Security Engineering Problem Class 1

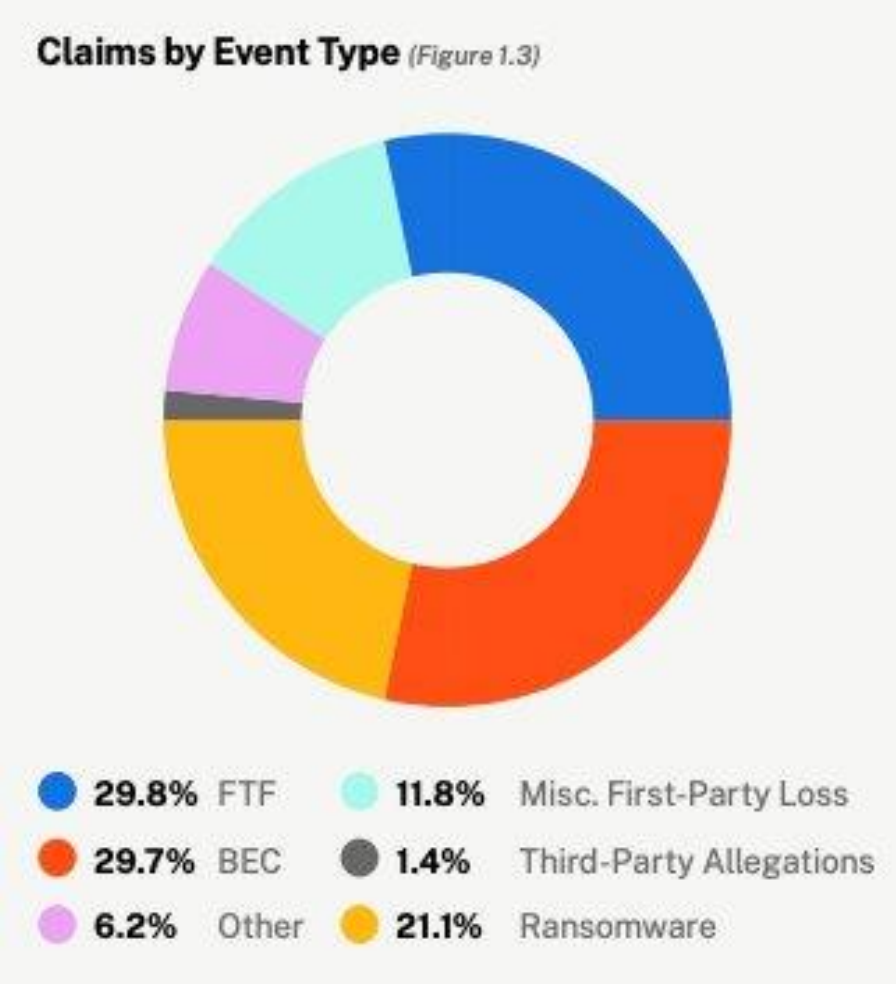
2/2/2026

Q1

- Cyber insurance claims data reveals business email compromise funds transfer fraud, ransomware and data breaches are the riskiest cyber incidents (see Lecture 1).

To what extent do the findings in the FBI's IC3 report align with the cyber insurance claims.

Q1



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

- Aligned on BEC/FTF at number 2, but diff names
- Not aligned on victims. FBI mostly individuals, insurance mostly corporations
- Ransomware much less common in FBI
  - Reporting incentives
- Companies are less likely to authorize fraud? More likely to face external "hacks"

Q2

- All large software has bugs in it, and the most powerful nation-state actors will have a collection of zero-day attacks for all of the most popular systems.
- So why is installing the latest software updates still good security advice for most people despite this?

Q2

- Threat modelling matters
  - Spooks have powerful capabilities including 0days, but don't usually impose economic harm
  - Instead they horde data at a population level
  - Crooks far more likely to use n-days and this can lead to data breaches, ransomware, infostealer infections etc

Q3

Why did ransomware evolve from automated software targeting individuals with fixed demands to targeting companies and opening up negotiations?

Q3

- Targeting individuals is harder
  - Your grandma can't pay in bitcoins
  - Many will just buy a new device instead
- Need a form of price discrimination
  - A minority of victims will pay the vast majority of rewards
  - Reports of ransom payments in the £10m's
- Negotiation model allows gangs to extract their pound of flesh

Q4

- Recall Ross Anderson’s 4-way classification of the threat actor ecosystem (crooks, spooks, geeks and the swamp). Are there actors who fall into multiple categories? Any threat actors who don’t fall into any of these?

Q4

SO MUCH OVERLAP

- Some nation states use cyber crime gangs
- Some of the swamp will buy tools from cyber crime market places
- Nation states may fund disinformation campaigns that look like the swamp
  - Russia and hybrid war
- Geeks may become or have been spooks, or become crooks!

What's unique?

- Intimate partner violence doesn't really fit into the swamp
- IP theft in industry fits awkwardly (crooks? Geeks?

Q5

What are some similarities and differences between bug bounty programs and ransomware payments?

Q5

Similarities

- Both work in offensive security looking for vulnerabilities
- Both see insecure organizations pay more, whereas secure orgs avoid paying

Differences

- Legality
- Operational impact
  - Ransomware causes data leaks + outages
- Relative power of organizations vs researchers
- Ransomware can be nasty like targeting healthcare

Q6

Was the IC’s move to multi-level security for intelligence stored in computer systems more successful in protecting information than the equivalent physical system? What kind of security violations are possible despite MAC?

Q6

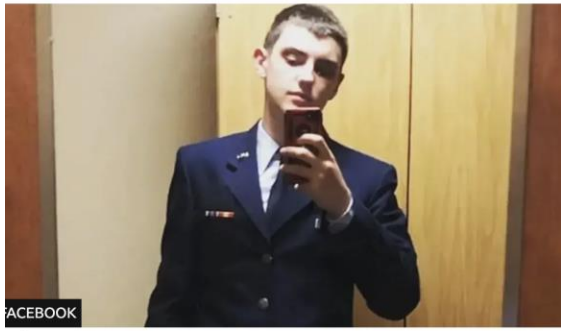
Most of the leaks we've heard about have not violated multi-level security as enforced by computer systems

Authorized with top secret clearance

Jack Teixeira: What we know about Pentagon leaks suspect

27 April 2023

Pentagon leaks



Jack Teixeira in a photo posted on social media

Antoinette Radford and Chloe Kim

BBC News

Q7

Why is the concept of “trusted computing” particularly important in power metering situations? How are the associated security assumptions supported by periodic physical inspections of the meter?

Q7

- The adversary has local access and incentives to alter the meter to get free energy
- Physical inspections help see if tamper resistant seal has been broken

Q8

Why is the optimal amount of card not present fraud non-zero? Who benefits from the current liability regime for card not present fraud, and who shoulders the cost?

Q8

- Diminishing Returns on Prevention: Achieving zero fraud would require security measures so draconian (e.g., constant identity verification, frequent transaction blocks) that they would "kill" the user experience.
- Cost of false positives: If a bank or merchant sets fraud detection filters too high, they begin rejecting legitimate customers. The lost revenue and damaged brand loyalty from these "false declines" are often more expensive than occasionally absorbing a fraudulent transaction.
- Liability Beneficiaries: Consumers benefit most from the current regime. Card holders don't usually have to pay for fraud, even when they were sloppy with details
- Cost Bearers: Merchants shoulder the primary burden. In CNP transactions, if a fraudster uses a stolen card, the merchant typically loses both the product and the revenue via a "chargeback," while also paying administrative fees to the bank.

READ IT: https://www.bitsaboutmoney.com/archive/optimal-amount-of-fraud/

Q9

Many banking apps now use on-device biometrics (like finger prints) to authenticate users. How could a criminal log into the victim’s account using the only using the criminal’s finger print? (There are at least 2 examples, with varying digress of likelihood)

Q9

1. Unlikely but physical kidnap could be a way, evidence of this in Colombia and even in London
2. Another option is finding a "collision". Some people have the same finger print reading as you
3. Much more likely is registering the app on a new phone, which will attest the finger print is valid
    - Mitigations are to force an approval on the old device to register on a new one

Q10

Historically, joint bank accounts required a signature from both account owners on both cheques and bank transfer requests. What are the barriers to adopting a similar separation of duties in online banking? Which cybercrimes would this help prevent?

Q10

- Friction to get approvals from both sides for a transaction, could lead to bad situations for customers who need to move money in a pinch
- However, it would reduce incidence of all kinds of push payment fraud as it forces a second party to intervene
  - Investment fraud if the 2nd person is more risk averse/sensible, romance fraud a lot

Q11

Microsoft issued patches for 1,246 Common Vulnerabilities and Exposures (CVEs) across its products in 2025. What economic ideas help explain why individuals and businesses continue to use Microsoft products?

Q11

LOCK IN

- Windows was first to market and quickly established dominance, especially in corporate
- Companies find it hard to migrate many accounts at once, especially as there are interdependencies between diff solutions
  - Mostly new tech companies who use Apple, Gsuite etc
- Users like the excel shortcuts, the Windows layout etc

Q12

Antivirus software is sometimes considered a “market for lemons”. To what extent is this true, and is it down to hidden information, hidden action, or both?

Q12

Hidden info

- Hard to evaluate the quality of software that detects malicious software, unless you have a big sample
  - But even then, maybe they're good at detecting known malware samples, what about new samples/techniques
  - See MITRE EVALUATIONS

Hidden action

- To a lesser extent, you don't know how good they'll be at investing in the product moving forward

Q13

- Provide an example of a cyber attack technique that exploits each of: (1) skill-based behaviour; (2) rule-based behaviour; and (3) knowledge based-behaviour.
- Can you think of an example that exploits multiple?

Q13

1. Skills: Get user to click on a link with a malicious URL that looks benign
2. Rules: Get malware listed as top result in Google and impersonate as legitimate software. User searches google, finds app, installs your malware..
    - Following habituated rule for installing new software
    - I've heard of this with malicious Teams and Bloomberg apps
3. Knowledge: Contact user and convince them you're part of the IT teams and need access to their machine to do some checks, getting them to install a remote access tool.

3 could be combined with 1 if you make first contact via a spoofed email.

Q14

Imagine that you are designing a spear-phishing attack designed to scam Edinburgh students out of money. How would you do it, who (or what) would you impersonate, how would you extract the money, and could you use Prospect Theory to increase your chances? Are there any other social-psychology tricks that might help?