Security Engineering

INFR11208 (UG4) // NFR11228 (MSc)

Daniel W. Woods* **and Jingjie Li**
Email: daniel.woods@ed.ac.uk **and** jingjie.li@ed.ac.uk

Chapter 8, Security Engineering

CHAPTER

8

Economics

The great fortunes of the information age lie in the hands of companies that have established proprietary architectures that are used by a large installed base of locked-in customers.

– CARL SHAPIRO AND HAL VARIAN

There are two things I am sure of after all these years: there is a growing societal need for high assurance software, and market forces are never going to provide it.

– EARL BOEBERT

https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3-ch8.pdf

Why economics

"LO3: Compare and synthesise the perspectives of different system stakeholders and threat actors, using economic and psychological viewpoints as well as technical ones."

Q: How did the Mirai botnet infect so many devices?

Technical explanation:

"Many IoT devices are shipped with a default password"

Economic explanation:

"IoT device vendors made more money if they shipped devices with default passwords"

Alexander Martin

April 29th, 2024

UK becomes first country to ban default bad passwords on IoT devices

Security economics

- If Alice guards a system but Bob pays the cost of failure, you can expect trouble!
- Economic analysis lets us identify
  - When firms have no incentive to collaborate at all
  - How firms acquire and abuse market power
  - How market failures lead to security failures
  - What sort of crimes scale
- Economic tools also let us quantify harm and prioritise responses
- Language of policymakers

Xkdc

Who is the principal, who is the agent?

1. Cloud provider and customer
2. Cyber insurance customer and the insurer
3. Bank and customer
4. Email provider and phishing victim

Principal Agent Problems

If Alice guards a system but Bob pays the cost of failure, you can expect trouble!

Principal-agent problems

Example of Banking Security

- Account owner as principal
  - Their bank balance is at risk if card details/PIN are stolen, or card is cloned.
- Many agents control the information/devices used for authentication
  - Ecommerce merchants
  - ATM/card machine owners
  - Physical security of ATM

Security economics of PINs

- With cheques, a forged signature was null and void
  - Account holder isn't even party to the transaction
  - Instead assign liability to the party who receives the check and can verify the signature
- With PINs, banks pushed hard for the risk to move to the user
  - ‘Your card and PIN were used so you were negligent or complicit’

Ask yourself, who has the power to prevent fraud? Who pays the costs?

My debit card and pin were stolen but Barclays is treating me as the criminal

It had sent me new ones but before they arrived £1,000 disappeared from my account

The card and pin were used five times in an ATM by the fraudster. Photograph: Panther Media GmbH/Alamy

Security economics of card data

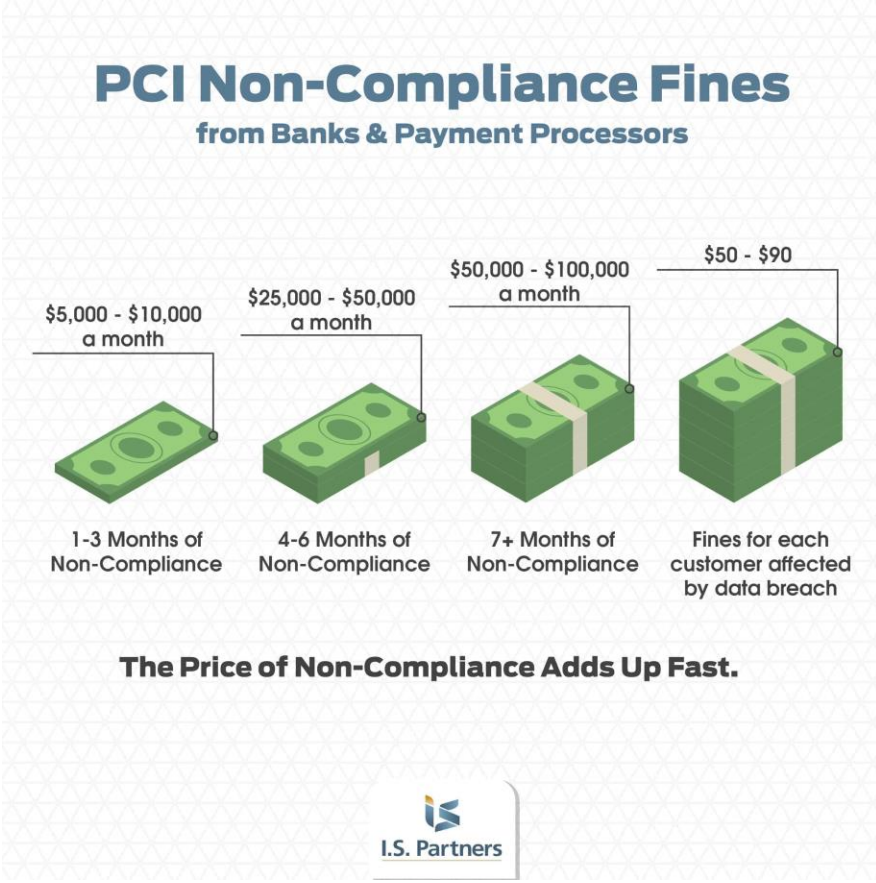
- **Principal**
  - Account owner who uses their credit card to buy goods in person or online
- **Agent**
  - Retail company who processes credit card data

Ask yourself, who has the power to protect data? Who pays the costs?

- Network intrusion
  - Threat actor installs software to exfiltrate unencrypted card data
- Impact
  - 45.7million credit and debit cards were stolen from its computers by hackers
  - Personal information from 451,000 customers who returned goods was also stolen

Payment Card Industry Data Security Standards (PCI DSS)

- **Idea:** Force agent to protect principal's data
- Security requirements
  - **Merchants can’t keep CVVs at all**
  - Protect cardholder data;
  - Patch their kit; etc
- Enforcement
  - Report compliance ex-ante
  - Audited by PCI accredited practitioner
  - Serious fines following a breach
    - TJ Max lost 45mn cards --> settled with Visa for $41m and Mastercard for $24m

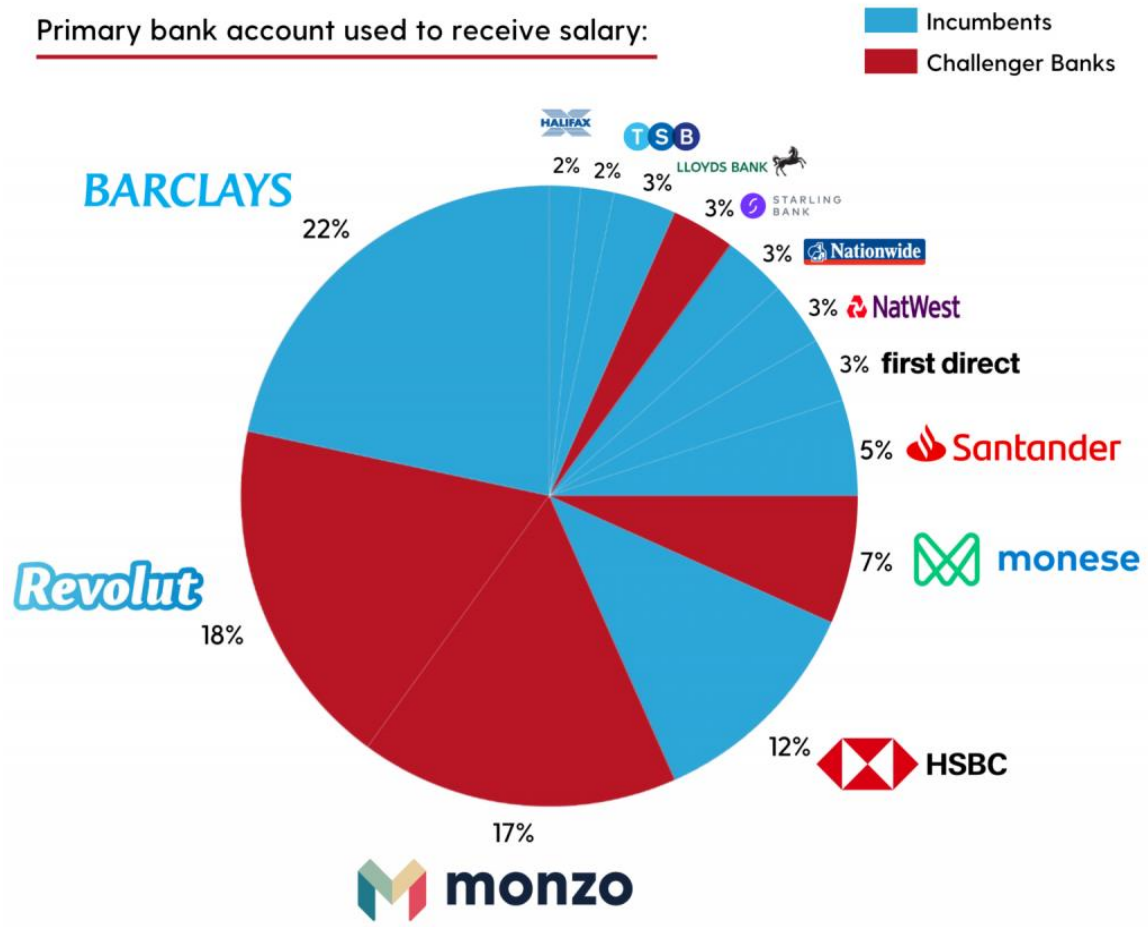


Externalities

If Alice can take an action that impacts Bob, Charlie, Doris, Emily, Francisco, etc… then you need to take extra care in designing incentives

Security economics of PINs

- If a bank can pay an extra £10 per terminal to make 1m PIN entry devices secure, and thereby save £100m in global fraud, will they?



Ask yourself, what is the cost of preventing fraud? Who gets the benefit?

Security economics of botnets

Negative externality

- IoT manufacturers knew default passwords are insecure and the fix is well known
  - Why not fix?
- Who bears the cost?
- What's the fix?

Extreme Externalities = Public Goods/Bads

- A public good (bad) is **non-rivalrous** and **non-excludable**
  - Example: scientific knowledge. The producer can appropriate a small part of the benefit (e.g. PhD thesis); the rest spills over to all
  - Example of a public bad: CO_2 emissions. Again, everyone gets to 'consume' the same amount
- Strong temptation for people to free-ride!
- Cybersecurity examples:
  - policing cybercrime. The US agencies (FBI, secret service…) spend as much as the next 10 countries together (as with conventional defence!)
  - The CVE database + surrounding ecosystem

The NCA announces the disruption of LockBit with Operation Cronos

The NCA has revealed details of an international disruption campaign targeting the world's most harmful cyber-crime group, LockBit.

Why the CVE Funding Crisis is a Wake-Up Call for Cyber Resilience

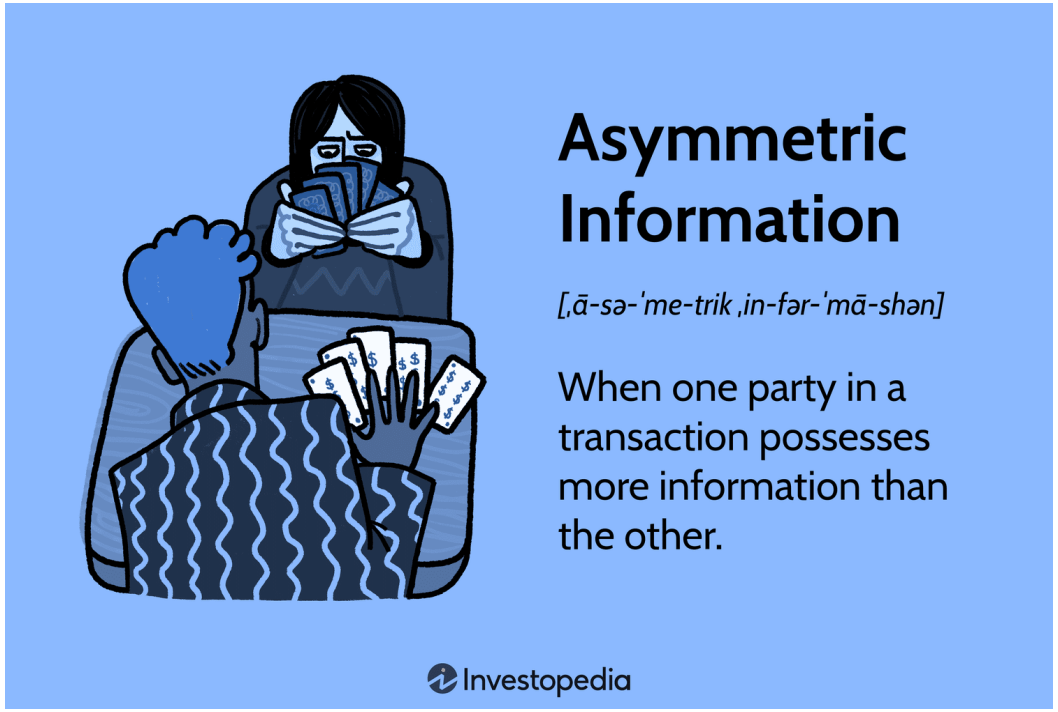
Apr 16, 2025 • 3 min

Ryan Knisley
Chief Product Strategist, Axonius

Information Asymmetries

If Alice is transacting with Bob, but Bob has more information (about security relevant to the transaction).

Asymmetric information



Hidden Information (Before the Deal)
One party knows something about the quality or risk level that the other does not:

- Consumer buys IoT device without knowing the security.
- Firm with weak security controls buy cyber insurance.

Hidden Action (After the Deal)
One party changes their behaviour—usually taking on more risk—because they know the other party will bear the cost of that risk:

- IoT vendor stops shipping security updates once sales slow down.
- Cyber insurance customer doesn't invest in security because insurance covers the loss.

Asymmetric information

- Akerlof won the Nobel for the ‘market for lemons’
  - 100 used cars for sale – 50 good cars worth $2000, 50 lemons worth $1000
  - Buyers can’t tell difference – so price $1000

- Woods won nothing for pointing out parallels in cybersecurity:
  - 🍑 **cost $200k** — security reviews throughout dev lifecycle, bug bounty program etc
    🍋 **cost $100k** — none of the above
  - If the buyer cannot identify insecure software, do they buy 🍋 or 🍑?

Akerlof, 1970. The Market for "Lemons": Quality Uncertainty and the Market Mechanism, *The Quarterly Journal of Economics*, Oxford University Press, vol. 84(3), pages 488-500

How to solve a lemons market?

Liability (from courts)

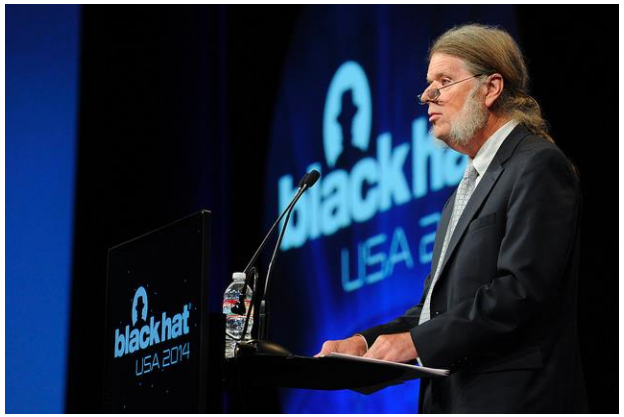
“the only two products not covered by product liability today are **religion** and **software**”

Liability (from contract)

"Our preliminary analysis suggests the majority of cyber warranties cover the cost of repairing the device alone."

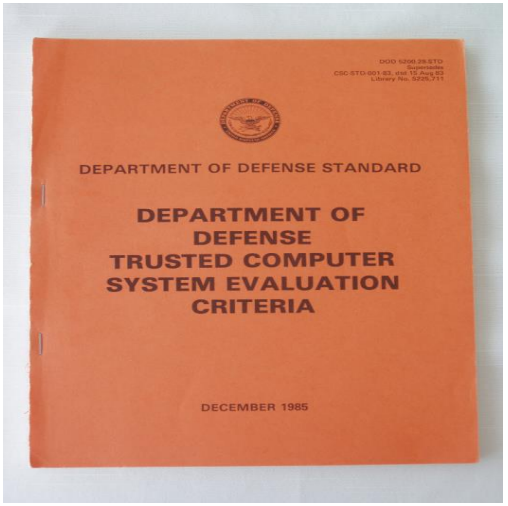
Certifications

Certifying software is hard --> see Assurance lectures later.



Cybersecurity as Realpolitik (27:08)

Cyber Warranties: Market Fix or Marketing Trick?



Solutions don't work if seller is blind too

Lemons vs silver bullets market:

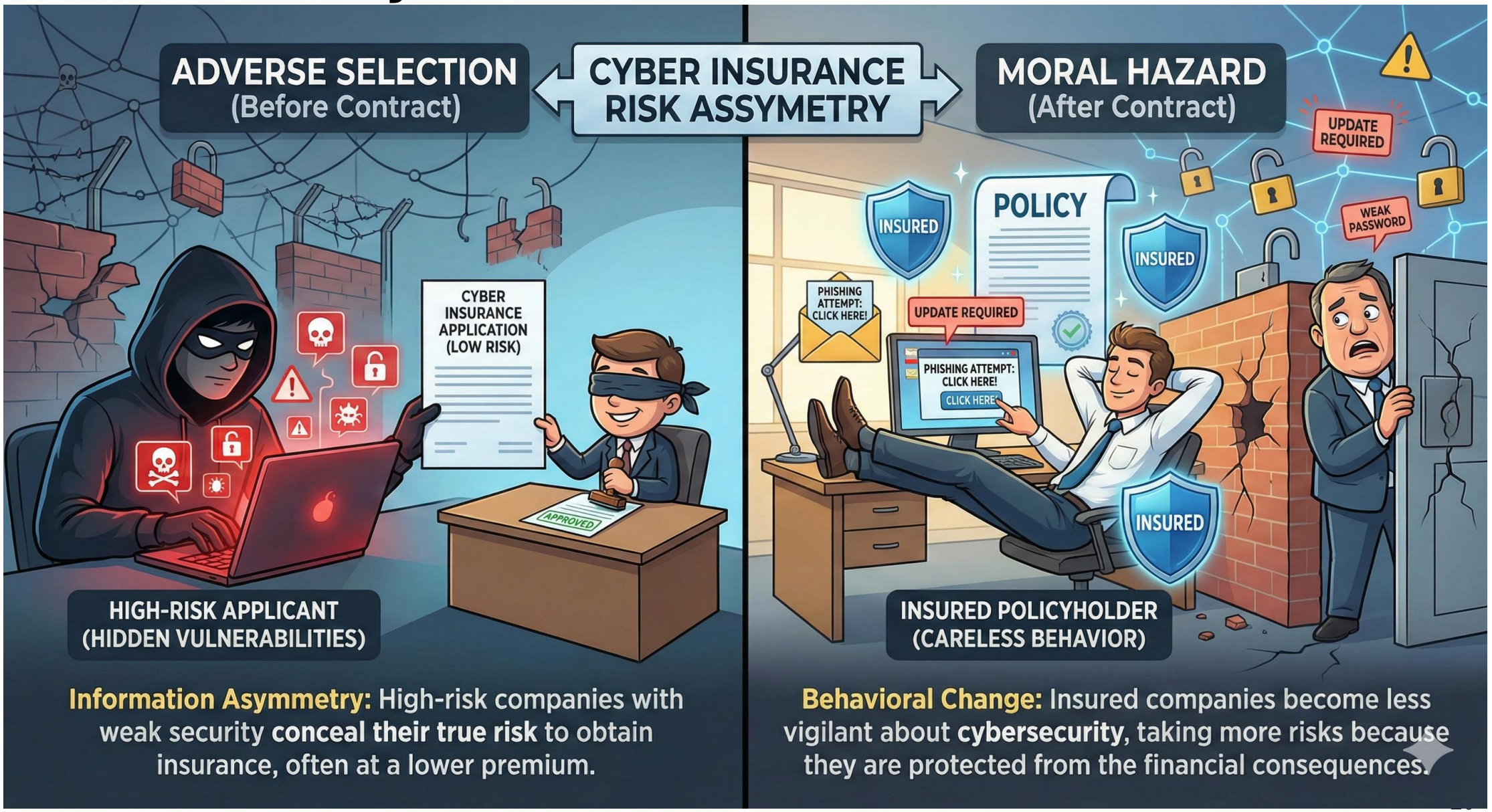
- Warranties/inspections/liability fail
  - Neither party can verify the product's efficacy until it fails
- Sellers compete on "myth-making" and buzzwords
- Buyers stop trying to optimize for utility and start optimizing for liability protection
  - "No-one gets fired for buying IBM"
- Silver Bullets market often booms with useless products

The Market for Goods, as described by Information and by Party	**Buyer Knows**	**Buyer Lacks**
Seller Knows	Efficient Goods	Lemons (used cars)
Seller Lacks	Limes (Insurance)	**Silver Bullets (Security)**

Figure 1. Security is a Symmetrically Insufficient Market

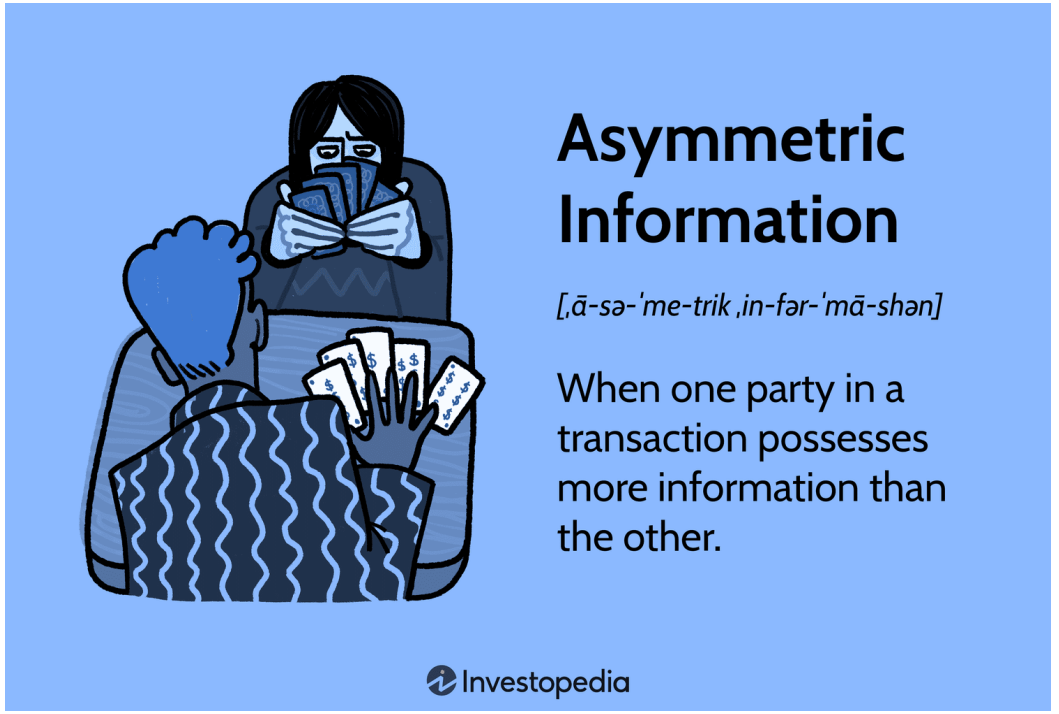
https://ventureinsecurity.net/p/cybersecurity-is-not-a-market-for

When the buyer has more info than the seller



Describe the info asymmetry (if one exists)

1. Customer wants to use a bank with a strong fraud detection team
2. Vendor receives a vuln report in a product that is no longer produced.
3. Bug hunter reports a vulnerability to the vendor.
4. Bug hunter reports a vulnerability to a vulnerability broker.



Market Power

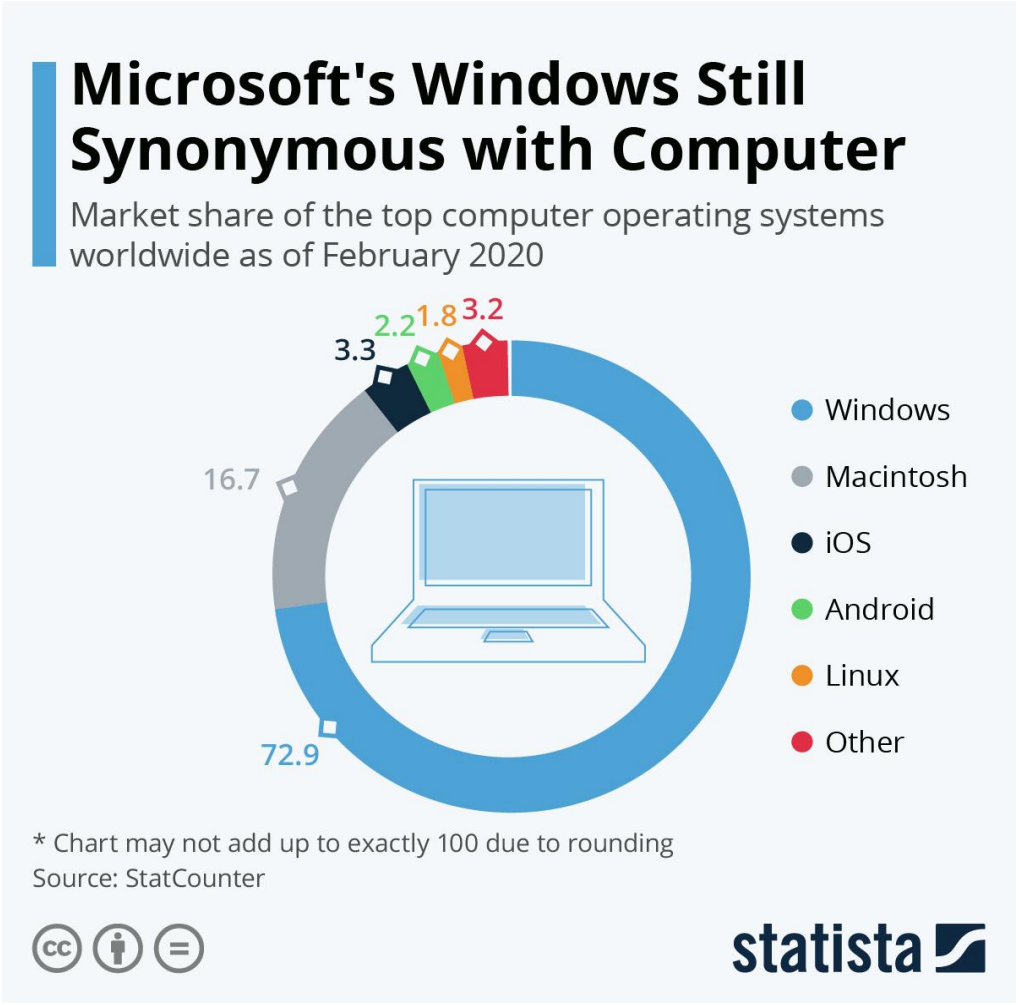
If Bob is the only person selling security, how does that impact Alice?

Why is tech prone to monopoly?

Dominant-firm arises due to:

1. Low marginal costs of production
2. Technical lock-in
3. Network externalities

Given all three, monopoly is even more likely

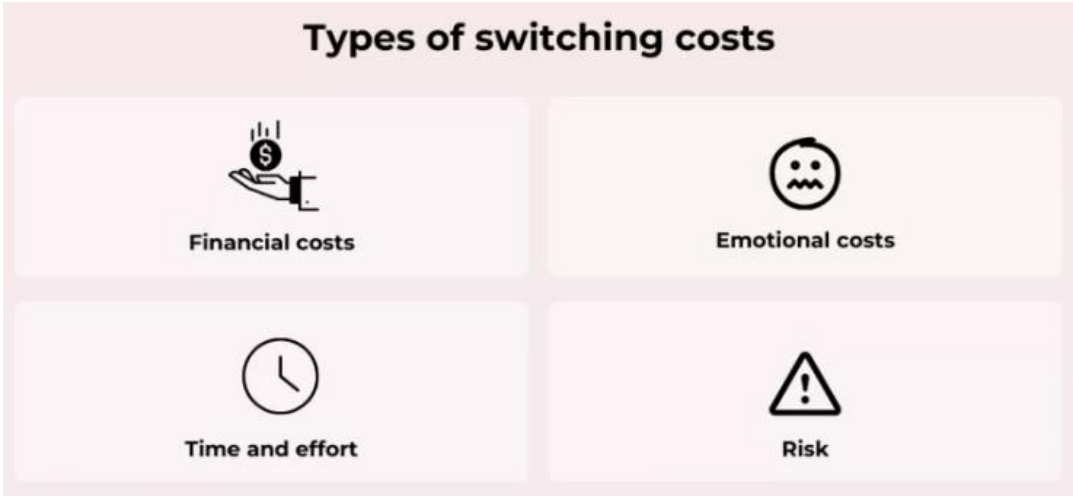


Low marginal costs

- The marginal cost of reproducing information is close to zero
  - So that's often the market clearing price, especially in price wars
- Example – machine-readable phone books
  - 1986 – Nynex charge $10,000 per disk
  - ProCD had the phone book retyped in Peking and started selling for $300
  - ABI joined in and the price collapsed to $20
- Hence Wikipedia, Linux, and the Free Software Foundation slogan:
  'information wants to be free'

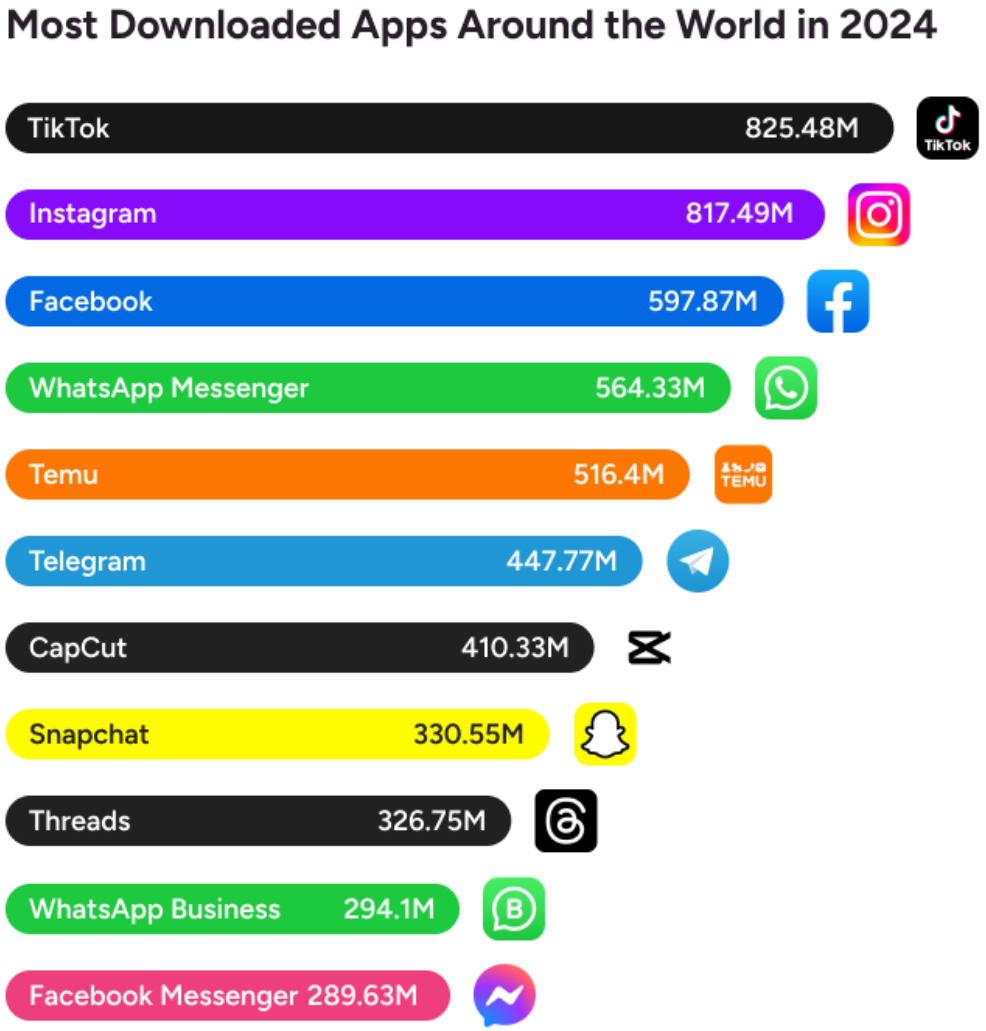
Switching costs

- ‘Fundamental theorem’ (Shapiro, Varian); the net present value of your customer base is the total cost of switching
  - Suppose you’re an ISP and it costs £25 to set up a new customer
  - Suppose it costs a customer £50 of hassle to switch
  - If your new business model makes the customer worth £100, offer them £60 cashback to switch
  - They’re £10 ahead, you’re £15 ahead
- So the value of Microsoft is what it would cost people to switch to Google Docs and Linux …



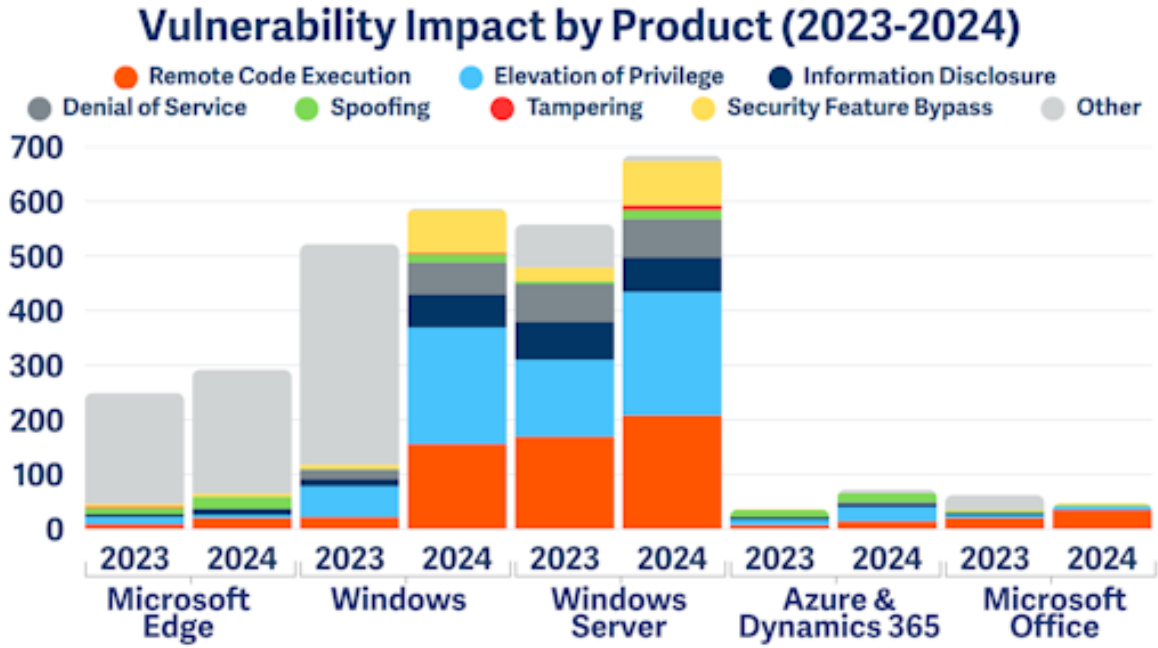
Network externalities

- Many networks become more valuable to each user the more people use them
- Metcalfe's law: the value of a network is proportional to the square of the number of users
- Overall effect: past some threshold, network use takes off rapidly (and creates lock-in)
  - Telephone – late 19th century
  - Email – 1995–99
  - Facebook – 2008–11



How drive for dominance impacts security

- Hence the race for market share whenever a new product or service market opens
  - Microsoft ‘ship it Tuesday and get it right by version 3’
  - AI today
    - "Abuse risks are inherent to product features"
- The rise of agile development
  - Feedback on security is usually expensive and harmful!



Monopoly and correlated risk

ANDY GREENBERG EXCERPT SECURITY AUG 22, 2018 5:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

Amazon reveals cause of AWS outage that took everything from banks to smart beds offline

AWS explains in a lengthy post how a bug in automation software brought down thousands of sites and applications

Josh Taylor *Technology reporter*

Fri 24 Oct 2025 06.25 BST

Private equity and security

Scenario:

- A networking firm has 1k users who would have to pay on average $1m to switch to a competitor.
- Re-writing all products in Rust would cost $100m.
- What does a private equity firm do?

SolarWinds lawsuit claims private equity owners 'sacrificed cybersecurity to boost short-term profits'

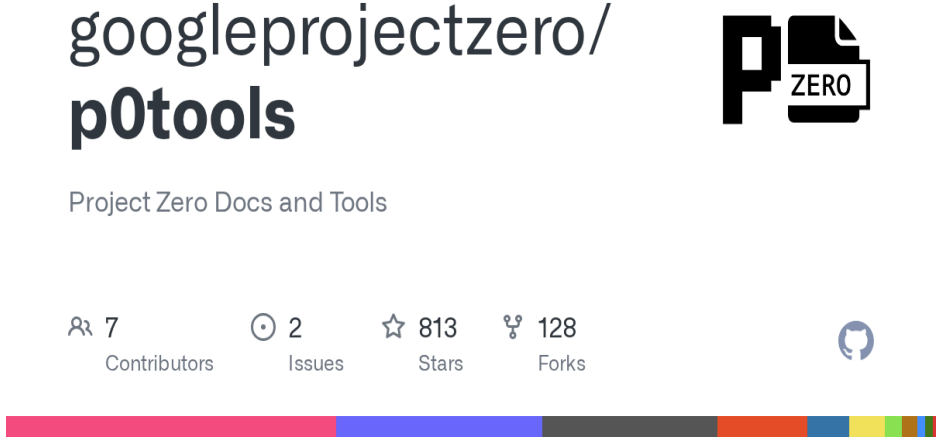
June 2, 2021 Share

By Derek B. Johnson

https://www.scworld.com/news/solarwinds-lawsuit-claims-private-equity-owners-sacrificed-cybersecurity-to-boost-short-term-profits

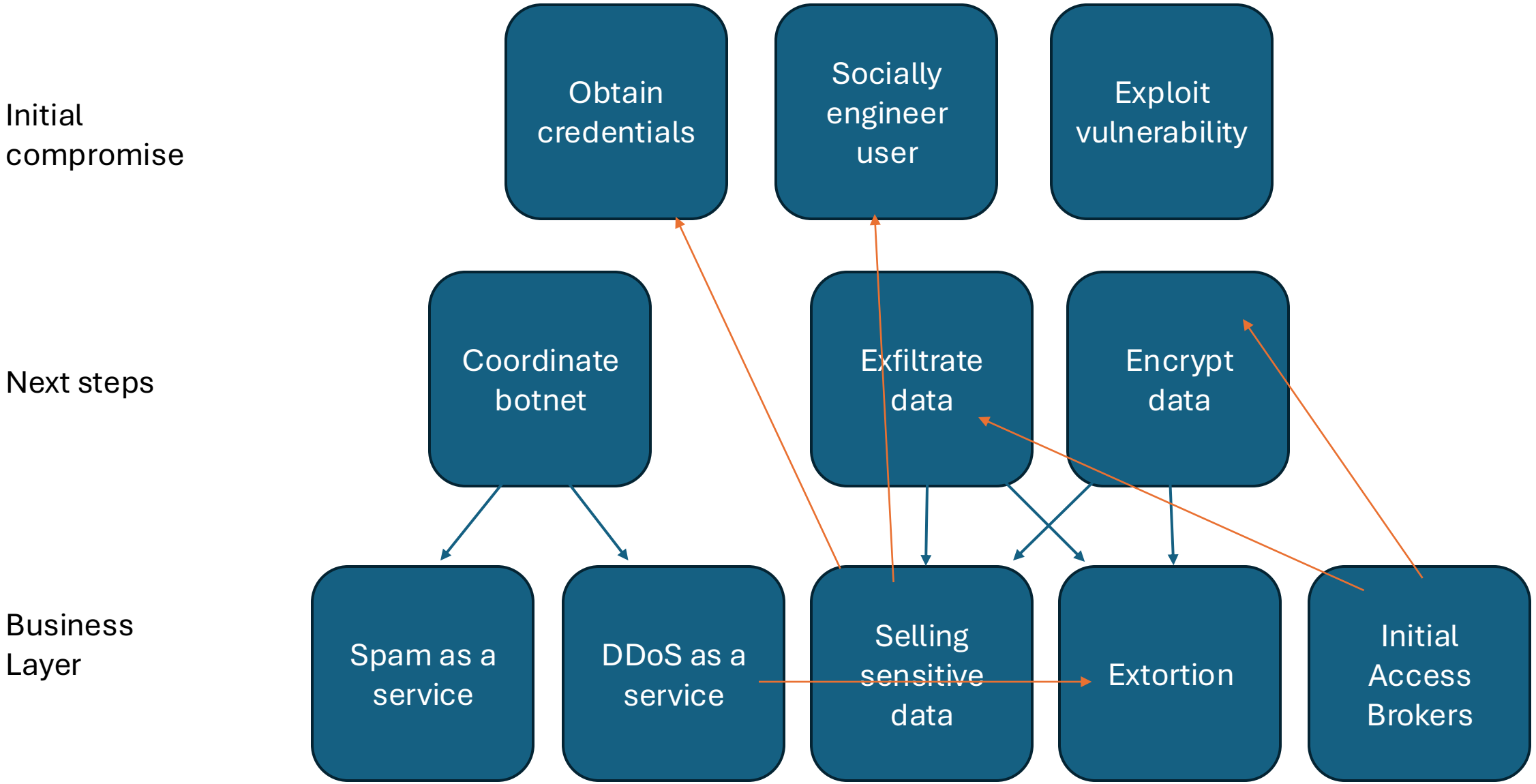
The good side of monopoly?

- Security as a "luxury" property
- In fierce competition, security is the first to go
  - See IoT manufacturers
- By contrast, a monopoly may allow a company to invest in security
  - Maybe?



Economics of Cybercrime

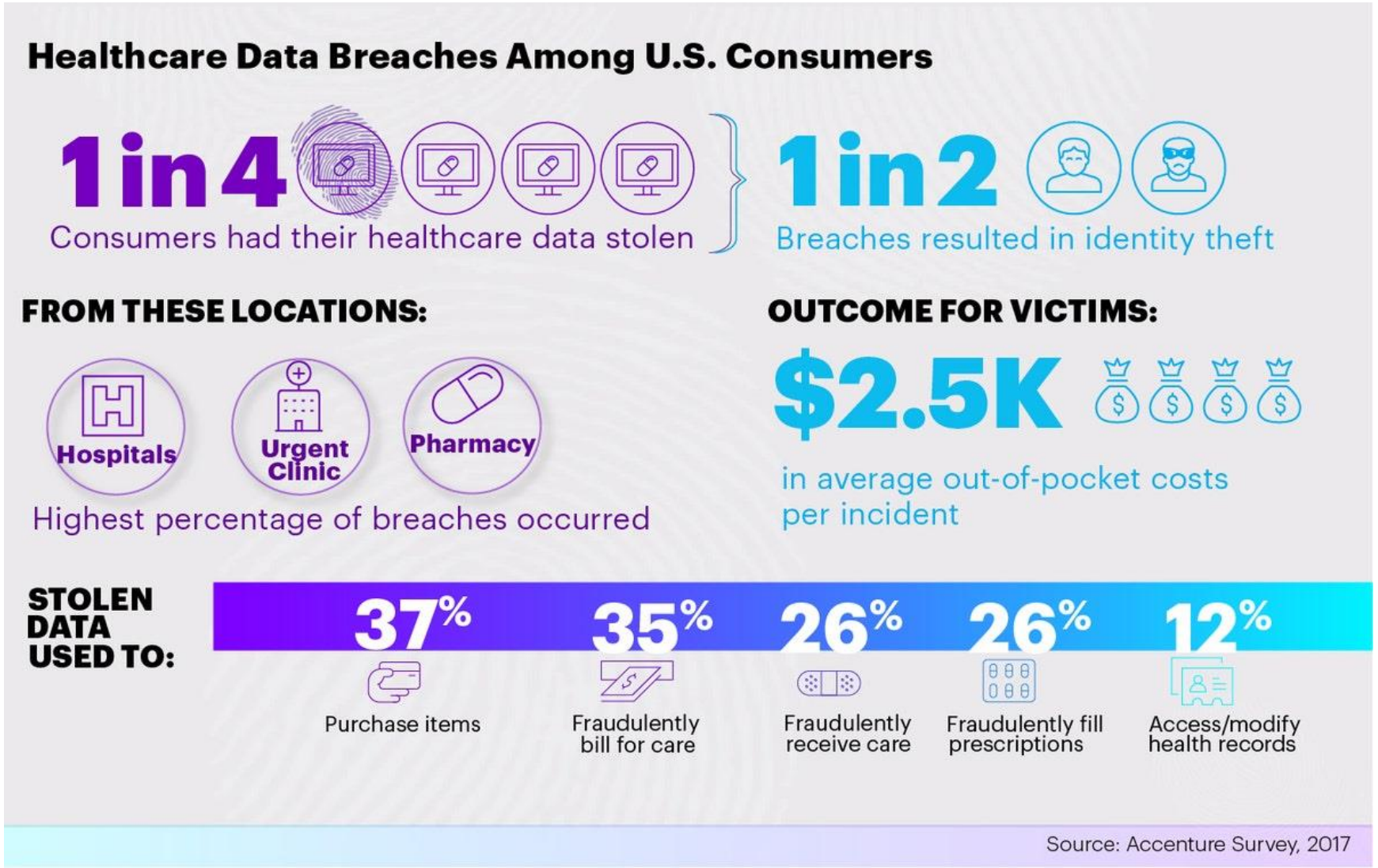
Economics all the way down



Examples

Try to identify the economic principle.

What economic concepts are relevant here…



What economic concepts are relevant here…

Security

Cybersecurity News: Insurance refuses to cover cyberattack claim due to lack of MFA

Hamilton's cyber insurance claim was denied after a ransomware attack due to lack of MFA, highlighting the critical need for modern cybersecurity practices.

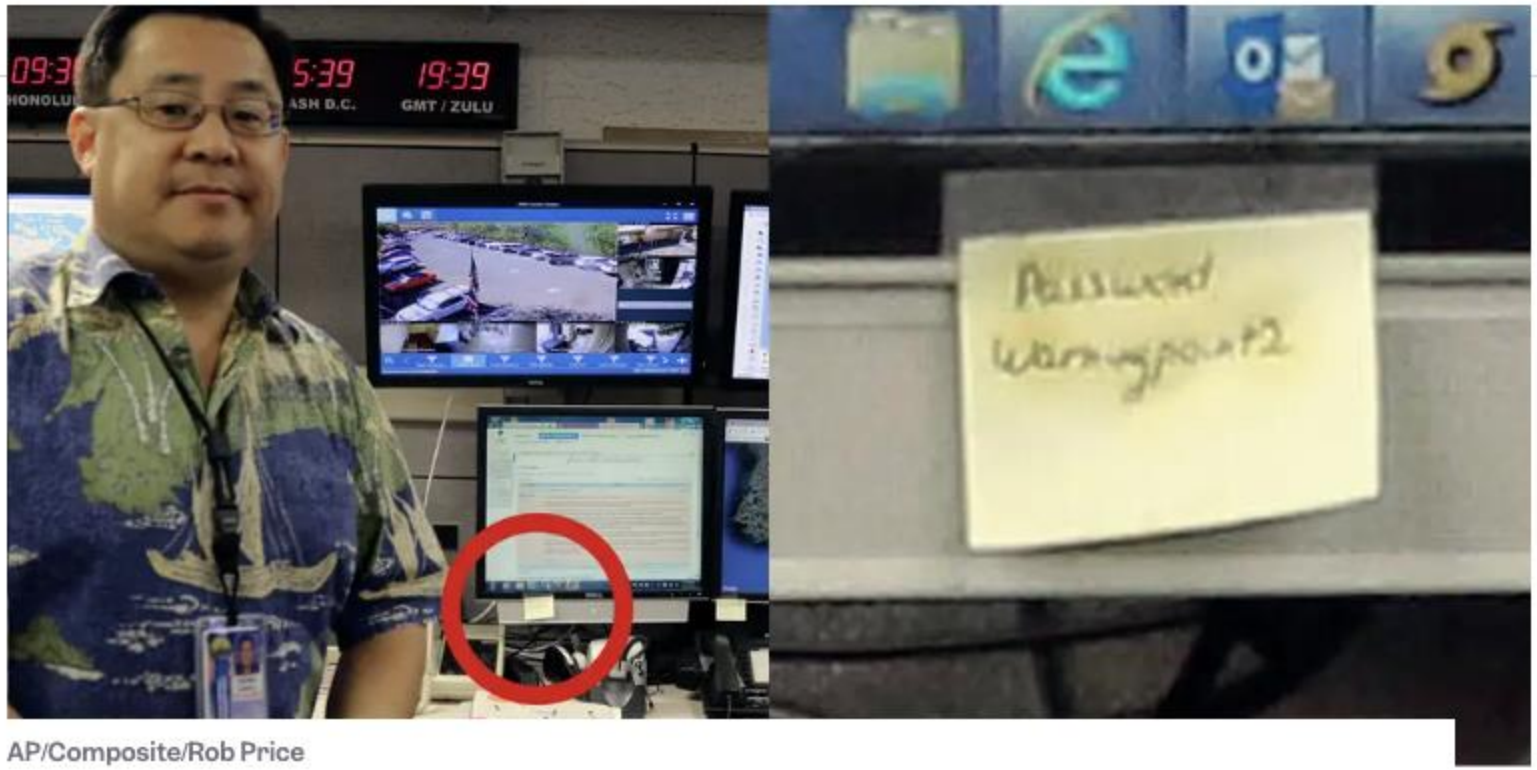
Patrick Pilotte August 21, 2025

https://devolutions.net/blog/2025/08/cybersecurity-news-insurance-refuses-to-cover-cyberattack-claim-due-to-lack-of-mfa/

What economic concepts are relevant here…

A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note

By Kif Leswing



AP/Composite/Rob Price

What economic concepts are relevant here…

Ivanti Connect Secure zero-day patches delayed

Researchers observed attackers attempting to manipulate Ivanti's internal integrity checker, and the cause for the patch delay remains unclear.

Published Jan. 29, 2024

David Jones
Reporter

Share License Add us on Google

•Ivanti confirmed a patch designed to mitigate two zero-day vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure will be delayed until this week, according to an updated blog post released Friday.
•The authentication-bypass and command-injection vulnerabilities have been actively exploited since early December, impacting thousands of organizations and leading the Cybersecurity and Infrastructure Security Agency to issue an emergency directive for Federal Civilian Executive Branch agencies.

What economic concepts are relevant here…

Supply chain risks overwhelm cybersecurity leaders, report finds

phishing # martech # cartech

Wed, 22nd Oct 2025

By Jed Nykolle Harme, Editor

New research has found that 60% of cybersecurity leaders in the UK and US consider security risks from third parties and supply chain partners to be "innumerable and unmanageable."