Introduction: CIS8630 Business Computer Forensics and Incident Response

Richard Baskerville

Motivation: Why this topic matters

- Policy Enforcement
- Information Security
- Legal Protection and Preparedness
- Privacy Protection
- Performance Assurance
Interaction of Left & Right Paradigms

Left of Incident

- Threat
- Indications & Warnings
- Prevent
- Deter
- Legislate & Policy Setting

Right of Incident

- Refine
- Contain, Recover, Harden
- Detect
- Respond
- Investigate, Notify, Sue, Prosecute, Retaliate

Information System Resource

Left of incident

- Prevention
- Indications and Warnings
- Deterrence
- Crime or Policy Violation

Right of incident

- Detection
- Response
  - Contain/recover/harden
  - Legislate/Policy
  - Investigate, Notify, Sue, Prosecute, Retaliate

Left vs. Right Paradigms

Assumptions

<table>
<thead>
<tr>
<th>Features</th>
<th>Left of Incident</th>
<th>Right of Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat tempo</td>
<td>Premise 1: Incident threats are persistent.</td>
<td>Premise 1: Incident threats are transient.</td>
</tr>
<tr>
<td>Safeguards tempo</td>
<td>Corollary 1.1: Effective safeguards must be persistent.</td>
<td>Corollary 1.1: Effective safeguards must be agile.</td>
</tr>
<tr>
<td>Threat-safeguard timing</td>
<td>Corollary 1.2: Threats and safeguards share a static relationship.</td>
<td>Corollary 1.2: Threats and safeguards share a dynamic relationship.</td>
</tr>
<tr>
<td>Threat forecasting</td>
<td>Premise 2: Threats are predictable.</td>
<td>Premise 2: Threats are unpredictable.</td>
</tr>
<tr>
<td>Threat measurement</td>
<td>Corollary 2.1: Threats are measurable.</td>
<td>Corollary 2.1: Threats are not measurable.</td>
</tr>
<tr>
<td>Threat safeguard logical form</td>
<td>Premise 3: The relationship of safeguards to threats is determinate.</td>
<td>Premise 3: The relationship of safeguards to threats is consequential.</td>
</tr>
</tbody>
</table>

### Left vs. Right Paradigms

#### Logical Structure

<table>
<thead>
<tr>
<th>Features</th>
<th>Left of Incident</th>
<th>Right of Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Causal Structure</td>
<td>Variance</td>
<td>Process</td>
</tr>
<tr>
<td>Unit of analysis</td>
<td>Variables</td>
<td>Events</td>
</tr>
<tr>
<td>Safeguard-Threat Risk</td>
<td>Safeguard is necessary and sufficient to reduce risk</td>
<td>Safeguards are part of a necessary sequence of conditions to reduce risk</td>
</tr>
<tr>
<td>Reduction Definition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relationship to time</td>
<td>Static</td>
<td>Dynamic</td>
</tr>
<tr>
<td>Logical Form</td>
<td>“if X then Y”</td>
<td>“if not X then not Y”</td>
</tr>
</tbody>
</table>


#### Organizing Principles

<table>
<thead>
<tr>
<th>Features</th>
<th>Left of Incident</th>
<th>Right of Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating mathematics</td>
<td>Probability</td>
<td>Possibility</td>
</tr>
<tr>
<td>Strategic goal</td>
<td>Quality</td>
<td>Agility</td>
</tr>
<tr>
<td>Learning strategy</td>
<td>Exploitation</td>
<td>Exploration</td>
</tr>
</tbody>
</table>

Information Security Incident


- Any information-related activity with negative security implications.
  - Usually means that the activity violates an explicit or implicit information security policy.

Information Security Incident


- A security incident is a change of state in a bounded information system from the desired state to an undesired state, where the state change is caused by the application of a stimulus external to the system.
Basic types of Information Security Incident:

- Penetration
- Fraud
- Denial-of-service
- Virus/worm infection


Business Computer Incident Response

- Incident response: procedures that mitigate the immediate impact of the threat, eliminate any possible consequential loss and prevent any possible future recurrence

Incident Response Methodology

- Interdiction: Stopping or interrupting the incident
- Containment: Isolating damage and preventing it from spreading
- Recovery: Returning the business to the pre-incident state
- Analysis: Post-incident root cause analysis (post-mortem)

Computer Security Incident Response Team (CSIRT)

- Analysis of security vulnerabilities and new threat research, and dissemination of countermeasures information
- Coordination of response to all information security incidents, such as malicious code (worms, viruses, trojan horses, etc.),
- Investigation of security incidents involving company computing resources (including abuse, harassment, blackmail, sabotage, and theft)
- Resolution (both hands-on and on a coordination level) of general threats to confidentiality, availability and integrity of the company’s data and systems
- Education of the users and the engineering and support organization about security issues and trends
The application of forensic science techniques to computer-based material, the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is acceptable to legal proceedings.

Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. Computer forensics is also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination.
Digital forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
Forensics Community of Practice

- Frequent visiting experts
  - Business forensics experts
  - Legal technical experts
  - Law enforcement

Introduction: CIS8630
Business Computer Forensics and Incident Response

Richard Baskerville