 3rd party damage claims
 - 3rd party litigation
 - Web media damage claims (e.g. copyright or trademark infringement, defamation, invasion of privacy)
 - Regulatory defense and penalties



Montana Lessons Learned

May 2014 HIPAA Breach



1.3 Million Dept. of Health
Patient Records.
\$5M Cost So Far
\$3M Insured
No HIPAA Fine To-Date

- **Cyber Liability Insurance Worked**
- **Response Services Worked**
 - Rapid Response
 - Event/Crises Management
 - Forensic Analysis
 - Root Cause
 - Determine Data Exposure
 - Legal Services
 - Public Relations Services
 - Notification Production
 - Call Center Operation
 - Manage Internal Reporting (Gov)



Think About This

- **Most Breaches Are Avoidable**
 - 92% of attacks are not highly difficult
 - 83% of victims were targets of opportunity
 - 92% stemmed from external agents
 - 17% implicated insiders
 - 96% of breaches were avoidable through simple or intermediate controls

Source: Verizon Data Breach Investigations Reports (2011-2015)



Questions

Thank you!



Speaker Contact Information

Doug Selix, CISM, CISSP, PMP

Cyber Liability Program Manager

Department of Enterprise Services, Office of Risk Management

Office Phone: 360-407-8081

Email: doug.selix@des.wa.gov

