Washington State Auditor's Office

Troy Kelley

Integrity • Respect • Independence

The New Frontier: Cybersecurity for Auditors

Briefers:

Peg Bodin, Local IS Audit Manager

Aaron Munn, Chief Information Security Officer

Erin Laska, Performance Audit Supervisor

Outline

- Risk
- Threat
- Audit Approach

Hackers hit small US town, steal tax payer data and $400,000

Hackers hit small US town, steal tax payer data and $400,000

by Paul Roberts on October 15, 2012 | 3 Comments
FILED UNDER: Data loss, Law & order

The town of Burlington, Washington has warned residents that they could be the targets of identity theft, after hackers compromised a number of town systems used to run an online automatic utility billing system and emptied $400,000 from a city bank account.

In a notice posted on the town's website, Bryan Harrison, the City Administrator, said that a city-run automatic payment system - that was used by residents to pay sewer and storm drain charges - was compromised.

EMERGENCY ALERT! **ATTN: UTILITY CUSTOMERS**

It has come to the City's attention that the City's Utility Billing Automatic Withdrawal information (for sewer and storm drain charges) has been compromised. If you are enrolled in Autopay, you should assume that your name, bank, bank account number and routing number have been compromised.

ALL AUTOPAY CUSTOMERS SHOULD IMMEDIATELY CONTACT THEIR BANK OR FINANCIAL INSTITUTION.

The City immediately closed the affected bank account and will not be withdrawing the funds owed for your July/August 2012 City of Burlington Utility Bill on October 15, 2012 as previously stated on your bill.

Please make arrangements to do one of the following to pay your bill by October 31, 2012:

1. Use your online bill pay option through your banking institution
2. Pay by check (mail to 833 S Spruce Street, Burlington, WA 98233)
3. Call 360-755-0531 and pay with a VISA , MasterCard or Discover credit or debit card

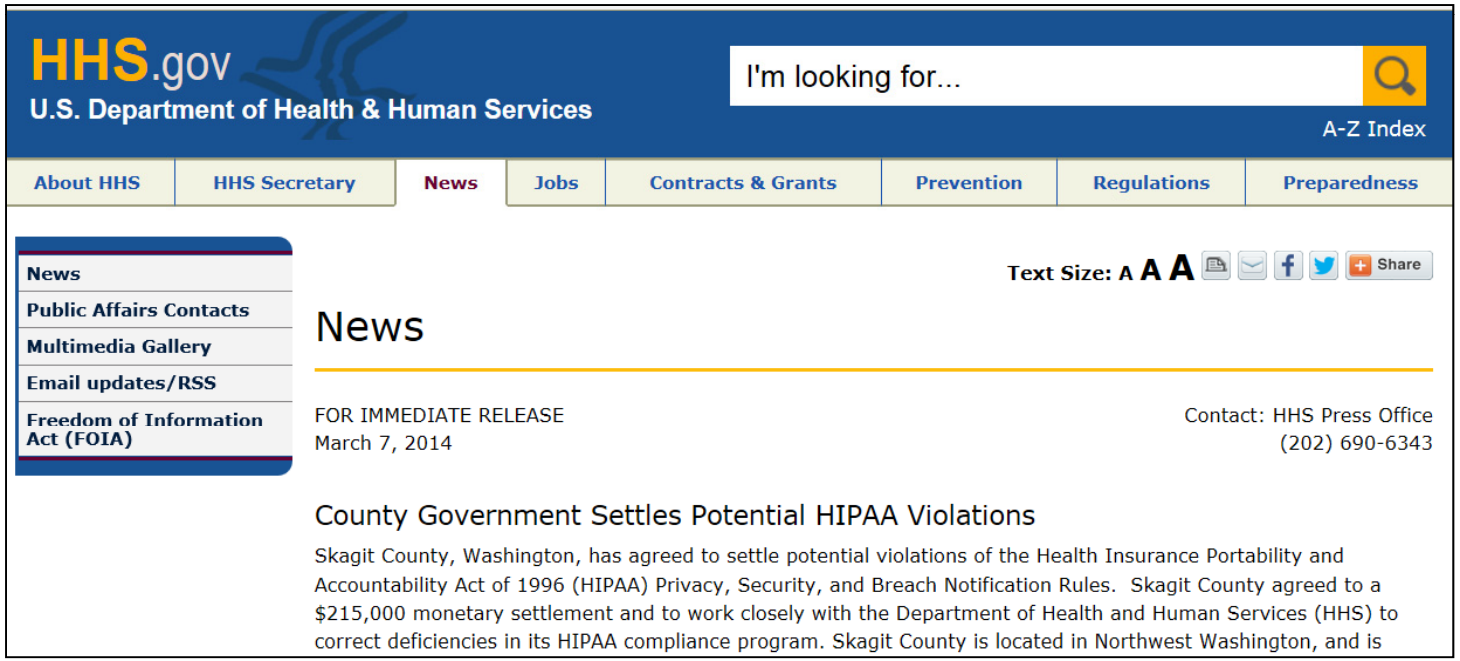
WE APOLOGIZE FOR THE INCONVENIENCE!

Bryan Harrison, City Administrator


KrebsonSecurity
In-depth security news and investigation
30 Wash. Hospital Hit By $1.03 Million Cyberheist
APR 13


In Hours, Thieves Took $45 Million in A.T.M. Scheme
By MARC SANTORA
Published: May 9, 2013

County Government Settles Potential HIPAA Violations



HHS.gov
U.S. Department of Health & Human Services

I'm looking for...

A-Z Index

About HHS | HHS Secretary | News | Jobs | Contracts & Grants | Prevention | Regulations | Preparedness

- News
- Public Affairs Contacts
- Multimedia Gallery
- Email updates/RSS
- Freedom of Information Act (FOIA)

Text Size: A A A Share

News

FOR IMMEDIATE RELEASE
March 7, 2014

Contact: HHS Press Office
(202) 690-6343

County Government Settles Potential HIPAA Violations

Skagit County, Washington, has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules. Skagit County agreed to a $215,000 monetary settlement and to work closely with the Department of Health and Human Services (HHS) to correct deficiencies in its HIPAA compliance program. Skagit County is located in Northwest Washington, and is

PCWorld

Work. Life. Productivity.

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWA

Antivirus Privacy Encryption

LifeLock
Relentlessly Protecting Your Identity

Has your data been breached?
Get LifeLock ID theft protection
Enroll in minutes.
Protection starts immediately.

SECURITY

Montana data breach exposed 1.3 million records

Jeremy Kirk

Jun 24, 2014 8:50 PM

Up to 1.3 million records, including health care and bank account information, may have been exposed after a server at Montana's public health department was hacked in May, the state said Tuesday.

Washington Courts data breach in 2012

WASHINGTON COURTS

Get Email Updates | FAQs & eService Center

Search WA Courts Site

Forms | Court Directory | Opinions | Rules | Courts | Programs & Organizations | Resources

Courts Home > Washington Court News > Data Breach Information

Washington Courts Data Breach Information Center

Provided by the Administrative Office of the Courts

The Data Breach

The Washington State Administrative Office of the Courts (AOC) announced that a security breach occurred on its public website. No court records were altered and no personal financial information, such as bank account numbers or credit card numbers, is maintained on the site. However, up to 160,000 social security numbers and 1 million driver license numbers may have potentially been accessed.

Data Breach Links

- Data Breach Information
- Common Questions
- How to Protect Your Credit

Individuals meeting the following criteria could potentially be affected by the breach:

- **Social Security Numbers:**
  - If you were booked into a city or county jail in the state of Washington between September 2011 through December 2012, you may have had your name and social security number accessed.
- **Driver License Numbers:**
  - If you received a DUI citation in Washington State between 1989 through 2011; or
  - If you had a traffic case in Washington State filed or resolved in a district or municipal court between 2011 through 2012; or
  - If you had a court criminal case in Washington State filed against you or resolved between 2011 through 2012,

you may have had your name and driver license number accessed.

Could this happen to you?

- Employee clicked on link with malware
- Malware installed key stroke logger
- Key stroke logger captured the employee user-id and password
- The user-id and password was used to change employee's direct deposit bank account
- Pay check went to someone else's bank account
- Employee noted missing check
- Employee changes password…

RISK

- Very large dollars
- Very hard to recover
- Very difficult to prosecute

Government as the target: Why?

- Dollars
- Data
- Infrastructure

Likelihood

A 2014 study, by the Ponemon Institute, estimated

governments have a one-in-four chance of experiencing a material data breach (more than 10,000 records) in the next two years.

http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Cost of a Data Breach

The 2014 study by the Ponemon Institute, estimated:

- the average cost for each government record lost is $172
- A formal ***incident response plan*** in place prior to the incident reduces the cost
- Data breaches caused by ***third parties*** increase cost
- incidents involving the loss or theft of ***data bearing devices*** increased cost

http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Costs of a Data Breach

Direct financial costs

- Fraudulent wire transfers 100,000 - 200,000

(2010 avg per MS-ISAC http://msisac.cisecurity.org/)

Wash. Hospital Hit By $1.03 Million Cyberheist

Hackers hit small US town, steal tax payer data and $400,000

Costs of a Data Breach

In addition to direct financial losses:

- Forensic experts
- Notifying affected victims
- Identity / credit card monitoring
- Regulatory penalties
- Repairing public relations
- Legal assistance

South Carolina

A Department of Revenue employee clicked on a link in an email and installed malware.

As many as 3.6 million Social Security numbers and 387,000 credit and debit card numbers used by state taxpayers could have been exposed as a result of the cyber-attack.

South Carolina

Initial estimated costs according to one source:

$ 500,000	Mandiant, IT expert assistance
$12,000,000	Experian Credit Monitoring Reports
$ 800,000	Improved information security capabilities
$ 100,000	Outside legal help
$ 150,000	Public relations campaign
$ 740,000	Notify out-of-state taxpayers

Subsequent reports have doubled this cost to $25 million

Costs of a Data Breach

Regulatory

- HIPAA fines
- PCI non-compliance penalties
- Prohibited access

FOR IMMEDIATE RELEASE
March 7, 2014

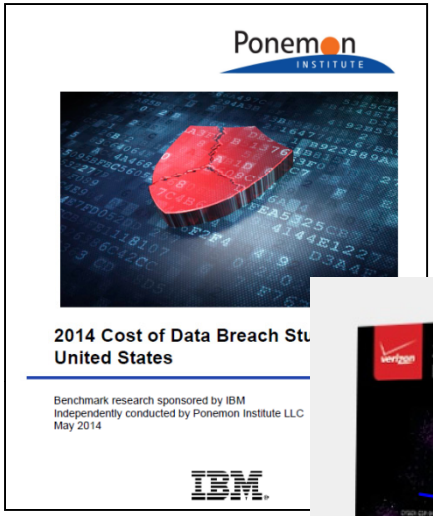
Contact: HHS Press Office
(202) 690-6343

County Government Settles Potential HIPAA Violations

Skagit County, Washington, has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules. Skagit County agreed to a $215,000 monetary settlement and to work closely with the Department of Health and Human Services (HHS) to correct deficiencies in its HIPAA compliance program. Skagit County is located in Northwest Washington, and is

Nature of risks (most common causes)

- Malware, Malicious or Criminal attacks
- Insider Misuse
- Theft or Loss
- Misc. Errors
- PEOPLE



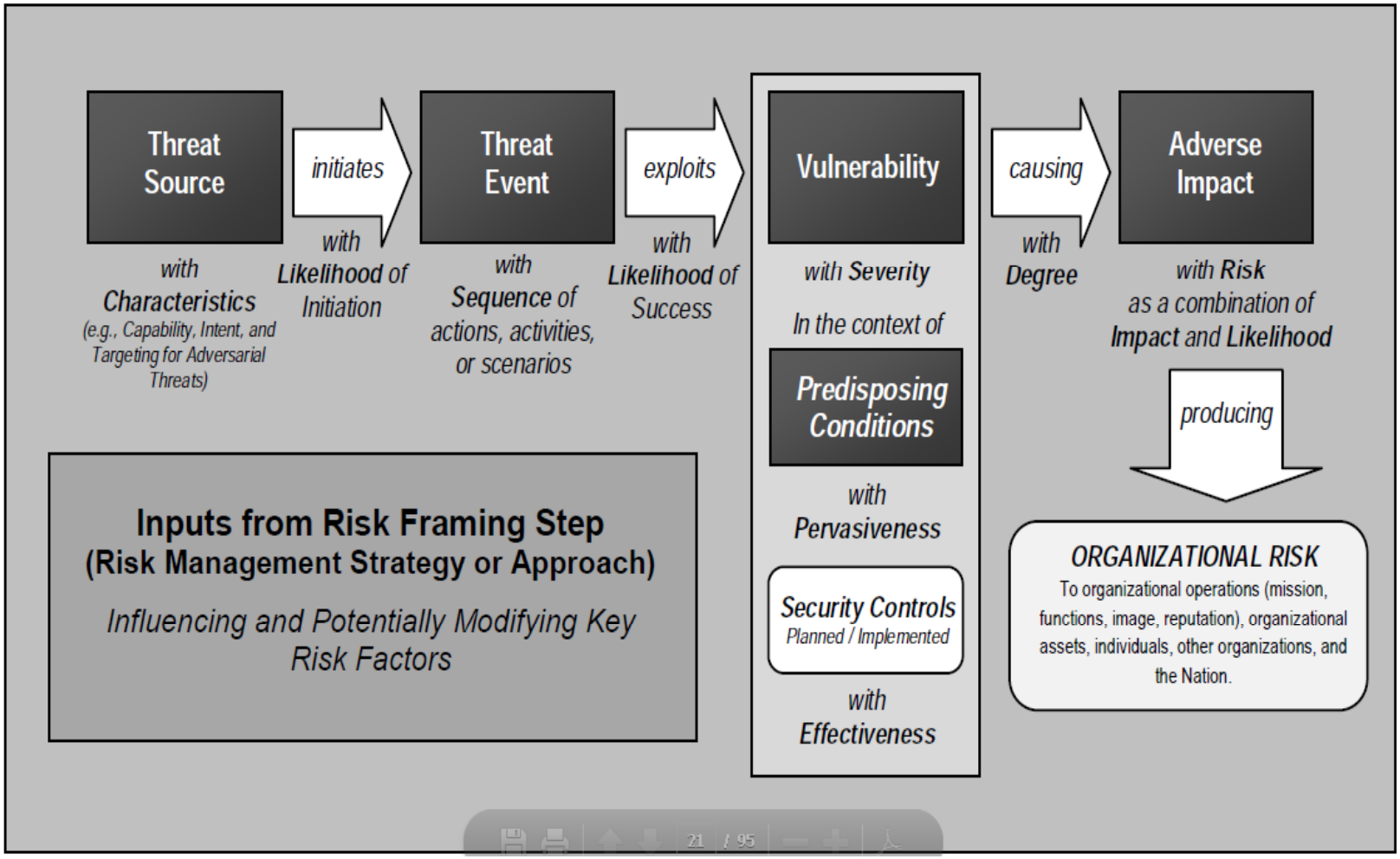
http://www.verizonenterprise.com/DBIR/2014/

Okay, it's a problem. Where do we start?

Risk is the probability of a threat agent exploiting a vulnerability to cause harm to an asset and the resulting business impact

Source: *McGraw Hill Education, CISSP exam guide*

Risk Assessment



Risk Assessment

- Focus efforts on the most critical information or assets
- Be dynamic and iterative
- Reflect internal and external threats

Threat

- Characteristics
- Capabilities
- How do they do it?
- What are they after?
- Future threat

Characteristics

- Malicious actors
  - Disgruntled Employee(s)
  - Activists
  - Criminal organizations
  - Extremist / Terrorist Groups
  - Nation States
- Requirements
  - Low barrier to entry
  - Internet connection
  - Internet capable device

Capabilities

- Phishing / Spear-phishing
- Web site exploitation
- Malicious Software (Malware)
- Man-the-middle attacks
- Distributed Denial of Service (DDoS)
- Social Engineering
- Botnet

How do they do it?

"Company loses $17m in email scam," article from Omaha.com

- Fake email addresses
- Fake phone numbers
- Impersonating corporate Auditors and the CEO
- Targeted emails to corporate controller
- Wire transfers to Chinese entities

How to they do it?

"Bank hackers steal millions via malware," article from New York Times

- Spear-phishing
- Worked with Botnet controllers for target information
- Established own botnet for exploitation
- Owned the banks email server
- Remote control over ATM's
- Common tools for remote control functions
- Create methods to hide transactions
- Changing firewall rules
- Possibly years of exploitation

How to they do it?

"Anthem Breach May Have Started in April 2014," article from Krebs on security

- 80 million SSN #'s exfiltrated
- Same forensics footprint of "Deep Panda"
- Privileged network credentials compromised
- Possible compromised VPN
- Possible phishing web site called we11point.com (former name of Anthem)

What are they “After”

Driver license Information

Date of birth

Bank account information

Social Security Number

Electronic Medical Record

Login / passwords

Address

Credit Card Information

Phone Number

Your Computer!

Future threat

Kaspersky: 'A very bad incident' awaits critical infrastructure

Planning an IT Security Audit

Presentation topics reviewed

- Audit Scope
- Before you get started
- Considerations for contracting
- Planning for the report

Scope

- **Compliance with:**
  - Entity policies
  - Best practice
- **Ensure entity policies align with best practice**
- **Recent experience an State in Washington state**
  - State agencies are required to comply with Office of the Chief Information Officers IT Security Standards

Scope

Vulnerability assessment

- Examples of the types of findings
- Appropriate Expertise

Scope

Penetration testing

- Different than a vulnerability scan
- Non technical methods
- Examples of the types of findings

Before you get started

Consider your own IT security

- How will you protect the information you gather during the audit

Considerations for contracting

For compliance, vulnerability assessment and penetration testing

- Non disclosure agreements
- Data sharing agreement
- Insurance
- Background check
- Subcontracting

Consideration for contracting

For penetration testing

- Location of the testers
- Rules of Engagement

Plan for the Report

Will there be a public report?

- If yes, what level of detail will be included?

The level of detail in IT security audits reports varies widely

- State Auditor's Office
- Federal agencies (Inspector Generals and GAO)
- Other State's

Questions

Aaron Munn
Chief Information Security Officer
(360) 725-5418
munna@sao.wa.gov

Erin Laska
Senior Performance Auditor
(360) 778-2697
laskae@sao.wa.gov

Peg Bodin
Local IS Audit Manager
(360) 464-0114
bodinp@sao.wa.gov

Website: www.sao.wa.gov

Twitter: www.twitter.com/WAStateAuditor