Security Engineering

INFR11208 (UG4) // NFR11228 (MSc)

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

What is Security Engineering?

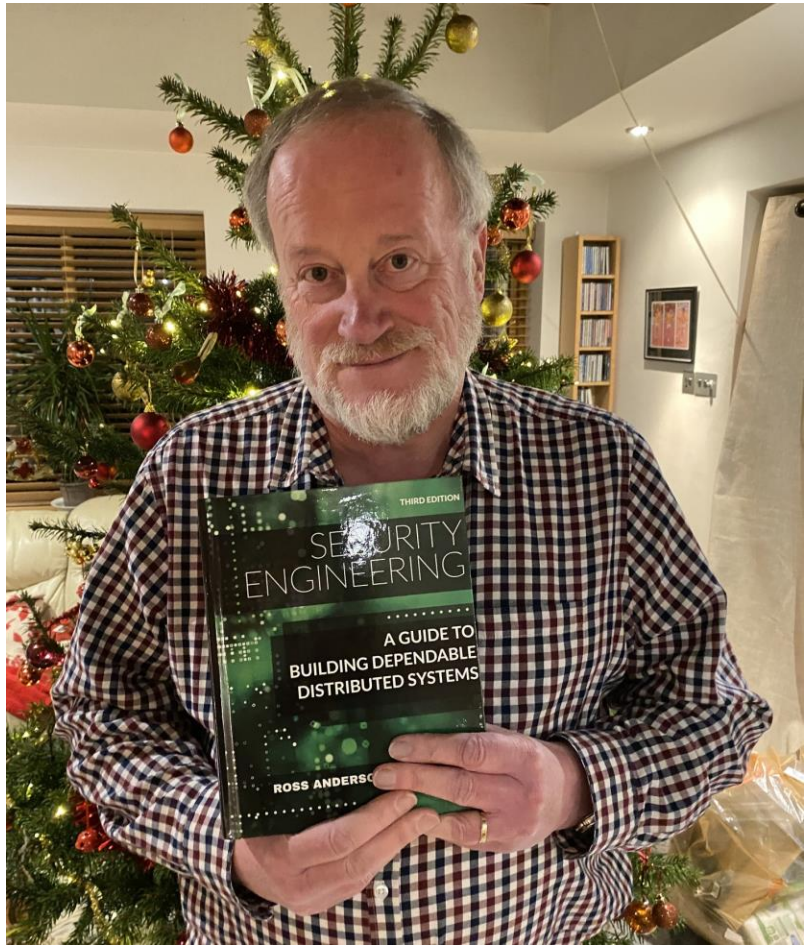
"Security engineering is about building systems to remain dependable in the face of **malice**, error and mischance."

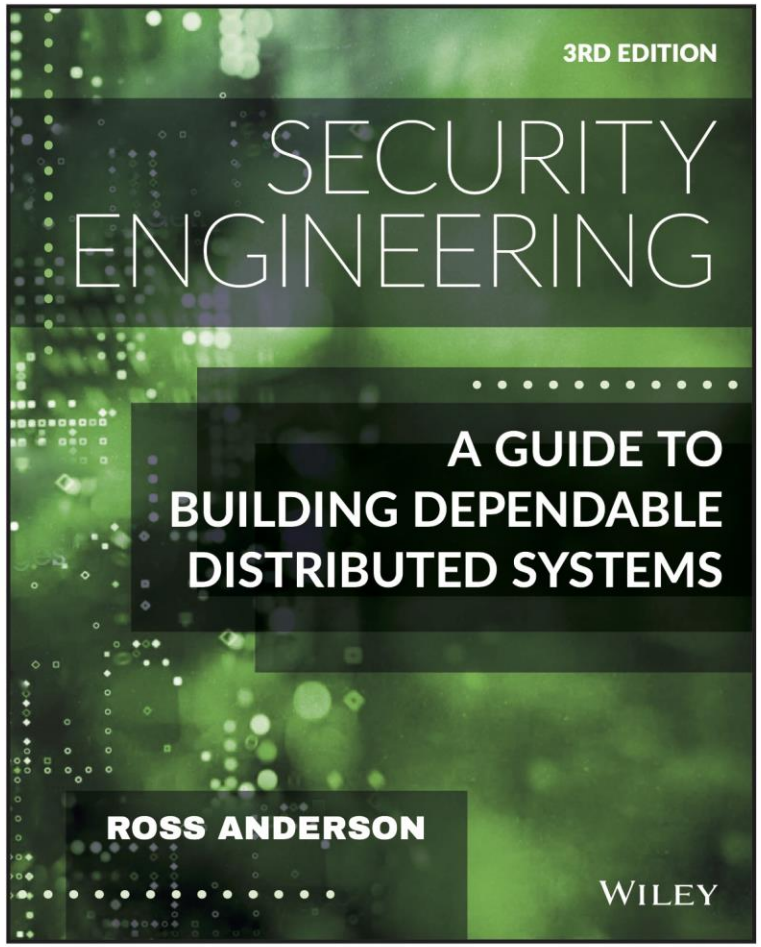
This involves thinking about:

- Attacker behaviour
- Technical properties of systems
- User behaviour (psychology, usability etc)
- Market incentives (economics)

This will teach a new way of thinking.

Ross Anderson (1956 – 2024)





This Course

- Lectures by Daniel Woods on ‘breadth’
  - Threat models, security policies, banking, psychology & econ (lectures 1-7)
  - Assurance & governance (lectures 13-15)
- Lectures by Dr Jingjie Li on ‘depth’
  - networks, hardware, operating systems, ecosystems (lectures 7–12)
- Guest lecture

Assessment

- 30% Coursework, 70% Exam

Coursework

- Released 19/01/2026
- ~20 hours of effort
- Submit by 12:00 on 27/02/2026
- You will be given a hypothetical defender, and the task will be to conduct a threat assessment.
  - More guidance to follow.

Security engineering is different

- In most areas of computer science, the problem is stable, clear and universal
  - Boost accuracy on a task with known ground truth
  - Establish a performance bound on an algorithm
  - Prove a theorem
- By contrast, security problems depend on the defender and what attackers are up to
  - Possibility an employee or customer may "join the other side"
  - Defenders face different threats
  - Threat actors will adapt to the defences that are in place

Understanding the problem (aka threat modelling) is half the battle.

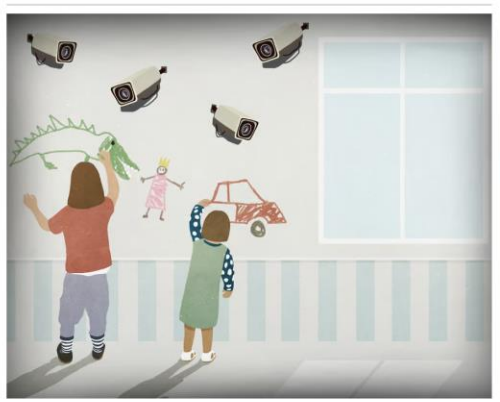
Why security engineering?

Aka how do we know what to focus on

Focus on the news cycle

July 2025

+ Rapid updates
+ Access to sources
+ Things generally "matter"
+ ...



'Hacking is assumed now': experts raise the alarm about added risk of surveillance cameras in childcare centres

11 Jul 2025 17.00 CEST

Louis Vuitton says UK customer data stolen in cyber-attack

11 Jul 2025 16.21 CEST

June 2025

- Biased to newness
- Focus on celebrity/govt
- May not report on boring but important trends
- ...

UK 'woefully' unprepared for Chinese and Russian undersea cable sabotage, says report

CSRI finds China and Russia may be coordinating 'grey zone' tactics against vulnerable western infrastructure

15 Jun 2025 19.28 CEST

European journalists targeted with Paragon Solutions spyware, say researchers

Citizen Lab says it found 'digital fingerprints' of military-grade spyware that Italy has admitted using against activists

12 Jun 2025 14.39 CEST

ANU investigates possible hack after vice-chancellor's account liked 'highly offensive' LinkedIn posts

University spokesperson says Genevieve Bell's account had 'liked' posts she had never seen before about Julie Bishop and Gaza

5 Jun 2025 03.44 CEST

Focus on the law/an international standard

+ You have to do it anyway

+ Security certifications may help sales

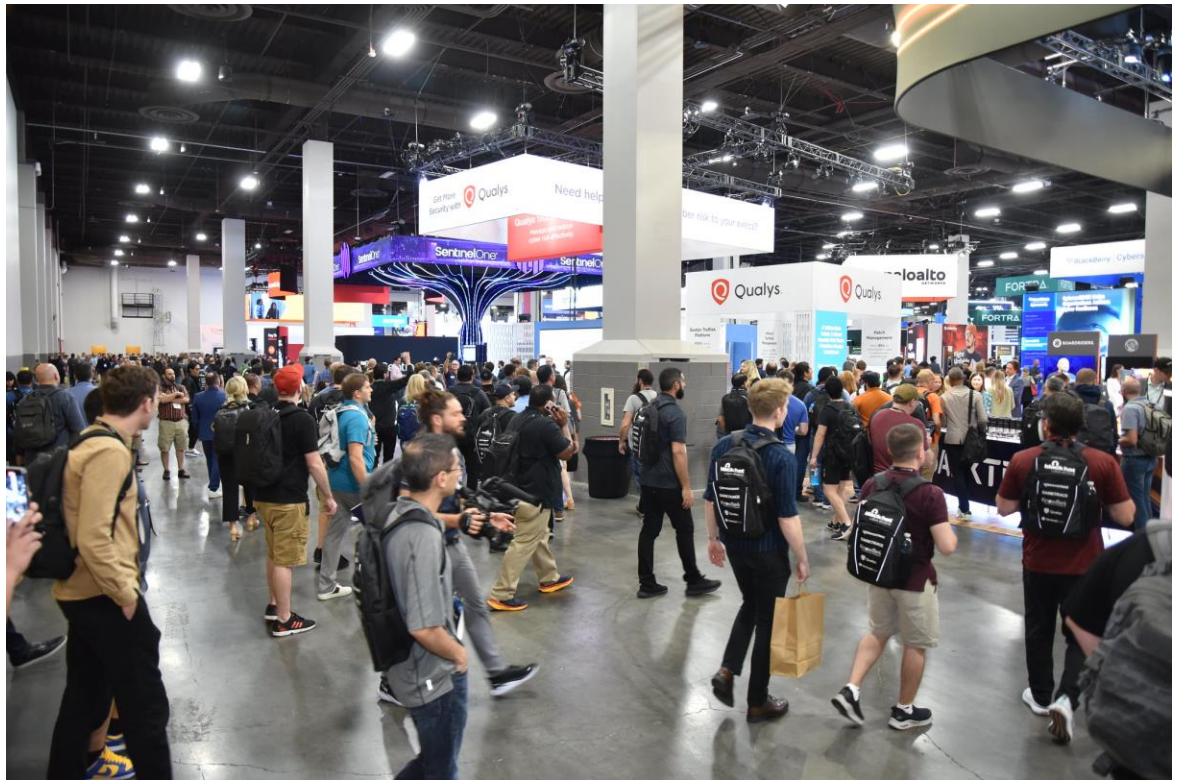
- Slow to be updated
- Not tailored to your company
- Assumes regulators know what to do

Standard	Focus Area	Scope	Industry Coverage	Geographical Relevance
ISO 27001	Information Security Management Systems (ISMS)	Organization-wide security	All industries	Global
GDPR	Data Privacy and Protection	Personal data processing	All industries handling EU data	European Union (affects global entities handling EU data)
NIST	Cybersecurity Framework	Risk management	Primarily government and tech	United States (influential globally)
HIPAA	Health Information Protection	Personal health information	Healthcare	United States
PCI DSS	Payment Card Security	Payment cardholder data	Retail, banking, e-commerce	Global
SOC 2	Trust Service Criteria for Data Handling	Service providers and vendors	Technology and cloud services	Primarily United States
COBIT	IT Governance and	IT processes and	All industries	Global

Focus on the market

+ Vendors are specialists
+ "No-one gets fired for buying IBM"
+ Easier to buy than build

- Misaligned incentives
- Expensive
- May not be tailored to your risk profile



Focus on security engineering

- Start with a **threat model**.
  - Who might attack us, why, and how? People or malware? Insiders or outsiders?
- Use this to write a **security policy**.
  - What protection properties are we trying to provide?
- Implement the security policy via **protection mechanisms**
  - What tools and processes do you use to achieve protection goals, and how?
- Finally, **assurance**.
  - How do you know you've done enough, and how do you convince others of that?

Step 1: Model threat actors you will face

Cybercrime statistics

The threat landscape from the top down

FBI – Internet Crime Report 2024

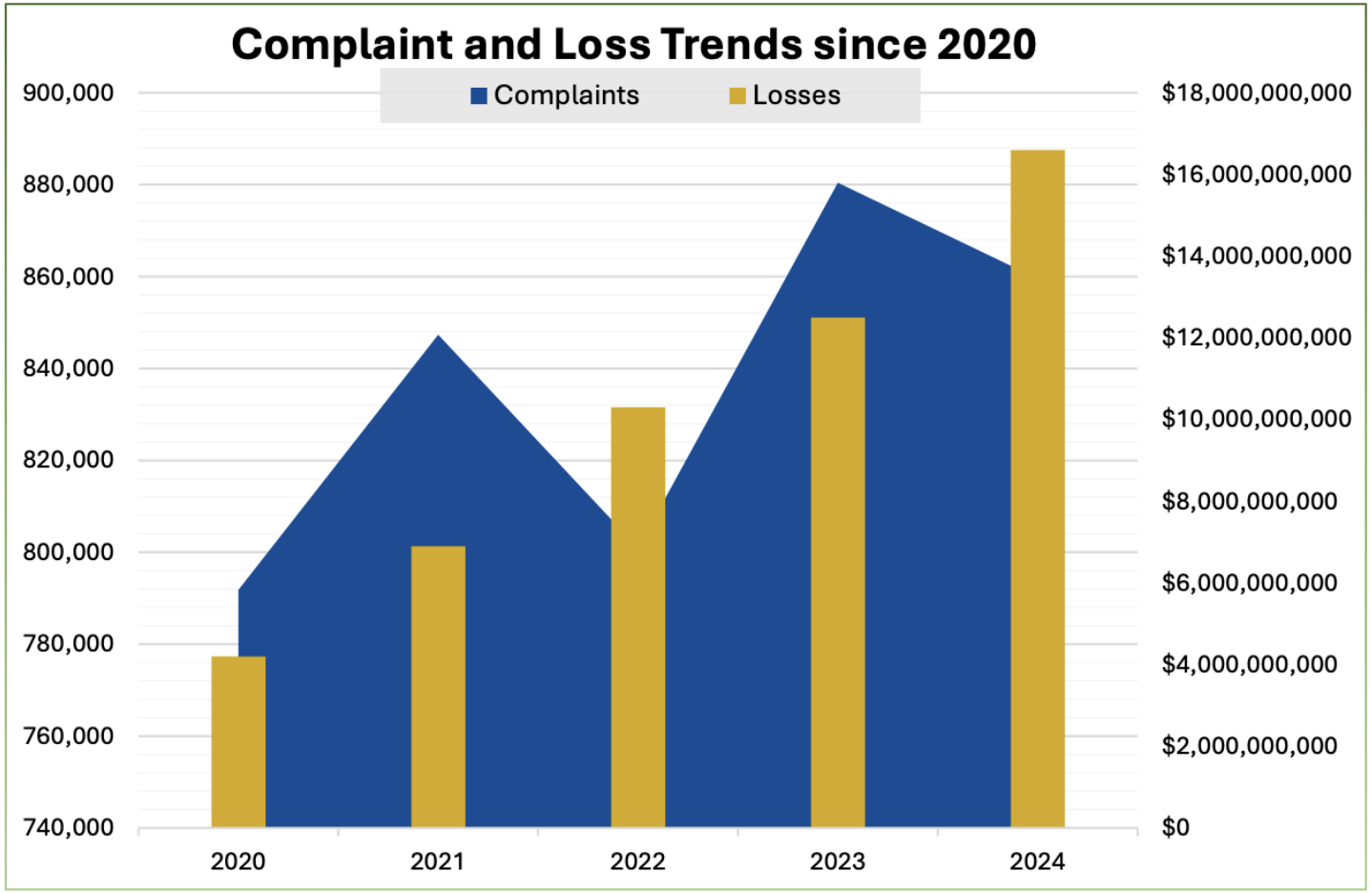
859,532 Total Complaints in 2024

$16.6 Billion Losses in 2024

33% Increase in Losses from 2023

256,256 Complaints with Actual Loss

$19,372 Average Loss



$16.6 billion of cybercrime losses in perspective

UK shoplifting reaches highest level in 20 years

Employers are pushing for tougher penalties and better protection · Retail Insight Network

Industry data points to retail crime costing UK businesses approximately £2.2 billion in 2024

Biden says Hurricane Milton caused staggering $50bn in estimated damage

Sixteen people killed by storm but state spared 'worst-case scenario' as accusations fly between political candidates

Bodycam video shows dramatic rescues from Milton flood waters – video

Most common/harmful crimes

2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints
Phishing/Spoofing	193,407
Extortion	86,415
Personal Data Breach	64,882
Non-Payment/ Non-Delivery	49,572
Investment	47,919
Tech Support	36,002
Business Email Compromise	21,442
Identity Theft	21,403
Employment	20,044
Confidence/Romance	17,910
Government Impersonation	17,367
Credit Card/Check Fraud	12,876
Other	12,318

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss
Investment	$6,570,639,864
Business Email Compromise	$2,770,151,146
Tech Support	$1,464,755,976
Personal Data Breach	$1,453,296,303
Non-Payment/Non-Delivery	$785,436,888
Confidence/Romance	$672,009,052
Government Impersonation	$405,624,084
Data Breach	$364,855,818
Other	$280,278,325
Employment	$264,223,271
Credit Card/Check Fraud	$199,889,841
Identity Theft	$174,354,745
Real Estate	$173,586,820

Definitions Matter

Most Common Crimes

- **Phishing/spoofing** (193k / $70m): The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.
  - What about follow on effects … phishing is commonly used in other crimes
- **Extortion** (86k / $143m): Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.
  - Why doesn't this include ransomware?
- **Ransomware** (3k / $12m): A type of malicious software designed to block access to a computer system until money is paid.

Definitions Matter

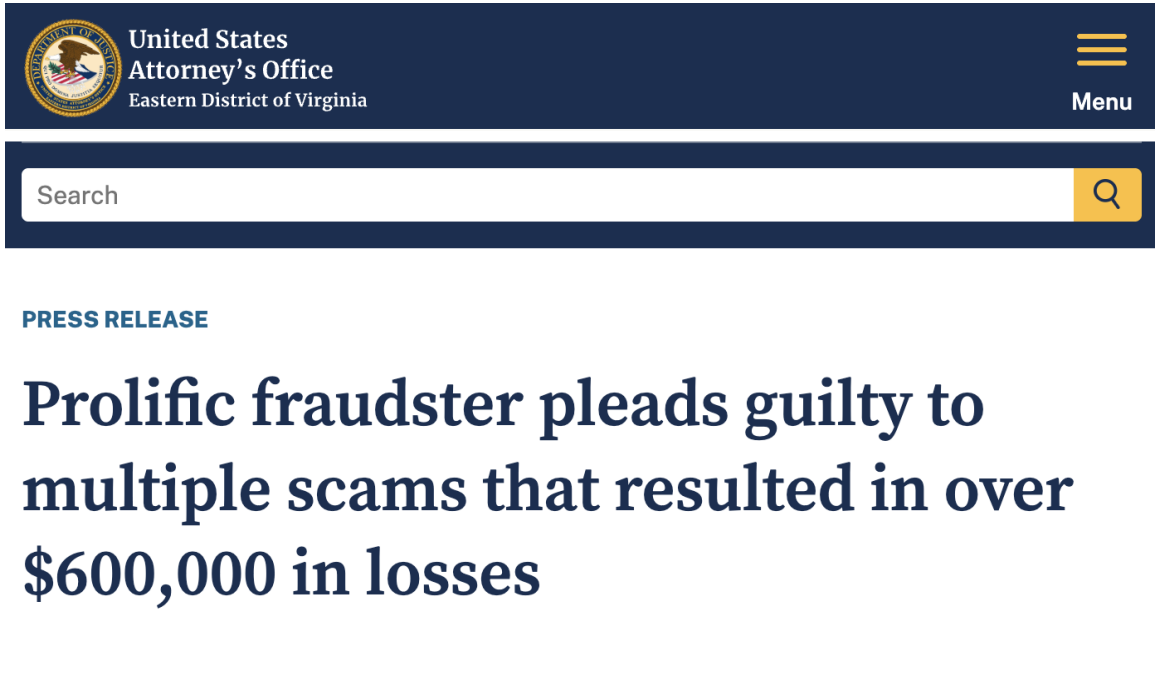
Most "Impactful" Crimes

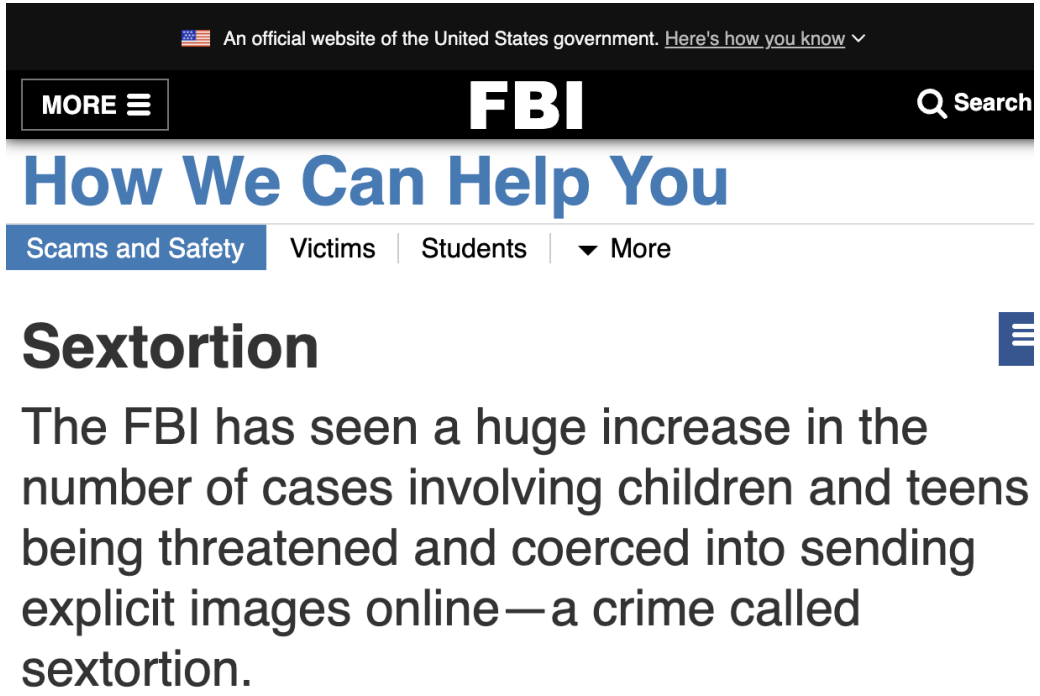
- **Investment** ($6.5bn): Deceptive practice that induces investors to make purchases based on false information.

- **Business Email Compromise** ($2.7bn): BEC is a scam targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments.

Why are these the most "impactful" cyber crimes?

Quantifying the "impact" of non-financial harm is hard





Most crimes are authorized by the victim

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss	
Investment	$6,570,639,864	→ Social engineer individuals
Business Email Compromise	$2,770,151,146	→ Social engineer business, sometimes via hack
Tech Support	$1,464,755,976	→ Social engineer individuals
Personal Data Breach	$1,453,296,303	→ Mostly remote hacking
Non-Payment/Non-Delivery	$785,436,888	→ Defraud ecommerce buyers
Confidence/Romance	$672,009,052	} Social engineer individuals
Government Impersonation	$405,624,084	
Data Breach	$364,855,818	→ Mostly remote hacking
Other	$280,278,325	
Employment	$264,223,271	→ Weird but not remote hacking
Credit Card/Check Fraud	$199,889,841	→ Auth failures, but not via remote hacking
Identity Theft	$174,354,745	→ Auth failures at banks, using data from hacking
Real Estate	$173,586,820	→ Social engineer renters/house buyers

The police don't hear everything

Crimes aren't reported...

- When the incident is too small to be worth the effort
- When the victim doesn't trust the police (to take action)
- When involving the police will hurt the victim
- When the incident is reported elsewhere
- ...

Takeaway: Cybercrime statistics are useful, but imperfect.

What about risk estimates?

For individuals and businesses

Cyber Crime Surveys

- The six cybercrimes studied – estimated by FBI reports to cover nearly 30% of cybercrime in the U.S. – are rare
  - only two crimes having an annual prevalence above 1%, and none having a prevalence above 3.5%.
- Typical monetary harm sustained is quite low. The median loss across all cybercrimes was $100
- Older Americans and Black Americans are significantly more likely to be the victims of cybercrimes
  - Exceptions of scams that involve the victim selling goods on the internet

	Prevalence	Money Lost (Dollars)		
Cybercrime	Direct Estimate (%)	Median	Q_{10}	Q_{90}
Bank/CC (any)	12.110			
Bank/CC (lost money)	1.082	265.95	32.34	1000.00
Non-Delivery	3.205	57.05	15.00	300.00
Advanced Fee	0.280	500.00	14.32	3000.00
Non-Payment	0.344	100.00	13.66	700.00
Extortion	0.116	300.00	56.65	1442.25
Overpayment	0.052	88.01	35.00	854.27

Table 5: Annualized cybercrime prevalence estimates in the U.S. from our direct survey. The banking and non-delivery categories are estimated with $N = 1,002$, all other categories with $N = 11,953$.

Source: Breen, C., Herley, C., & Redmiles, E. M. (2022, April). A large-scale measurement of cybercrime against individuals. In Proceedings of the 2022 CHI conference on human factors in computing systems (pp. 1-41).

Expected Financial Risk is Low

Cybercrime Type		Frequency (%)	Severity ($)		Expected Risk*
			Median	90th Percentile	
Bank/CC	Lost money	1.1	266	1000	$11
	Refunded	11	-	-	
Sales fraud	Non-delivery fraud	3.2	57	300	$9.60
	Non-payment fraud	0.3	100	700	$2.11
Financial fraud	Advanced fee	0.28	500	3000	$8.40
	Overpayment	0.05	88	854	$4.30
Cyber extortion		0.1	300	854	85¢

* Expected risk = frequency x 90th percentile loss to account for heavy-tailed distribution
Nationally-representative US survey data (n = 11,963) collected in July 2020.

Source: Breen, C., Herley, C., & Redmiles, E. M. (2022, April). A large-scale measurement of cybercrime against individuals. In Proceedings of the 2022 CHI conference on human factors in computing systems (pp. 1-41).

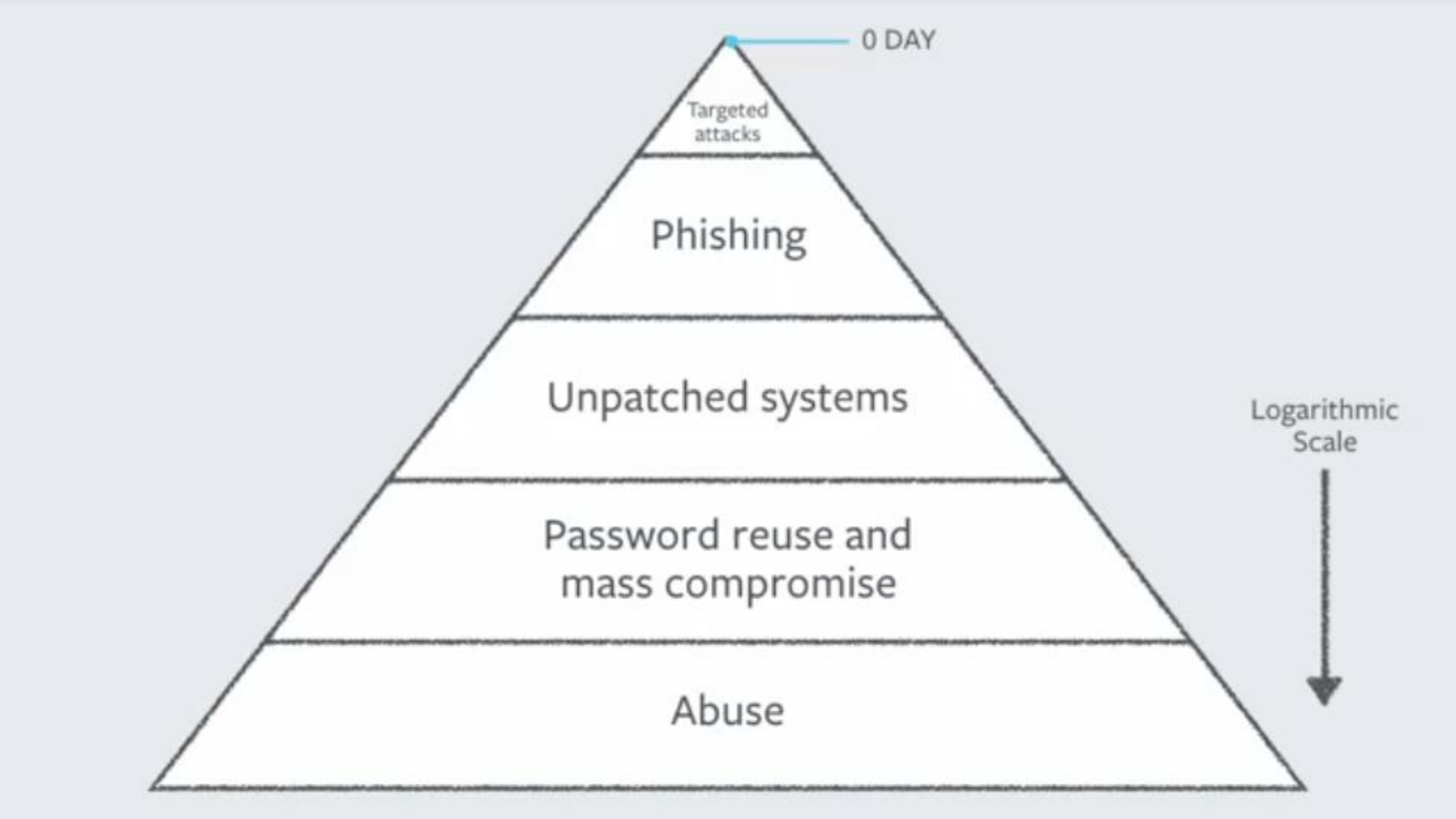
Hate, Harassment, and Abuse is much more common

Type	Abuse mechanism	2016–2018 Global	2016–2018 US-only	Pew 2017 (US-only)	DS 2016 (US-only)	ADL 2018 (US-only)	DCI 2018 (Global)
Moderate	Been exposed to unwanted explicit content	19%	16%	–	–	–	23%
	Been insulted or treated unkindly	16%	14%	–	–	–	–
	Had someone make hateful comments	16%	14%	–	–	–	–
	Been called offensive names†	14%	13%	27%	25%	41%	20%
	Been concerned because specific information about me appeared on the Internet	11%	8%	–	–	–	–
Severe	Been stalked†	7%	5%	7%	8%	18%	5%
	Had an account hacked by someone I know	6%	3%	–	–	–	
	Been sexually harassed†	6%	3%	6%	8%	18%	–
	Been harassed or bullied for a sustained period†	5%	4%	7%	5%	17%	4%
	Had someone post private photos of me to embarrass me	5%	3%	–	5%	–	3%
	Been impersonated by someone I know	5%	2%	–	6%	–	–
	Been physically threatened†	4%	2%	10%	11%	22%	5%
	Had someone I know use spyware to monitor my activities	4%	1%	–	–	–	4%
Aggregate	Been target of any online abuse	48%	35%	41%	36%	53%	40%
	Been target of any moderate online abuse	40%	32%	22%	–	–	–
	Been target of any severe online abuse	25%	13%	18%	–	37%	–

TABLE II: Frequency that participants reported experiencing hate and harassment online. We compare our results against previous surveys. We denote questions where the framing exactly matches a previous PEW survey with a dagger †. Our question framing differs from the other listed surveys, though the abuse mechanisms studied overlap.

Source: Thomas, K., Akhawe, D., Bailey, M., Boneh, D., Bursztein, E., Consolvo, S., ... & Stringhini, G. (2021, May). Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE symposium on security and privacy (SP)* (pp. 247-267). IEEE.

“Abuse is the technically correct use of the products we build, to cause harm” Alex Stamos



Is abuse a security engineering problem?

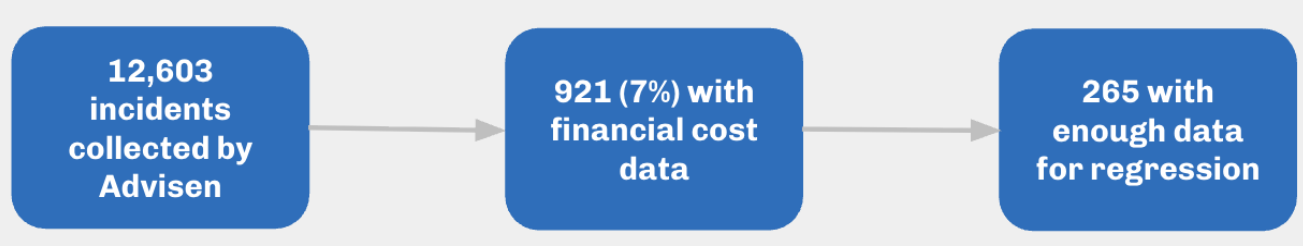
"Security engineering is about building systems to remain dependable in the face of **malice**, error and mischance."

Summary for individuals

- Most measurable losses result from fraud
  - Typically where victim is socially engineered, **not** hacked
  - Losses are relatively rare (<1% a year)
  - Size of loss is relatively small (<£2k) compared to physical damage
- However, measuring cyber harm is difficult
  - Online abuse appears to be very frequent
  - Harder to quantify the cost here, especially for systematic + targeted abuse

Cyber risk for businesses

- Advisen collect public reports of incidents
  - News reports, court files, company statements etc
- But there are major gaps in reporting
  - Not all incidents are reported
  - Rare to get £££ estimates of the cost
- Losses are "heavy tailed"



Mean financial cost	$7.8m
Median financial cost	$250k

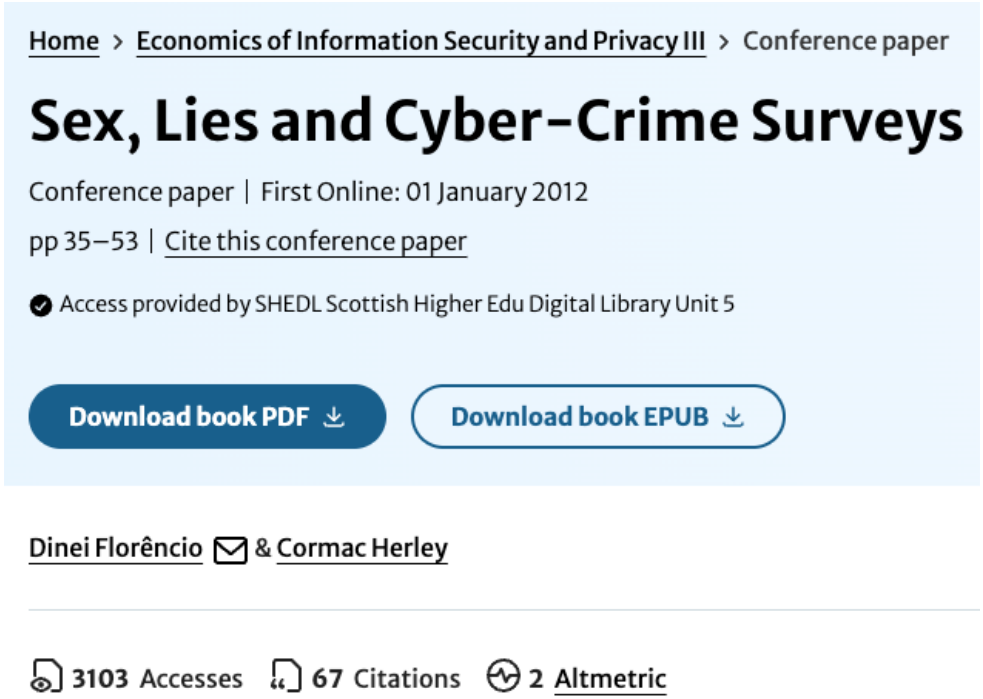
Source: Romanosky, Sasha. "Examining the costs and causes of cyber incidents." *Journal of Cybersecurity* 2, no. 2 (2016): 121-135.

Victimization surveys

Victimization surveys ask a sample of individuals or organizations which cyber incidents they have suffered in a fixed period of time.

Estimates are highly influenced by:

- Who is in the sample
- The type of incident
- Wording of the question
- Incentives to report



Home > Economics of Information Security and Privacy III > Conference paper

Sex, Lies and Cyber-Crime Surveys

Conference paper | First Online: 01 January 2012

pp 35–53 | Cite this conference paper

Access provided by SHEDL Scottish Higher Edu Digital Library Unit 5

Download book PDF Download book EPUB

Dinei Florêncio & Cormac Herley

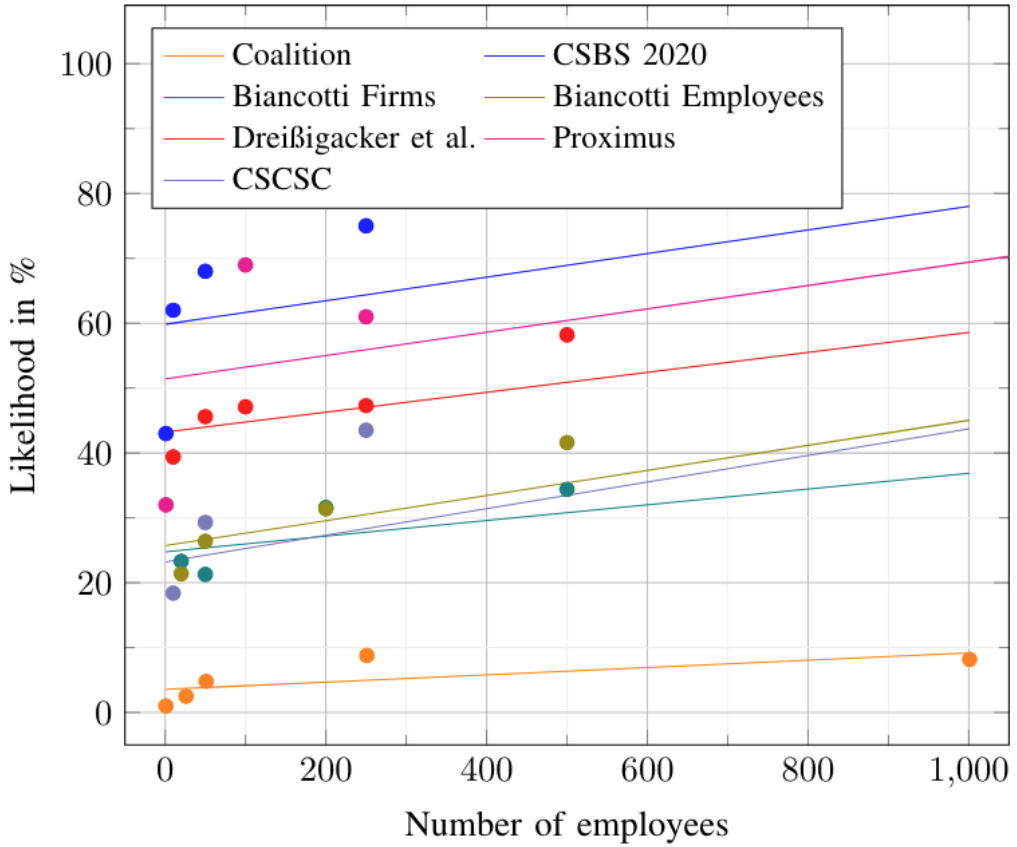
3103 Accesses 67 Citations 2 Altmetric

^ fun read if interested

More employees, more compromise

- This result holds within studies
  - Difficult to compare effect sizes across studies due to different questionnaire designs.

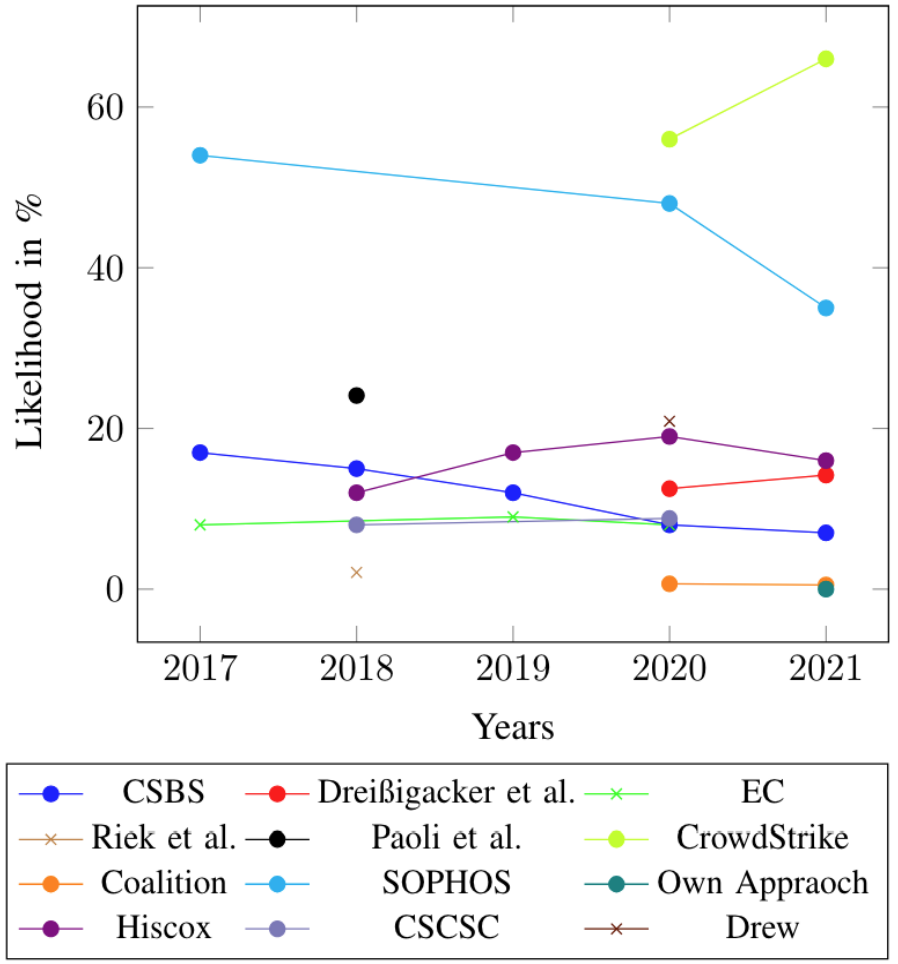
Why do bigger organizations suffer breaches more frequently?



Source: Woods, Daniel W., and Lukas Walter. "Reviewing estimates of cybercrime victimisation and cyber risk likelihood." *In 2022 IEEE European Symposium on Security and Privacy Workshops*, pp. 150-162. IEEE, 2022.

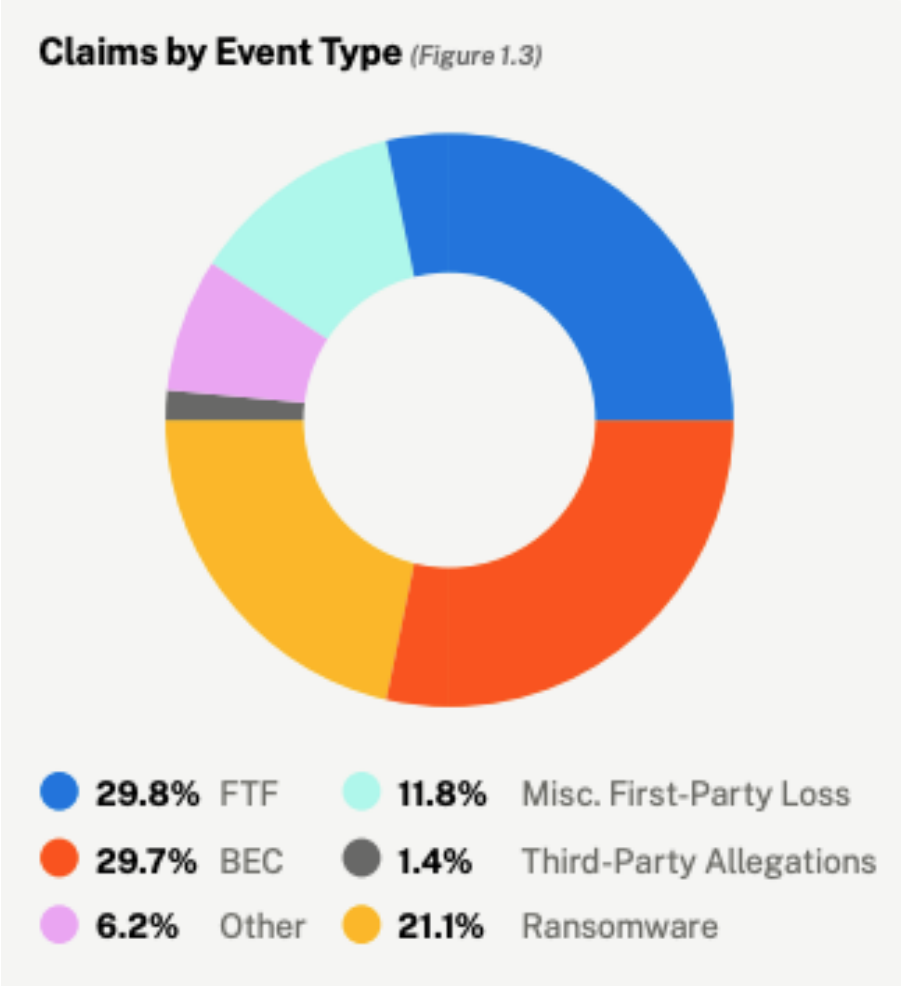
Lies, damn lies and statistics?

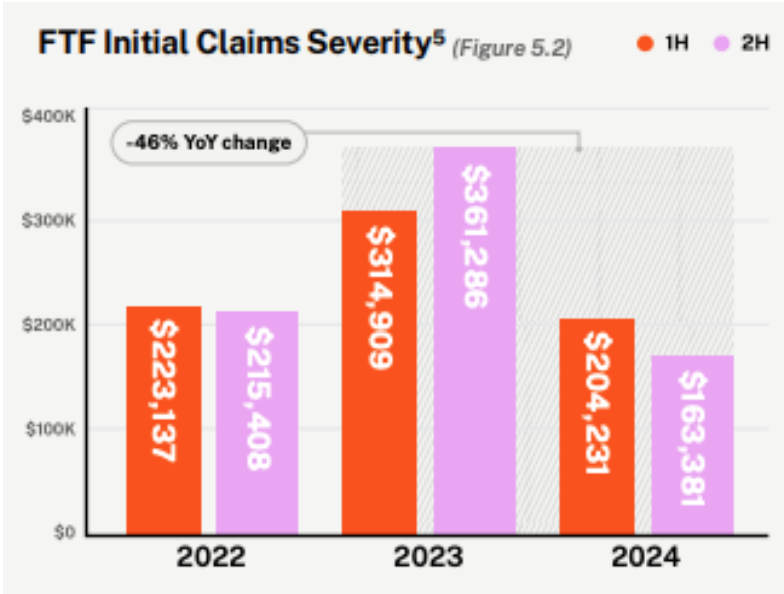
- Security vendors like Sophos and Crowdstrike estimate higher frequency
- Official crime surveys (EC/CSBS) find lower frequency
- Insurance company (Coalition) finds lower still

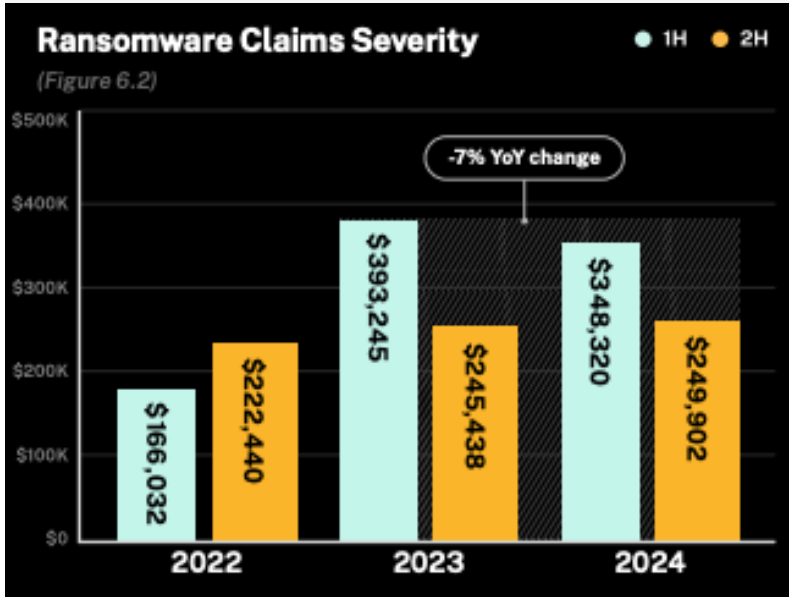


Source: Woods, Daniel W., and Lukas Walter. "Reviewing estimates of cybercrime victimisation and cyber risk likelihood." *In 2022 IEEE European Symposium on Security and Privacy Workshops*, pp. 150-162. IEEE, 2022.

Cyber insurance claims as a proxy for harm

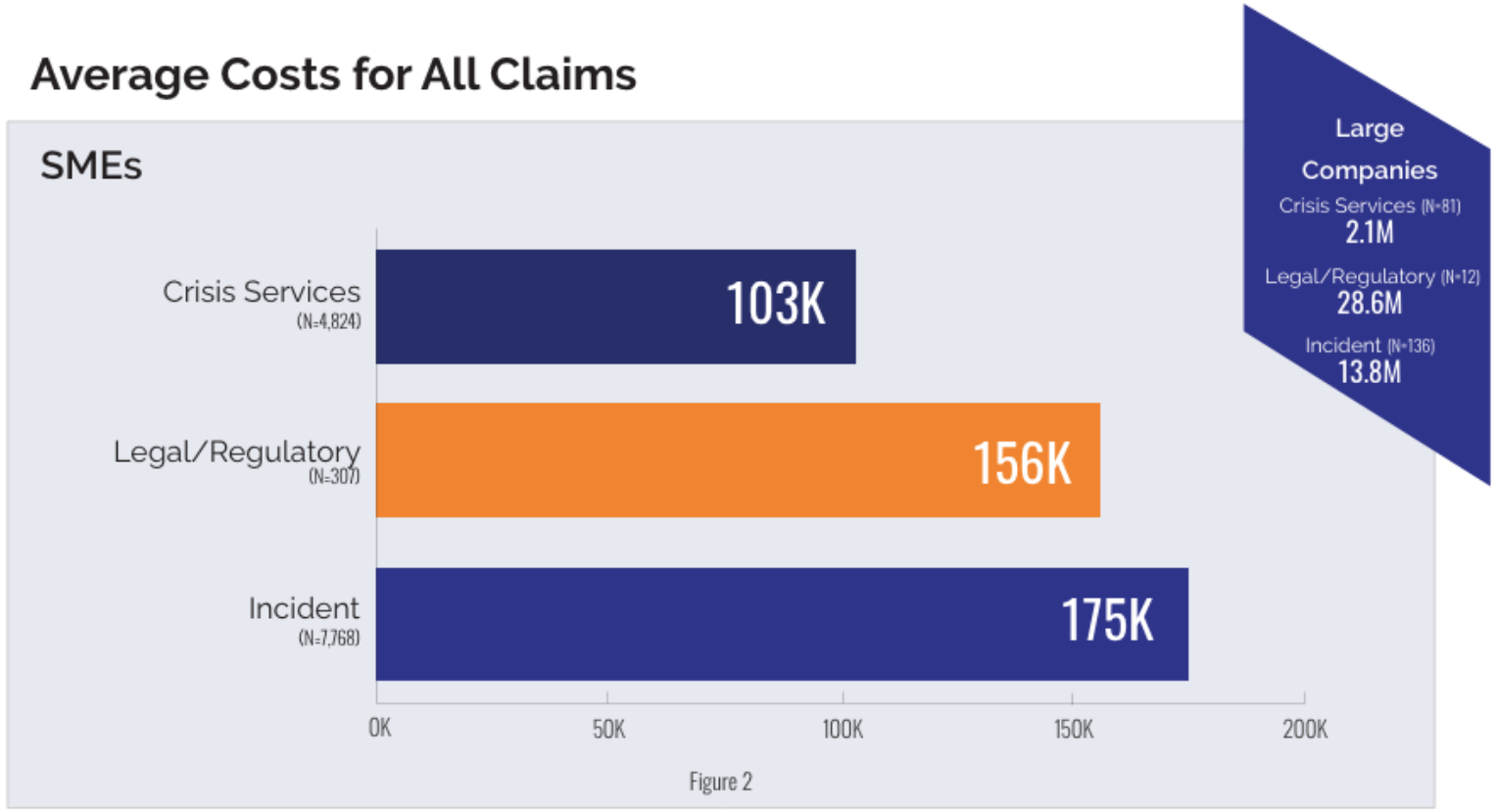






Source: Coalition. 2025 Cyber Claims Report.

Larger firms have larger losses



Based on 9,000 claims collected from multiple insurers.

Source: NetDilligence. "Cyber Claims Study: 2023 Report" (2023).

Comparing apples, oranges, and blood oranges

Incident Type	Observations (SME only)	Mean Cost
Ransomware	2,556	$334k
Business Email Compromise	1,441	$91k
Hacker	931	$76k
Theft of money	319	$53k
Staff mistake	216	$11k
All	**7,768**	**$175k**

Source: NetDilligence. "Cyber Claims Study: 2023 Report" (2023).

Summary for organizations

- The most common losses are BEC/FTF, ransomware and data breach
  - BEC/FTF are frequent, FTF costlier. Both involve emails and seek to divert funds to criminal.
  - Ransomware is less frequency but can be very costly in terms of business interruption.
  - Data breaches harder to monetize but can bring huge damages in terms of lost reputation/IP.
- Quantifying losses is difficult
  - Financial losses are more straight forward
  - Loss of IP/reputation harder
  - Harm to third parties yet harder still
- But there are weird outliers
  - Governments don't really care about financial losses
  - Some organizations have risk of corrupt insiders
  - Etc etc etc

The limits of statistics

At-risk individuals and organizations

Measurement issues (yet again)

NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history"

The loss of industrial information and intellectual property through cyber espionage constitutes the "greatest transfer of wealth in history," the nation's top cyber warrior Gen. Keith Alexander said Monday. U.S. companies lose about $250 billion per year through intellectual property theft, with another $114 billion lost due to cyber crime, a number that rises

Risk and Anxiety: A Theory of Data Breach Harms

Daniel Solove, *George Washington University Law School*
Danielle K. Citron, *Boston University School of Law*

Follow

HOWDEN

Beneath the surface - exploring the hidden costs of a cyber attack

1. Reputation damage
2. Loss of Customers and Revenue
3. Disruption of Business Operations
4. Impact on Business Partners and Stakeholders in Supply Chain
5. Legal and Regulatory Consequences

https://www.howdengroup.com/sg-en/insight/exploring-hidden-costs-cyber-attack

At-risk users face different risks

Crime statistics may not generalize to at risk users based on:

- Age
  - Children, Teens, Foster teens, Older adults
- Roles
  - Political campaigners, Teachers, Journalists, Sex workers, ER staff, NGO staff, Crowd workers
- Identity
  - LGBTQ+ people, Marginalized racial group, nationality, immigration status
- Threat profile
  - People involved with armed conflict, survivors of sexual assault/intimate partner abuse/trafficking
- Health status
  - People with an illness, cognitive impairments, visual impairments, disabilities

Source: Warford, Noel, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. "Sok: A framework for unifying at-risk user research." In 2022 IEEE Symposium on Security and Privacy (SP), pp. 2344-2360. IEEE, 2022.

(Some) organizations get even weirder

- Wants to share research widely*, but to protect student + staff data
- Network access to 100k+ people across staff, students, visiting researchers etc
  - Trust students to not phish the finance dept, but not to not access exams

- Almost never wants to share information
- Targeted by other nation states
- Network access only to individuals with security clearance
  - Additional legal rules to protect

*apart from when we don't (preliminary results, industry research, spin outs etc)

What's unique about the threat landscape for...

(or any other bank)

What's unique about the threat landscape for...

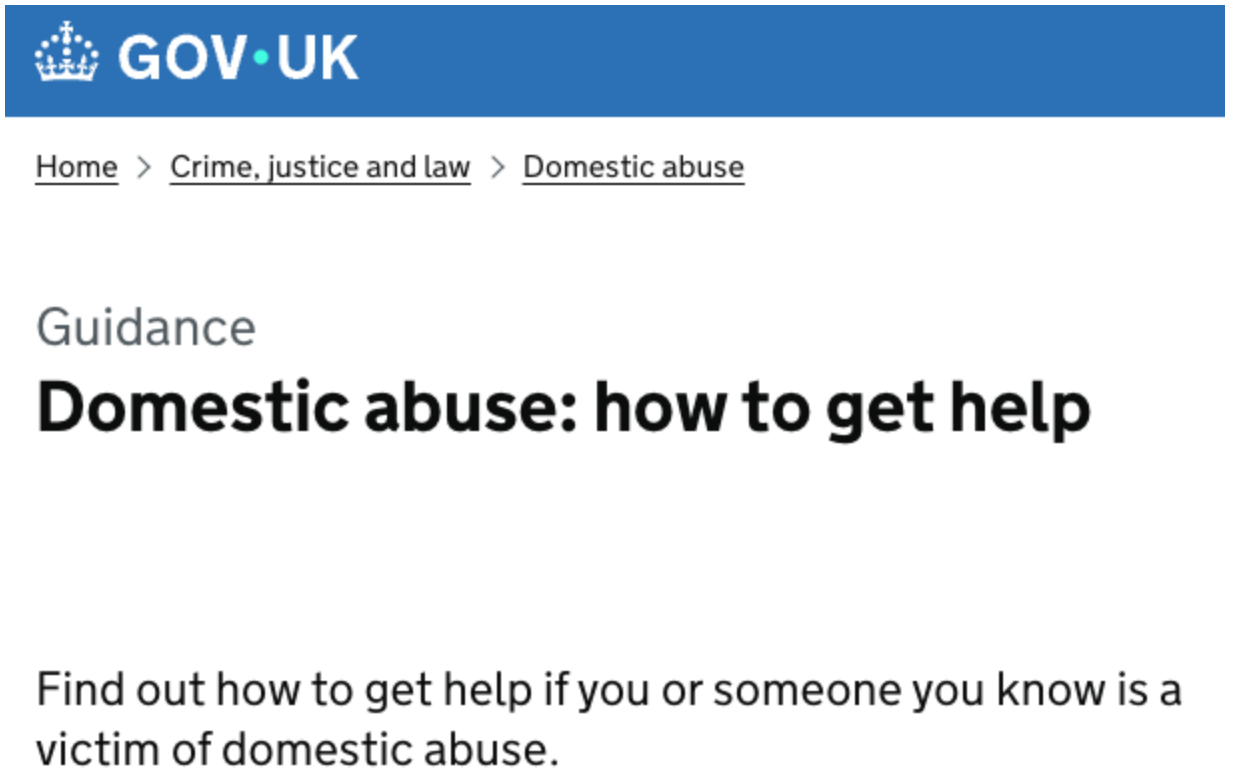
(or any other school child)

What's unique about the threat landscape for...

Law enforcement

What's unique about the threat landscape for...

Victims of domestic abuse



Exercise for next week

Think about and jot down answers to the following questions about how to prevent investment fraud.

1. **Who are the stakeholders in investment fraud?**
2. **What are the most common mechanisms to prevent investment fraud?**
3. **Do they work? Why?**
4. **What are possible mechanisms that can help prevent investment fraud**

We will discuss in the lecture next week.

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss
Investment	$6,570,639,864
Business Email Compromise	$2,770,151,146
Tech Support	$1,464,755,976
Personal Data Breach	$1,453,296,303
Non-Payment/Non-Delivery	$785,436,888
Confidence/Romance	$672,009,052
Government Impersonation	$405,624,084
Data Breach	$364,855,818
Other	$280,278,325
Employment	$264,223,271
Credit Card/Check Fraud	$199,889,841
Identity Theft	$174,354,745
Real Estate	$173,586,820