Understanding the Legal Aspects of Cybersecurity

The Legal and Ethical Drivers for Public Sector Attorneys and their Clients
Your Humble Presenters
David R Matthews

• Director of Managed Services, MKH&A
• Director of Global Incident Response, Expedia
• Deputy CISO, City of Seattle
• IT Manager, City of Seattle Legislative
• Entire IT Department, Public Relations firm
• Cattle Ranch Foreman
• Forest Service Trail Crew Foreman
Your Humble Presenters
Suzanne Skinner

• 30 years federal, state and local gov’t experience
• Former Civil Division Director, Seattle City Attorney’s Office
• Currently attorney in private practice and consultant to MK Hamilton and Associates
What’s the Problem & Why Should You Care?

• Information technology is ubiquitous
• All critical infrastructure is ultimately under control of local government
• Cities and small agencies are low hanging fruit
• Compromise of public safety or life supporting utilities (water, sewer, power, transportation) can threaten quality of life or life itself

• Examples...
Inventory Of Bad Outcomes

What’s really important?

• Service infrastructure disruption and damage
• Loss of protected records
• Electronic theft
• Potential violation of state and federal law
• Potential customer lawsuits
Regional Incidents

- Leavenworth and Burlington financial losses
- HVAC systems compromised
- Power marketers targeted
- Deeply compromised energy utility infrastructure
- Denial of service attacks
- Vulnerable transportation management
- Telephone equipment compromised
Washington Town Loses $400,000 in Cyber-Heist

By Fahmida Y. Rashid on October 16, 2012

Burlington, Wash. officials admitted that cyber-criminals had stolen more than $400,000 from the city's bank account and also obtained individual financial data belonging to employees and some residents.

Cyber-criminals compromised systems used to run the town's utility billing system used for sewer and storm drain charges, according to an alert posted on the town's Website Monday morning. All customers who use the autopay feature to pay their utility bills should assume their names, bank name, account number, and routing numbers have all been compromised as well, Bryan Harrison, the city administrator, wrote in the alert. Customers should immediately contact their bank to protect their accounts.

The utility breach comes shortly after criminals electronically transferred $487,000 from Burlington's Bank of America account to various personal and business accounts throughout the country over a two-day period, according to various local media outlets. Bank of America froze the affected account on Thursday.
WENATCHEE — Hackers stole more than $1 million from an electronic bank account held by Cascade Medical Center in Leavenworth, leading to a multi-state criminal investigation that could yield federal charges.

On Monday morning, Chelan County Treasurer David Griffiths’ office noticed three unauthorized transaction files that had been logged the previous Friday. The files moved an estimated $1.03 million out of the public hospital district’s ACH account to 96 different bank accounts, most of them in the Midwest and East Coast.

By notifying the recipient banks, the treasurer’s office has been able to retrieve about $133,000 of the lost funds, Griffiths said Friday. The process is ongoing, and it may take at least 30 days to learn how much money was lost and how much can be recovered.

“We are proactive in this,” Griffiths said. “We’re not only in a heightened alert because of the situation, we’re also taking measures to add even greater security precautions.”
Infrastructure Disruption!

Call Type: Sdot Traffic - Bo Signals And Down Signs
Disp. Loc.: Ne 75 St / Sand Point Wy Ne
Cross: 7501-7699 Sand Point Wy Ne/5824-5998 Ne
Zone: L3 Grid: 175 Com: SE

Remarks: ELECTRONIC TRAFFIC REVISION SIGN AT ENTRANCE TO MAGNUSON PK HAS BEEN HACKED, READS F-WORD, C-WORD, AND S-WORD IN THAT ORDER.

Complainant:
Sex: MALE
State: Washington
Home: Type: CELL

Report: N Founded: Y Cleared:
Prime Unit: 3L31
Potential for Worse: Turkey 2008
All Too Easy Access: Shodan

**The search engine for Power Plants**

Shodan is the world's first search engine for Internet-connected devices.

**Explore the Internet of Things**
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

**Monitor Network Security**
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Websites or refrigerator

Get a C Who is using empirical m
Taxonomy of Cyber Threats

- Unsophisticated criminals of opportunity
- Hacktivists
- Insiders
- Organized Crime
- Nation-State
- Terrorists
- Hybrids (terrorists that pay organized criminals for capabilities)
Emerging Duty to Protect Data

• Regulated businesses and public sector utilities: Well-established federal laws for financial services, healthcare, critical infrastructure

• Local governments and Unregulated businesses: federal, state and common law sources for the emerging duty
  1. Federal Laws
  2. Washington’s Laws (and especially the Updated Unfair and Business Practice Law)
  3. Common Law & FTC Developments
  4. Ethical Duties for Lawyers
What is Data Security Anyway?

• Technical Security Measures—Ensuring System Availability, Authentication of Users, Protecting the Integrity of ESI; Protecting Confidential ESI As Needed

• Procedural Security Measures: Management & Maintenance Procedures, Access & Usage Policies; Monitoring; Response; Audits/Compliance

• Physical Security Measures--Locks and Closed Doors

PROTECTIVE, DETECTIVE AND REACTIVE
1. Federal Data Security & Local Govts.

- Patchwork of industry specific federal laws and standards
- Several bills in Congressional hopper
  - Consumer Privacy Act of 2015: All govt entities exempted thus far
  - Cybersecurity for Critical Infrastructure bill
- Presidential Executive Action
  - EO 13636: Improving Critical Infrastructure & Cybersecurity
  - Led to National Institute of Standards & Technology’s Cybersecurity Framework
FTC Advocacy in the Void

• Section 5 of FTC Act: protection of consumers from unfair or deceptive practices
• Between 2002-2014, FTC entered into 50 settlements with non-regulated businesses regarding “unreasonable” data security practices violating its cybersecurity guidance per Section 5
• What is “reasonable” data security for FTC? Continuous Process of Assessing and Addressing Risks
FTC Guidance: Common sense for local governments

– Know what consumer data you have, and who has access to it.
– Know how data moves into, through and out of the business (or agency).
– Limit the amount of data collected and retained to legitimate business needs.
– Protect the data using Physical, Technical and Procedural Security Measures
– Dispose of Unneeded data—Document Governance
– Have a Data Breach Response Plan
2. Washington’s Data Security Laws

• Data Disposal Requirements Chap. 19.215 RCW
  – Local govts potentially liable for failing to reasonably dispose of personal financial and health information
  – Broad definition of PI
  – 2014 State Auditor report: of 4 agencies studied that surplused computers 9% contained PI

• And effective July 24, 2015: ESHB 1078—RCW Ch. 19.255 & 42.56.590 Washington sets bar for strict data security requirements
Data Security Consumer Protection: ESHB 1078

• Same definition of government as PRA. Three big changes over prior law
  1. Effectively changes the standard for what is secure data.
  2. Attorney General authorized to prosecute failures to notify consumers of data breaches of PI as unfair or deceptive practice under Consumer Protection Law
  3. Individuals also can sue. Injunctive relief possible.
Government Duties Under ESHB 1078

• Explicit Duty to Notify of Breaches of Data that Govt owns or licenses.
  – Notice required to any state resident following discovery of breach IF
    • Personal Information (PI) was or reasonably believed to be taken
      – AND PI not secured
      – OR the “Rosetta Stone” to decipher was taken too.
    Notice within 45 days of breach discovery (law enforcement exception)
    BUT Notice not required if breach not reasonably likely to cause consumers harm.

• Implicit Duty to Secure PI
What is Secured Personal Information?

- **ESHB 1078 Limits PI to:**
  - SS#; **OR**
  - Bank acct #, Credit or Debit # OR required security/access code/password; **OR**
  - Driver’s license or Washington ID number

- **ESHB 1078 Deems PI Secured if:**
  - Encrypted to or beyond National Institute of Standards and Technology (NIST) standards
  - **OR** is otherwise modified so that PI is unreadable by unauthorized person. Section 3 (7)
    - Puts burden on local government to show that encryption method is equivalent to NIST).
3. Common Law Duty and other developments

No Common law duty thus far—Attempts Failed to Survive Motion to Dismiss

• *In Re TJX Companies Retail Security Breach Litigation cite (1st Cir. 2009)* Negligent misrepresentation claim allowed on theory defendants made implied representations re: certain security measures to issuing banks required by industry practice

• *Several cases (and putative consumer class actions) dismissed at pleading stage failure to state a claim (causation and damage) and for lack of Article III standing*

*Katz v. Pershing, LLC, 11-1983 (1st Cir. 2012)*

*Paul v. Providence Health System-Oregon, 273 P.3d 106 (Or. 2012)*
4. Lawyers’ Cyber-Ethics Duties

ABA’s RPC 1.1 Competence
• The ABA’s comment [8] on Model Rule 1.1: Maintaining Competence: “Keeping abreast of changes in the law and its practice includes the benefits and risks associated with relevant technology.”
• ABA’s Resolution 109 (August 2014):
  – Firms and their clients should “develop, implement, and maintain an appropriate cybersecurity program that complies with applicable legal and ethical obligations, & is tailored to the nature and scope of the organization, and the data and systems to be protected.”

ABA’s RPC 1.6 Confidentiality
• Maintaining client’s secrets includes electronic documents:
  – keeping those documents “safe” and secure
  – scrubbing metadata from transmitted documents.
• Maintaining confidentiality is part of competence.
Washington Ethics & Electronic Documents

- **WSBA Advisory Op. 2215**: Attorney using cloud computing duty of competence to ensure that confidentiality protections meet a reasonable standard of care.

- **WSBA Advisory Op. 2216**: Competence creates an implicit obligation to be knowledgeable about IT matters. Duty is made explicit in recent amendments to CR 26 (j) and 34.

- Parallel to E Discovery: *Zubulake v. USB Warburg*:
  - Know client’s IT system and institute ligation hold
  - Ensure compliance with hold
The emerging standard of care—how to be legally and ethically prepared
Defining the Current State of the State

• Our Survey
  – Process
  – Question Examples/Types
  – Audience
  – Response/Participation

• Focus Groups
  – Participants
  – Process & Discussion Points
Findings

• Most everyone had some basic controls in place
• Policies and procedures were not comprehensive and rarely updated or exercised
• Exec level understanding and buy-in was minimal at best
• Many smaller jurisdictions lack resources
Solutions (1 of 2)

• Accessible, affordable, and understandable user awareness training especially programs specifically designed for executives, legal staff and risk managers

• Third party vendor contract templates with security provisions and language

• Templates for information security policies and procedures, including incident response plans and business continuity procedures
Solutions (2 of 2)

• Response exercise opportunities
• Vetted, consolidated threat/risk information
• Standard assessment framework and tools
  – Measure current state of information security capability maturity
  – Create risk-based strategic plans to increase those capabilities
What YOU Can Do (1 of 2)

• Know your stakeholders and be engaged
• Understand your specific responsibilities
• Help to clarify roles and responsibilities for IT security management and response
• Establish a baseline – know your current capability maturity
What YOU Can Do (2 of 2)

• Assist in the creation of a strategic risk-based information security plan
• Advocate for ongoing operational and maintenance resources and a plan for continual assessment and improvement
### Example Assessment

<table>
<thead>
<tr>
<th>ACCESS CONTROL</th>
<th>Policies, Procedures and Account Management</th>
<th>NIST AC-1 to AC-6; AC-17 to AC-20; PCI 3.2; 7; 8; WCIA/20 CrCtrl CSC 1; CSC 7; CSC 12; CSC 15</th>
<th>Current Maturity Rating</th>
</tr>
</thead>
</table>

This control addresses the need for policy and procedures that effectively implement controls around access to computer systems and devices. An optimized set of policies and procedures would require dedicated personnel to document, maintain and manage access and authentication provisioning.

- Procedures for activating, monitoring and auditing all network authentication and connections
- Procedures for provisioning new user accounts, including least privilege standards (only grant privileges to systems and shares that are required for their job)
- A regularly scheduled review of all accounts and purging of cancelled, stale or unused accounts
- Current contact information for all account owners or managers
- Vendor and 3rd party access procedures, auditing and standards
- Remote access procedures, auditing and standards
- Wireless access procedures, auditing and standards
- Mobile device procedures, auditing and standards
Conclusions

• A real problem – coming soon to a City near you
• You are not alone
• You are the government and you’re here to help
• Support efforts to raise the bar in your organization
• Call us if you need us
Questions?

David R Matthews  
DavidM@MKHA.US  
206.272.0580  

Suzanne Skinner  
SuzanneS@MKHA.US  
206-605-0461