# Surveying the World of Cyber Risk

**Agnes Kirk**
**Chief Information Security Officer**
**State of Washington**

# Threats to State Government

1. Insider Threat (58%)
2. Network Vulnerability (46%)
3. Botnet (42%)
4. Mobile (25%)
5. Phishing (18%)

*Source: 2012 CISO Study*

# Nearly a Billion Records Were Compromised in 2014

CSO Online 11/2014.

# Business Disruption From a Data Breach Alone Can Cost $930K

2013 FireEye, Inc.

# 85% of Breaches Were Due to External Hackers

## Major Causes

- Inadequate protection of supply chain
- Lack of awareness training for staff and vendors

## Results

- Weak access for 3rd party vendors
- Successful Phishing attacks

CSO Online 11/2014.

# The Changing Landscape

## We are an Interconnected World

- Interdependencies Drive Business
- Little Fish; Big Fish

## Big Data Leads to Big Theft

- Criminals Savvy About Risk vs. Reward
- Big Plies of Data – More Willing to Put in Effort

# The Changing Landscape

## Criminals favor PII over Financials

- Easier to Sell and Leverage
- Banks are making it harder to use stolen credit cards
- Harder to Recover your Identity Than Cancel a Credit Card

# The Challenge

## Ability to Effectively Detect and Respond to Security Threats on a Network Requires Specialized Training and Skills

- Sophistication of Attacks
- Multiple Points of Entry Into Systems
- Time Sensitivity
- Need to Share Information

# Cyber Is A Risk Category That Has The Potential to Impact Other Business Risks

# Business Risks

- Strategic Risk
- Financial Risk
- Operational Risk
- Compliance Risk

# How Much Does Enough Security Cost?

- Percentage of IT Budget Spent on Security
  - Average Company 3 - 5%
  - IT Industry 11.3 %
  - Finance 8.3%
  - Education <4 %*

- Average Security Spend (% of Revenue)

  .12% - .30% ~ Cost of Insurance

# What Have We Learned?

## Basic Security Controls Are Still Missing

- Don’t Know Where the Data Is
- Devices Have Default Config and Passwords
- Patching Isn't Up to Date
- Lack of Access Control to Critical Systems
- Little or No Employee Security Awareness Training
- Security Policies & Practices

# Personal Cheat Sheet-The Do's

- Turn in USB thumb drives that you find without plugging them in
- Be aware of phishing emails that follow natural disasters and large news stories.
- Remember that once you send something electronically, it can easily be out there forever.
- Clear your browsing cache and history after using a public or shared computer.

# Personal Cheat Sheet-The Do's

- Lock your computer when you leave, even if it is for a moment.
- Don't charge your phone by plugging it into your workstation –malware can jump between them.
- Use unique and complex passwords. If you need help remembering, try a password vault.

# Personal Cheat Sheet-The Dont's

- Don't use the same USB thumb drive for work and at home
- Don't check personal email from your workstation
- Don't trust unexpected emails, even if they are from people you know
- Don't provide your password to anyone, even the help desk

# The Big Phish

Phishing is one of the most common ways to install malware on your system. Here are a few ways to detect a phishing email. If you find one, report it to your help desk!

# The Big Phish

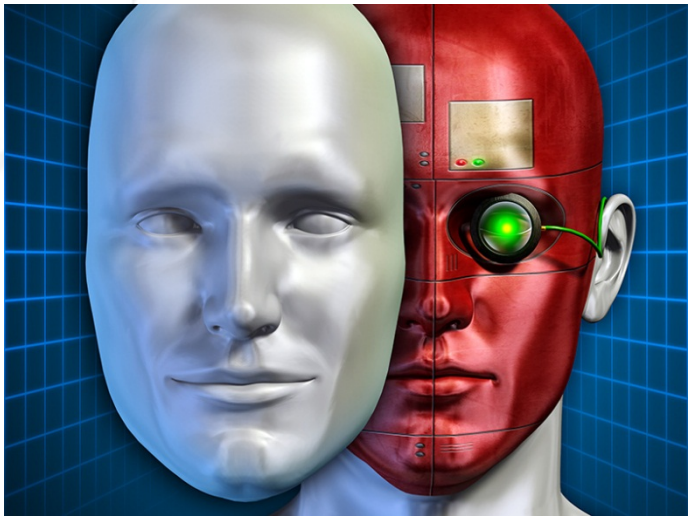
- Misspelled words
- Improper grammar
- The email asks you to click a link or open an attachment to get the full message
- Threats or alarming statements are used to create a sense of emergency
- The domain shown when you mouse-over a link doesn’t match who the sender claims to be

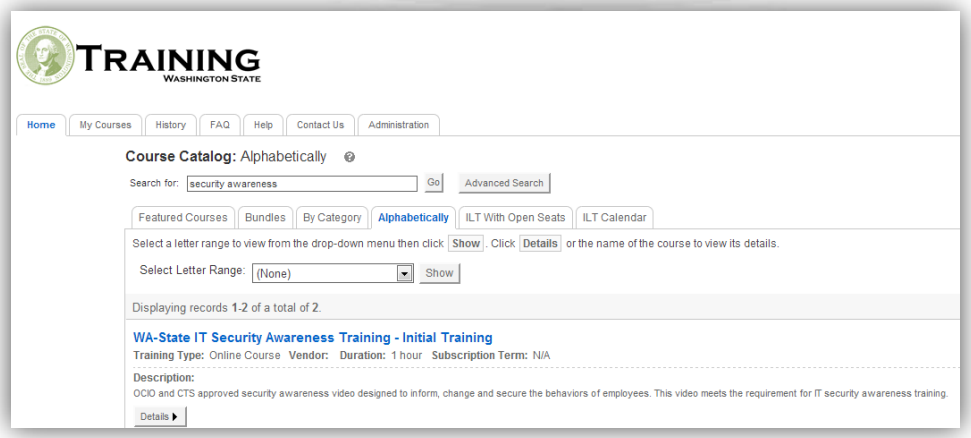
# What Are We Doing?

- Security Operations Center
- Logging & Monitoring Services
- Enterprise Forward Proxy
- Vulnerability Scanning
- Discovery Tool
- Data Loss Prevention
- Security Assessments

# Security Awareness Training

*Available from the DES Enterprise LMS.*





# Service – Awareness
# Monthly Newsletters, Tips, and Tabletops

- Posted on SharePoint
- http://sharepoint.dis.wa.gov/soc/default.aspx
- Weekly Security Tips
- Monthly Newsletters
- Monthly Tabletop Ideas

CTS Enterprise Security Services

Consolidated Technology Services • WA

**Monthly Security Tips NEWSLETTER**

**September 2012**

**Using Encryption to Protect Data**

According to the Privacy Rights Clearinghouse, more than 19 million records have been involve
far this year. Protection of data requires multiple layers of defense, and the use of encryption to

**The September 2012 Tabletop Exercise Scenario:**

*The browser deployed on all machines in your organization has a signifi*
*actively being exploited. You have already identified 10 machines that a*
*and the help desk call volume due to this problem continues to increase*

*There is currently no vendor patch or vendor workaround. A patch is an*

What do you do?

1. Temporarily suspend web based access to the Internet until a patch is
2. Employ a different browser and tell everyone to use this new browser?
3. Employ a 3rd party patch which resolves this current zero day vulnerability?

News

***Security Tip***

## Lock your workstation before you leave your desk

March 25, 2013

Did you know there are keyboard shortcuts other than CRTL+ALT+DEL that you can use to lock your desktop? This
prevent people from walking up and snooping on your computer. You can save a keystroke by simultaneously press
the Windows key + L. The Windows key has four wavy squares.

Or, to make things even easier, create a desktop shortcut.

# MS-ISAC

Join online at:
http://msisac.cisecurity.org/members/register/

The MS-ISAC membership is open to representatives from all 50 states and local and tribal governments. There is no cost to become a member.

# Washington State Patrol

- Capitol Campus Agencies contact Lt. Jeff Swanson of Special Operations Division
- All other state agencies contact local jurisdictions

The State Patrol High Tech Crime Unit focuses upon localized crimes.

# FBI Cyber Task Force

- Contact local field office

The mission of the Cyber Task Force is to support the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors…

# Questions?

**Agnes.Kirk@cts.wa.gov**