Cybersecurity Investment Optimization with Risk: Insights for Resource Allocation

Senay Solak, Ph.D.
Department of Operations and Information Management
Isenberg School of Management
University of Massachusetts Amherst

September 19, 2014
Motivation

- **Modeling and optimization can help organizations make better decisions for cybersecurity, e.g.**
  - Threat models that help devise better security products and policies
  - Game theoretic models to better understand and manage the different players in cybersecurity
  - Optimization models to better utilize available resources in fighting against cyber threats, etc.

- **Practical use somewhat limited, as models themselves are mostly limited due to complexities in the cybersecurity framework**
  - Data availability and access is a major challenge!
Motivation

- But **progress is being made**: improved, more realistic models with more practical relevance are being developed
  - Need more generic policy results, which are easier to implement or adopt
  - Customized solutions for individual firms are valuable, but require more significant investment

- An area where modeling and optimization can help significantly is in defining investment policies on cybersecurity countermeasures
Motivation

- Global cybersecurity investments expected to reach $120 billion by 2017: an annual growth of ~11%

- Most firms utilize separate cybersecurity budgets

- Most common utilization of these budgets: obtain products from third-party providers

- Concern for firms: How efficient and effective are these investments?
Motivation

- Difficult to answer due to challenges in:
  - Measuring returns from cybersecurity investments
  - Defining the uncertainty around the returns
  - Consideration of the ever-changing dynamics of the cyber environment

- Also, the definition of effectiveness and efficiency can differ based on the firm and industry, especially when risk is involved

- There exist important and impactful analyses in the literature
Motivation: Current State of Knowledge

- **Empirical studies:** industrial survey reports
  - CSI Computer Crime and Security Survey; Verizon Data Breach Investigation Report; Ponemon Institute Cost of Cybercrime

- **Economic approaches:** cost-benefit metrics such as NPV, ROI in deciding among options
  - Gordon and Loeb (2002, 2006a, 2006b); Baryshnikov (2007); Huang et al. (2008)

- **Portfolio models:** capture combinations of investment options and other limitations
  - Hoo (2000); Rees et al. (2011); Garvey and Patel (2013)
Motivation

- But including all the challenges in models make them intractable
  - Hence, proposed approaches provide mostly specific insights on a given component of cybersecurity investment process

- **Goal:** Build and utilize a high-level framework to derive *some general industry-specific insights for cybersecurity resource allocation*
General Cybersecurity Investment Framework

- **Countermeasures**
  - **Preventive countermeasures**: hedging against cyber attacks before any breach can take place
  - **Detective countermeasures**: identifying and removing an attack during or after the occurrence of a breach

- **Attacks**
  - **Basic attacks**: unsophisticated and opportunistic attacks, not specific to a given target
  - **Advanced attacks**: Deliberately customized for an individual organization
General Cybersecurity Investment Framework

- **Assets**
  - **Confidential assets**: data containing information that should not be disclosed to any third parties
  - **Non-confidential assets**: hardware, facility, and human labor

- **Unique combinational effects between components**
# General Cybersecurity Investment Framework

## Attacks

**Basic attacks:**
- Keyloggers and spyware
- Backdoor or command control
- Unauthorized access via weak access control lists
- Unauthorized access via stolen credentials
- Physical theft of assets
- Brutal force attack

**Advanced attacks:**
- Abuse of system access/privileges
- Violation of acceptable use and other policies
- Phishing
- Packet sniffer
- Pretexting

## Countermeasures

**Detective countermeasures:**
- Anti-virus software
- Anti-spyware software
- Content monitoring
- Forensic tools
- Intrusion detection system software
- Log management software

**Preventive countermeasures:**
- Biometrics
- Data loss prevention
- Encryption
- Firewall
- Intrusion prevention system
- Public key infrastructure
- Server-based access control list
- Static account logins/passwords
- Specialized wireless security
- Smart cards and other one-time tokens
- Virtualization-specific tools
- Vulnerability/patch management
- Virtual private network

## Assets

**Non-confidential assets:**
- Point of sale server
- Network devices
- Database server
- End-user system
- Mobile devices

**Confidential assets:**
- Customer personal information
- Payment card information
- Off-line data
General Cybersecurity Investment Framework

- Attack and asset distributions vary over industries

![Diagram showing the ratio of confidential assets with respect to total value at risk against the ratio of advanced attacks among all attacks for various industries such as finance, retail, technology sector, energy, professional services, manufacturing, transportation, public sector, hospitality, and healthcare.]

- As such, investment policies are expected to vary, too
General Cybersecurity Investment Framework

- **Typical decision process** for cybersecurity investment by organizations:

  - **Assessment of asset value**
  - **Decide on cybersecurity budget**
  - **Identification of investment options**
  - **Allocate budget to different cybersecurity investment options**
  - **Execution of investment plan**

  Inputs:
  - Budget limitation
  - Investment options
  - Attack environment
  - External constraints
  - Uncertainty and risk factors
  - Observation of cybersecurity dynamics

[Diagram showing the decision process]
Modeling Returns

- Quantifying the return on investment in cybersecurity: effectiveness in reducing expected total loss
  1. increasing with increasing investment level
  2. eventually approaching to an asymptotic value
  3. diminishing marginal returns as investment level increases

[Diagram showing the relationship between investment level and effectiveness of countermeasure]
Modeling Returns

- **Joint effectiveness of countermeasures:**

![Diagram showing joint effectiveness of countermeasures](image-url)
Modeling Returns

- Quantifying the return on investment in cybersecurity investment: effectiveness

  - Losses without countermeasures:
    \[ \sum_{s \in S} \sum_{a \in A} f_{a|s} \]
    - Expected losses due to a given type of attack on a given type of asset
    - Frequency of a given attack type

  - Losses reduced with countermeasures:
    \[ L(x) = \sum_{s \in S} \sum_{a \in A} f_{a|s} \left( \prod_{o, o' \in O} \sqrt{1 - \epsilon_{oo'}(x_o, x_{o'})} \right) \]
    - Impact of individual and joint effectiveness of countermeasures
Modeling the Dynamics

- Both attack frequencies and countermeasure effectiveness evolve over time.

- Can represent attack frequencies as a function of time as $f_a(t)$.

- Effectiveness of a countermeasure follows a life-cycle pattern.
Modeling the Dynamics

- Estimates based on analysis of data from McAfee and Symantec

Three stages of countermeasure life-cycle curve

Effectiveness life-cycle curves for preventive and detective measures
Modeling the Dynamics

- **Dynamic investment process**
  - Resource allocations adjusted based on observed effectiveness levels and changing attack types/frequencies

\[ \beta_{oa}(t) \]

Effectiveness parameter

Stage I

Invest

Observe

Stage II

Invest

\[ \beta_{oa}(t) \] estimate revealed
Modeling the Uncertainty

- Firms cannot know exactly how effective the countermeasure is, as defined by the position on the underlying life cycle curve.

- Hence, effectiveness uncertainty is captured by considering potential shifts in the life-cycle based effectiveness curves between the assumed and actual (unknown) effectiveness levels.

- Each potential level of deviation has an associated probability.
Modeling the Uncertainty

Learning takes place as the countermeasure is being utilized.
Modeling Risk

- Risk is indispensable in any type of investment problem.

- It is a challenge as to how to define and measure risk in a cybersecurity optimization setting – mainly due to mathematical tractability.

- An approach based on reduction of variance around the expected losses to minimize the likelihood of extremely high losses is a practical assumption.
Modeling Risk

- To that end, we utilize conditional value at risk (CVaR) as a risk measure in optimizing cybersecurity investments.
  - CVaR represents the expected loss that will be incurred if the realized losses lie in some given percentile of the total loss distribution.

Ref: Smartfolio.com
Optimization

- **Goal:** Identify an investment policy over different countermeasure categories, such that a weighted function of the expected total losses and the conditional value at risk is minimized.

- By also considering:
  1. Individual and joint effectiveness levels of different countermeasure categories.
  2. Dynamics of the cyber environment.
  3. Uncertainty in the effectiveness levels.
  4. Learning effects over time as countermeasures that are invested in are put in use.
  5. Any regulatory requirements on minimum protection levels, etc.
Insights for Resource Allocation

- Based on data obtained from cybersecurity literature and surveys we conducted
- Investigated findings separately for categories of industries, where the categorizations are based on the distribution of attack types as reported in the literature

<table>
<thead>
<tr>
<th>Industry category</th>
<th>Industry name</th>
<th>( \frac{f_{2i}}{f_{1i} + f_{2i}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category I</td>
<td>technology sector</td>
<td>0.34</td>
</tr>
<tr>
<td></td>
<td>finance</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>energy</td>
<td>0.42</td>
</tr>
<tr>
<td></td>
<td>professional service</td>
<td>0.43</td>
</tr>
<tr>
<td>Category II</td>
<td>manufacturing</td>
<td>0.51</td>
</tr>
<tr>
<td>Category III</td>
<td>retail</td>
<td>0.58</td>
</tr>
<tr>
<td></td>
<td>transportation</td>
<td>0.63</td>
</tr>
<tr>
<td></td>
<td>public sector</td>
<td>0.63</td>
</tr>
<tr>
<td>Category IV</td>
<td>hospitality</td>
<td>0.92</td>
</tr>
<tr>
<td></td>
<td>healthcare</td>
<td>0.96</td>
</tr>
</tbody>
</table>
Insights for Resource Allocation: Optimal Budget

What should be the optimal level of cybersecurity investment by the firm?

- Optimal cybersecurity budget varies for each industry
- Finance, technology, and energy firms have to invest more in cybersecurity than hospitality and healthcare firms in general.
Insights for Resource Allocation: Optimal Budget

- Asset configuration (confidential assets vs. non-confidential assets) doesn’t influence optimal budget size.

- Attack ratio largely affects the investment decision, but not always in a linear manner.
Insights for Resource Allocation: Optimal Budget

- Specific value of the optimal cybersecurity budget, however, is dependent on the value of assets that a firm maintains.

- Value of assets is measured by the cost of perfect asset protection (COPP), which a firm should develop estimates for.
Insights for Resource Allocation: Optimal Budget

- If the COPP is more than the potential total loss, the allocations by Cat I-II categories are significantly higher.

- Gordon and Loeb (2002) notes that the cybersecurity investment of a firm should not exceed 37% of the potential total loss, which is in line with our findings.
Insights for Resource Allocation: Optimal Budget

- The higher the COPP, the higher the cybersecurity budget, as long as COPP is less than twice the total potential loss.

- The optimal budget decreases with respect to potential total loss, for high COPP values.
Insights for Resource Allocation: Optimal Budget

- The optimal cybersecurity budget is relatively insensitive to the risk attitude of the firm.

- The higher the emphasis on risk reduction, the higher the value of information. Hence, information sharing is especially of importance for risk-averse firms.

- Firms should utilize a gradually increasing rate of resource usage of the cybersecurity budget within a given planning period.
  - The higher the emphasis on risk reduction, the higher this rate should be.
Insights for Resource Allocation: Investments

- Cat. I industries such as the finance and technology sectors should invest more on detective countermeasures over preventive measures (around 65% vs. 35%)

- A more even allocation of resources should be made for other industries, especially the hospitality and healthcare industries.

- Such split is not so sensitive to the risk attitude of the firm.
Insights for Resource Allocation: Value

- Ratio of COPP and ‘optimal cost’, which can be defined as a measure for the value of optimization, does not follow a linear trend.

- When COPP is the same as potential total loss, optimal cost is ~40% of COPP.

- When COPP is 5 times the potential total loss, optimal cost is ~4% of COPP.
Insights for Resource Allocation: Value

- The value of optimization is slightly higher for Cat. IV industries, i.e. hospitality and healthcare.

- As expected, value of optimization decreases as the firm places more emphasis on risk reduction.
Conclusion: Big Picture

- Modeling and optimization is a necessary component of cybersecurity.

- Such methods provide means to improve the effectiveness and efficiency of tools and policies against cyber attacks.

- Valuable models exist, but challenges are significant:
  - Measuring returns, capturing the ever-changing dynamic behavior, existence of multiple players, characterizing uncertainty and risk.

- Need more practically valid, implementable models and solutions: But, what is required to achieve these?
Thank you…

Senay Solak
solak@isenberg.umass.edu
Questions

- **GENERAL MODELS AND METHODS:**
  - What models, techniques and tools would be helpful to a given organization in the near-term? More long-term?

- **DECISION MAKING AND RISK:**
  - How should “risk” be defined, measured, and modeled for cybersecurity decision making?

- **COLLABORATIVE DECISION MAKING:**
  - Are collaborative decision making models for cybersecurity practically viable approaches within or across different industries?
  - Would there be any value in developing a system where cybersecurity decisions, such as those involving countermeasures, are made collectively? What are the challenges?

- **DATA:**
  - How can cybersecurity data be made more accessible to analysts and researchers for modeling purposes? Can some data sharing by firms be regulated / required?