



# Office of the Washington State Auditor

---

Pat McCarthy

## Internal Cybersecurity Risks

**Peg Bodin, CISA – Local IS Audit Program Manager**

**Michael Hjermsstad – Local IS Audit Assistant Manager**

**Utchay Okorie, CISSP, CCNA Security, Security+,**

**– Performance Audit Info Security Analyst**

# The risk

The following BEC/EAC statistics were reported in victim complaints to the IC3 from **October 2013 to December 2016:**

Total U.S. victims:	22,292
Total U.S. exposed dollar loss:	\$1,594,503,669
Total non-U.S. victims:	2,053
Total non-U.S. exposed dollar loss:	\$626,915,475

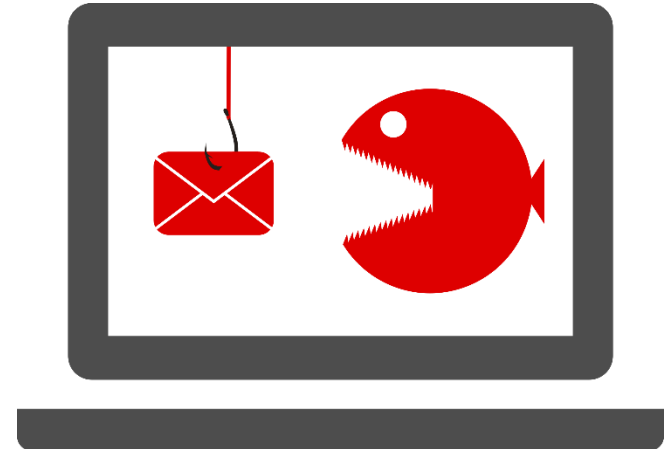
*BEC = Business Email Compromise*

*EAC = Email Account Compromise*

Source: IC3 (Internet Crime Complaint Center)

# Phishing emails

- Your W-2 is available online, click here (sent in mid- to late January)
- Win Seahawks tickets!



## **Phishing Campaign:**

Open: 1 minute, 40 seconds

Click: 3 minutes, 45 seconds

*Source: Verizon 2016 DBIR*

# Business email and email account compromise scams

- I'm your boss, please respond to me, via return email, an employee report (with SSNs)
- I'm your boss, I need you to transfer \$\$\$ to this bank account
- I'm your vendor, pay this invoice and send the \$\$\$ to this bank account



# Phishing really works — well



- *“most successful variety [of social engineering] is phishing”*
- *“30% of phishing messages were opened”*



- *Reliance on employees for advanced phishing detection*



- *Phishing as a service is twice as profitable as traditional phishing*

# What is phishing?

## ANATOMY OF A SPEAR PHISHING ATTACK

9. The hacker uses the backdoor to steal information



1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/smartphone/network.



7. A link is clicked or attachment opened.



6. The email is opened because they 'know' the sender.



2. Following the social trail, he identifies other people the employee may know.

5. The email passes the spam filter and arrives at the employee's inbox.



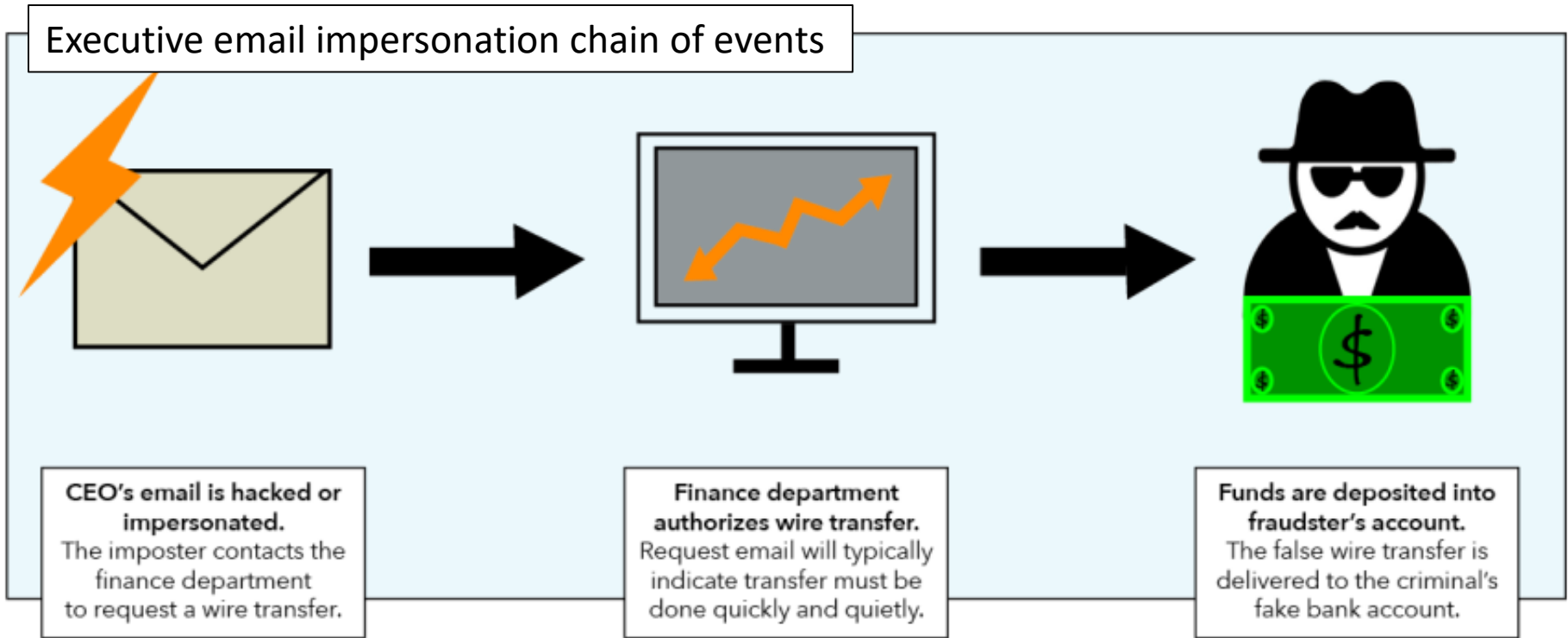
3. A fake but recognizable email address is created to impersonate a colleague or boss.



4. A personalized email is sent to the employee from the fake address with a link or attachment.

<http://madhatmedia.com.au>

# Executive email scam



# Executive email scam example

From: John Doe <John\_Doe@example.com>  
Sent: Thursday, April 17, 2014 11:46 AM  
To: Smith, Jim  
Subject: Fwd: Wiring instructions..... ANGTAI WIRING INSTRUCTION.pdf (88 KB)

Process a wire for \$260,536.17 to the attached instructions, code this to admin expenses.  
Send me the wire confirmation once completed.

John

----- Forwarded message -----

From: Joe Jones <Joe\_Jones@example.com>

Date: Apr 18, 2014

Subject: Wiring instructions

To: John Doe <John\_Doe@example.com>

John,

Per our conversation, attached is the wiring instructions. Forward wire confirmation when you have it.

Joe

Sanitized sample of an email used in this campaign to trick targets into wiring funds to the attacker's account

The attached PDF contains instructions for the wire transfer, including the destination account

WIRING INSTRUCTION

.....BANK NAME:.....SHANGHAI PUDONG DEVELOPMENT BANK,  
.....OFFSHORE BANKING UNIT.

.....BANK ADDRESS:.....NO 12 ZHONGSHAN DONG YI LU, SHANGHAI

.....ACCOUNT NAME:.....ANGTAI INTERNATIONAL CO LIMITED.

.....ACCOUNT NUMBER:.....[REDACTED] 2009

.....SWIFT CODE:.....[REDACTED] HOSA



# Mitigations to consider

- Have a system for reporting phishing
- Provide training that emphasizes:
  - ❑ Know who to contact; quicker is better
  - ❑ Pick up a phone before acting on the email
  - ❑ Be wary of suspicious phone calls
  - ❑ Do not use a website connected to the email

# Mitigations to consider

- Set up an internal phishing program
- Use email system rules
- Scrutinize all e-mail requests for fund transfers to determine if the requests are out of the ordinary
- Patch systems for critical vulnerabilities

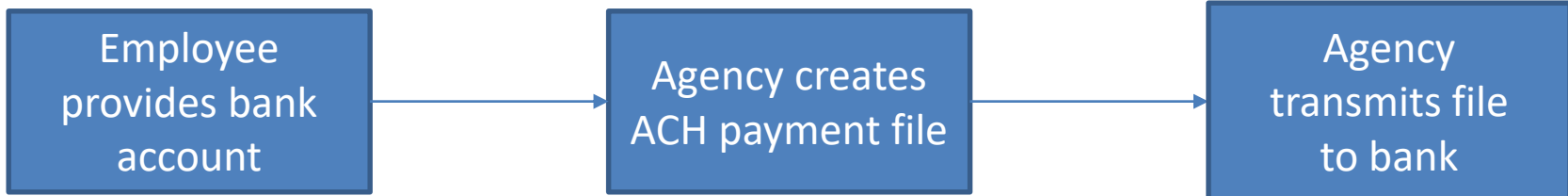
# Business credentials compromise scams

I'm from your IT department, I need you to confirm your password by going to this site

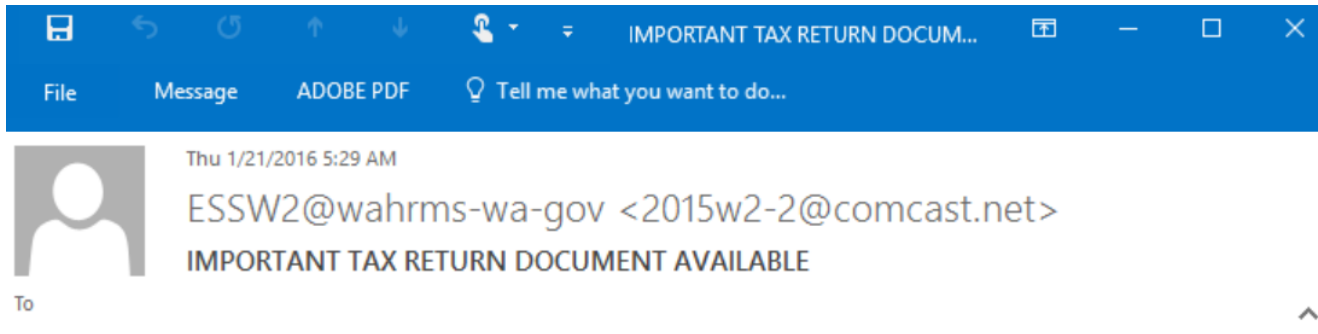


# Business credentials compromise

- Computerworld:  
Hacker steals  
teacher's direct  
deposit paycheck
- KrebsOnSecurity:  
Crooks hijack  
retirement funds  
via SSA portal



# Phishing for credentials?



Dear Account Owner,

Our records indicate that you are enrolled in the Washington State paperless W2 Program. As a result, you do not receive a paper W2 but instead receive e-mail notification that your online W2 (i.e. "paperless W2") is prepared and ready for viewing.

Your 2015 W2 corrected statement is ready for viewing, follow the link below

[Click Here](#) to Login

To opt out of the Paperless W2 Program, please login to Employee Self Service at the link above and go to the W2 Delivery Choice webpage and follow the instructions.

Washington State's Human Resource Management Systems

Your 2015

[Click Here](#) to Login

When you  
"mouse over"  
the hidden link

<http://martinbinder.com/admin/wa/wa-esslogin.htm>  
Click or tap to follow link.

# Phishing for credentials for HR system

A compromised website with a fake Washington HRMS web link

Martin Binder Jeweler x +

← → ↻ 🏠 martinbinder.com

MARTIN BINDER JEWELER

FOREVER Starts at \$999

MARTIN BINDER JEWELER

WELCOME TO WASHINGTON STATE'S HUMAN RESOURCE MANAGEMENT SYSTEMS

HRMS PORTAL

Logon ID \*

Password \*

[Log on](#)

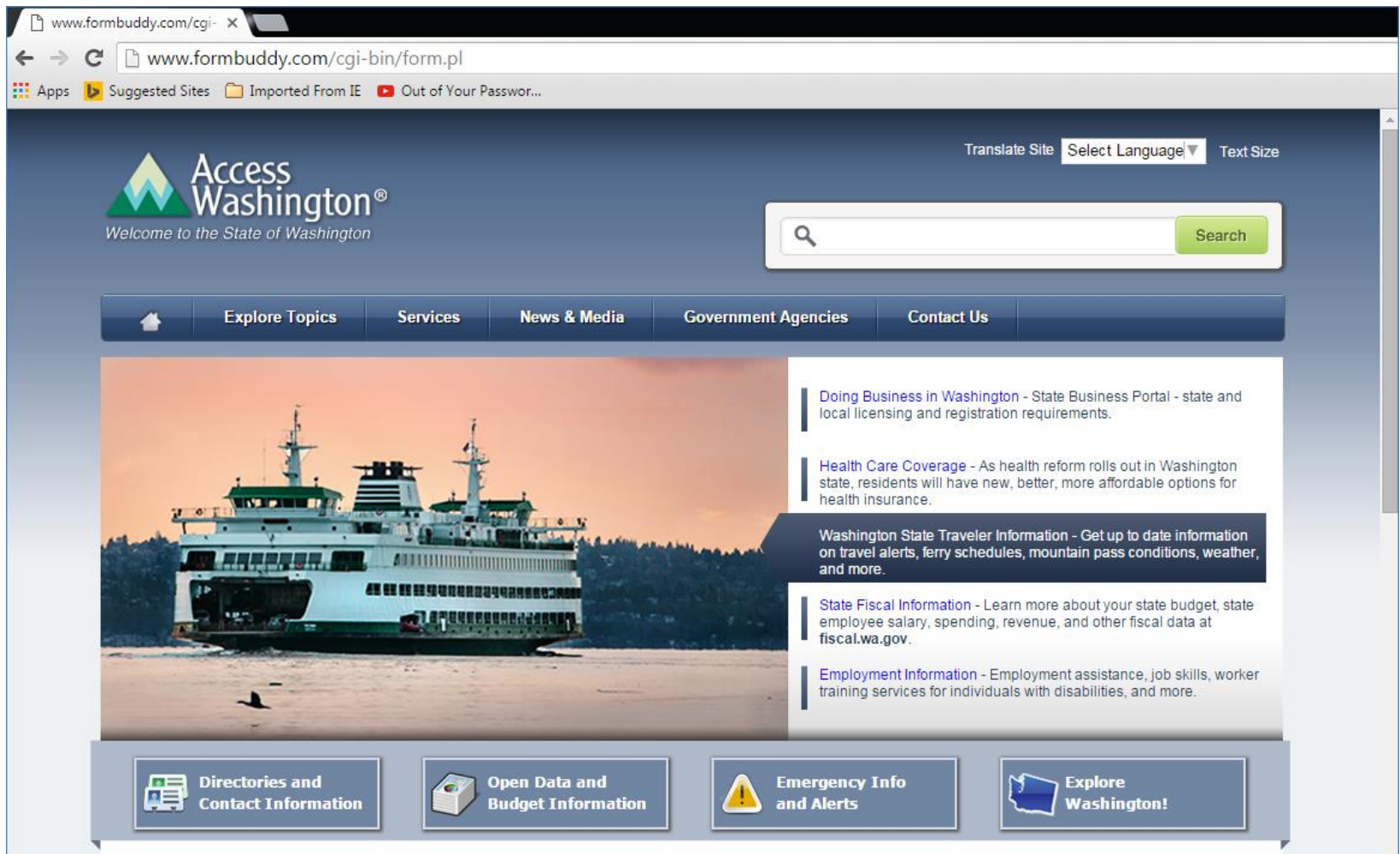
[Reset Password](#) or [First Time User](#)

[Having Trouble Logging In?](#)

[More ESS Information](#)

# After putting in credentials

Convincing web page to make victim think everything is OK



The screenshot shows a web browser window displaying the Access Washington website. The browser's address bar shows the URL [www.formbuddy.com/cgi-bin/form.pl](http://www.formbuddy.com/cgi-bin/form.pl). The website header features the Access Washington logo with the tagline "Welcome to the State of Washington". To the right of the logo are links for "Translate Site", "Select Language", and "Text Size". A search bar with a magnifying glass icon and a "Search" button is positioned below the header. A navigation menu contains links for "Explore Topics", "Services", "News & Media", "Government Agencies", and "Contact Us". The main content area is divided into two sections: a large image of a ferry on the left and a list of service links on the right. The service links include "Doing Business in Washington", "Health Care Coverage", "Washington State Traveler Information", "State Fiscal Information", and "Employment Information". At the bottom of the page, there are four buttons: "Directories and Contact Information", "Open Data and Budget Information", "Emergency Info and Alerts", and "Explore Washington!".

# Political phishing

## Spear-phishing email used in DNC attacks

*Text of spear-phishing email sent to John Podesta, the chairman of the 2016 Clinton presidential campaign.*

\*From:\* Google <no-reply@accounts.googlemail.com>  
\*Date:\* March 19, 2016 at 4:34:30 AM EDT  
\*To:\* [REDACTED]@gmail.com  
\*Subject:\* \*Someone has your password\*

Someone has your password  
Hi John

Someone just used your password to try to sign in to your Google Account  
[REDACTED]@gmail.com.

### Details:

Saturday, 19 March, 8:34:30 UTC

IP Address: 134.249.139.239

Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <<https://bit.ly/1PibSU0>>

Best,

The Gmail Team

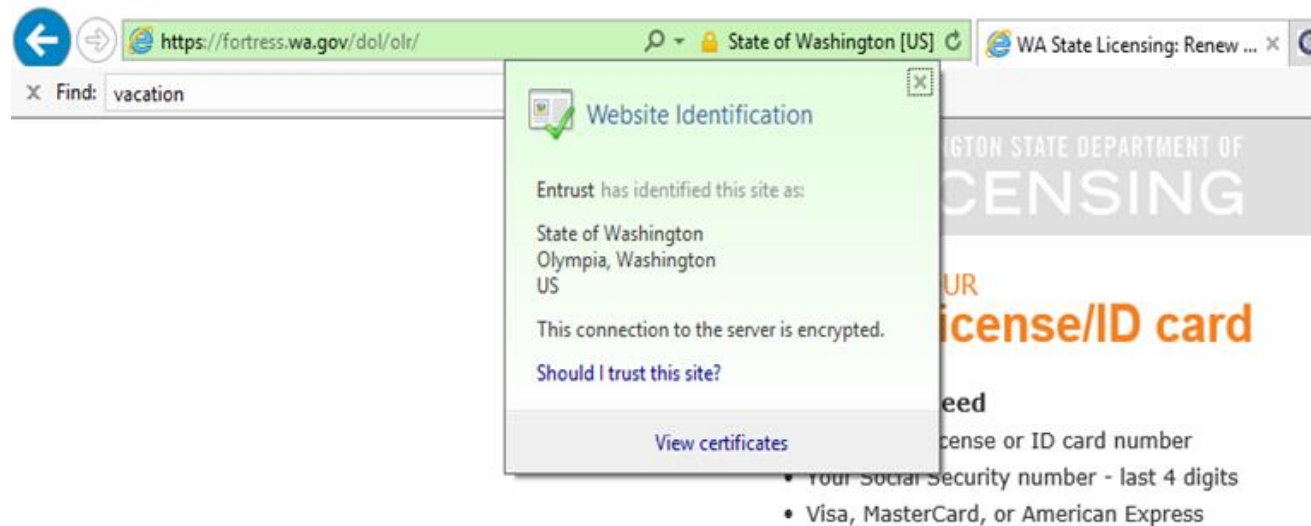
You received this mandatory email service announcement to update you about important changes to your Google product or account.

*Source: Symantec Internet Security  
Threat Report*



# Mitigations to consider

- Only conduct financial or secure transactions on a secure webpage with encryption
- Verify by hovering



# Mitigations to consider

- Reputable organizations do not ask for personal information via email
- Spam email filters reduce phishing email
- Dual-factor authentication
- No password multi-use
- Risk assessment
- Incident response

# Mission critical systems

## Mission critical systems

- Emergency communications
- Air traffic control
- Electrical systems
- Heating/cooling systems
- Water/sewer systems
- What else?



# Serious impacts

## Major events

- Ransomware
- Exfiltrated confidential information



# Serious impacts

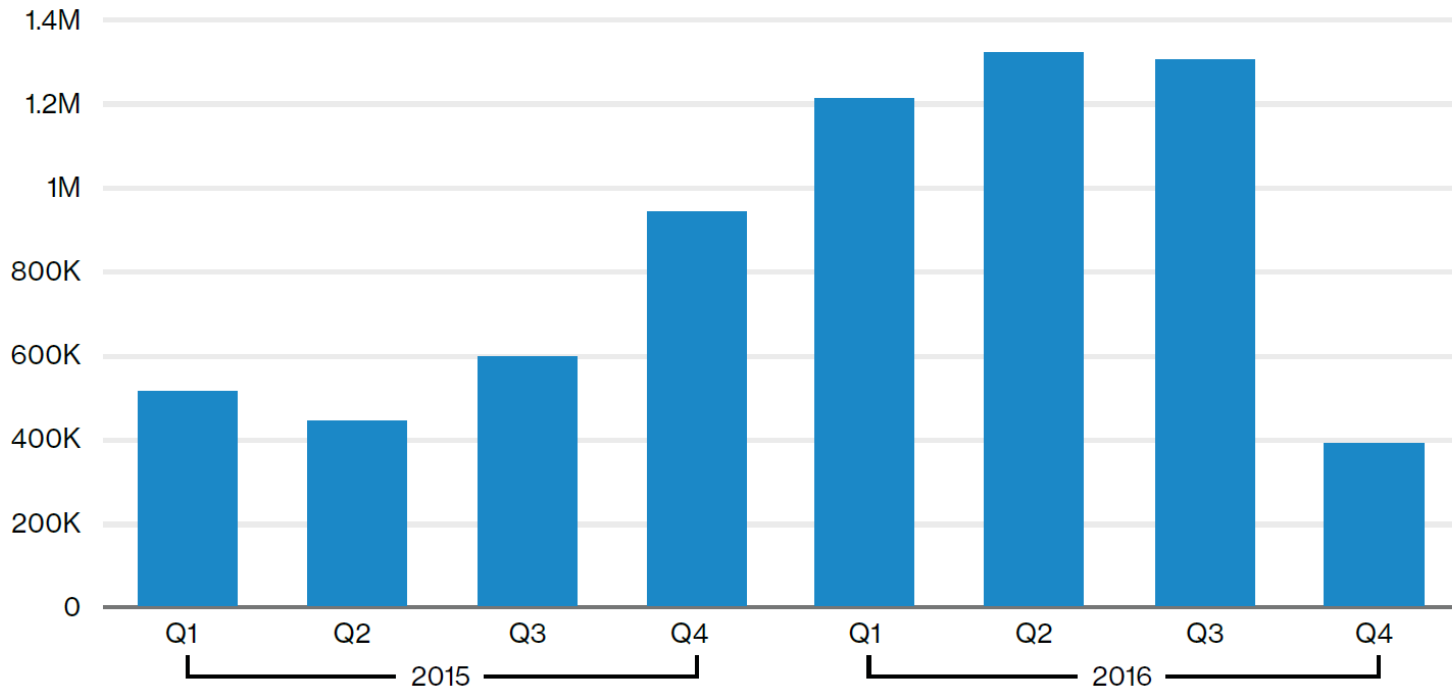
## Costs

- Loss of trust
- Breach notifications (multi-state)
- Lawyers
- Security experts
- Lost revenue



# The rise of ransomware

## The rise of ransomware



*Source: 2017 Verizon DBIR*

# Phishing and ransomware



Sun 4/12/2015 11:55 AM



Internal Revenue Service <office@irs.gov>

[!!Spam KSE]Payment confirmation for tax refund request # 75991792

To



Attachments

 confirmation\_75991792.doc (58 KB);  ATT00001.txt (236 B)

Dear taxpayer,

You are receiving this notification because your tax refund request has been processed.

Please find attached a copy of the approved 1040A form you have submitted, containing your personal information and signature.

On the last page, you can also find the wire transfer confirmation from the bank.

Transaction type : Tax Refund

Payment method : Wire transfer

Amount : \$7592

Status : Processed

Form : 1040A

Additional information regarding tax refunds can be found on our website: <http://www.irs.gov/Refunds>.

Please note that IRS will never ask you to disclose personal or payment information in an email.

Regards,

Internal Revenue Service

Address: 1111 Constitution Avenue, NW

Washington, DC 20224

Website: <http://www.irs.gov>

Phone: 1-800-829-1040

# Ransomware

## 5 STAGES OF CRYPTO-RANSOMWARE

### 1 INSTALLATION

After a victim's computer is infected, the crypto-ransomware installs itself, and sets keys in the Windows Registry to start automatically every time your computer boots up.



### CONTACTING HEADQUARTERS 2

Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.



### 3 HANDSHAKE AND KEYS

The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.



### ENCRYPTION 4

With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.



### 5 EXTORTION

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, \$300 to \$500, must be paid in untraceable bitcoins or other electronic payments.





# Have bitcoin?

CryptoLocker



Private key will be  
destroyed on

1/6/2015 1:11:47 PM

Time left

71:52:21

Checking wallet..

Received: 0.00 BTC

## Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

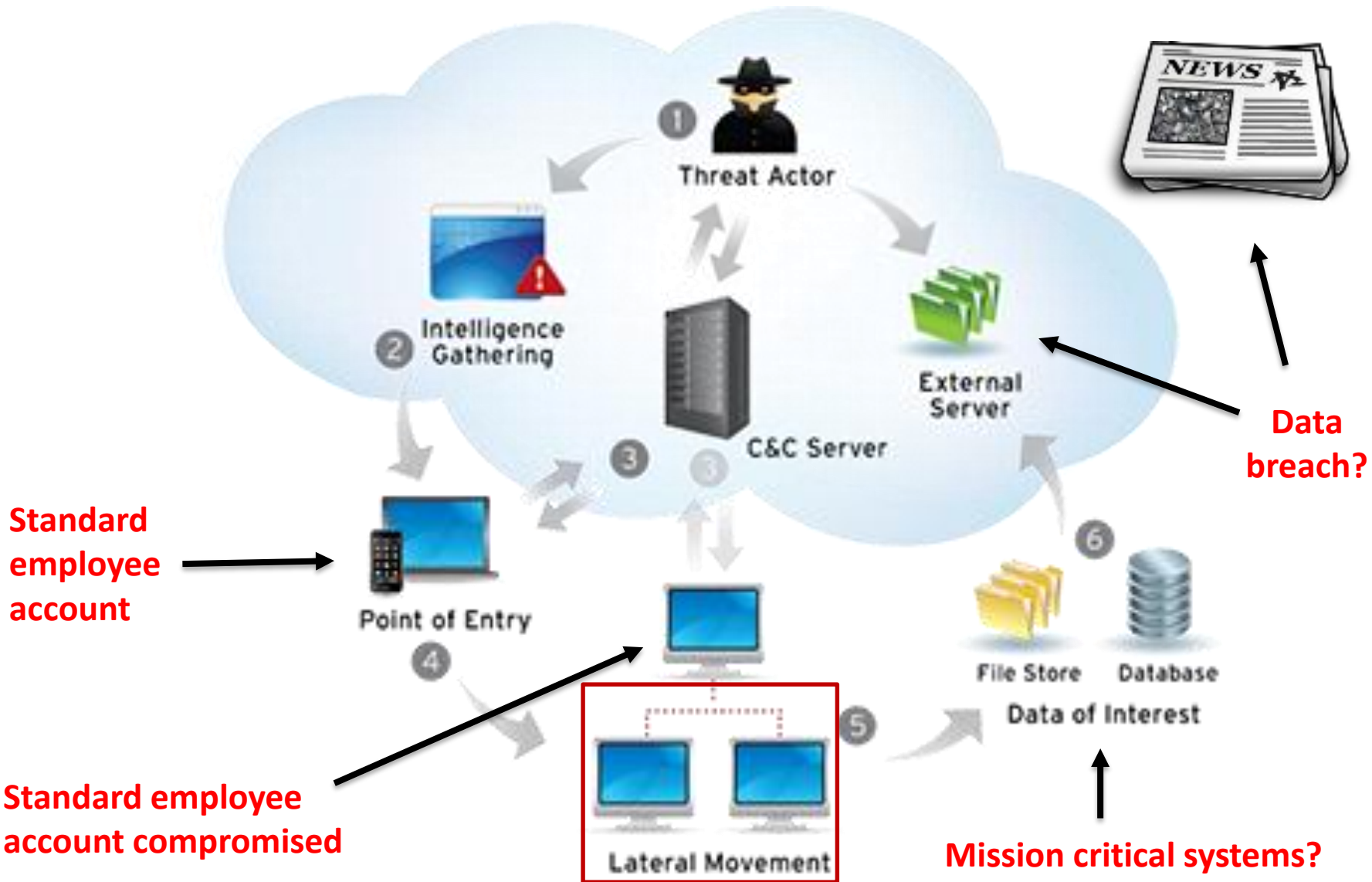
For more information on how to buy and send bitcoins, click "Pay with Bitcoin"  
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

Show files

Pay with Bitcoin

# Phishing as point of entry to 'pivot' a network



# Mitigations and other considerations

- Back up your critical information (air gapped)
- Limit user access to only what employees need
  - Least-privilege rule or role-based security
- Segment the network – not all systems have access to all other systems
- Devise a continuity-of-operations plan; identify key systems
- Complete and test an IT data recovery plan

# Reporting incidents

- For government agencies, report fraud or theft to our Office:  
<http://portal.sao.wa.gov/saoportal/public.aspx/LossReport>
- Data breach notification:  
<http://www.atg.wa.gov/data-breach-notifications>
- File a complaint with FBI Internet Crime Complaint Center:  
[www.ic3.gov](http://www.ic3.gov) (regardless of loss size)  
[BEC.IC3.gov](http://BEC.IC3.gov) (business email compromises)
- Consumers can report identity theft to Federal Trade Commission:  
[IdentityTheft.gov](http://IdentityTheft.gov)

# Audits

- Performance audits
- Financial statement audits
- Accountability audits
  - Backups
  - User access
  - IT vendor management/contracts
  - Current policies and procedures
- Federal financial assistance audits

# Questions?

**Pat McCarthy**

State Auditor

(360) 902-0360

[Pat.McCarthy@sao.wa.gov](mailto:Pat.McCarthy@sao.wa.gov)

**Peg Bodin, CISA**

Local IS Audit Program Manager

(360) 464-0114

[Peggy.Bodin@sao.wa.gov](mailto:Peggy.Bodin@sao.wa.gov)

**Mike Hjermsstad**

Assistant Audit Manager

(253) 372-6250

[Michael.Hjermsstad@sao.wa.gov](mailto:Michael.Hjermsstad@sao.wa.gov)

**Utchay Okorie, CISSP, CCNA Security,  
Security+**

Performance Audit Info Security Analyst

(360) 725-5569

[Utchay.Okorie@sao.wa.gov](mailto:Utchay.Okorie@sao.wa.gov)

Websites: [www.sao.wa.gov](http://www.sao.wa.gov) <https://auditconnectionwa.org/>

Facebook: <https://www.facebook.com/WAStateAuditorsOffice>

Twitter: [www.twitter.com/WAStateAuditor](http://www.twitter.com/WAStateAuditor)