2019

An Evidence Based Cybersecurity Approach to Risk Management: Risk Management and "Market for Lemons"

David Maimon

Follow this and additional works at: https://scholarworks.gsu.edu/ebcs_presentations
An Evidence Based Cybersecurity Approach to Risk Management
Agenda

• 9:00 -10:30 Keynotes
• 10:30 Break
• 10:45 Group discussions
• 12:00 Lunch
• 1:00 Group discussions
• 2:15 Group discussions summaries
• 2:45 Conclusions
Risk Management and “Market for Lemons”

Dr. David Maimon
Risk

• The extent to which an entity is threatened by a potential circumstance or event.

• Risk is typically a function of:
  • The adverse impacts that would arise if the circumstance or event occurs;
  • The likelihood of occurrence.
Information Security Risks

- Those risks that arise from loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations, organizational assets, and individuals.
Risk Management

• The process of identifying, assessing and evaluating the level of risk facing the organization, and then deciding what countermeasures to take in reducing risk to an acceptable level.
Risk Management Process (NIST)
Assess

• Identify

  • Threats to organizations (i.e., operations, assets, or individuals)
  • Vulnerabilities internal and external to organizations;
  • The harm (i.e., adverse impact) that may occur
  • The likelihood that harm will occur.

• The end result is a determination of risk
Respond

• Developing alternative courses of action for responding to risk
• Evaluating the alternative courses of action
• Determining appropriate courses of action consistent with organizational risk tolerance;
• Implementing risk responses based on selected courses of action
Monitor

• Determine the ongoing effectiveness of risk responses
Problem

• The current common approaches for risk assessment (likelihood and impact) and the implementation of response are problematic at best
Likelihood of Occurrence

The *likelihood of occurrence* is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).
Determine the Likelihood a Harm will Occur

<table>
<thead>
<tr>
<th></th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>0-25% chance of successful exercise of threat during a one-year period</td>
</tr>
<tr>
<td>Moderate</td>
<td>26-75% chance of successful exercise of threat during a one-year period</td>
</tr>
<tr>
<td>High</td>
<td>76-100% chance of successful exercise of threat during a one-year period</td>
</tr>
</tbody>
</table>
Potential Impact

• The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
<table>
<thead>
<tr>
<th>Areas of vulnerability and possible effects of damage</th>
<th>Risk of monetary loss</th>
<th>Risk of productivity loss</th>
<th>Risk of loss of customer confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel</td>
<td>H M L</td>
<td>H M L</td>
<td>H M L</td>
</tr>
<tr>
<td>Unauthorized disclosure, modification, or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadvertent modification or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nondelivery or misdelivery of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial or degradation of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilities and equipment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized disclosure, modification, or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadvertent modification or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nondelivery or misdelivery of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial or degradation of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized disclosure, modification, or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadvertent modification or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nondelivery or misdelivery of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial or degradation of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized disclosure, modification, or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadvertent modification or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nondelivery or misdelivery of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial or degradation of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software and operating systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized disclosure, modification, or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadvertent modification or destruction of information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nondelivery or misdelivery of service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial or degradation of service</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Market for Lemons (Akerlof 1970)

• A market with asymmetric information
Cybersecurity Market

• Vendors may make claims about the security of their products, but in the absence of evidence regarding the effectiveness of the products, buyers have no reason to trust them.
Solutions for Lemon Markets

• Warranties

• More information regarding the product
The Million Dollar Question

• What should be done in effort to support CISOs’ and General Counsels’ decision making regarding the assessment of risks as well as the adoption of security policies and tools within their organizations?
Evidence-Based Cybersecurity (EBCS)

• Stresses moving beyond decision makers’ political, financial, social background and personal experience to a model in which tools’ adoption and policy enforcements decisions are made based on scientific studies findings.
Cybercrime Ecosystem

Targets

Offenders

Guardians

Enablers

The Surface Web

The Deep Web and Darknet
Rigorous Scientific Research Designs
Resources

The resources below are available for free download. Please enter your email address and a download link will be sent to you.

- **Prompt Patching**
  - Description: A description about how Prompt vulnerability helps in providing cyber security.
  - Size: 257.88 KB
  - Downloads: 2

- **Passwords**
  - Description: How Passwords can help in authentication and help in preventing the development of the... (text cut off)
  - Size: 196.18 KB
  - Downloads: 0

- **Intrusion Detection System (IDS)**
  - Description: A device or software application that monitors a network or systems for malicious... (text cut off)
  - Size: 19308 KB
  - Downloads: 0

- **Honeyhogs**
  - Description: Tools which permits the collection of information on hackers and real system trespassing...
  - Size: 191.29 KB
  - Downloads: 0

- **Firewalls**
  - Description: (text cut off)
  - Size: 194.16 KB
  - Downloads: 2
Key Principals of the Approach

Generate and employ empirical evidence to:

- Identify online threats and vulnerabilities and educate targets of cybercrime
- Guide policy development and guardians’ efforts to secure cyberspace
- Guide the design and configuration of computing environments that can mitigate effectively the consequences cybercrime events
Evidence Based Cybersecurity and Threat Assessments (Examples)
A Threat-Oriented Approach

• A threat-oriented approach starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are identified based on adversary intent.
The Origin and Time of Attacks Against a Network (Maimon et al 2013)
Data

- Intrusion Prevention System (IPS) data from a large university computer network
  - Potential attack attempts (unlike for incidents, false alarms might exist)
  - Collected between September 2007 and until 2009
## Hourly Distribution of Computer-Focused Crimes

<table>
<thead>
<tr>
<th>Time of day</th>
<th>2007 (N = 2,168,478)</th>
<th>2008 (N = 3,270,895)</th>
<th>2009 (N = 645,554)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00am – 4:59pm</td>
<td>59.04%</td>
<td>38.25%</td>
<td>50.06%</td>
</tr>
<tr>
<td>5:00pm - 12:59am</td>
<td>16.19%</td>
<td>27.36%</td>
<td>21.44%</td>
</tr>
<tr>
<td>1:00am-8:59am</td>
<td>24.8%</td>
<td>34.39%</td>
<td>28.5%</td>
</tr>
</tbody>
</table>
## Foreign Network Users and Computer-Focused Crimes Against the Network

<table>
<thead>
<tr>
<th></th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IRR</td>
<td>95% CI</td>
<td>IRR</td>
</tr>
<tr>
<td>Population between 15-64 years</td>
<td>1.13***</td>
<td>1.06, 1.20</td>
<td>1.15***</td>
</tr>
<tr>
<td>% Urban</td>
<td>1.04***</td>
<td>1.02, 1.06</td>
<td>1.01*</td>
</tr>
<tr>
<td>Internet users</td>
<td>1.03***</td>
<td>1.01, 1.05</td>
<td>1.03***</td>
</tr>
<tr>
<td>Foreign network users per 1000 users</td>
<td>1.64*</td>
<td>1.00, 2.98</td>
<td>1.58*</td>
</tr>
</tbody>
</table>

*\(p<0.05\)  **\(p<0.01\)  ***\(p<0.001\)
An Asset/Impact-Oriented Approach

• An asset/impact-oriented approach starts with the identification of impacts or consequences of concern and critical assets, possibly using the results of a mission or business impact analyses and identifying threat events that could lead to and/or threat sources that could seek those impacts or consequences.
Refund Notification

Due to a system error you were double charged for your last order. A refund process was initiated but could not be completed due to errors in your billing information.

REF CODE: 2550CGE

You are required to provide us a valid billing address.

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days.

We hope to see you again soon.

Amazon.com

Email ID: [redacted]
- 545 logins (20 per 1000 users)

- 178 phishing (6.87 per 1000 users)

- 21% of the logins and 25% of the phishing occurred from university network
Predicted Probability of Students and Non-Students to Click on Links Embedded in Suspicious Emails while Using University and Non-University Networks

- University Network:
  - Student: 34%
  - Not a Student: 47%

- Other Network:
  - Student: 32%
  - Not a Student: 18%
Predicted Probability of Employees and Non-Employees to Click on Links Embedded in Suspicious Emails while Using University and Non-University Networks

- University Network:
  - Employees: 39%
  - Not an Employee: 37%

- Other Network:
  - Employees: 17%
  - Not an Employee: 34%
A Vulnerability-Oriented Approach

- A vulnerability-oriented approach starts with a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environments in which the systems operate, and identifies threat events that could exercise those vulnerabilities together with possible consequences of vulnerabilities being exercised.
Diffusion of Viruses, Worms and Trojans
Evidence Based Cybersecurity and Response Effectiveness (Example)
Antivirus Programs and Companies

- Avast!
- F-PROT
- Symantec
- AVG
- ClamWin
- McAfee
- GRISoft
- Microsoft Security Essentials
- Trend Micro
- Sophos
- Eset
- Kaspersky
38% of the study participants were exposed to malware.

20% of the computers were infected by some form of malicious software that was not detected by the antivirus.
In conclusion,

- Risk assessments should be guided by the design of rigorous scientific studies and the collection of evidence which will provide more accurate probabilities of threats to develop.

- Rigorous evaluations of the effectiveness of cybersecurity tools and policies could improve the security posture of organizations and individuals, and in turn, reduce the occurrence of successful cybercrime events.

- To guide CISOs and GC decision making regarding security related issues, such information should be publicly available and accessible.
David Maimon
Email: dmaimon@gsu.edu
Website: www.davidmaimond.net
Twitter: @david_maimon