Introduction to Security Economics

Tyler Moore

Tandy School of Computer Science
The University of Tulsa

Brown University Computer Science Seminar
March 8, 2017
1. What can economics tell us about cybersecurity?
   - The power of incentives
   - Market failures
   - Policy options for improving security

2. How do firms manage cybersecurity investment today?
   - In theory: risk management approach
   - In practice: results from semi-structured interviews
Outline

1. What can economics tell us about cybersecurity?
   - The power of incentives
   - Market failures
   - Policy options for improving security

2. How do firms manage cybersecurity investment today?
   - In theory: risk management approach
   - In practice: results from semi-structured interviews
Why is a computer scientist talking about economics?

- The conventional CS approach to security has failed
  1. Enumerate possible threats
  2. Define attacker capabilities
  3. Build systems to protect against these threats
- Worked for encryption algorithms, but not Internet security
Why is a computer scientist talking about economics?

- The conventional CS approach to security has failed
  1. Enumerate possible threats
  2. Define attacker capabilities
  3. Build systems to protect against these threats
- Worked for encryption algorithms, but not Internet security
- Attackers and defenders operate strategically
  - Profit-motivated adversaries break systems in unanticipated ways
  - Defenders don’t make decisions based on what will maximize security; instead they consider costs and their own interests
The power of incentives

- Systems often fail because people who could protect a system lack incentive to do so
The power of incentives

- Systems often fail because people who could protect a system lack incentive to do so.
- Example: Retail banking in the 1990s
  - US banks have long been required to pay for ATM card fraud.
  - In the UK, regulators favored banks, often made customer pay for fraud.
  - Which country suffered more ATM fraud?
The power of incentives

- Systems often fail because people who could protect a system lack incentive to do so
- Example: Retail banking in the 1990s
  - US banks have long been required to pay for ATM card fraud
  - In the UK, regulators favored banks, often made customer pay for fraud
  - Which country suffered more ATM fraud? The UK
The power of incentives

- Systems often fail because people who could protect a system lack incentive to do so
- Example: Retail banking in the 1990s
  - US banks have long been required to pay for ATM card fraud
  - In the UK, regulators favored banks, often made customer pay for fraud
  - Which country suffered more ATM fraud? The UK
  - Since US banks had to pay for disputed transactions, banks had strong incentive to invest in technology to reduce fraud
  - Since UK banks could blame customers for fraud, they lacked incentive to invest in same anti-fraud mechanisms, hence the higher fraud
The power of incentives

- Systems often fail because people who could protect a system lack incentive to do so.

- Example: Retail banking in the 1990s
  - US banks have long been required to pay for ATM card fraud.
  - In the UK, regulators favored banks, often made customers pay for fraud.
  - Which country suffered more ATM fraud? **The UK**
  - Since US banks had to pay for disputed transactions, banks had strong incentive to invest in technology to reduce fraud.
  - Since UK banks could blame customers for fraud, they lacked incentive to invest in same anti-fraud mechanisms, hence the higher fraud.

- Other examples: insecure devices in auto supply chains, private vs. public interests in critical infrastructure protection, ...
Incentives for critical infrastructure protection

Figure 2.1: Example exposure time-map with red marking systems with known exploits
Incentives for critical infrastructure protection

- Critical infrastructure operators
  - Upgrading to IP-based systems brings huge efficiency gains
  - Maintaining physical separation of networks reduces efficiency and drives up operating costs
  - Likelihood of an attack is low (based on history)
  - Cost of attack largely borne by society

Consumers
- Value reliability of service, including against attack
- Prefers low cost service
- Cannot distinguish between security investments among firms

Governments
- Value reliability of service, including against attack
- Fears political consequences of an attack, given national defense remit
- Lack of budget to fund security
- Lack of expertise to secure privately-controlled systems
Incentives for critical infrastructure protection

- Critical infrastructure operators
  + Upgrading to IP-based systems brings huge efficiency gains
    - Maintaining physical separation of networks reduces efficiency and drives up operating costs
    - Likelihood of an attack is low (based on history)
    - Cost of attack largely borne by society

- Consumers
  + Value reliability of service, including against attack
    - Prefers low cost service
    - Cannot distinguish between security investments among firms
What can economics tell us about cybersecurity?

**The power of incentives**

### Incentives for critical infrastructure protection

- **Critical infrastructure operators**
  - Upgrading to IP-based systems brings huge efficiency gains
  - Maintaining physical separation of networks reduces efficiency and drives up operating costs
  - Likelihood of an attack is low (based on history)
  - Cost of attack largely borne by society

- **Consumers**
  - Value reliability of service, including against attack
    - Prefers low cost service
    - Cannot distinguish between security investments among firms

- **Governments**
  - Value reliability of service, including against attack
  - Fears political consequences of an attack, given national defense remit
    - Lack of budget to fund security
    - Lack of expertise to secure privately-controlled systems
Incentives in critical infrastructure protection

- Absent regulation to compel behavior, stakeholders act in their own interest based on their incentives and capabilities
  - Only operators, not consumers or governments, are capable of improving security
  - So their incentives matter most!
  - On balance, they are likely to tolerate a high level of insecurity in their systems
Outline

1. What can economics tell us about cybersecurity?
   - The power of incentives
   - Market failures
   - Policy options for improving security

2. How do firms manage cybersecurity investment today?
   - In theory: risk management approach
   - In practice: results from semi-structured interviews
Market failures occur when the free-market outcome is inefficient
- Monopolies/oligopolies
- Public goods
- Information asymmetries
- Externalities

Market failures justify regulatory intervention, and inform how public policy should be designed

They help explain why private cybersecurity investment is often suboptimal
What can economics tell us about cybersecurity?

Markets with asymmetric information
Akerlof’s market for lemons

- Suppose a town has 20 similar used cars for sale
  - 10 “cherries” valued at $2,000 each
  - 10 “lemons” valued at $1,000 each
  - What is the market-clearing price?
Akerlof’s market for lemons

Suppose a town has 20 similar used cars for sale
- 10 “cherries” valued at $2,000 each
- 10 “lemons” valued at $1,000 each
What is the market-clearing price?
Answer: $1,000. Why?
- Buyers cannot determine car quality, so they refuse to pay a premium for a high-quality car
- Sellers know this, and only owners of lemons will sell for $1,000
- The market is flooded with lemons
Secure software is a market for lemons

- Vendors may believe their software is secure, but buyers have no reason to believe them
- So buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to do so
What can economics tell us about cybersecurity?

Market failures

Information asymmetries in cybersecurity markets

1. Secure software is a market for lemons
   - Vendors may believe their software is secure, but buyers have no reason to believe them
   - So buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to do so

2. Lack of robust cybersecurity incident data
   - Unless required by law, most firms choose not to disclose when they have suffered cybersecurity incidents
   - Thus firms cannot create an accurate a priori estimate of the likelihood of incidents or their cost
   - Without accurate loss measurements, defensive resources cannot be allocated properly
Consequences of asymmetric information

1. Adverse selection
   - In health insurance, adverse selection occurs when sick people are more likely to buy coverage than healthy people.
   - Difficulty of discriminating between firms with good or bad operational security practices has hampered the development of the cyber-insurance market.

2. Moral hazard
   - People may drive recklessly if fully insured with $0 deductible.
   - Often claimed that consumers engage in moral hazard due to $0 card fraud liability.
   - Cuts both ways: when regulations favor banks, they can behave recklessly in combating fraud.
What can economics tell us about cybersecurity?

Externalities
Externalities

- **Negative externality**: harm imposed on third parties as a consequence of another’s actions
- Environmental pollution is a negative externality
  - Factory produces a good and gets paid by buyer
  - Pollution caused by production is not accounted for in the transaction
- Information insecurity is a negative externality
Botnet-infected computers impose negative externalities
What can economics tell us about cybersecurity?

Market failures

How positive network externalities impact security (1)

- **Positive externality**: benefit imposed on third parties as a consequence of another’s actions
- Positive network externalities tend toward dominant platforms with big first-mover advantage
  - Platforms become more valuable as more people utilize the platform (e.g., telephone networks, operating systems, social networks)
How positive network externalities impact security (1)

- **Positive externality**: benefit imposed on third parties as a consequence of another’s actions
- Positive network externalities tend toward dominant platforms with big first-mover advantage
  - Platforms become more valuable as more people utilize the platform (e.g., telephone networks, operating systems, social networks)
- Implications for security
  1. Successful firms push products out quickly, ignore security until a dominant position is reached
  2. Dominant platforms exhibit correlated risk
What can economics tell us about cybersecurity?

How positive network externalities impact security (2)
Many technical security solutions become effective only when many people adopt them

- Introduced in 1996, S-BGP authenticates the paths routers advertise and could have prevented Pakistan telecom from shutting down YouTube
- However, S-BGP is only valuable if all ISPs switch
- Why is email still sent unauthenticated?

Security protocols which have succeeded offer immediate value to adopting firms (e.g., SSH)
Outline

1. What can economics tell us about cybersecurity?
   - The power of incentives
   - Market failures
   - Policy options for improving security

2. How do firms manage cybersecurity investment today?
   - In theory: risk management approach
   - In practice: results from semi-structured interviews
When is a policy intervention needed?

- The presence of market failures justify policy interventions
- Many traditional interventions don’t work well in the cyber context
- We discuss two interventions that have been adopted: *certification schemes* and *information disclosure*
Certification schemes for mitigating information asymmetries

- A government-led approach: Common Criteria certification
  - Sometimes useful, but may be gamed
  - Evaluation is paid for by vendor seeking approval, leading to test-shopping
Another certification scheme “fail”
Not all shoe sites are created equal

zappos.com

mbtsport-sale.com

SHOP WITH CONFIDENCE
SHOPPING ON ZAPPOS.COM IS SAFE AND SECURE. GUARANTEED!
You’ll pay nothing if unauthorized charges are made to your credit card as a result of shopping at Zappos.com.

SAFE SHOPPING GUARANTEE

All information is encrypted and transmitted without risk using a Secure Sockets Layer (SSL) protocol.

Learn How We Protect Your Personal Data »
Self-regulatory approach: website security seals

- Edelman uses data from SiteAdvisor to identify sites distributing spam and malware as “bad”
  - He then found that such “bad” websites are more likely to be TRUSTe-certified: 5.4% of TRUSTe-certified sites are “bad”, compared with 2.5% of all sites.
  - Similarly, untrustworthy sites are over-represented in paid advertisement links compared to organic search results
Edelman uses data from SiteAdvisor to identify sites distributing spam and malware as “bad”

- He then found that such “bad” websites are more likely to be TRUSTe-certified: 5.4% of TRUSTe-certified sites are “bad”, compared with 2.5% of all sites.
- Similarly, untrustworthy sites are over-represented in paid advertisement links compared to organic search results

- Poorly implemented signaling devices exhibit adverse selection

- The upshot: both private- and public-sector efforts to certify security can be gamed by criminals
Information disclosure

- Louis Brandeis: “sunlight is said to be the best of disinfectants”
- Cybersecurity incidents are often hidden from public view, so one light-touch intervention is to mandate disclosure
Data breach legislation

California Civil Code 1798.82 (2002):
“Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

Deirdre Mulligan

© 2017 Tyler Moore
What can economics tell us about cybersecurity?

Policy options for improving security

Many high-profile breaches came to light

---

[Article link]

---

© 2017 Tyler Moore
Many high-profile breaches came to light

TJX data breach: At 45.6M card numbers, it's the biggest ever

It eclipses the compromise in June 2005 at CardSystems Solutions

By Jaikumar Vijayan
March 28, 2007 12:00 PM ET

Computerworld - After more than two months of refusing to reveal the size and scope of its data breach, TJX Companies Inc. is finally offering more details about the extent of the compromise.

In filings with the U.S. Securities and Exchange Commission yesterday, the company said 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders. That number eclipses the 40 million records compromised in the mid-2005 breach at CardSystems Solutions and makes the TJX compromise the worst ever involving the loss of personal data.

In addition, personal data provided in connection with the return of merchandise without receipts by about 451,000 individuals in 2003 was also stolen. The company is in the process of contacting individuals affected by the breach, TJX said in its filings.
Effect of data breach legislation

- Most cybersecurity risk can be managed if (1) it can be measured and (2) responsibility for failures clearly assigned.
Effect of data breach legislation

- Most cybersecurity risk can be managed if (1) it can be measured and (2) responsibility for failures clearly assigned.
- Most “hard” security problems arise by failing to meet one or both of these conditions.
- Data breaches used to be a “hard” problem, but the information disclosure legislation corrected many limitations.
Outline

1. What can economics tell us about cybersecurity?
   - The power of incentives
   - Market failures
   - Policy options for improving security

2. How do firms manage cybersecurity investment today?
   - In theory: risk management approach
   - In practice: results from semi-structured interviews
Risk management terminology overview

- Risk analysis
  - identification
  - quantification
How do firms manage cybersecurity investment today?

In theory: risk management approach

Risk management terminology overview

- Risk analysis
  - identification
  - quantification

- Risk management
  - acceptance
  - mitigation
  - avoidance
  - transfer
Risk management terminology overview

- Identification
- Quantification
- Acceptance
- Mitigation
- Avoidance
- Transfer
- Validation
- Documentation
How do firms manage cybersecurity investment today?  

In theory: risk management approach

Risk management example: credit card issuers

Credit card issuers regularly manage fraud
How do firms manage cybersecurity investment today?

Risk management example: credit card issuers

Credit card issuers regularly manage fraud

1. Risk acceptance: fraud is paid from the payment fees charged to merchants
Risk management example: credit card issuers

Credit card issuers regularly manage fraud

1. Risk acceptance: fraud is paid from the payment fees charged to merchants
2. Risk mitigation: install anti-fraud technology (raises costs of security)
Risk management example: credit card issuers

Credit card issuers regularly manage fraud

1. Risk acceptance: fraud is paid from the payment fees charged to merchants
2. Risk mitigation: install anti-fraud technology (raises costs of security)
3. Risk avoidance: downgrade high-risk cardholders to debit or require online verification (leads to lost business)
How do firms manage cybersecurity investment today?

In theory: risk management approach

Risk management example: credit card issuers

Credit card issuers regularly manage fraud

1. Risk acceptance: fraud is paid from the payment fees charged to merchants
2. Risk mitigation: install anti-fraud technology (raises costs of security)
3. Risk avoidance: downgrade high-risk cardholders to debit or require online verification (leads to lost business)
4. Risk transfer: buy a cyberinsurance contract to cover excess losses
Outline

1. What can economics tell us about cybersecurity?
   - The power of incentives
   - Market failures
   - Policy options for improving security

2. How do firms manage cybersecurity investment today?
   - In theory: risk management approach
   - In practice: results from semi-structured interviews
How do firms manage cybersecurity investment today?

- Level of attention paid to cybersecurity by firms has skyrocketed
- But how do these firms manage cybersecurity risks?
  - Do they follow risk management guidelines?
  - Are quantitative metrics used to guide investment decisions?
  - Are market failures actually a barrier to investment?
- In 2015, we interviewed 40 chief information security officers (CISOs) and other executives from large organizations to better understand how decisions are made in “the real world”

Organizational support for cybersecurity

- Support from upper-level management
  - 81% said upper-level management are supportive or very supportive of cybersecurity efforts
  - 85% said that the level of support has been increasing
  - “Senior management has gotten religion about how important security is”
Organizational support for cybersecurity

- Support from upper-level management
  - 81% said upper-level management are supportive or very supportive of cybersecurity efforts
  - 85% said that the level of support has been increasing
  - “Senior management has gotten religion about how important security is”

- How have budgets changed over time?
  - 88% of participants report that their security budget has increased
  - “Honestly, I have not seen a case where I asked for money and it’s been turned down. It’s a unique time in the field because of the hype.”
  - Note: CISOs in government face steep budgetary constraints
Is all this spending going to the right places?

- 46% believe their organizations are spending the right amount on security, but only 7% think their peers are
- 64% said peers are spending too little
- 29% believe peers are spending too much in the wrong areas
Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.
Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.
- Almost nobody used quantitative metrics to guide investment decisions
  - Exception: minority translated budget requests into ROI, but still expressed skepticism that these were important in driving any decision
Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.
- Almost nobody used quantitative metrics to guide investment decisions
  - Exception: minority translated budget requests into ROI, but still expressed skepticism that these were important in driving any decision
  - One CISO stated he doesn’t want to sell security to the board by saying “there’s a 20% chance of a $20 million breach in a given 5 years”; argument doesn’t resonate
Do organizations calculate ROI to make investment decisions?

- Some firms use quantitative metrics to measure and improve operational security: counting # unpatched machines, # malware infections remediated, etc.
- Almost nobody used quantitative metrics to guide investment decisions
  - Exception: minority translated budget requests into ROI, but still expressed skepticism that these were important in driving any decision
  - One CISO stated he doesn’t want to sell security to the board by saying “there’s a 20% chance of a $20 million breach in a given 5 years”; argument doesn’t resonate
  - Healthcare CISO: “in security, ROI is a fallacy. We are a cost center”
The rise of frameworks

- Few CISOs rely on quantitative risk calculations to guide investment decisions
  - Quantitative investment metrics encouraged by risk management approaches can be difficult to calculate
  - Often depend on figures that are not readily available (e.g., probability of loss, loss amount)
The rise of frameworks

- Few CISOs rely on quantitative risk calculations to guide investment decisions
  - Quantitative investment metrics encouraged by risk management approaches can be difficult to calculate
  - Often depend on figures that are not readily available (e.g., probability of loss, loss amount)
- Frameworks emphasize the process of managing cybersecurity without explicit regard to loss, likelihood of attack
How do firms manage cybersecurity investment today?

In practice: results from semi-structured interviews

A simple early framework: SANS 20 Critical Controls

Critical Security Controls

Version 5

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

Source: https://www.sans.org/critical-security-controls/controls
How do firms manage cybersecurity investment today?

In practice: results from semi-structured interviews

NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Function</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>

- Organized around 5 core functions: identify, protect, detect, respond, recover
- Each function has categories and subcategories
- Voluntary to adopt
Frameworks: good or bad?

- Frameworks are a powerful communications tool
  - CISO: frameworks make it “fairly easy to discuss and to convey to different layers of leadership”
  - CISO: frameworks clearly communicate risk rating to senior management and how much investment is needed to bring rating down to acceptable level
Frameworks: good or bad?

- Frameworks are a powerful communications tool
  - CISO: frameworks make it “fairly easy to discuss and to convey to different layers of leadership”
  - CISO: frameworks clearly communicate risk rating to senior management and how much investment is needed to bring rating down to acceptable level

- Security frameworks: the new checkbox?
  - Frameworks stimulate a broader, systematic examination of risk
  - While frameworks look more “scientific”, they aren’t
  - By focusing on process, rather than secure outcome, it is not clear how much the frameworks actually improve security
How do firms manage cybersecurity investment today?

Markets with asymmetric information
Do CISOs view security as a market for lemons?

- We asked if organizations feel they have adequate information to manage risk and prioritize threats
  - 45% said yes; most “no’s” arise from fear of “unknown unknown”
  - CISOs in finance and energy sector regularly briefed on threats by government colleagues
Do CISOs view security as a market for lemons?

- We asked if organizations feel they have adequate information to manage risk and prioritize threats
  - 45% said yes; most “no’s” arise from fear of “unknown unknown”
  - CISOs in finance and energy sector regularly briefed on threats by government colleagues
- 85% of CISOs feel they have enough information to select the right security controls
Do CISOs view security as a market for lemons?

- We asked if organizations feel they have adequate information to manage risk and prioritize threats
  - 45% said yes; most “no’s” arise from fear of “unknown unknown”
  - CISOs in finance and energy sector regularly briefed on threats by government colleagues
- 85% of CISOs feel they have enough information to select the right security controls
- Information sharing groups (sectoral and regional) seen as highly valuable in mitigating information asymmetries
- Open research question: studying whether these perceptions match reality

© 2017 Tyler Moore
Pay attention to the often conflicting incentives to protect cybersecurity

The presence of market failures, notably information asymmetries and externalities, indicate the need for a strong policy role in promoting cybersecurity

Firms are investing more in cybersecurity than ever before

It remains to be seen if these investments will produce more secure outcomes

For more information, email tyler-moore@utulsa.edu or visit http://tylermoore.ens.utulsa.edu