Security Economics Knowledge Guide

Tyler Moore

The University of Tulsa (tyler-moore@utulsa.edu)

contact@cybok.org
www.cybok.org

CyBOK

The CyBOK project would like to understand how CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.

Outline

1. Security Failures
2. Measurement
3. Firm-Level Solutions
4. Market-Level Solutions

Outline

1. **Security Failures**
2. Measurement
3. Firm-Level Solutions
4. Market-Level Solutions

The power of incentives

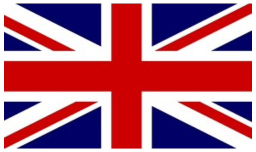
Systems often **fail** because people who could protect a system *lack incentive* to do so

Example: Retail banking in 1990s

USA

Banks forced to pay for ATM card fraud

UK



Regulators favored banks, often making customer pay for fraud

- Who suffered more 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

Example: industrial control systems

Global Exposure Surface Timeline

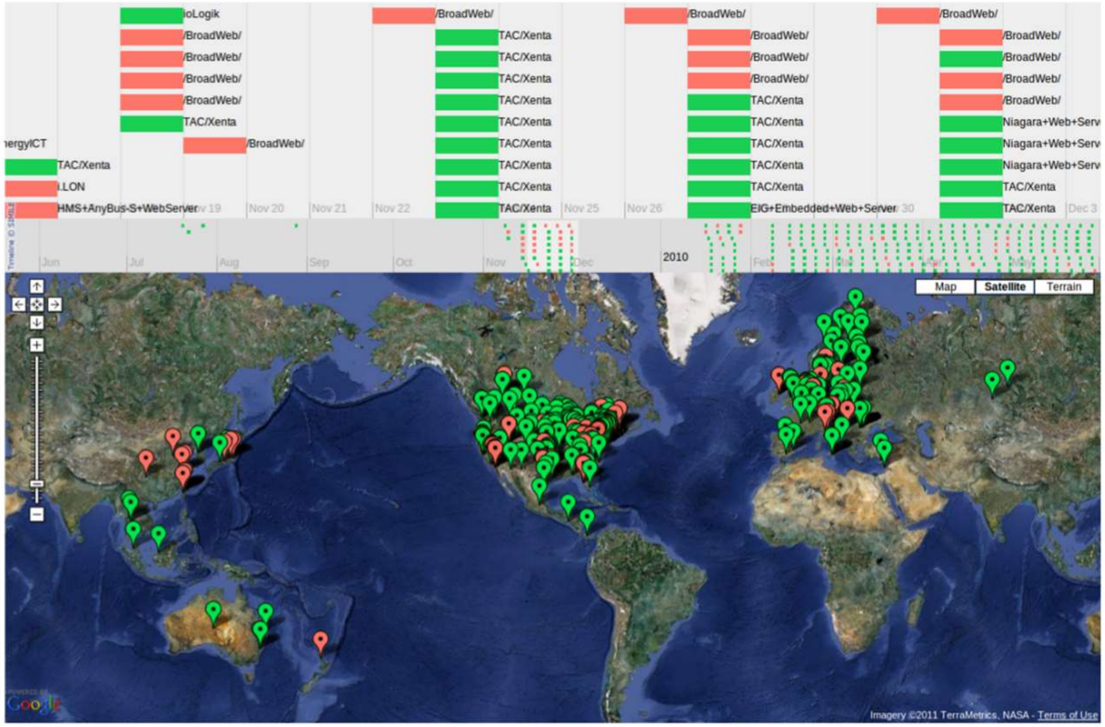


Figure 2.1: Example exposure time-map with red marking systems with known exploits

Stakeholder analysis of incentives

- Critical infrastructure operators
  - ✚ Vulnerable systems threaten service availability
  - – 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
  - – Prefer low cost of service
  - – Cannot distinguish between security investment among firms

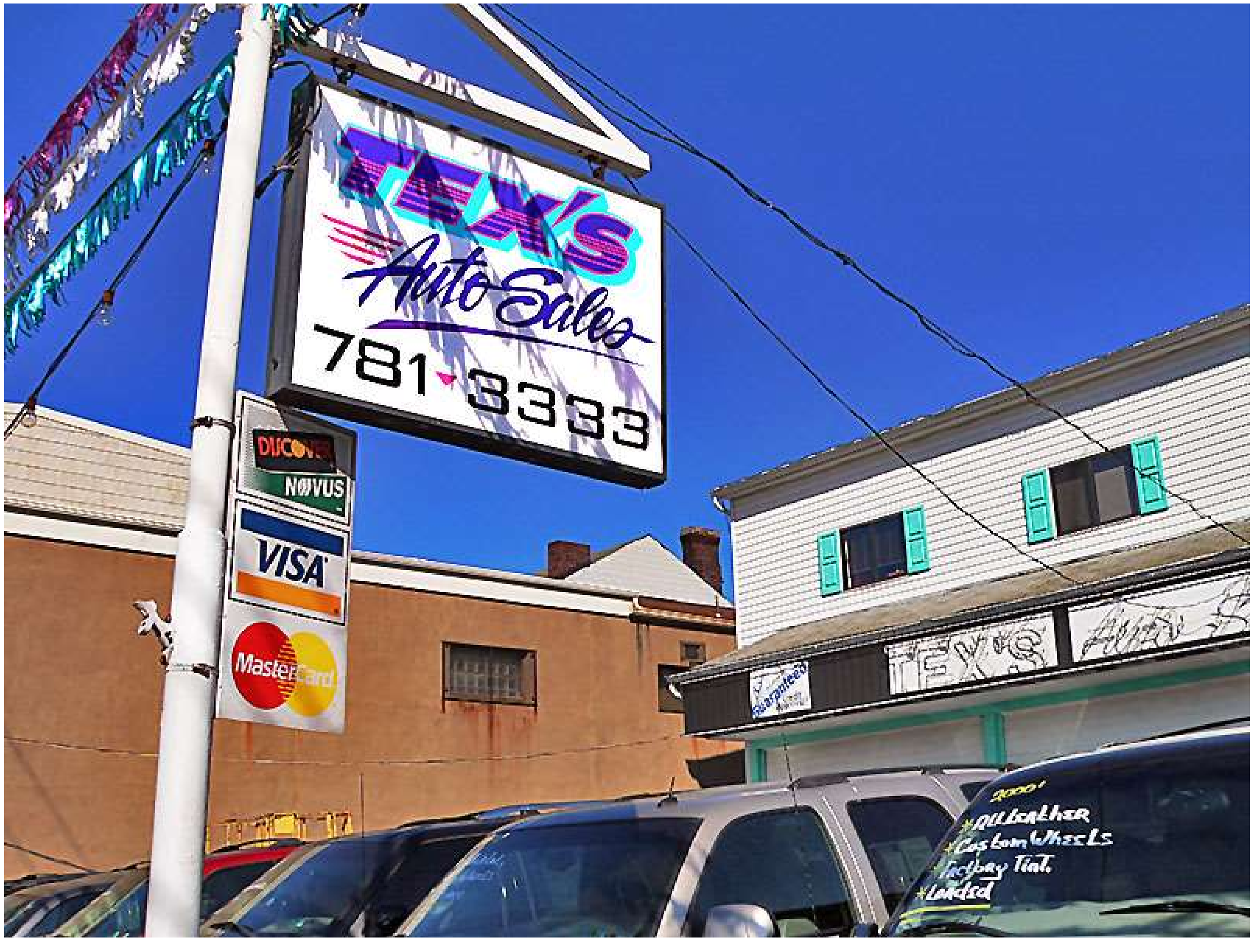
Stakeholder analysis of incentives

- Governments
  - +Value reliability of service, including against attack
  - +Fears political consequences of attack, given national defense remit
  - –Lack of budget to fund security
  - –Lack of expertise to secure privately-controlled systems

Stakeholder analysis of incentives

- 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

Markets with asymmetric information



Akerlof’s market for lemons

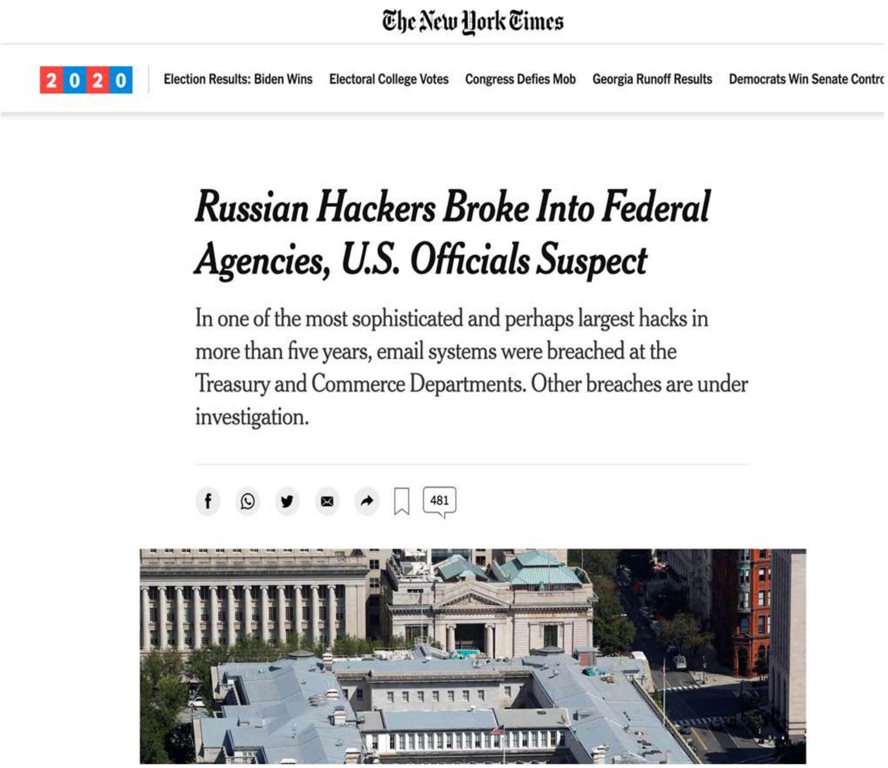
CyBOK

- Suppose a town has 20 similar used cars for sale
  - –10 “cherries” valued at $20,000 each
  - –10 “lemons” valued at $10,000 each
- What is the market-clearing price?
  - –Answer: $10,000. 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 $10,000. The market is flooded with lemons

Information asymmetries in cybersecurity markets

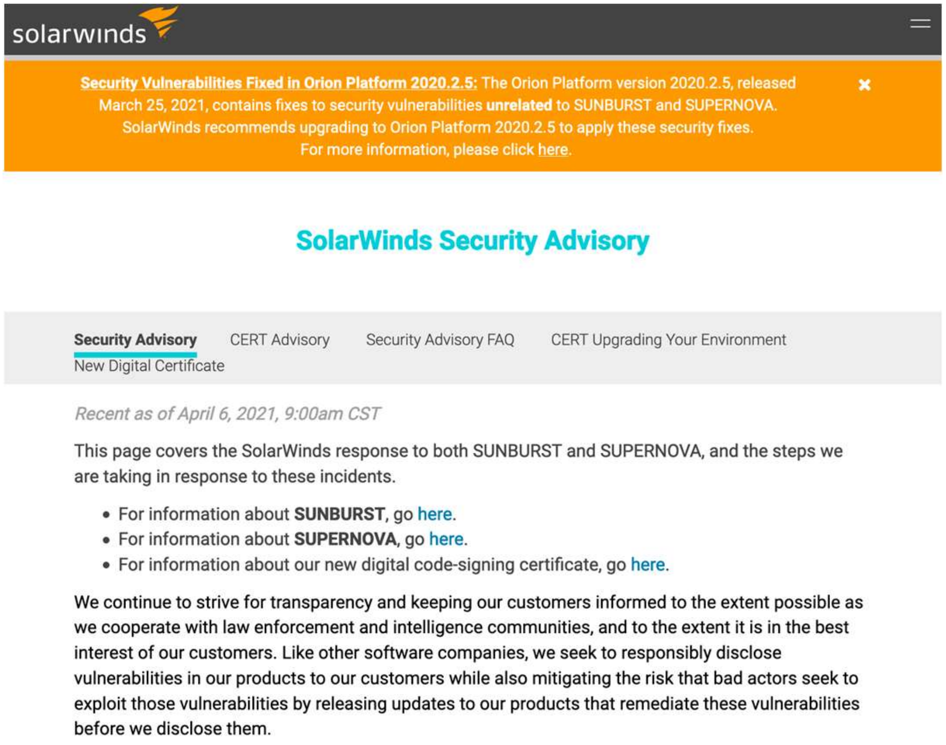
1. **Secure software is a market for lemons**
   - Vendors may believe their software is secure, but buyers have no reason to believe them
   - So buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to do so
2. **Lack of robust cybersecurity incident data**
   -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

Information asymmetries and the SolarWinds breach



Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect

In one of the most sophisticated and perhaps largest hacks in more than five years, email systems were breached at the Treasury and Commerce Departments. Other breaches are under investigation.



Security Vulnerabilities Fixed in Orion Platform 2020.2.5: The Orion Platform version 2020.2.5, released March 25, 2021, contains fixes to security vulnerabilities **unrelated** to SUNBURST and SUPERNOVA. SolarWinds recommends upgrading to Orion Platform 2020.2.5 to apply these security fixes. For more information, please click here.

SolarWinds Security Advisory

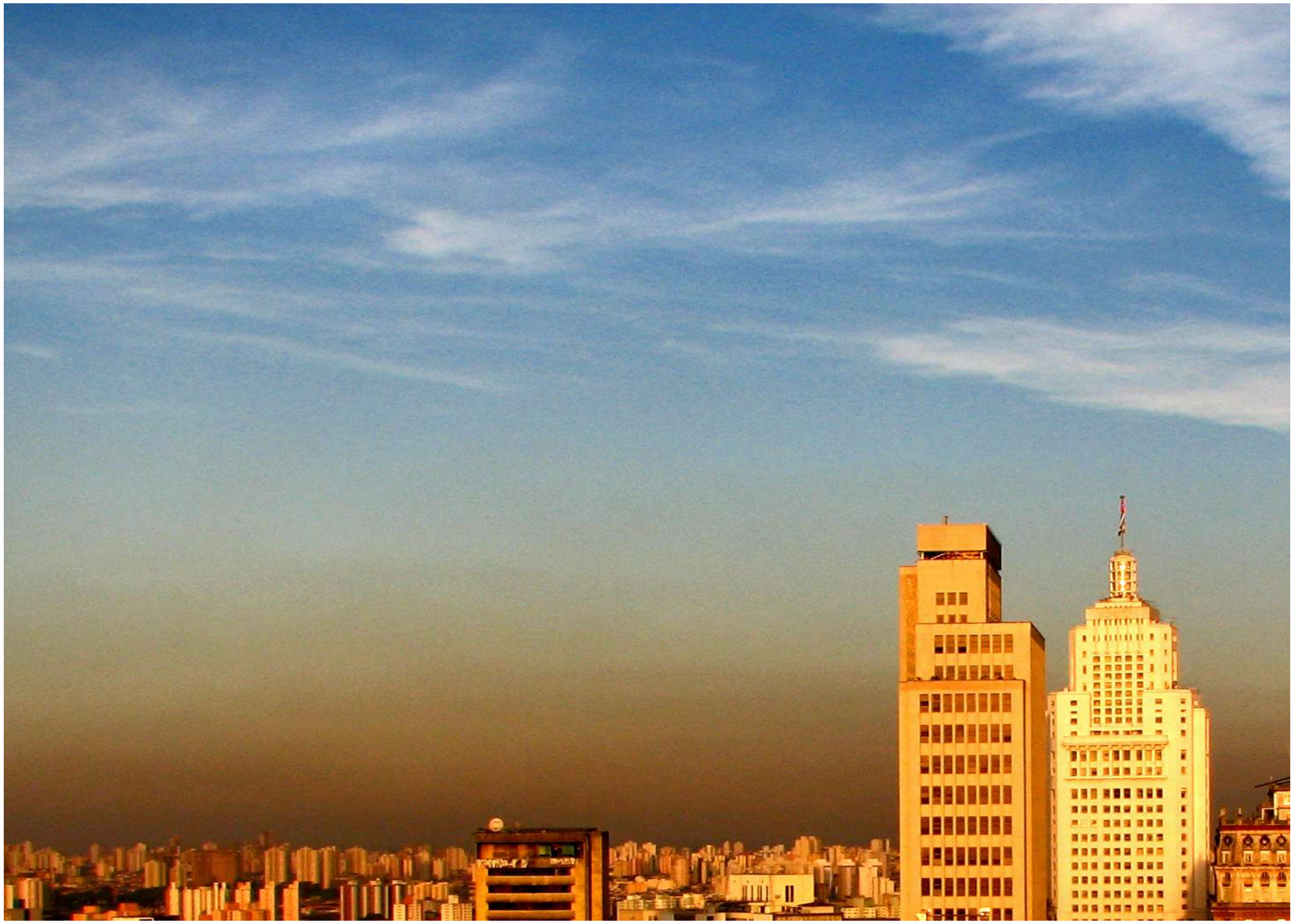
Recent as of April 6, 2021, 9:00am CST

This page covers the SolarWinds response to both SUNBURST and SUPERNOVA, and the steps we are taking in response to these incidents.

- For information about **SUNBURST**, go here.
- For information about **SUPERNOVA**, go here.
- For information about our new digital code-signing certificate, go here.

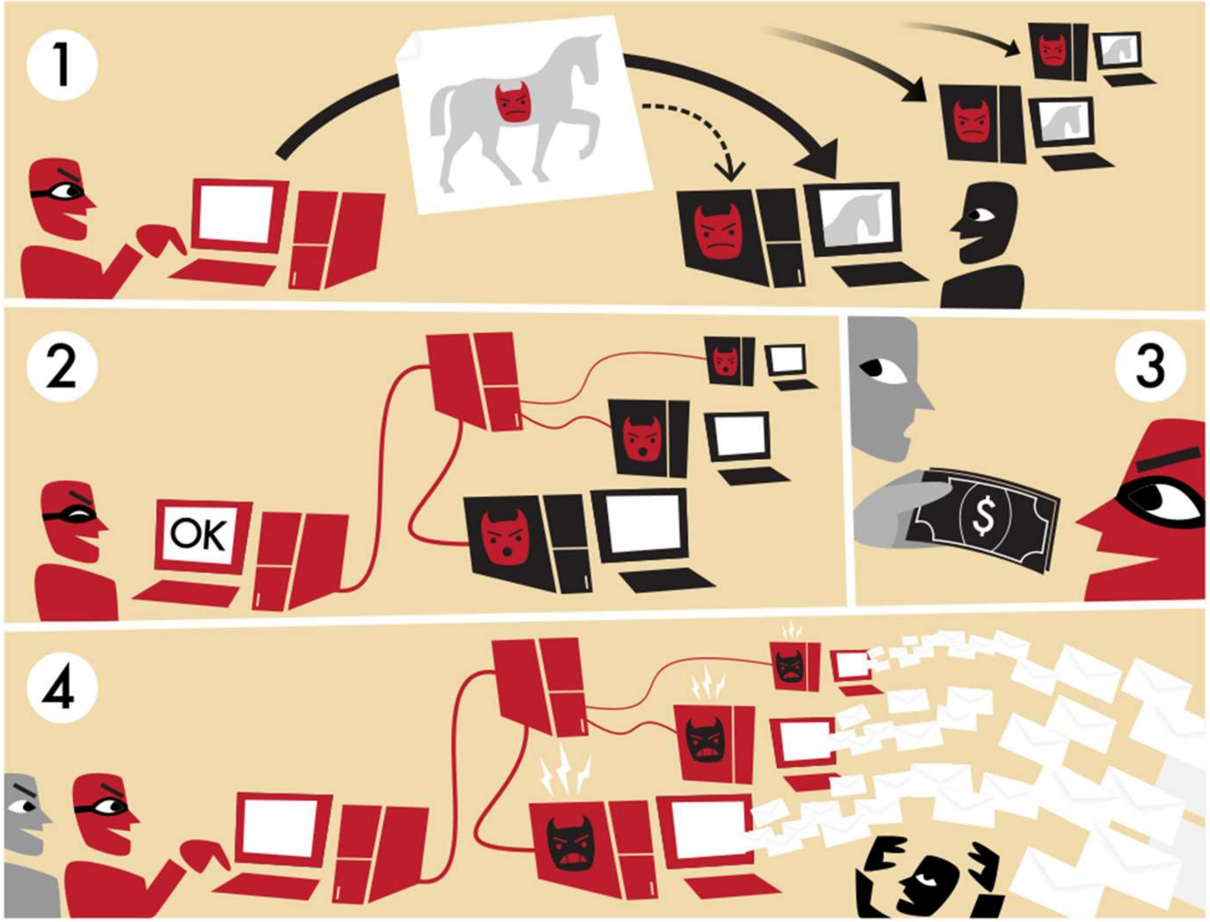
We continue to strive for transparency and keeping our customers informed to the extent possible as we cooperate with law enforcement and intelligence communities, and to the extent it is in the best interest of our customers. Like other software companies, we seek to responsibly disclose vulnerabilities in our products to our customers while also mitigating the risk that bad actors seek to exploit those vulnerabilities by releasing updates to our products that remediate these vulnerabilities before we disclose them.

Negative externality: pollution

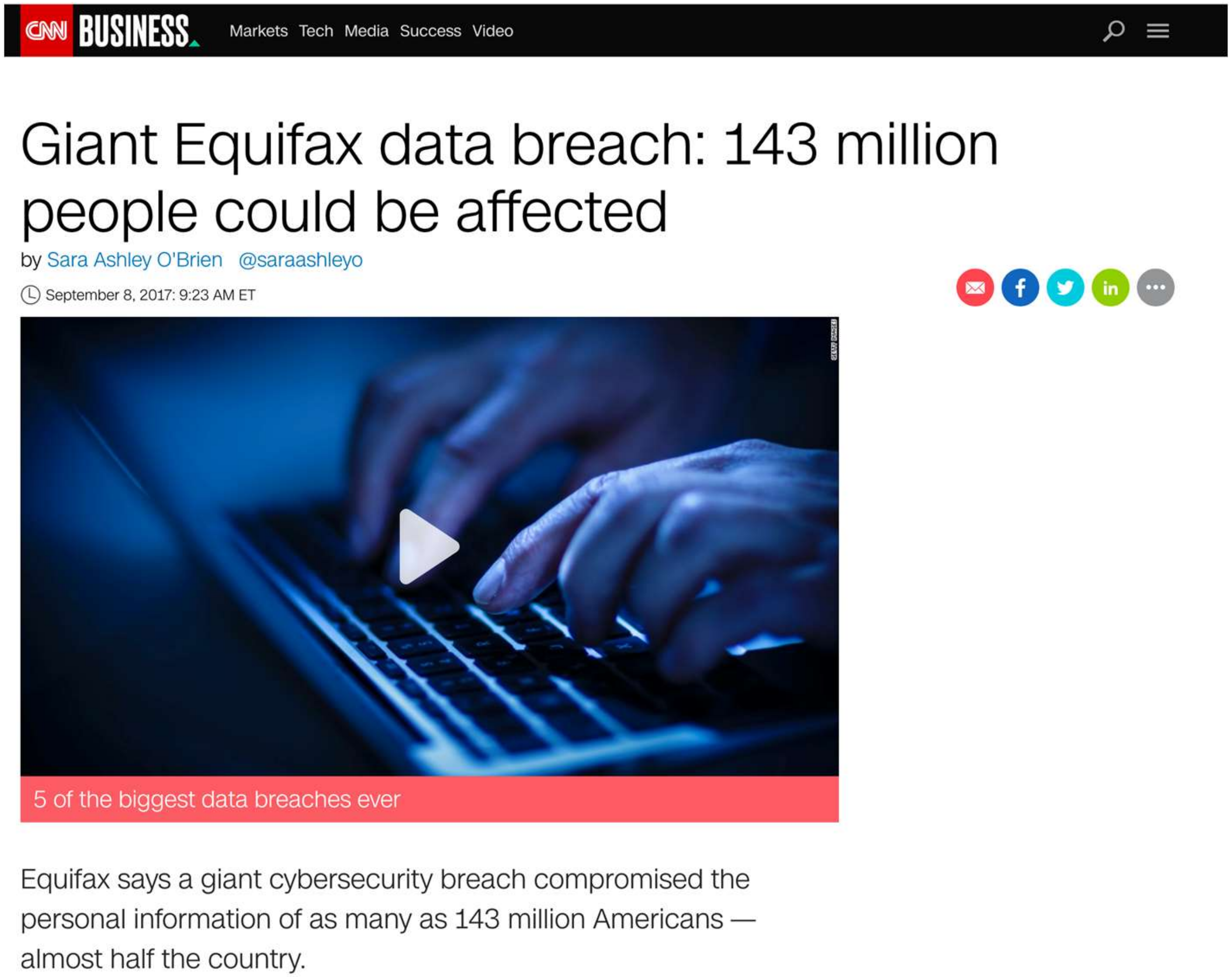


Negative externality: botnets

CyBOK



Negative externality: Equifax data breach



Giant Equifax data breach: 143 million people could be affected

by Sara Ashley O'Brien @saraashleyo

September 8, 2017: 9:23 AM ET

5 of the biggest data breaches ever

Equifax says a giant cybersecurity breach compromised the personal information of as many as 143 million Americans — almost half the country.

Negative externality: Equifax data breach

CyBOK

Positive network externalities

- **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

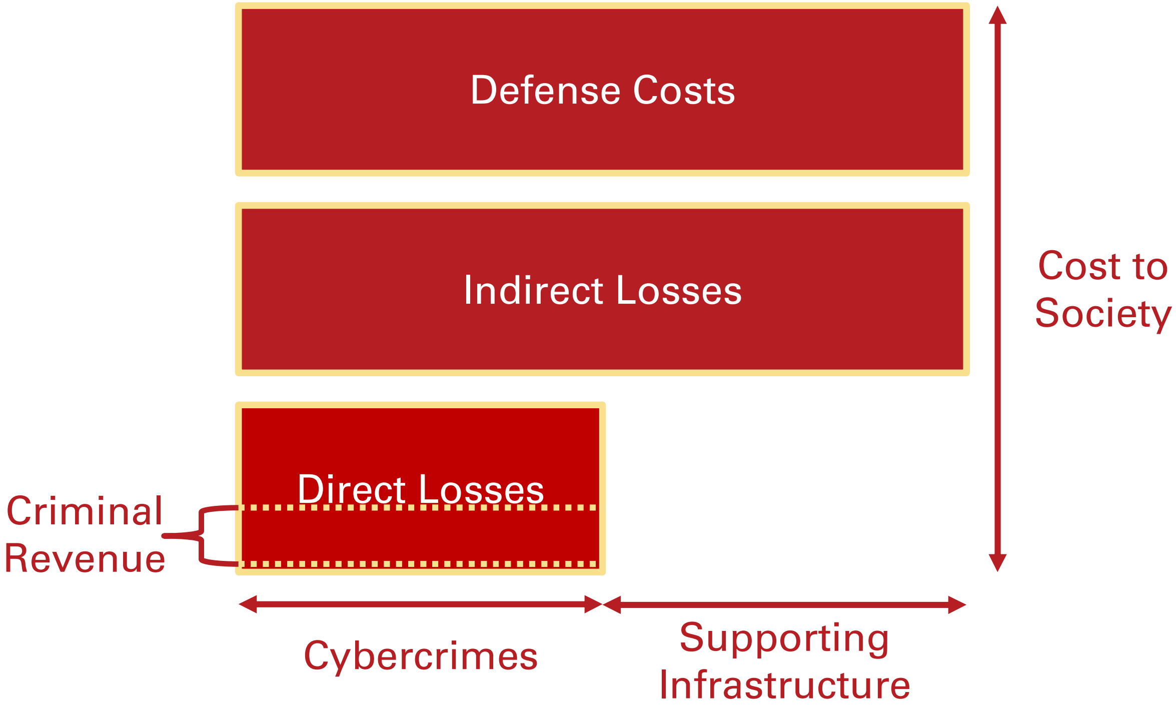
Implications of externalities

- Both positive and negative externalities are bad from an economic perspective
- Whenever you have a positive externality, you tend to have **less of the good** than you would like
- Whereas, when you have a negative externality you end up with **more of the bad** thing than you'd like from a social perspective

Outline

1. Security Failures
2. **Measurement**
3. Firm-Level Solutions
4. Market-Level Solutions

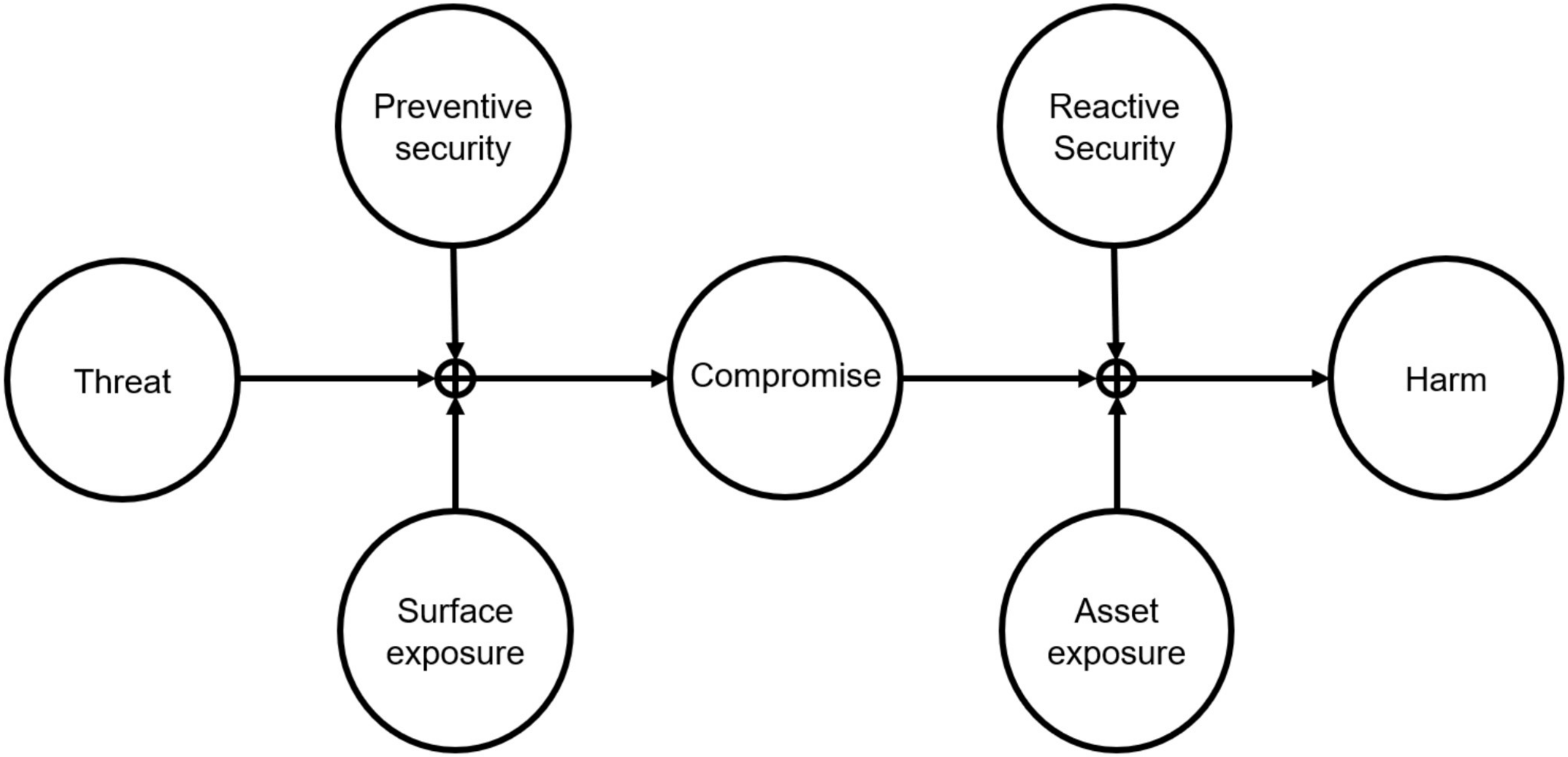
Decomposing the costs of cybercrime



Definitions for cost categories

1. **Criminal revenue**: gross receipts from a crime
2. **Direct losses**: losses, damage, or other suffering felt by the victim as a consequence of a cybercrime
3. **Indirect losses**: losses and opportunity costs imposed on society because a certain cybercrime is carried out
4. **Defense costs**: cost of prevention efforts

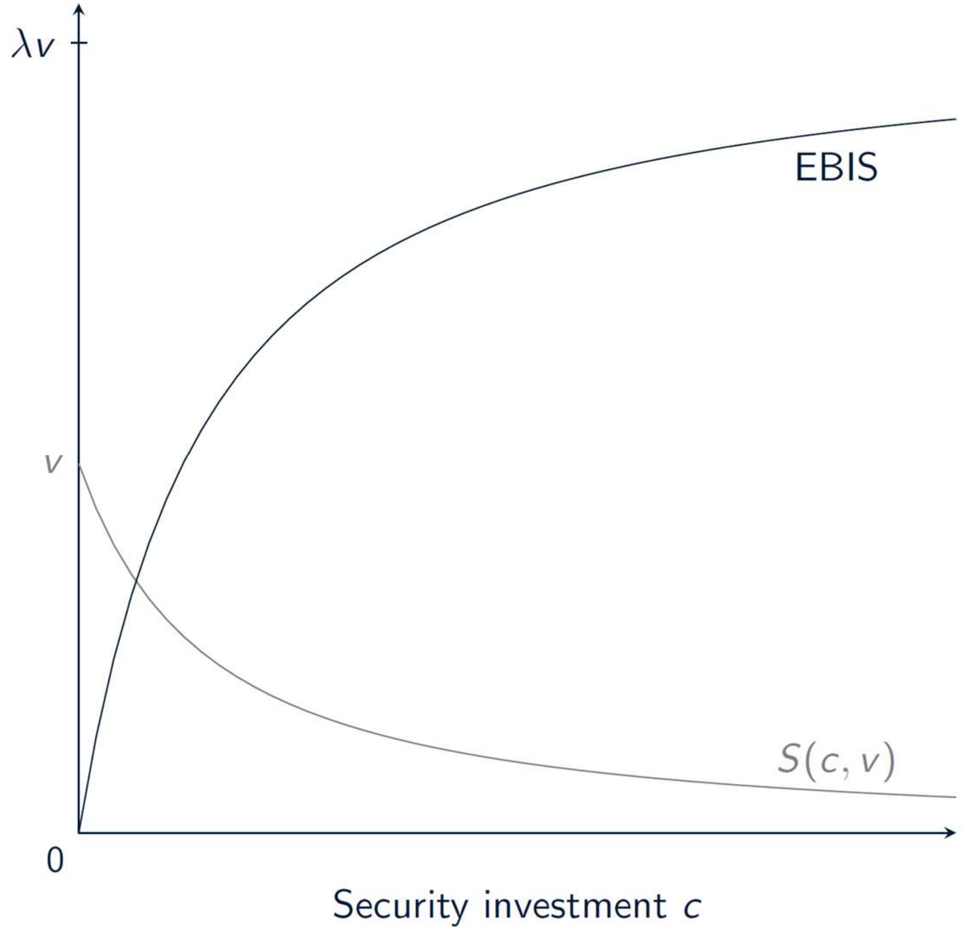
Measuring security effectiveness



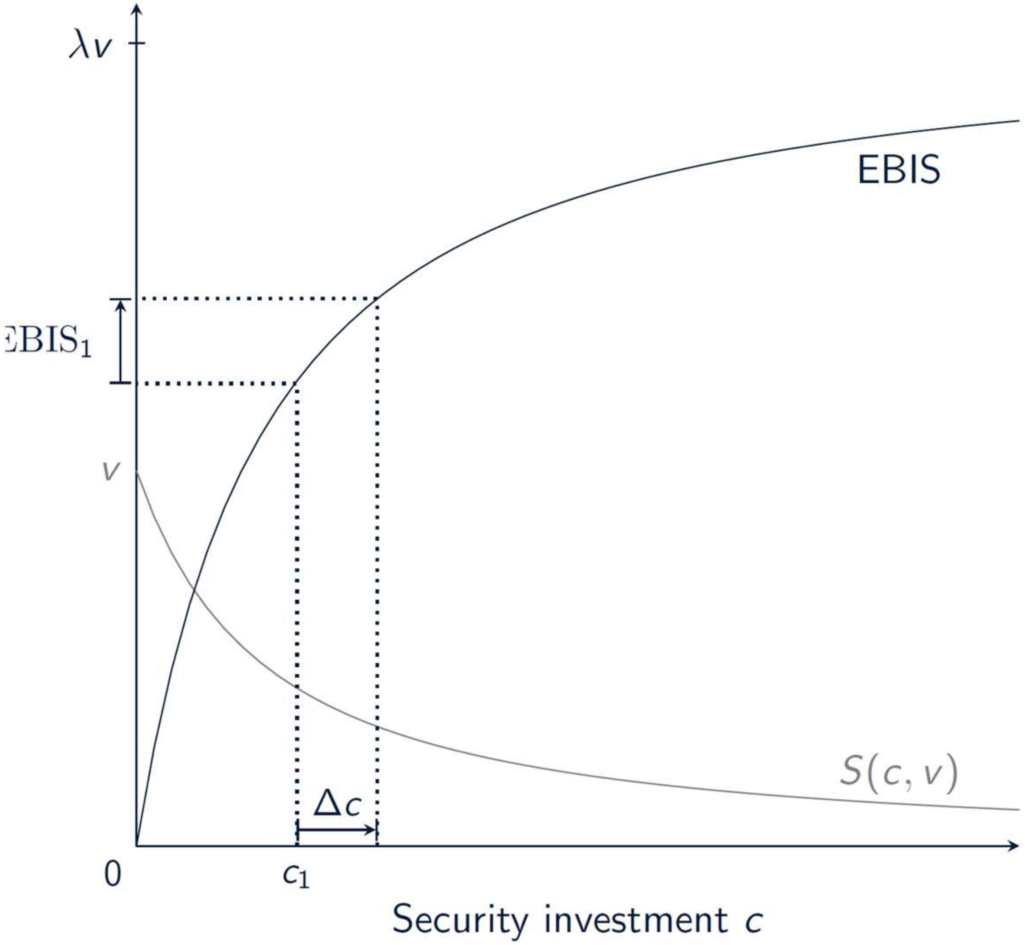
Outline

1. Security Failures
2. Measurement
3. **Firm-Level Solutions**
4. Market-Level Solutions

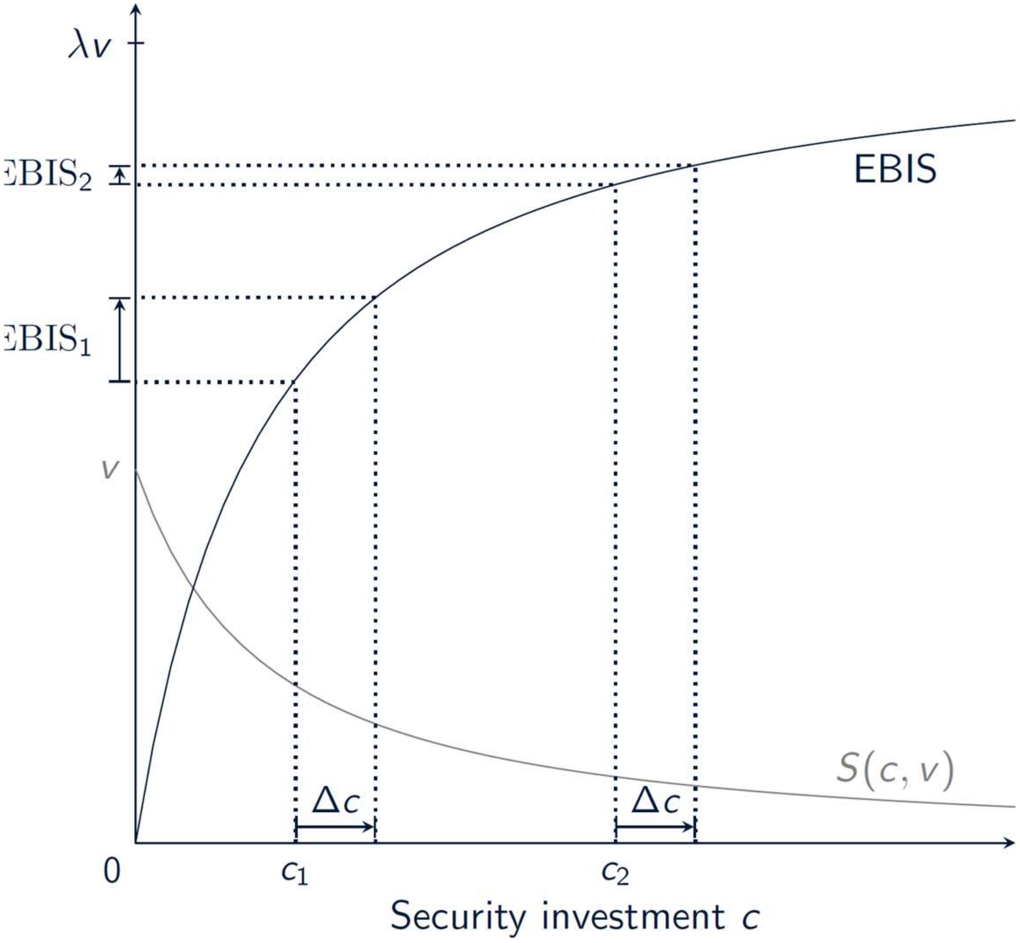
Decreasing marginal returns to security investment



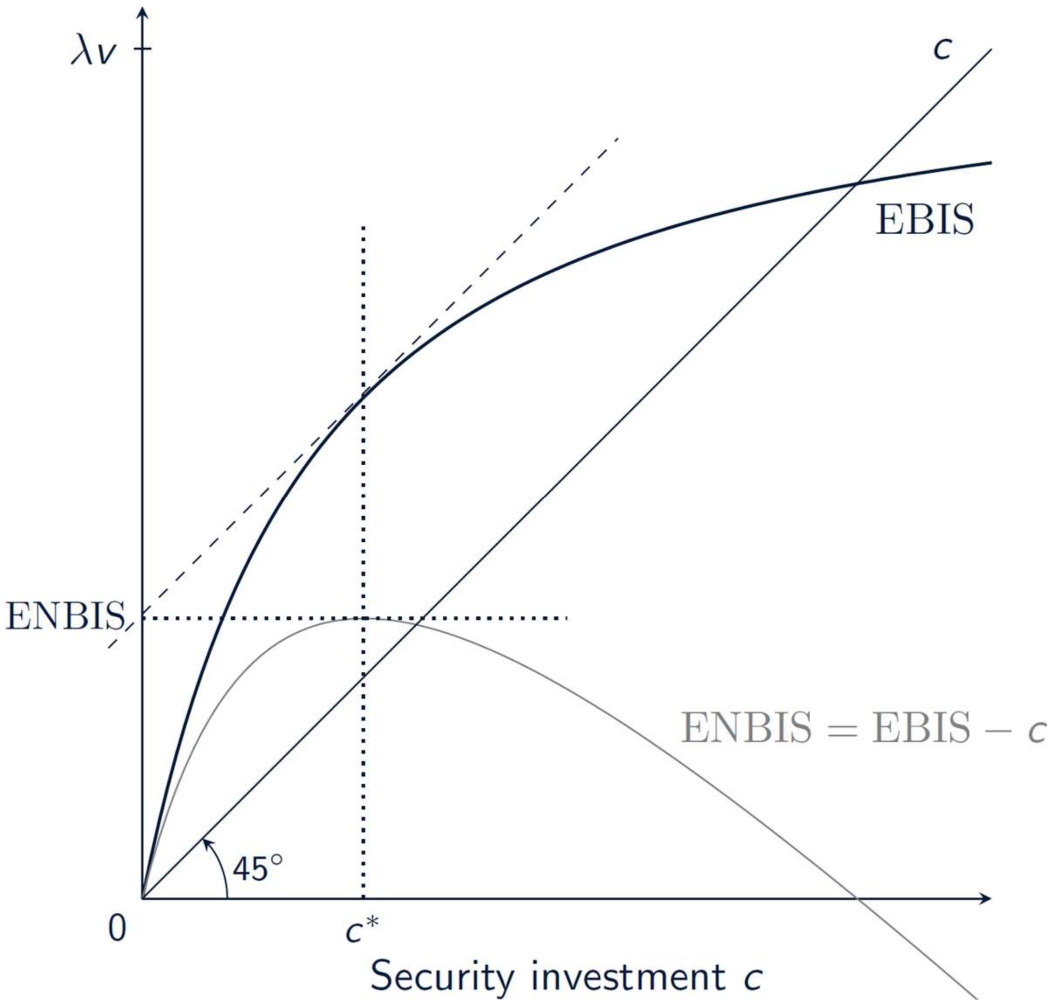
Decreasing marginal returns to security investment



Decreasing marginal returns to security investment



Gordon-Loeb model of security investment



Security investment frameworks

- Quantitative investment metrics 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

Outline

1. Security Failures
2. Measurement
3. Firm-Level Solutions
4. **Market-Level Solutions**

Ex ante safety regulation

When is safety regulation warranted?

When the potential **harm is large** and **remedies are costly**

When it's better to avoid the harm in the first place

Ex ante safety regulation

- Advantages
  - Potentially prevent bad outcome before it happens
  - Establishes floor for minimum acceptable practice
- Disadvantages
  - Risk of race to the bottom for standards
  - Politically difficult to implement broadly
  - Risk of regulatory capture
  - Adaptability hard to achieve in practice

Ex post liability

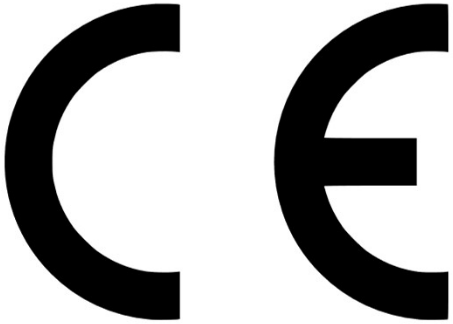
- Instead of regulating behavior up front, another option is to assign liability for bad outcomes
- Assign liability to **least cost avoider**: party to a transaction who incurs lowest cost to avoid harm
- Done well, assigning liability can deal with
  - **Information asymmetries**: assign liability to the party with best information
  - **Externalities**: can be internalized to party assigned liability

What to do about software vulnerabilities?

- Evidence indicates that software developers often do not do enough to avoid introducing vulnerabilities to code
- **Software liability** places the responsibility for vulnerabilities on authors of software
- Advantages
  - Software makers are least cost avoiders
  - Incentivizes investment in secure dev practices
- Disadvantages
  - Bug-free code is impossible
  - Trade-off between innovation and safety
  - Impact on open-source development

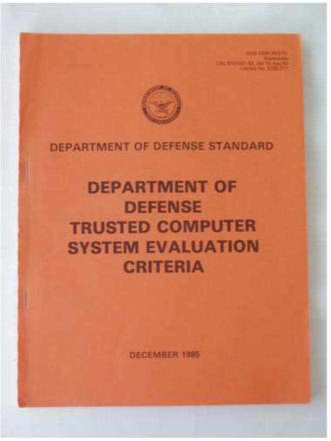
Certifying products

- Can remedy information asymmetries
- Certification enables non-experts to verify product security approved by experts



Certification schemes for mitigating information asymmetries

- Common Criteria certification
  - –Can be useful, but also gamed
  - –Evaluation is paid for by vendor seeking approval, leading to test-shopping



DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

DECEMBER 1985

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
- Poorly implemented signaling devices exhibit adverse selection
- The upshot: both private- and public-sector efforts to certify security can be gamed by criminals

Certifying processes

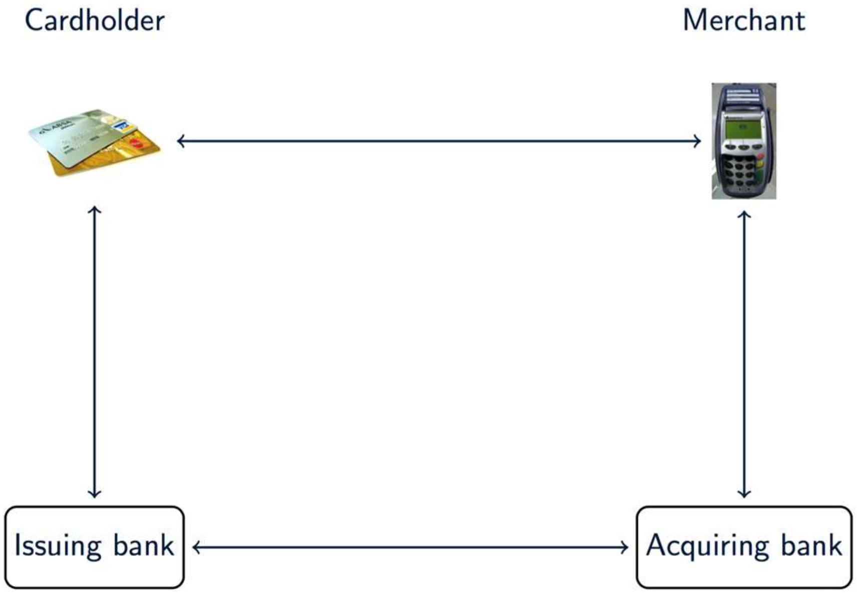
- Can remedy information asymmetries
- Supply chain security often depends critically on the security of suppliers
- How can you be assured that the business processes used by others are secure?

ISO 27001

- International standard for managing cybersecurity
- Provides a way to signal security proficiency to prospective customers

Payment Card Industry Data Security Standard (PCI DSS)

- Payment card networks developed rules for merchants to protect cardholder data

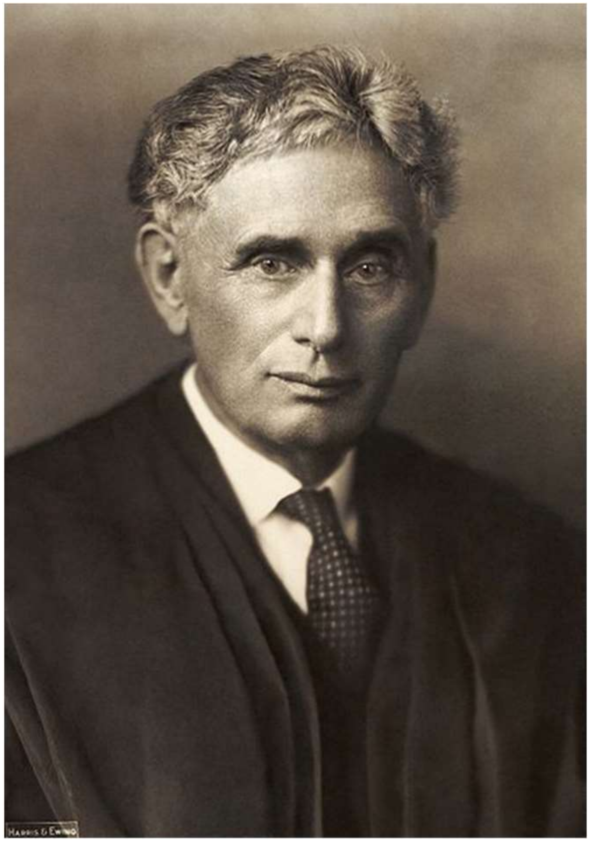


When certified processes fail

- PCI compliance widespread and growing
  - –Merchants are fined for non-compliance
  - –Most large merchants are PCI-compliant
- Many big breaches happened to PCI-compliant merchants
- Breached companies can be found non-compliant retroactively

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



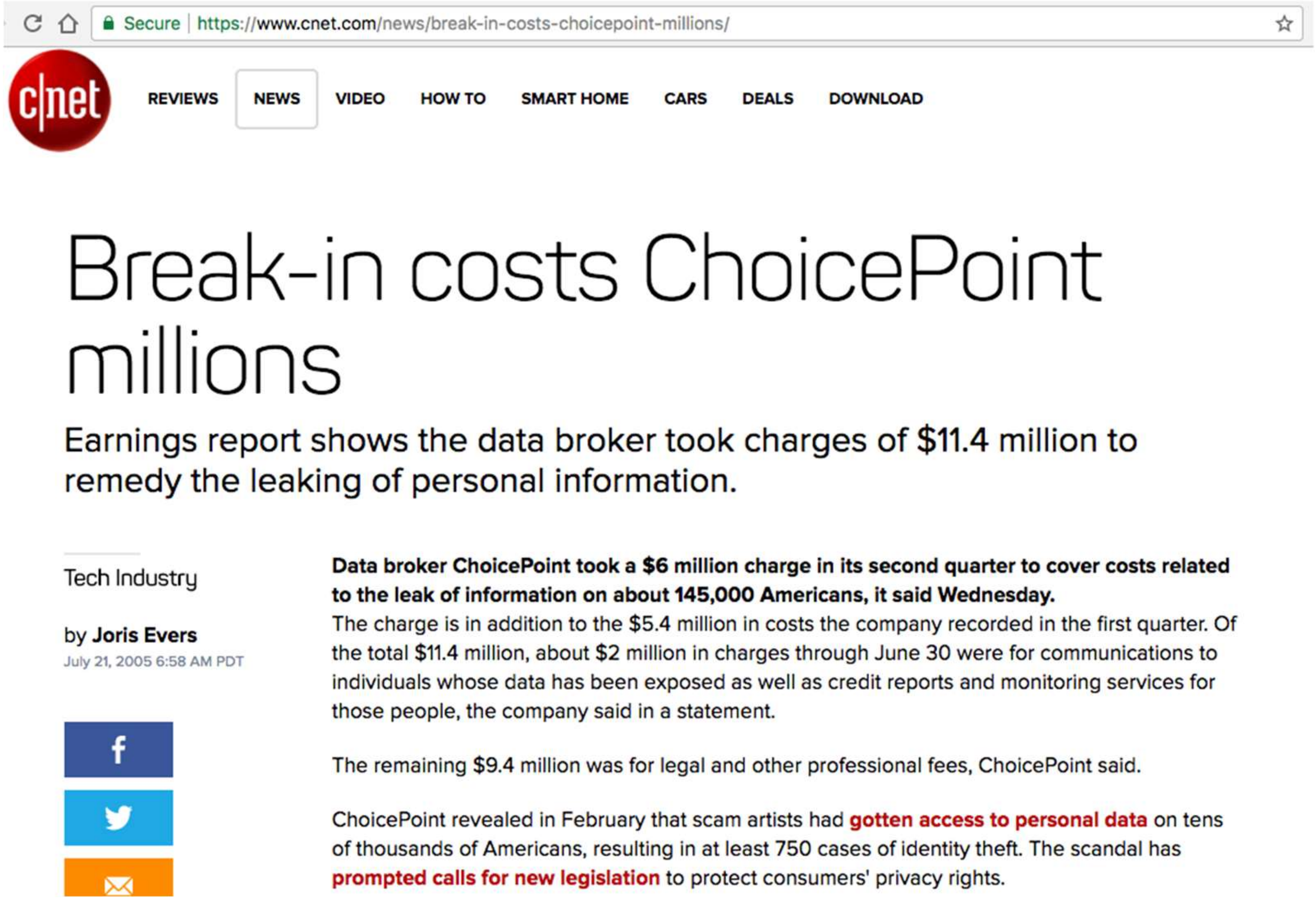
Data breach notification

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

Many high-profile breaches came to light


Secure
https://www.cnet.com/news/break-in-costs-choicepoint-millions/
c|net
REVIEWS
NEWS
VIDEO
HOW TO
SMART HOME
CARS
DEALS
DOWNLOAD

Break-in costs ChoicePoint millions

Earnings report shows the data broker took charges of $11.4 million to remedy the leaking of personal information.

Tech Industry

by **Joris Evers**
July 21, 2005 6:58 AM PDT

Data broker ChoicePoint took a $6 million charge in its second quarter to cover costs related to the leak of information on about 145,000 Americans, it said Wednesday.
The charge is in addition to the $5.4 million in costs the company recorded in the first quarter. Of the total $11.4 million, about $2 million in charges through June 30 were for communications to individuals whose data has been exposed as well as credit reports and monitoring services for those people, the company said in a statement.

The remaining $9.4 million was for legal and other professional fees, ChoicePoint said.

ChoicePoint revealed in February that scam artists had **gotten access to personal data** on tens of thousands of Americans, resulting in at least 750 cases of identity theft. The scandal has **prompted calls for new legislation** to protect consumers' privacy rights.

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
- It is no coincidence that the most mature market for cyber-insurance coverage is insuring against direct losses associated with data breaches

Where else in cybersecurity is sunlight needed?

1. Financial fraud figures
2. Cyber espionage incidents
3. Control systems incidents
4. Consistent collection of cybercrime losses

Where else do we see information disclosure in cybersecurity?

- US Securities and Exchange Commission requires publicly traded firms to disclose all “material” cyber incidents
- Software Bill of Materials (SBOM)

Recap of what economics offers cybersecurity

- Means of understanding strategic behavior (for attackers and defenders)
- The presence of market failures, notably information asymmetries and externalities, indicate the need for a strong policy role in promoting cybersecurity
- Makes information security empirically grounded
- Suggests policies to deploy technology better

CyBOK