45th Spring Conference
March 31, 2016
Austin, Texas

Practical Considerations before and after a Terrorist Attack

Claudia Rast

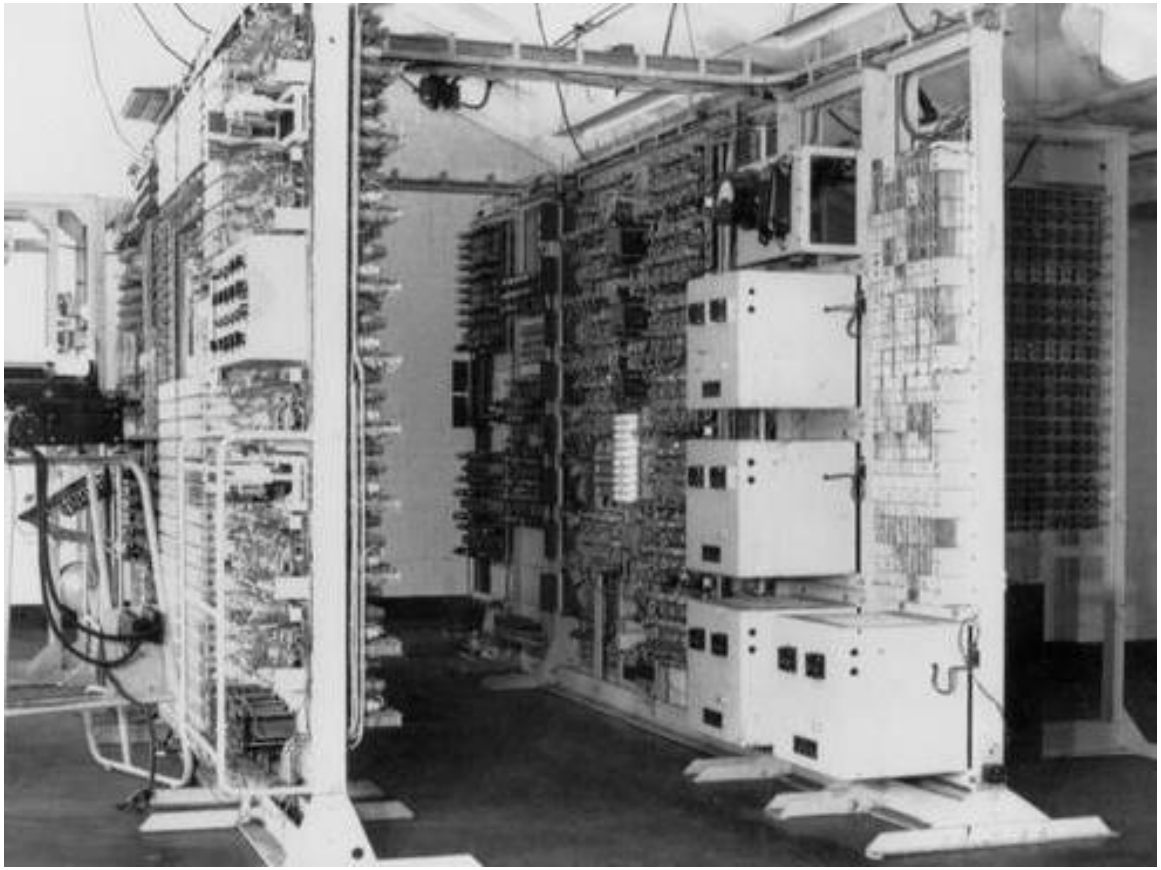
Butzel Long, PC

Salmon Fishing in Yemen?

Actually…on the Tamgas River near Metlakatla, Alaska

Cybersecurity Trends

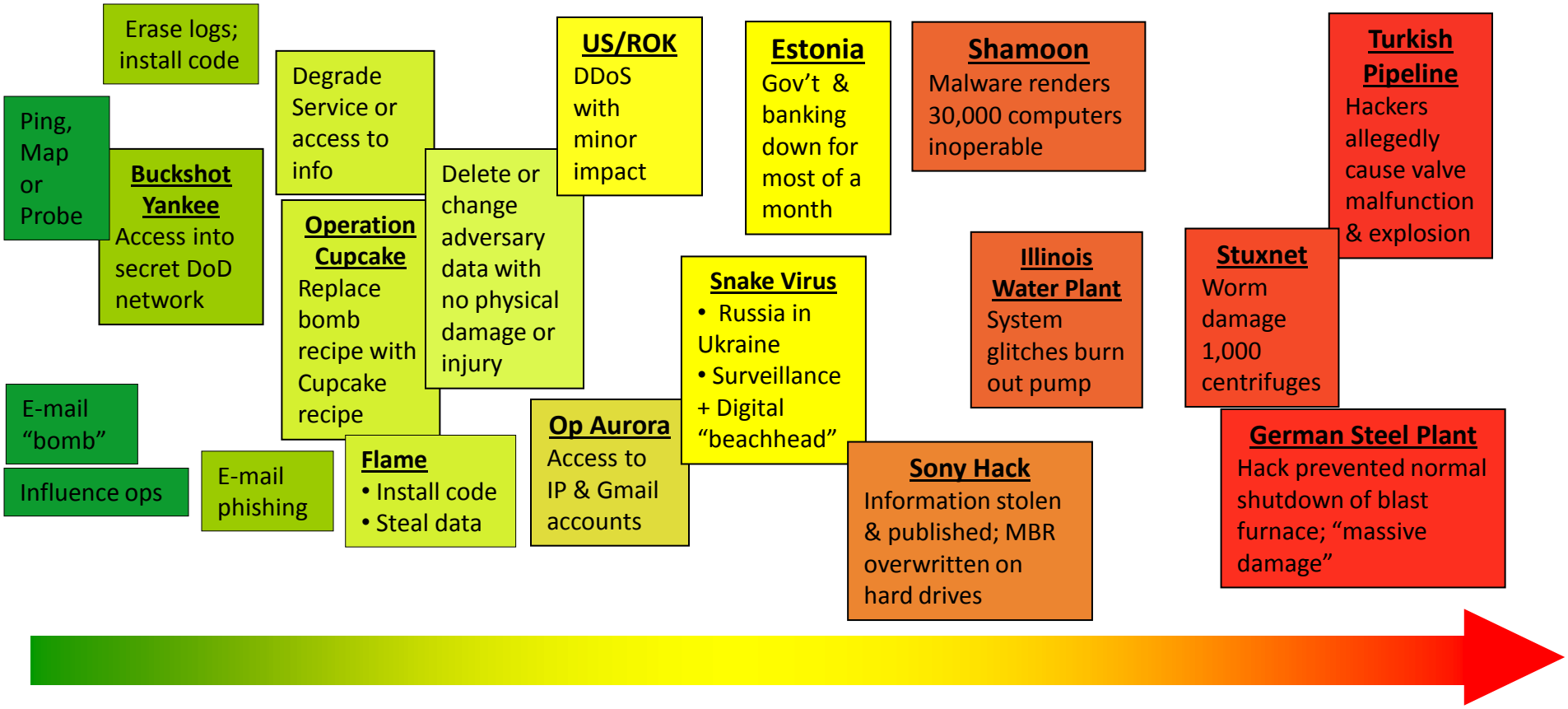
- Hacking as a service.
- Ransomware (data encryption-extortion).
- Smartphone kidnapping.
- Increase in social engineering attacks.
- Increase in music and movies to install malware.
- Hackers will continue to use and abuse cloud services.
- Mobile threats and more mobile threats.



Colossus: The World's First Electronic Programmable Computer at Bletchly Park, Buckinghamshire, England

Developed in 1943-45; Alan Turing contributed to its design, but this was not the computer used to decode Enigma

Spectrum of Cyber Operations



Enabling Operations

- Network characterization
- Internet Operations

Cyber Disruption

- Interrupt the flow of information or function of information systems without physical damage or injury

Cyber Attack

- Physical damage to property or injury to persons

More stealthy — Less stealthy

Adapted from Brown & Tullos, "On the Spectrum of Cyberspace Operations," *Small Wars Journal* (11 Dec. 2012)

Get to Know SCADA

- Supervisory Control and Data Acquisition (SCADA)
  - Energy
  - Oil & Gas
  - Transportation
  - Manufacturing
  - Power
  - Recycling
  - Water & Wastewater
  - Food & Beverage
- How do SCADA Systems Work?
  - Monitor, gather & process data
  - Interact with and control machines and devices, such as valves, pumps, motors, etc.—all connected through human-machine interface software
  - Records these events into a log file

What is a Breach?

- First: What is a Breach?
- Second: What was Disclosed, Published, Stolen, Accessed without Authority, Not Properly Secured…
- Federal Law & Regs: HIPAA/HITECH (Healthcare), FTC Act (Online Commerce), GLB Act & OCC (Financial)
- State Data Breach Laws (47 plus D.C., Puerto Rico, Virgin Islands & Guam)
- Other: Payment Card Industry
- Cybersecurity Framework (NIST Standard)
  - Connecticut, Maryland, Hawaii

The Risks to Law Firms & their Clients

- In 2009, the FBI issued a warning to law firms and PR firms that the Bureau had "high confidence" that hackers were attacking and exploiting law firms.
- In 2012, MI-5 informed 300 largest UK companies that their information was as likely to be stolen from their attorneys as it was from their own companies
- In 2012, Mandiant estimated that 80% of the 100 largest US law firms were subject to successful data breaches by malicious intruders in 2011.
- August 2015: Am Law 200 survey shows law firms rarely invest more than 1.9% of gross annual revenue on security
- But that's only what's reported…

Cyber Risks for Law Firms

- Mobile Lawyers & Staff
  - Ubiquitous "Public" WiFi
- Diverse "Work" Venues
  - Conference Centers
  - Hotels
  - Home
  - Foreign Travel
- BYOD
- IoT
- IOLTA Accounts
- Client Trade Secrets
- Client Contacts
- Push for Marketing & Visibility: Website "Success Stories"
- Electronic Payments (ACH)
- Wire Transfers
- PCI Compliance

Recent Case Study Examples

- Fraudulent ACH Transfer
  - Admin went to check firm acct at Bank
  - Odd delay
  - Email confirmation of Payroll
  - Police & local IT
- New Cryptolocker Variant/Open Door in Custom Software App
  - Partial encryption
  - Exfiltration of what, to whom?
  - Local IT & FBI

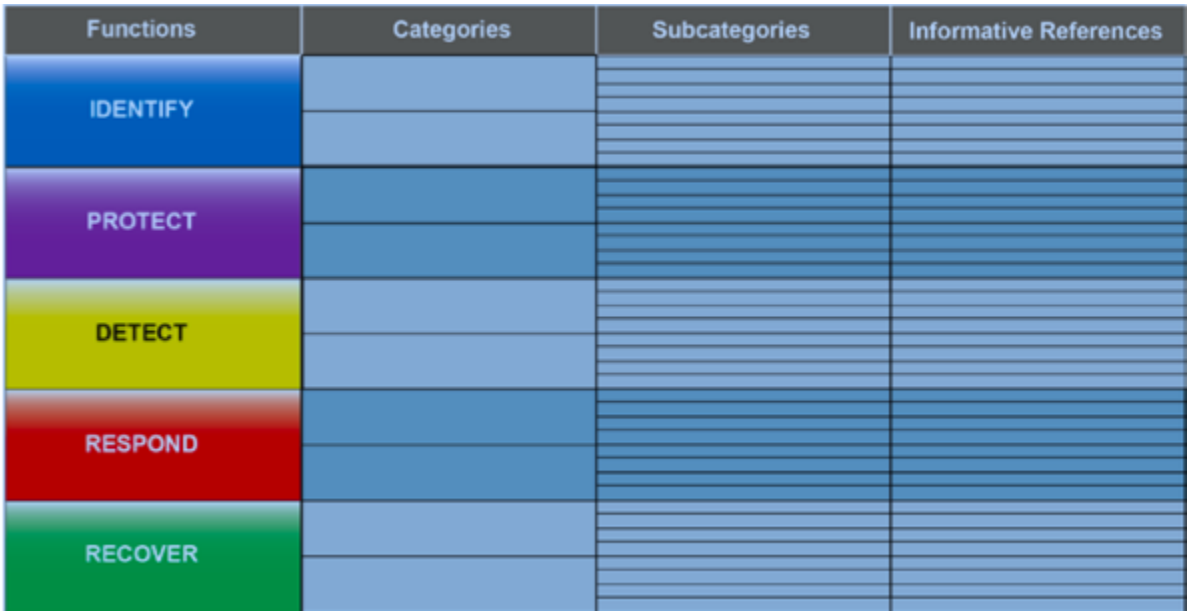
ABA Model Rule 1.1: Competency

- A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation
  - Comment [8] – *a lawyer should keep abreast of changes in the law and its practice,* ***including the benefits and risks associated with relevant technology***…

Current Federal Standard: NIST

NIST Cybersecurity Framework:

- Identify
- Protect
- Detect
- Respond
- Recover



Cyber Liability Insurance

- Data Breach: Failure to protect an individual's privacy – 1st Party Costs , Notification, Forensics, Legal Assistance, Credit Monitoring, PR Firms.
- Data Breach: Failure to protect an individual's privacy – 3rd Party Costs, Defense Costs & Settlements
- Network Security: Loss or damage to a network & data, 1st & 3rd Party (may include lost income)
- Media Liability: Web content (Libel, Defamation)
- Fines & Penalties (HIPAA, PCI)
- eVandalism & Extortion
- Property loss from Cyber Perils (Internet of Things)

Best Practices for Management

- Perform Risk Assessment (Physical Plant, Information Systems & Workforce)
- Segregate & Secure High Risk Information, Operations & Workers
- Encrypt Sensitive Data/Implement Robust Password Policy
- Implement Company-wide Training (Ongoing)
- Incorporate Security By Design (i.e., from the beginning)
- Acquire Cyber Liability Insurance
- Enable Network Security Monitoring & Review of Log Files (Lesson Learned from Target)
- Demand Compliance from Contractors & Suppliers (Another Lesson from Target)
- Conduct Table-Top Drills
- Have Experts at the Ready If/When an Attack Occurs

Best Practices for IT Departments

- Eliminate Unnecessary Data (don't pay fines on closed files)
- Conduct Ongoing & Active Risk Analysis
- Collect, Analyze & Share Incident Data
- Collect, Analyze & Share Tactical Threat Intelligence, Especially Indicators of Compromise
- Focus on Better & Faster Detection
- Establish Metrics: "Number of Compromised Systems" & "Mean Time To Detection" in Networks; Use Metrics to Drive Security
- Evaluate Threat Landscape to Prioritize Treatment Strategy (It's not a "One-Size Fits All" World)
- Track Workforce: Who's Who, What they Do & When they Leave