UNIVERSITY of WASHINGTON

Absorbed by the BORG

The tools and rules we need to manage liability in the 21st century

Dr. Barbara Endicott-Popovsky

5th International Symposium
“We shape our tools, and our tools shape us”

8 February 2013

Overview

- History
- UW Motivation
- Research Question
- Fraunhofer Motivation
- Current Evolution of our work
- Organizational Preparedness
- Research Agenda / Future Work

History

Forensic Readiness Research

Forensic Readiness

- Defined as:

'*maximizing the ability of an environment to collect credible digital evidence while minimizing cost of incidence response*.'

UW Motivation…

New Zealand Hacker Case vs.
Russian Hackers Case

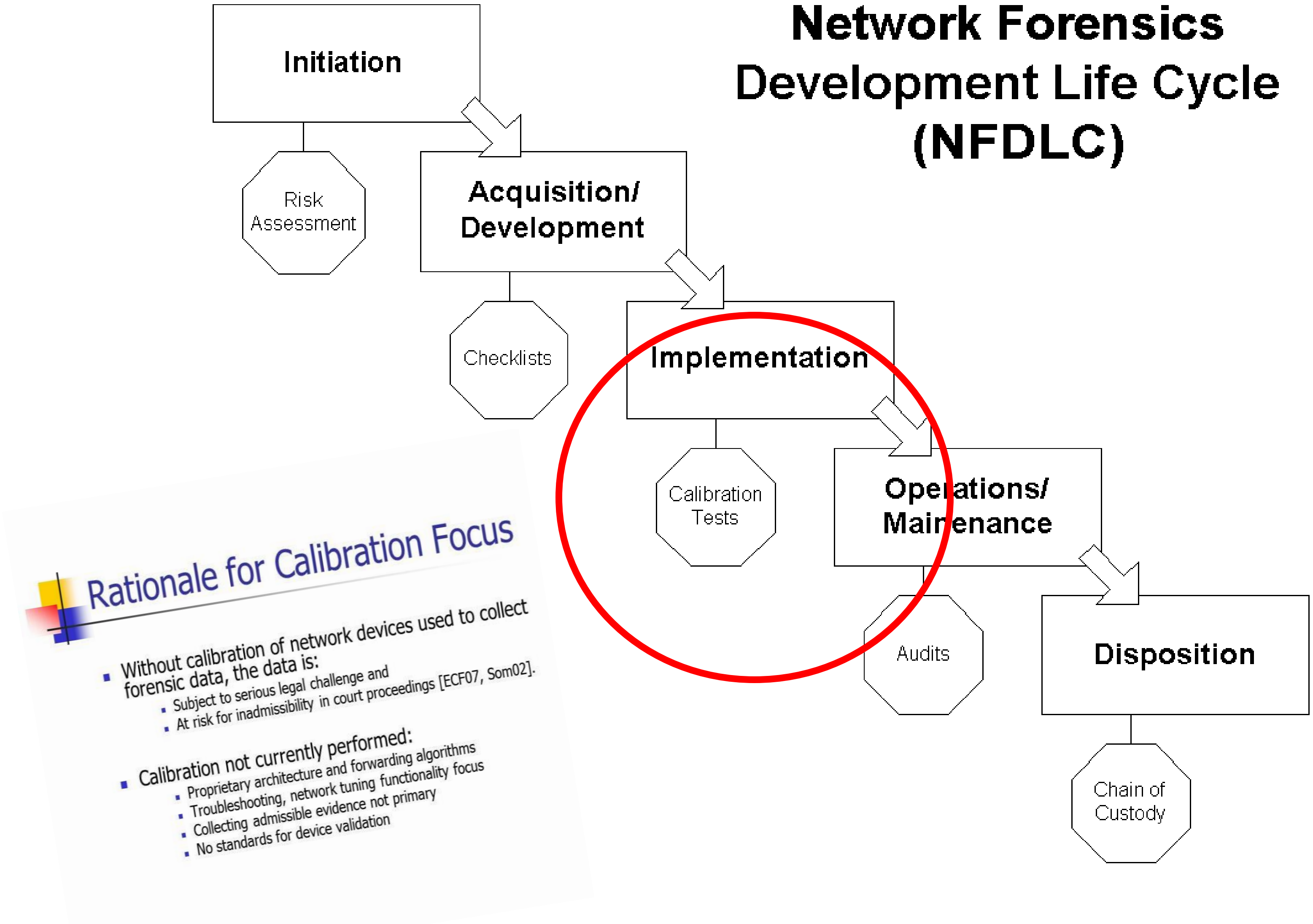
New Zealand vs. Russian Cases

Characteristics	NZ Hacker Case	Russian Hacker Case
Type of attack	Typical intrusion scenario	Online automated auction scam
Intruders	Script kiddies	Criminal hackers
Damages	$400,000	$25 million
Investigator time	417 hours	9 months
Investigator costs	**$27,800**	**$100,000** (partial)
Consequences	Community service	3 & 4 years in Federal prison
Investigator	Sys admins learning forensics	Expert recruited to work for the FBI
Network Forensic readiness	Reactive	Reactive

Research Question:

How can we overcome the inordinate effort/cost of investigations?

ISDLC Modifications Proposed: Embed Digital Forensics Capabilities



Observability Calibration Test Development Framework (OCTDF)

Step 1: Identify Potential Challenge Areas & Environment

- Briefly model interactions of interest;
- Identify whether lost network data could damage evidence value. -

Step 2: Identify Calibration Testing Goals

Identify testing goals that support evidence value.

Step 3: Devise a Test Protocol.

Devise a test regime that will appropriately calibration the device in question.

Forensic tap selected

Taps selected over switches

- Simple to test: they pass the data stream without introducing latency.

NetOptics 10/100BaseT Dual Port Aggregator Tap Chosen

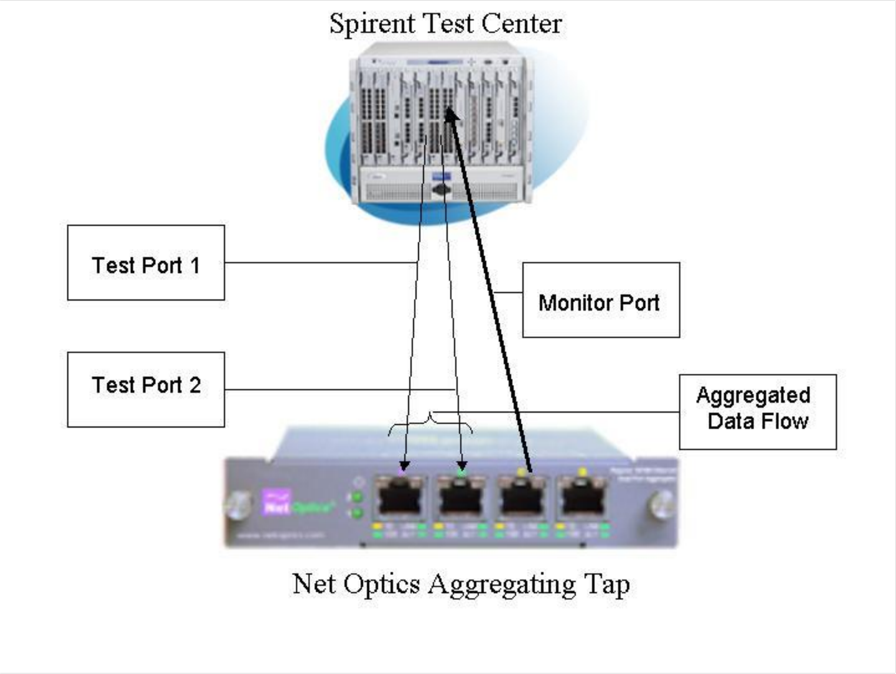
- First marketed as a forensic device

Test characteristics-RFC2544

- Same test device—send & receive
- UDP packets
- Same data rate in both directions
- 30 Second tests

Test Purpose:

- Verify 100% tap capacity (100mbps)



UNIVERSITY *of* WASHINGTON

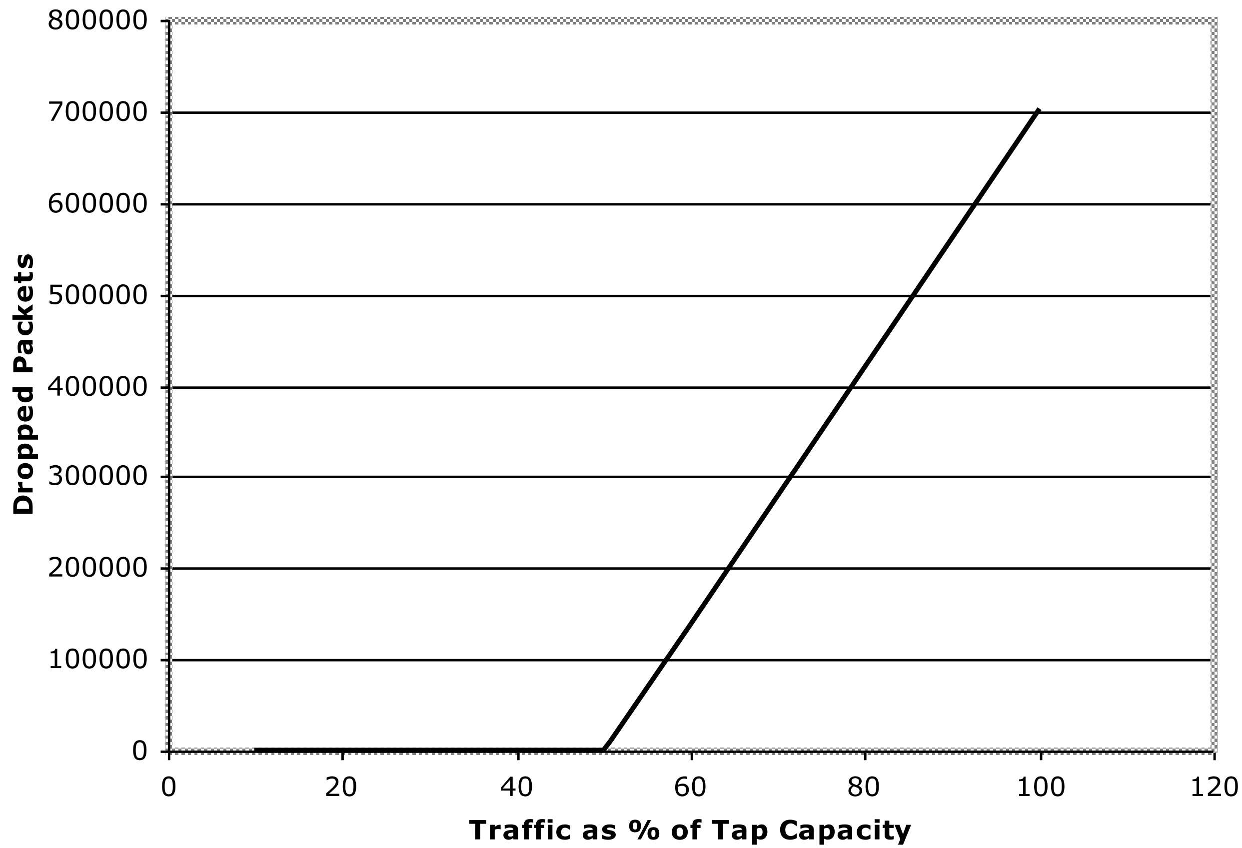
Test Results: Dropped Packets

(512k UDP Packets Transmitted 30 sec)

Test Case

- *T*sec = [*1* Mg x 8 bits]/ [(*102-100* Mbps)]
  = 4 seconds

- Where:
  - *Bf*bits = 1Mg
  - *BU*bits/sec = 102Mbps
  - *TC*bits/sec = 100Mbps



Status of device calibration

- NIST/CFTT
  - Calibrates law enforcement DF devices.
  - Software not hardware.

- Commercial device manufacturers
  - Customers not willing to pay.
  - Fluke, example

Fraunhofer Motivation…

Ensuring creation of secured digital evidence

ON THE CREATION OF RELIABLE DIGITAL EVIDENCE (8th IFIP 2012)

N. Kuntze, C. Rudolph, A. Alva, B. Endicott-Popovsky, J. Christiansen, T. Kemmerich

The authors suggest legal view be incorporated into device design as early as possible to allow for the probative value required of the evidence produced by such devices.

- Incorporate forensic readiness in requirements.
- Design-in features that support data use as evidence.
  - ID legal requirements evidence must meet.
  - Convert to technical requirements.

- Approach proposed to develop devices and establish processes crafted for the purpose of creating digital evidence.

- Produce hardware security anchor (e.g. TPM).
- Certify hardware security anchor.
- Certify platform.
- Produce software.
- Install, initialize and certify software.
- Define location, valid temperature, etc.
- Certify reference measurement values for calibrated devices.
- Generate and certify signing keys.
- Define location, valid temperature, etc. parameter ranges for correct use.
- Install device.
- Establish communication with server.
- Reference measurement record.
- Document and store reference records and transfer to server.
- Start the boot process and time synchronization.
- Collect evidence.

Conclusions

- Made the case for incorporating forensic readiness in design to ensure probative value of evidence.
- Provided concept for development of such a device.
- Laid out legal requirements for developing technical requirements.
- Described forensic readiness technology that exists, or is under development.
- Suggested approach for integrating forensic readiness into existing environments.
- Demonstrated complexity of modifications to existing systems to ensure data admissibility.
- Identified need for tight integration between technology and administrative procedures.
- Underlined need for more research to ensure more convenient/less complex designs.

UNIVERSITY of WASHINGTON

Current Evolution of our Work

Forensic Readiness Research

CASE 1
Secure Digital Evidence in Lawful Interception

- Scenario and requirements for digital evidence
  - Interception at network provider premises, possibly executed through another service provider.
  - Interface enabling data interception required and device connected to this interface.
  - Device collects all available data on interface.
- Specific device characteristics for scenario
  - Large streams of data must be signed.
  - Part of data can be deleted for privacy without invalidating the signature, but still showing where data was deleted. Example, VoIP streams.

Current Work

- Revises proposed approach
- Discusses three distinct scenarios where forensic readiness of devices and secure digital evidence are relevant.
- The scenarios are:
  - lawful interception of voice communication,
  - automotive black box,
  - precise farming.
- Different distinctive applications
- Shared common set of security requirements
  - processes to be documented
  - data records to be stored.
  - can be realized using a hardware-based solution.
- Strong incentives to tamper with data

Creating Secure Digital Evidence

- Device is physically protected to ensure it is tamperproof.
- The data record is securely bound to:
  - identity and status of the device (including running software and configuration)
  - All other relevant parameters (such as time, temperature, location, users involved, etc.)
- Data record not changed after creation.

CASE 1 (Cont’d.)
Secure Digital Evidence in Lawful Interception

- Possible realizations
  - Hybrid approach:
    - Bind key for stream signatures to the TPM.
    - Frequently change key.
    - Attest key bound to a particular device state.
    - Digitally sign and store signatures on the data stream so they can be clearly related.

Case 2: Secure Digital Evidence in Automotive Black Boxes

- Scenario and requirements for digital evidence
  - – Data recorded for diagnosis:
    - Typical use: Identify malfunction.
    - Increasing use: Resolve disputes.

Case 2: (Cont'd.) Secure Digital Evidence in Automotive Black Boxes

- Specific device characteristics for scenario
  - Separate control unit connected to central bus.
  - Monitors bus traffic, reports status or event information. Were brakes used? speed at impact? steering angle? Were seat belts worn?
  - Detects behavior/situation of car and driver.
  - Device under owner control; evidence suspect.
  - Consequences of such reconstruction.
    - used to determine liability.
    - Insurance companies want to use for rating insurance.
  - Strong incentive to modify EDR records.

Case 2: (Cont'd.) Secure Digital Evidence in Automotive Black Boxes

Specific device characteristics for scenario (cont'd)

- Assumes clearly defined data structures.
- Data stored is intentionally limited & reduced to small sizes. (supports crash records under time-critical situations.)
- Independent power supply not assumed due to cost and engineering reasons. Therefore, reduce write cycles to ensure relevant evidence is captured.
- Long-term data records storage should be local (within the box) providing an enclosed/isolated system with special measures against physical destruction.
- Only restricted memory available for long-term storage.

Case 2: (Cont'd.) Secure Digital Evidence in Automotive Black Boxes

- Possible realizations
  - Basic design applied to develop a black box.
  - Criticality of timing requires changes to protocol.
    - Store data record, subsequently sign, time-stamp and bind to quote information.
    - Unsigned recorded events can be considered valid if all prior signed data records show the device is okay.

Case 3: Secure Digital Evidence in Precise Farming

- Scenario and requirements for digital evidence
  - Large farms managed and controlled based on data records.
  - These technologies allow and record very precise use of seeding material, fertilizer, etc.
  - In sustainable/eco-farming, a need for monitoring processes and materials used.
  - Farming subsides encourage farmers to grow particular crops--automatically controlled using data records produced by the machines used in these processes.
  - Parameters include GPS positions to calculate the location and size of the area and the types of crop.

Case 3: Secure Digital Evidence in Precise Farming

- Scenario and requirements for digital evidence (Cont'd.)
- Devices are installed in different types of farm
- Central computer collects and evaluates data records.
- Different types of requirements:
  - Genetically manipulated crops: reliably document where crops are planted.
  - Fertilizers and pesticides or fungicides: wrong calculation create damage.
  - Origin of farm produce/proper verification of innocuousness of pesticide, etc.: more important as consumer concern increases—evidence of eco-farming.
  - Proof for subsidies: manipulating data records can support (or not) claims.
  - Integrate monitoring to ensure no deployment of forbidden material in fields.
- European research developing drone-system equipped with TMP.

Case 3: (Cont'd.) Secure Digital Evidence in Precise Farming

- Specific device characteristics for scenario
  - Large number of devices
  - Communication network to transfer data to central storage.
  - Internet as carrier platform.
  - 802.11 network employed.
  - Encryption of all data.
  - Documented access control to all entities.
  - Entire system much more complex than previous.
  - Devices hardened for use outdoors .

Case 3: (Cont'd.)
Secure Digital Evidence in Precise Farming

- Possible realizations
  - Basic concept of a device for generating secure evidence apply.
  - Various sensors contribute to data records and can be manipulated.
  - Solution must combine attestation of the platform with run-time validation for correctness of the sensor information.
  - Devices need physical protection.
  - Secured data transfer between devices and central storage
  - Overall (TPM) verification of data and condition of the sensors.
  - TPM certificates for authentication
  - Smart detection to detect insertion of manipulated devices.
    i.e. drone with infrared cameras (IR) and radar systems for detection of unusual behavior or manipulation of the field's infrastructure.

Conclusions

- Concept of forensic readiness is now available for specific applications.

- Although quite different, all three scenarios can use our 2012 solution.

- As the bar is raised on digital evidence admissibility, with successful implementation of the technology described, more applications will emerge requiring this solution.

Open Questions

- Identifying and analyzing additional scenarios
- Testing the solution in actual circumstances.
- Exploration of vast privacy implications
  – Where is data stored?
  – Who owns the data?
  – Opt in, out?

UNIVERSITY of WASHINGTON

Organizational Preparedness

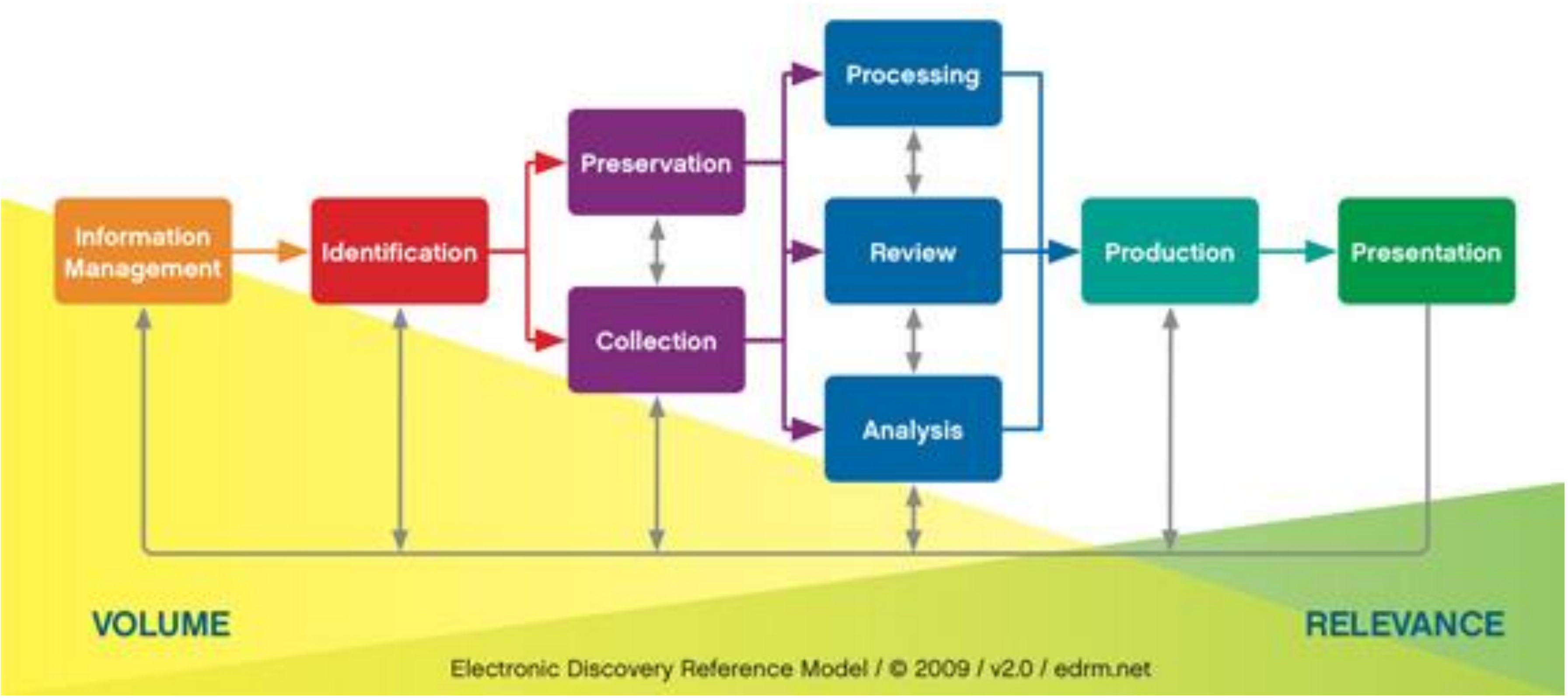
Forensic Readiness Research

Motivation

Planning for litigation is a valid approach to constructing forensically ready IT systems

Electronic Discovery requirements map back to technical system requirements

– Model for implementing ‘forensic-ready systems’



Method

Identify the barriers to eDiscovery

Apply first two (planning) steps of eDiscovery Reference model

-Information Management

-Identification

UNIVERSITY of WASHINGTON

Context: We're headed into the Clouds

- Electronic Discovery = legal requirements that compel orgs to make available relevant information in civil cases

- Only 16% surveyed had eDiscovery plan prior to cloud migration

Symantec. *Information Retention and eDiscovery Survey Global Findings 2011.* Accessed June 27, 2012. https://www4.symantec.com/mktginfo/whitepaper/InfoRetention_eDiscovery_Survey_Report_cta54646.pdf
Barry Murphy, "e-Discovery in the Cloud is Not As Simple As You Think," *Forbes*, November 29, 2011, accessed June 14, 2012, http://www.forbes.com/sites/jasonvelasco/2011/11/29/e-discovery-in-the-cloud-not-as-simple-as-you-think/

Legal Control Structures

- Service Level Agreements
  - Source of authority to resolve all issues and disputes between cloud provider and customer
  - ‘If it’s not in the contract, it’s not part of the formal relationship’

Issues with Cloud-SLAs

- Limited availability of forensic data
- Burden of producing evidence is still with customer,
  - Regardless of third-party provider (in)action
  - Particularly for data spoliation

Barriers to Usefulness & Admissibility of Cloud-Based Evidence

- Authenticity
- Jurisdiction
- Third-Party Control

Barriers to Usefulness & Admissibility of Cloud-Based Evidence

Authenticity: critical gate for admitting evidence

- How to show data meets authenticity standards?
- “Testimony of a Witness with Knowledge”
- “Evidence About a Process or System”

Fed. R. Evid 901

Barriers to Usefulness & Admissibility of Cloud-Based Evidence

Jurisdiction: What laws prevail?

- Question of nexus
  - Does a datacenter constitute nexus?
- "Conflict of Laws"
- New concepts (for legal community) of broad distribution of data
  - U.S. case law gives little direction

Barriers to Usefulness & Admissibility of Cloud-Based Evidence

Third-Party Control: Who's in charge?

- Reliance on one or more third party
  - introduces legal complexity
- Knowledge & data process mapping in eDiscovery "planning" phrase can mitigate risk
  - Requires understanding of agreements/SLAs, contracts, policies (legal/organizational)
  - Requires data mapping and analysis (technical)
- Data Destruction?

Justifying Costs

Quantifying value of forensically ready system

- ***Reactive costs:***
  - *Zubulake* test
    - – Seven factors to determine cost
  - Cost of data spoliation penalties
    - – Federal ‘common law’ of spoliation
  - Third-Party Cloud Provider contract costs

vs.

- ***Planned strategy:***
  - Organizational investment to ensure systems are forensically ready

Future Work

***Multidisciplinary research efforts*:**

- Authenticity, Jurisdictional, Third-Party Control legal processes for cloud-based forensics (ongoing)
  - more specific development
- Analyze legal eDiscovery requirements vs. appropriate technical controls for cloud-based systems
- Cloud SLA improvement
  - empirical research
  - guidelines for 'forensic ready SLAs'
- Analysis of forensic ready systems v. costs of litigation
- Educating legal professionals on digital forensics (ongoing)
- more

Forensic Readiness Book (Springer) Call for Chapters

- Part I The Problem (Editors)
  - Forensic Readiness models
  - Legal issues
  - Preservation and Authentication issues
  - Technical issues (timestamp issues, etc)
- Part II Current solutions
  - Engineered solutions (Fraunhofer and others) Peer-reviewed chapters current research.
- Part III Where we need to go (Editors)
  - Hardware and software forensic readiness
  - Network forensic readiness
  - Cloud forensic readiness Mobile forensic readiness
  - Digital Records forensic readiness
  - Need for research

Importance of the Forensic Readiness Problem

- Absent thoughtful intervention the results will be:
  - **A justice system subject to confusion**,
  - **Escalating growth in technology-related crimes**,
  - **Growing new liability for companies, individuals**,
  - **Decreasing trust in the economy/the "system"**,
  - **A general halt to the progress of the Information**.

"FRANKLY, I MISS THE OLD DAYS OF JOHN DILLINGER AND AL CAPONE."

UNIVERSITY of WASHINGTON

Questions?

Barbara Endicott-Popovsky

endicott@uw.edu

5^{th} International Symposium
"We shape our tools, and our tools shape us"

8 February 2013