CyBOK

The Cyber Security Body Of Knowledge

Security Economics Knowledge Guide

Tyler Moore

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

contact@cybok.org

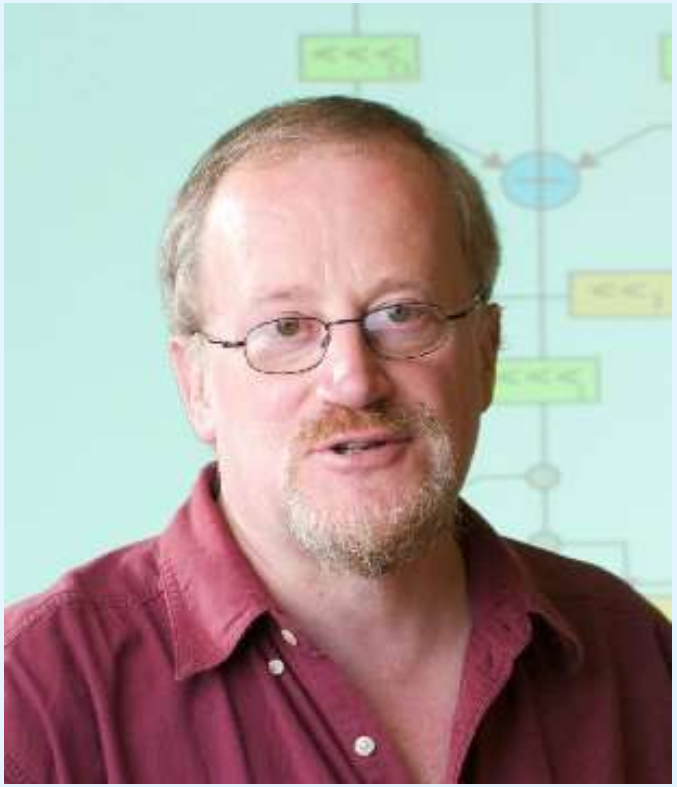
www.cybok.org

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

In Memoriam:
Prof Ross J Anderson FRS, FREng (1956-2024)



https://weis.utdallas.edu/in-memoria/

Outline

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

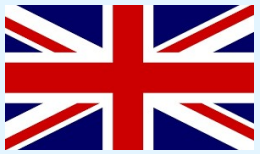
The power of incentives

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

Markets with asymmetric information

Akerlof's market for lemons

- 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

The New York Times

2020 Election Results: Biden Wins | Electoral College Votes | Congress Defies Mob | Georgia Runoff Results | Democrats Win Senate Contr

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.

481

solarwinds

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

Security Advisory | CERT Advisory | Security Advisory FAQ | CERT Upgrading Your Environment | New Digital Certificate

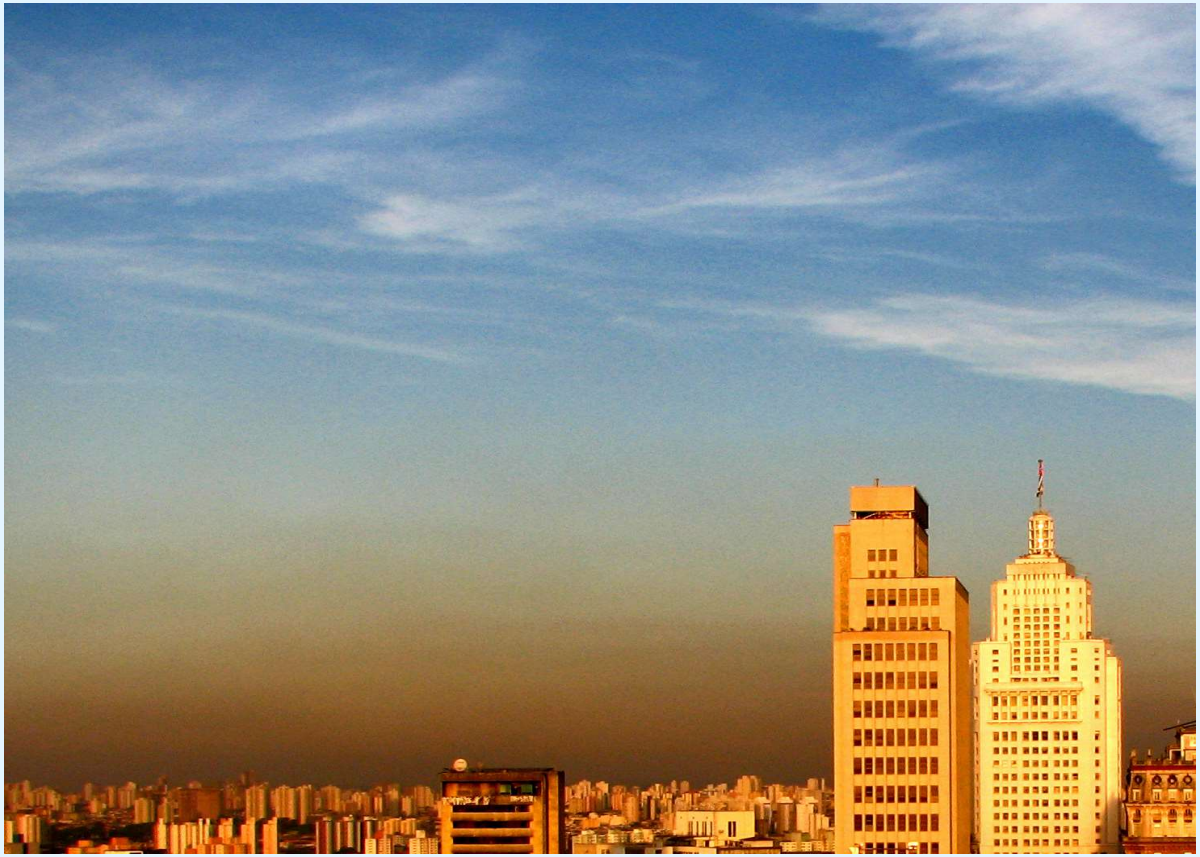
Recent as of April 6, 2021, 9:00am CST

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

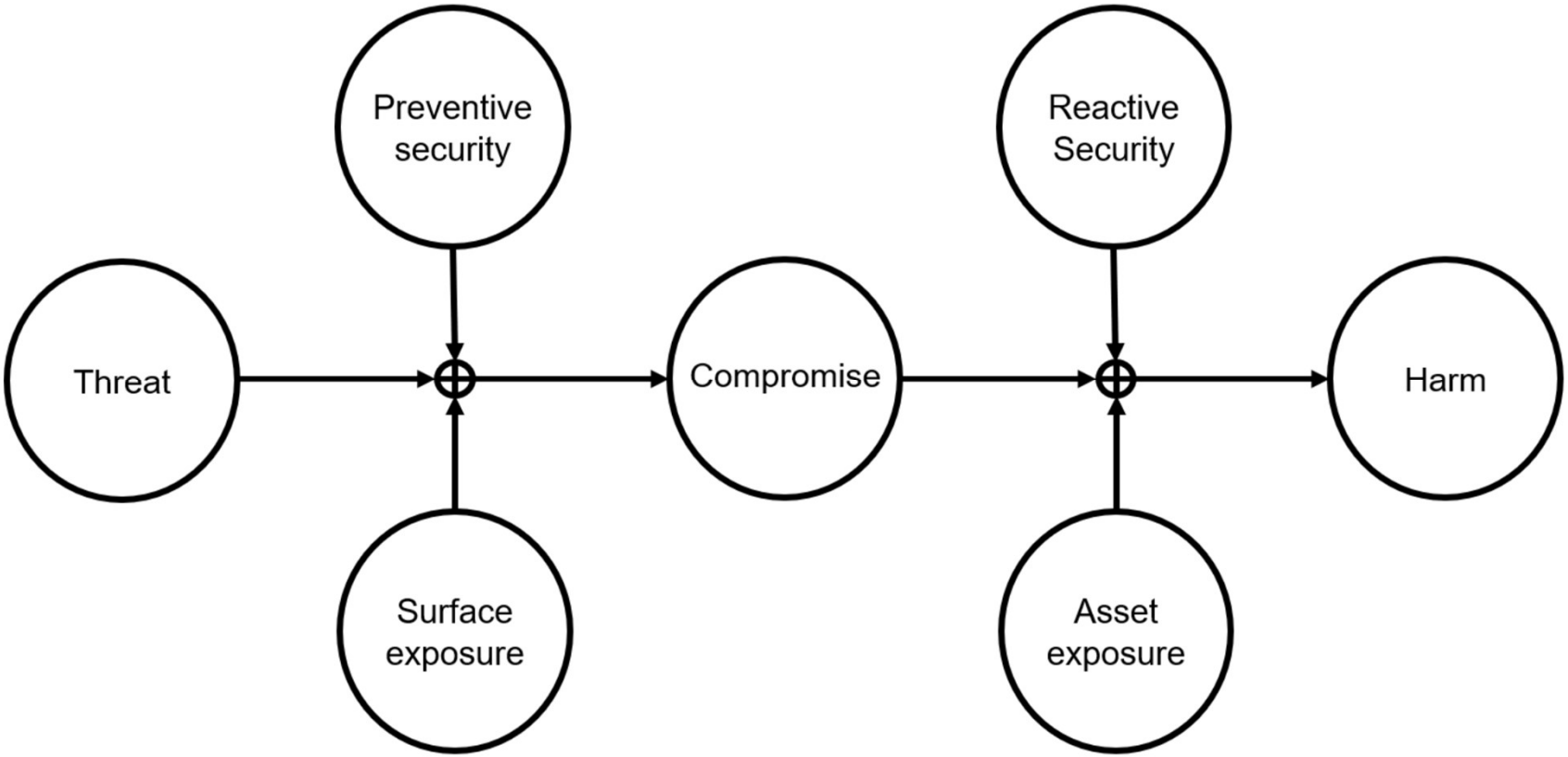


Negative externality: botnets

Outline

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

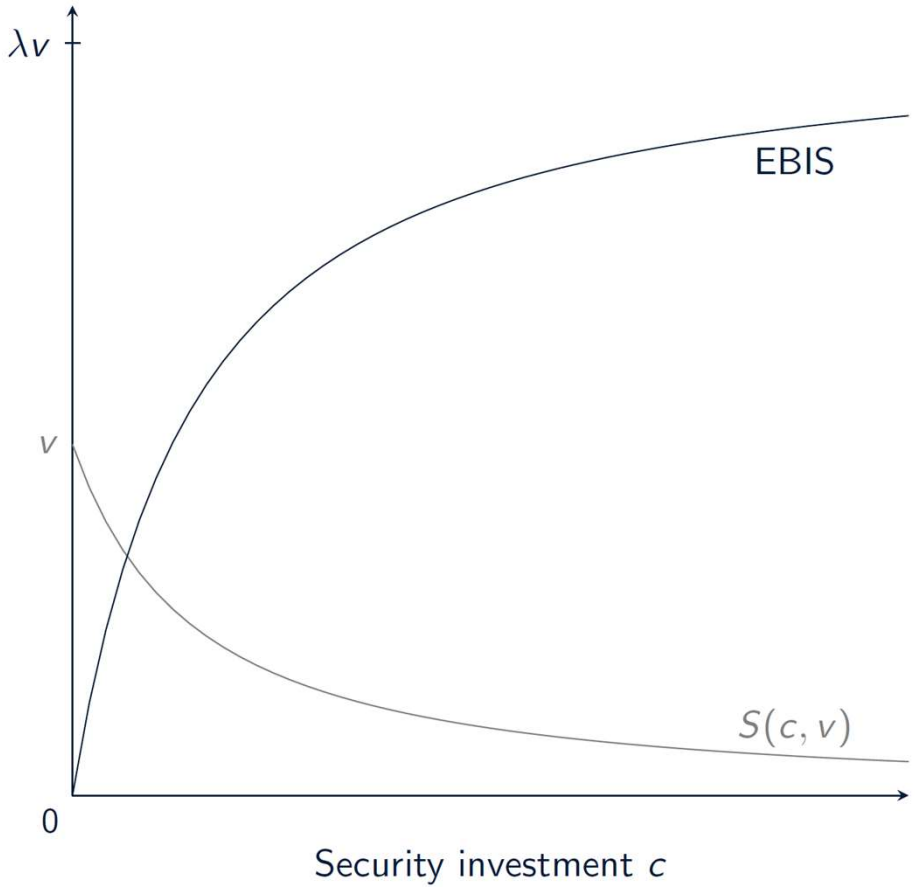
Measuring security effectiveness



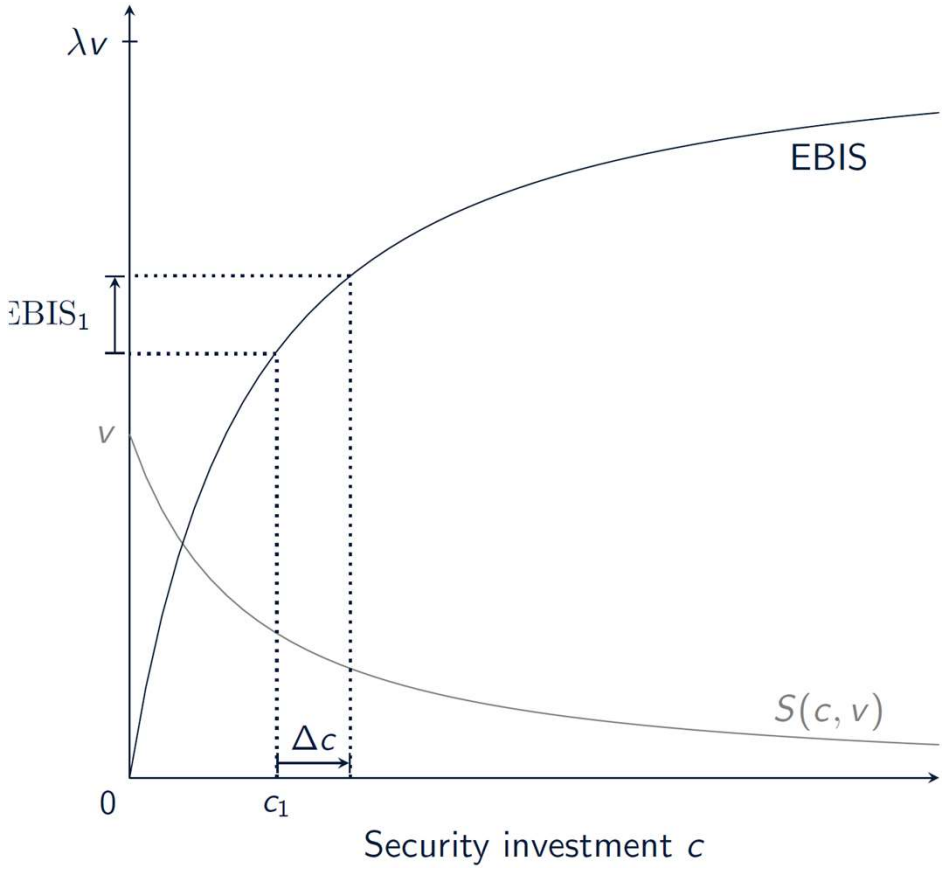
Outline

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

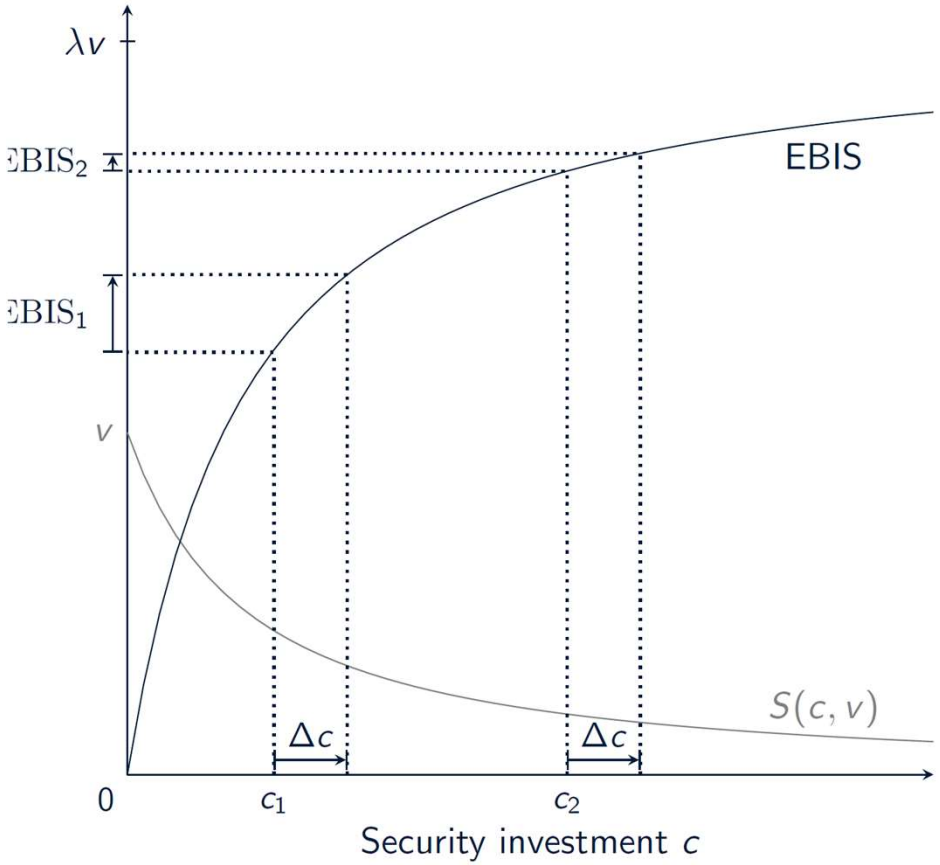
Decreasing marginal returns to security investment



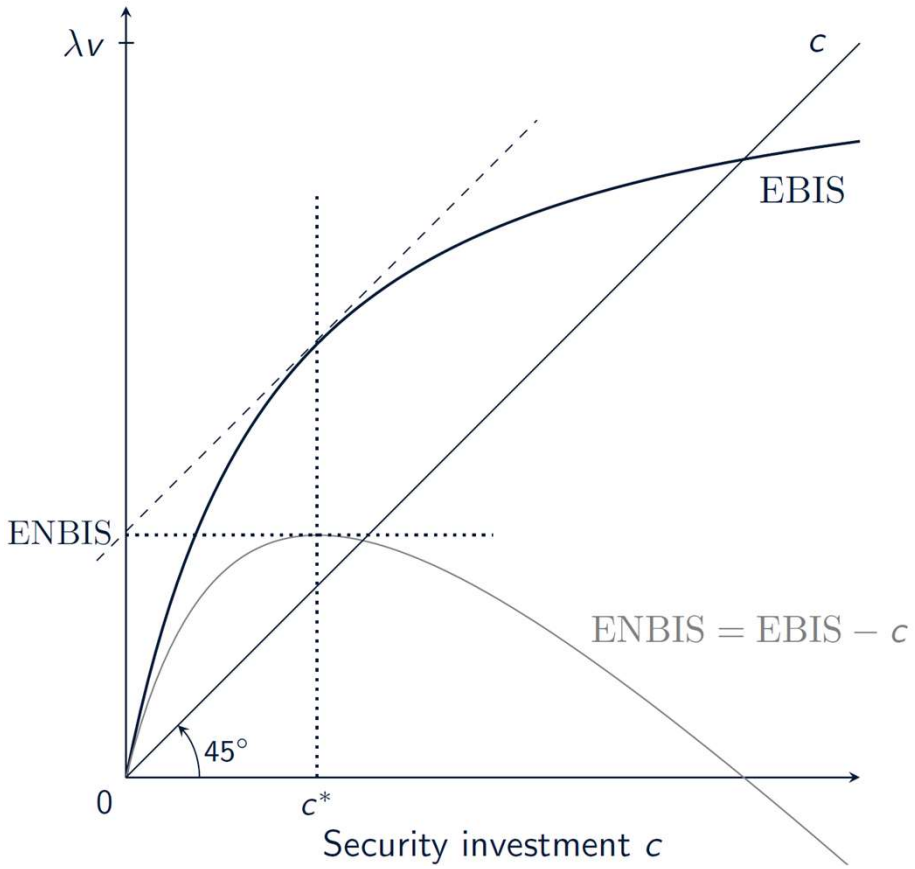
Decreasing marginal returns to security investment



Decreasing marginal returns to security investment



Gordon-Loeb model of security investment



CyBOK

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**

Market-Level Solutions

- Ex-ante safety regulation
- Ex-post liability
- Certifying products and processes
- Information disclosure

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