Security Engineering

INFR11208 (UG4) // INFR11228 (MSc)



Daniel W. Woods

Email: daniel.woods@ed.ac.uk

We cover three related concepts

- ✔ **Assurance:** whether a system will work, and how you're sure of this.
- ✔ **Sustainability:** how long will it work for?
- **Compliance:** how you can satisfy other people of this.

+ today **law and regulation** --- what you're required to do

Goal is to understand the security requirements outside your control.

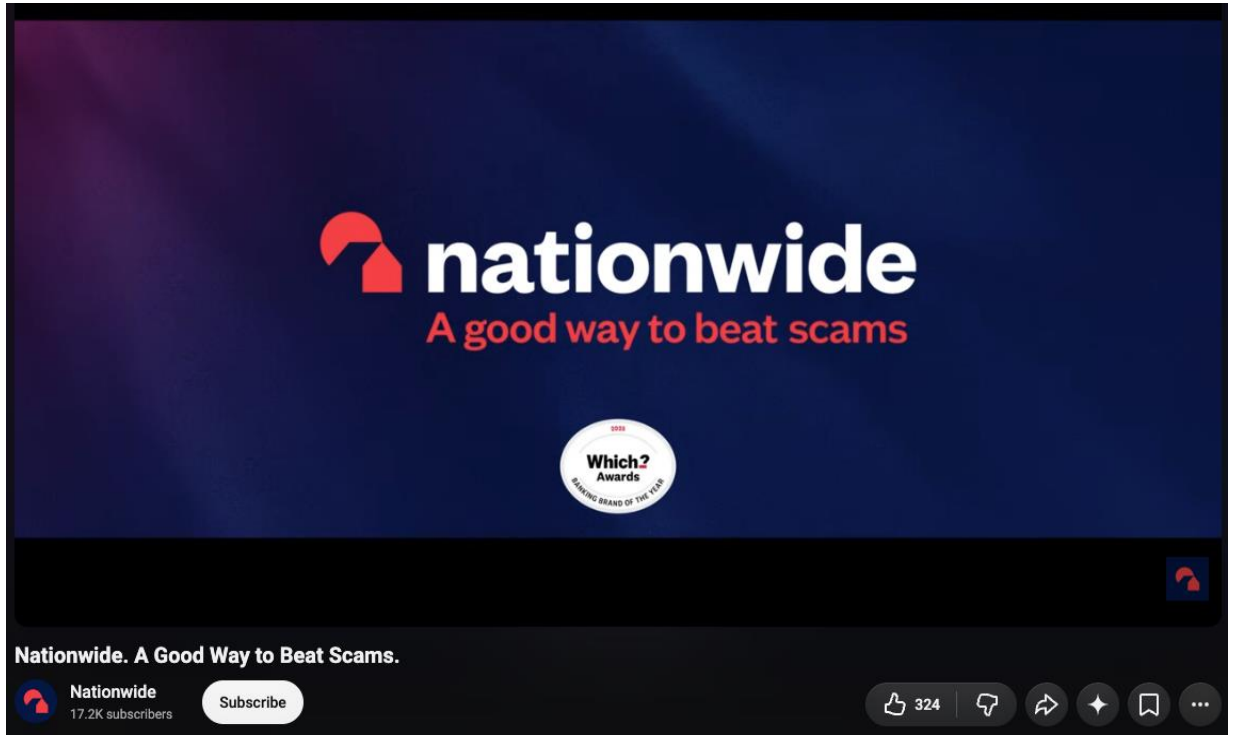
Compliance: how you can **convince others** that your system is secure.
(or what they force you to implement)

Who do you need to convince? And how?

- Who you need to convince
  - Customers may require security to do business
    - Individuals for B2C
    - Other organizations for B2B
  - Financial institutions
    - Payment Card Industry to process credit cards
    - Insurers to buy a policy
    - Investors or banks to raise capital
  - Regulators to avoid penalties, courts to avoid litigation
- How you convince them
  - Fill out questionnaires
  - External scans, pen tests etc
  - Certify to standards
  - Sign a contract promising to indemnify them
  - Legal case if you're sued or investigated

No clear requirements from consumers

- Consumers lack market power + sophistication
  - None say "implement X or we won't use you"
- Instead compliance is voluntary or via regulation
  - Voluntary --> marketing
    - See Apple on privacy
    - Some banks on security
      - Nationwide ad
  - Mandatory
    - Government certifications
      - Cyber Essentials



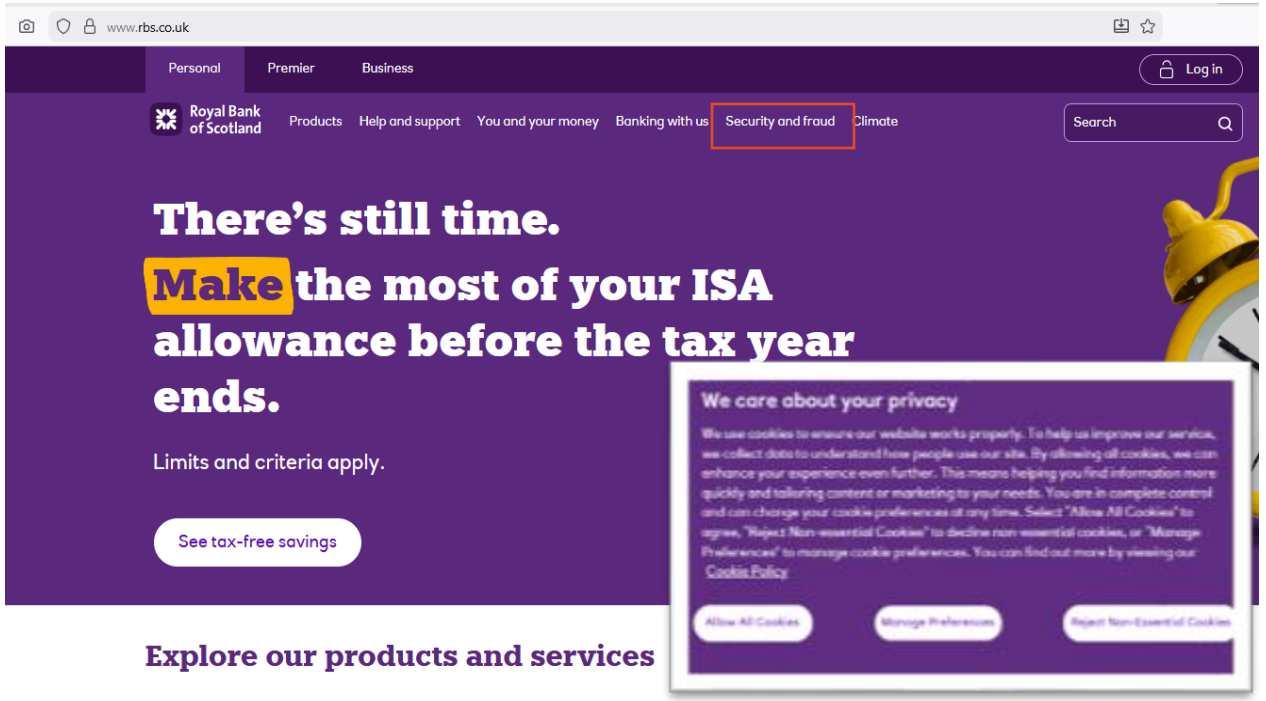
https://www.youtube.com/watch?v=jp_0Psoj6CU

Convincing B2C customers





How banks used to convince customers they could reliably store money



Do bank websites communicate they're secure digitally?

Certifications

Idea

- Investigator "certifies" the vendor's security to a given standard
- Consumers trust the certificate instead of the vendor

The Problem is Economics

- **Adverse selection**
  - Untrustworthy actors may be more motivated to seek certificate
    - See TRUSTe web certificates
- **Forum shopping**
  - Race-to-the-bottom as the laxest certifier wins all the business
    - See also Common Criteria



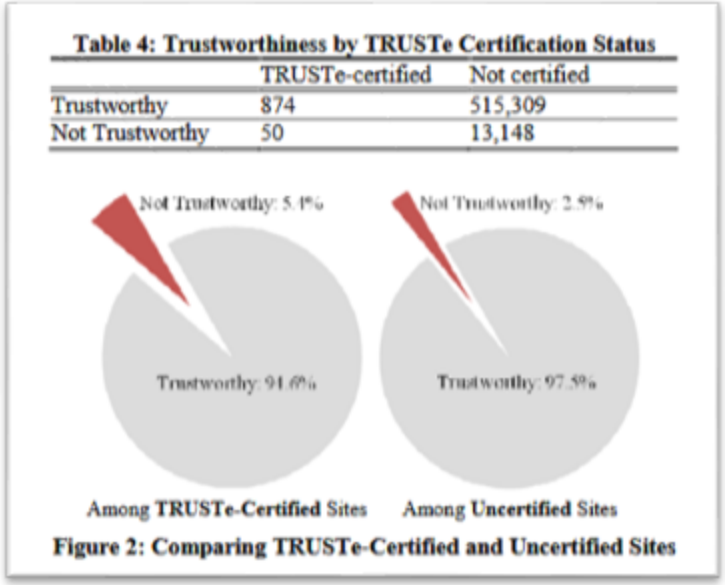


Table 4: Trustworthiness by TRUSTe Certification Status

	TRUSTe-certified	Not certified
Trustworthy	874	515,309
Not Trustworthy	50	13,148

Figure 2: Comparing TRUSTe-Certified and Uncertified Sites

Source: Edelman, Benjamin. "Adverse selection in online" trust" certifications." In *Proceedings of the 11th International Conference on Electronic Commerce*, pp. 205-212. 2009.

IoT Labelling

- Response to dire state of IoT security
- Idea is to visualize security + privacy to consumers
  - Active area of research
- People do value security, but price dominates



Security & Privacy Overview

Smart Security Camera, NS200
Firmware version 2.5.1: updated on: 6/15/2019
The device was manufactured in: United States

Casa

Security Mechanisms

Security updates	Automatic (available untill 1/1/2022)
Access control	Password, Factory default, User-changeable, Multiple user accounts are allowed

Data Practices

	Video	Audio
Sensor data collection		
Purpose	Providing device functions, research	Providing device functions, research
Data stored on device	Identified	Identified
Data stored on cloud	Identified, Option to delete	Identified, Option to delete
Shared with	Manufacturer	Manufacturer
Sold to	Not sold	Not sold

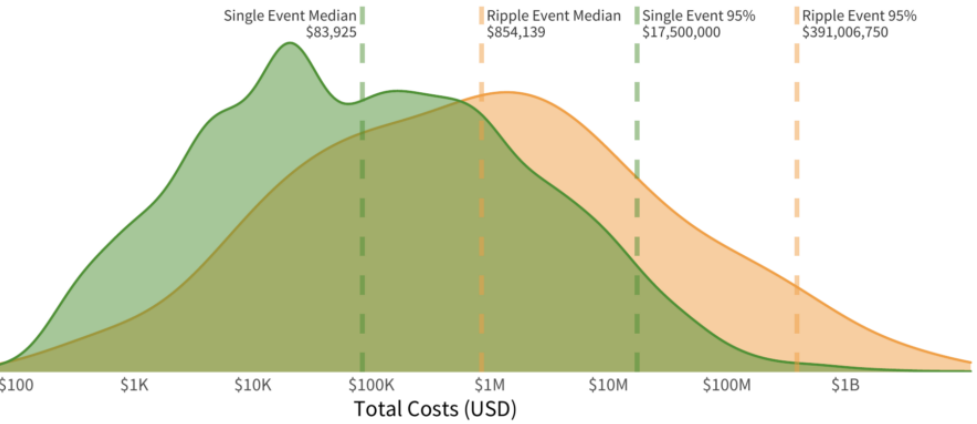
Other collected data: Presence, Temperature, Carbon monoxide, Usage information, User-entered information

More Information

Detailed Security & Privacy Label:
www.iotsecurityprivacy.org/labels

Privacy Policy:
www.NS200.example.com/privacypolicy

Why B2B customers need to be convinced



"Ripples are those cyber incidents which have effects (typically financial, legal, or in the form of legal entanglements) beyond the firm initially compromised."

Source: https://www.cyentia.com/ripple-effect-in-breaches-2021

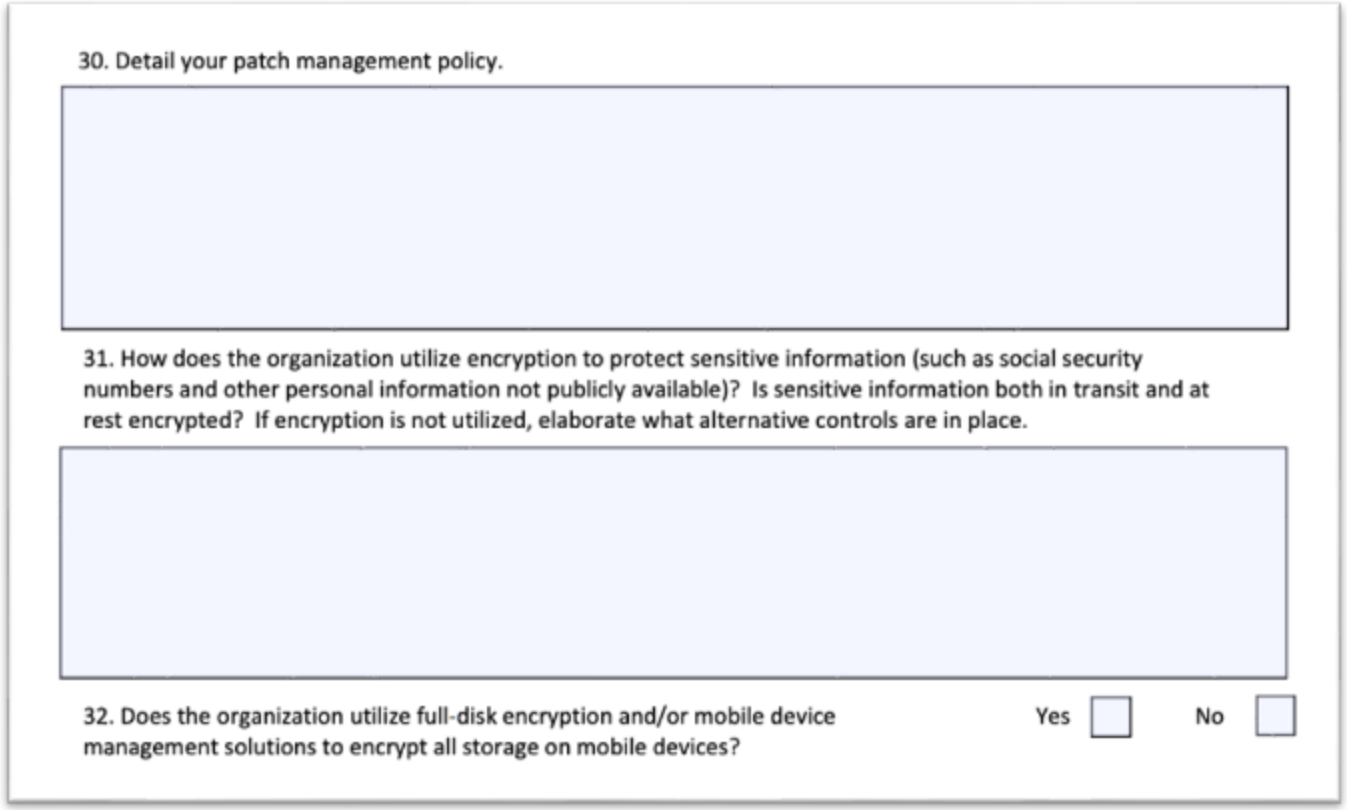


Source: https://cyberresilience.com/blog/2024-cyber-risk-year-in-review/



Types of third-party risk assessment

- Questionnaires
  - Ask **anything**, get written response
    - Useful in a dispute
  - Answers are only as reliable as their governance
- External scans
  - Assess external infrastructure and threat intel
  - Ground truth, but does it matter?
  - Business model considerations
- External verification
  - Pen tests, audits (SOC 2)
- Certifications
  - ISO 27001, CMMC etc
- Cyber insurance
  - Underwriting standards + financial recovery



30. Detail your patch management policy.

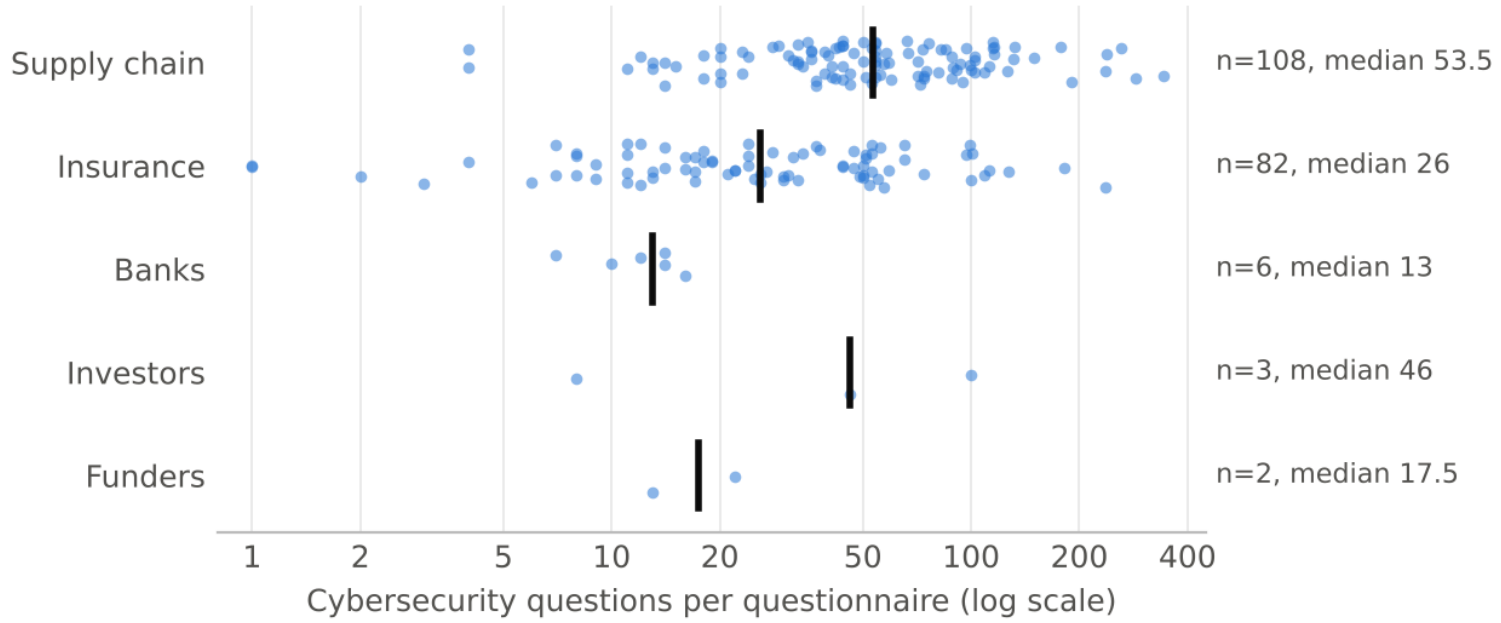
31. How does the organization utilize encryption to protect sensitive information (such as social security numbers and other personal information not publicly available)? Is sensitive information both in transit and at rest encrypted? If encryption is not utilized, elaborate what alternative controls are in place.

32. Does the organization utilize full-disk encryption and/or mobile device management solutions to encrypt all storage on mobile devices? Yes ☐ No ☐

Source: https://www.gny.com/sites/default/files/file/2023-08/third_party_questionnaire.pdf

Questionnaires by third-party

- If you can't answer right, you don't get:
  - The contract
  - The insurance policy
  - The loan/investment
- The problem is answers are subjective and the devil is in the details
- False answers have legal implications
  - Avoid insurance
  - Misrepresentation in contracts



Source: Reem Alshahrani's MSc thesis

External scans

- Use an outside in scan to measure the vendor/policyholder's security
  - Technical data
  - But only of external perimeter
- Less clear security can be mapped onto a 1 dimensional scale
  - See inconsistencies with risk scoring firms
  - See lack of academic progress with measuring security [1]
- Business model quirks
  - Misattribution of assets
  - Conflict of interest in consulting

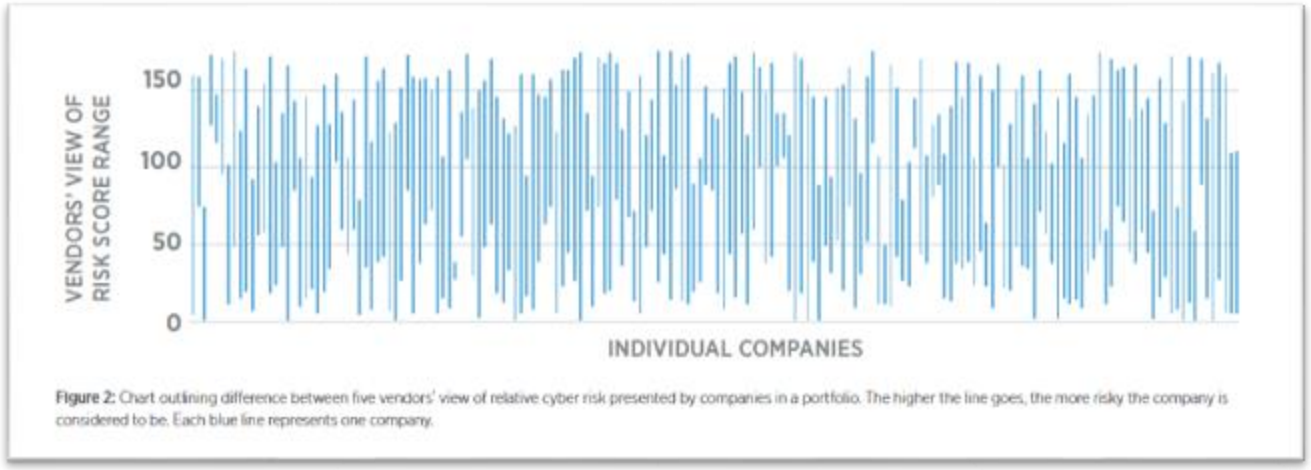


Figure 2: Chart outlining difference between five vendors' view of relative cyber risk presented by companies in a portfolio. The higher the line goes, the more risky the company is considered to be. Each blue line represents one company.

Source: www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/cyber-iq-report-can-scanning-technologies-predict-claims.pdf

different scoring vendors disagree widely on the same companies

[1] Woods, Daniel W., and Rainer Böhme. "SoK: Quantifying cyber risk." In *2021 IEEE Symposium on Security and Privacy (SP)*, pp. 211-228. IEEE, 2021.

External assessment

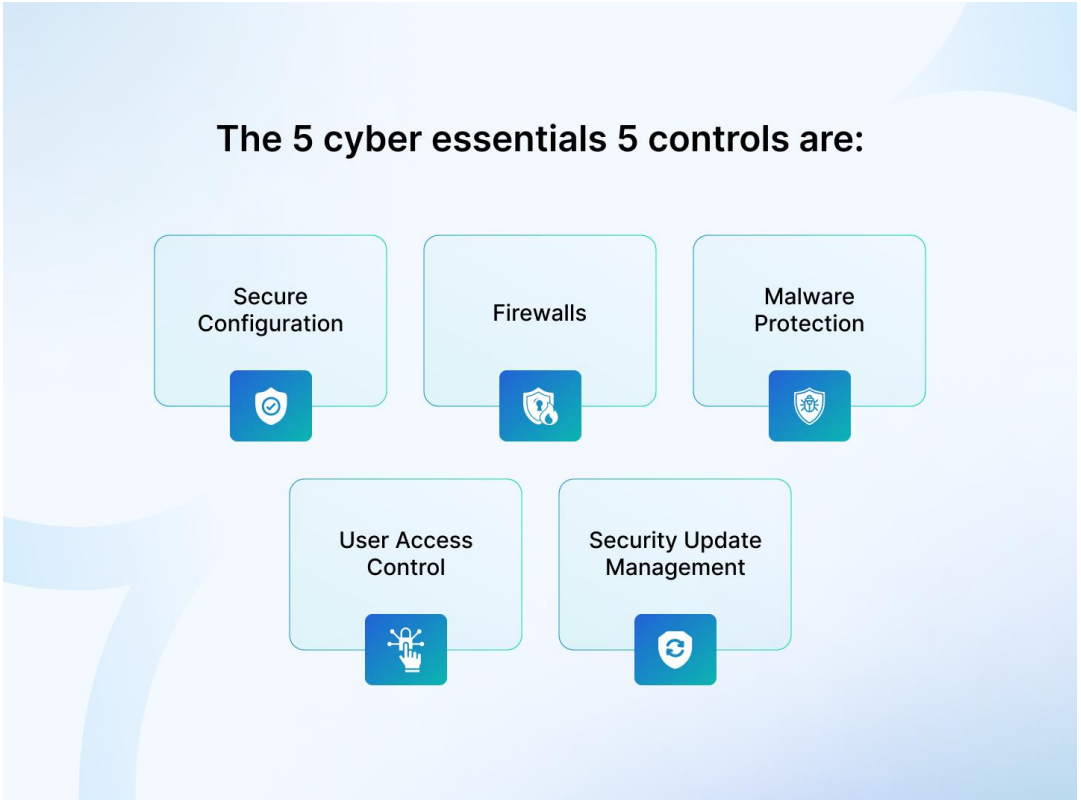
- Pen test and fix
- Scope ranges broadly
  - Some are full network + onsite
  - Others are web apps only
- Operations
  - Annual, find as many in scope vulns as possible
  - Did you fix what the attacker will exploit?
  - Expensive because it requires human
    - But new AI pen testing frameworks exist
      - ARTEX causing chaos atm
        - https://www.ibtimes.co.uk/fbi-warns-ai-artex-cyberattacks-1833001
- Forum shopping!!!

"Penetration testers described … how vulnerabilities emerge from properties of the existing built digital environments. This includes systems that are forgotten or lack ongoing maintenance. Moreover, penetration testers highlighted that although the testing is often predicated on planned methodologies, often they resort to serendipitous practices such as improvisation."

Source: De Paoli, Stefano, and Jason Johnstone. "A qualitative study of penetration testers and what they can tell us about information security in organisations." *Information Technology & People* 38, no. 1 (2025): 380-398.

Frameworks and checklists

- Many examples
  - UK Cyber Essentials
  - SANS Top 20 Controls
  - NIST Cybersecurity Framework
- But does checking off quick wins lead to better security?
- May help evidence you followed best practice



Compliance to win business

- Requirements vary by industry
  - Governments require suppliers to certify to InfoSec standards
    - UK to Cyber Essentials
    - USA to FedRamp
    - DoD to CMMC
  - Private sector may also require vendors to get certified
  - SOC2 audit common for data security
- Economic pressures
  - Expensive, but motivated by sales
  - External auditors "maintain" standards
    - Forum shopping again



Source: https://secureframe.com/hub/soc-2/audit-cost

Finance industry

- PCI DSS requires merchants to implement security mechanisms, audit, and fines them if they fail
  - See Lecture 5
- Banks may ask questions before a loan or as part of M&A
- Insurers underwrite before selling cyber insurance
  - More on Friday

PCI DSS Compliance Costs by Level & Transaction Volume

PCI DSS Level	Annual Card Transactions	Estimated Compliance Costs
Level 1	Over 6 million	$100,000 to 200,000
Level 2	1 to 6 million	$50,000 to 100,000
Level 3	20,000 to 1 million	$25,000 to 50,0000
Level 4	Fewer than 20,000	Under $25,000

Source: https://smartdev.com/fr/how-much-does-it-cost-to-develop-custom-gpt-solutions-for-global-fintech-companies-with-pci-dss-compliance/

Regulation: what you're required to do by law.

Government Regulation

- No blanket law
  - Usually sector and asset specific
- Tends to be risk-based, see EU GDPR Article 32
    - "taking into account the state of the art… the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the ris"
- Government reluctant to issue blanket rules
  - Industry pressure? Or rational because security is contextual?
  - By contrast, PCI DSS far more prescriptive
- IoT is an exception, largely because of woeful security

Subset of Regulatory Compliance in the EU/UK

Law / Regulation	Scope
NIS2 Directive (+ UK equiv)	18 "Essential" & "Important" sectors (Energy, Health, Digital Infra) must implement risk management and supply chain security.
DORA	Financial sector (Banks, Crypto, Insurance) implement strict requirements.
Cyber Resilience Act	Hardware & Software products sold in EU required to implement Secure by Default.
GDPR (+ UK equiv)	Any entity handling personal data implements "Appropriate technical and organizational measures".
AI Act	High-risk AI systems (HR, Credit, Health) must implement cybersecurity resilience for AI models.
UK Product Security and Telecomms Infrastructure Act 2022	Consumer IoT devices must implement basic measures like no default passwords.

*All require "security", but we're not going to track what is required by each in this course.

Subset of Regulatory Compliance in the US

Law / Regulation	Scope
CMMC 2.0	Defense & Critical Infra: 100k's of contractors (CMMC) and 16 critical sectors (CIRCIA).
NY DFS Part 500 (similar to DORA in the EU)	Financial Sector: Any entity licensed in NY (Banks, Insurance, Crypto).
State level data privacy laws (similar to EU GDPR)	Personal Data: Any business meeting size/data thresholds in CA.
Proposed State AI Laws (similar to EU AI Act)	High-Risk AI: Varies by state
IoT Cybersecurity Improvement Act (similar to UK PSTI) and California SB-327	Consumer & Govt IoT: Connected devices and "Smart" tech.

*All require "security", but we're not going to track what is required by each in this course.

Regulatory capture (Stigler)

- Regulators often end up run by ‘their’ industries
  - The expertise comes from there!
    - FCA, MHRA
- Sometimes politicians design regulators to be weak
  - ICO
- Sometimes there’s arbitrage too
  - Ireland’s data protection commissioner
- Sometimes there’s deception
  - Security standards weakened/with backdoors for intel access
    - Dual_EC_DRBG

Does compliance decrease risk?

- What determines compellence power
  - Governments, B2B customers, and payment card industry have the most power
  - Insurers and banks are weak due to competition, B2C consumers due to a lack of knowledge/attention
- How to ensure requirements are effective
  - Reducing risk vs jumping through hoops
  - Need engineers to help draft requirements
- Compliance is better than nothing?
  - Endlessly discussed



Regulating beyond ex-ante security

Ex-post regulation of incident response

- Liability
- Mandatory data breach notification to consumers
  - First in California in 2003
  - Truly could not have been done by B2B relationships
- Mandatory notification of authorities
  - Ransomware needs to be reported in Australia
- Direct support for victims
  - FBI helped Colonial Pipeline get some of their crypto payments back
- Ransomware payment sanctions and bans
  - UK proposed ban on public authorities + CNI



Law partly determines cost of security failures

- Set costs for security failures
  - Fines and investigations (tiny)
  - Create liability regimes by legislation
- Decide who is to blame
  - The hospital who didn't patch in time?
  - The vendor who released insecure software?
- Mandatory data breach response inadvertently added costs to breaches
  - End up dominating costs

Liability

Liability (from courts)

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



[Cybersecurity as Realpolitik (27:08)]

Liability (from contract)

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

Usually capped at contract fees.



[Cyber Warranties: Market Fix or Marketing Trick?]

Who should be held liable?

- Ransomware incident that exploited buffer overflow in VPN
- Ransomware incident that exploited VPN via stolen password
- Change Healthcare where half of US healthcare industry can't process payments bc vendor suffered ransomware
- Individuals, bank, or government for Govt impersonation fraud

There are exceptions though...

- EU Product Liability Directive will cover software
  - Product liability regimes were developed to address manufacturing defects
- If financial fraud results from third-party's BEC, then the third-party is often liable for the loss
- Consumers can (with variable success) sue businesses for losing their personal data
- Shareholders can sue the company for securities fraud
  - Matt Levine's favourite theory that corporate misstatements can be reframed as fraud in a lawsuit
  - See SolarWinds

More liability for consumer losses

- Issuing bank liable for **unauthorised** credit card transactions
- Ecommerce platforms set rules (e.g. seller liable for faulty goods)
- Since 2024, UK extends a similar rule to Advanced Push Payment (APP) Fraud
  - Covers **authorised** transfers
  - For individuals and micro businesses (<10 employees and <£2m revs)
  - Sending and recipient bank share liability 50-50 up to £85k
  - Exceptions for gross negligence, intl payments, civil disputes etc
    - Ignoring explicit, tailored scam warnings from their bank
    - Failing to report the fraud promptly, or refusing to consent to police reporting

Principles in assigning liability

- **Least Cost Avoider:** Who controls whether the loss happens?
  - Assign liability to them!
  - How much control do users have given what we know about psychology?
- **Deep pockets:** Who can actually afford to pay?
- **Practicality:** Which rule is cheapest to apply

Law enforcement (could be a whole course)

- Cybercrime takedowns
  - Botnets
  - Ransomware infrastructure
- Arrest warrants
  - For ransomware actors
  - For foreign intelligence operatives





Summary of Compliance and Regulation

Who	Lever	Enforced by	Efficacy
B2C consumers	Buy or don't; labels and marketing	Market choice	**None**
B2B customers	Questionnaires, scans, pen tests, SOC 2 / ISO 27001, contract terms	Loss of the contract	**High**
Payment card	PCI DSS	Fines , access to card processing	**Very High**
Insurers	Underwriting questions, scans, pricing	Decline cover or raise premium	**Medium**
Banks and investors	Due diligence questionnaires	Withhold capital	**Weak**
Regulators	NIS2, DORA, GDPR, CMMC, etc.	Fines, investigations, licences	**High**
Courts	Negligence, class actions, securities suits	Damages, fines + penalties	**High**

How effective is each?