Security Engineering

INFR11208 (UG4) // NFR11228 (MSc)



Daniel W. Woods

Email: daniel.woods@ed.ac.uk

Chapter 8, Security Engineering



https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3-ch28.pdf

We'll cover three related concepts

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

Assurance: whether a system is secure, and **how you're sure of this**.

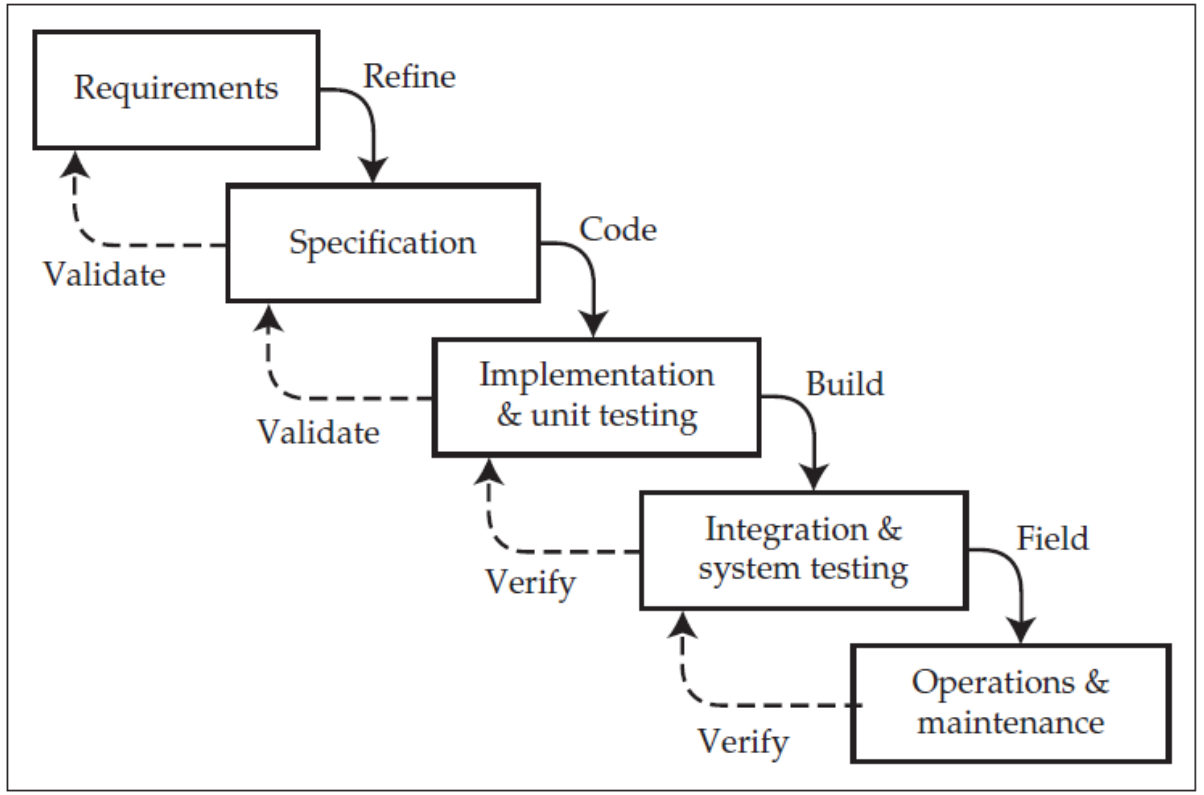
Routes to assurance

- Building systems
  - Formal methods
  - Testing
  - Bug reports
- Operating systems
  - Monitoring + measuring
    - SOC, ASM, Vuln scanning, TPRM, phishing simulation etc
  - Pen testing/red teaming
  - Standards, checklists etc

Building Assurance

Waterfall & Formal Methods

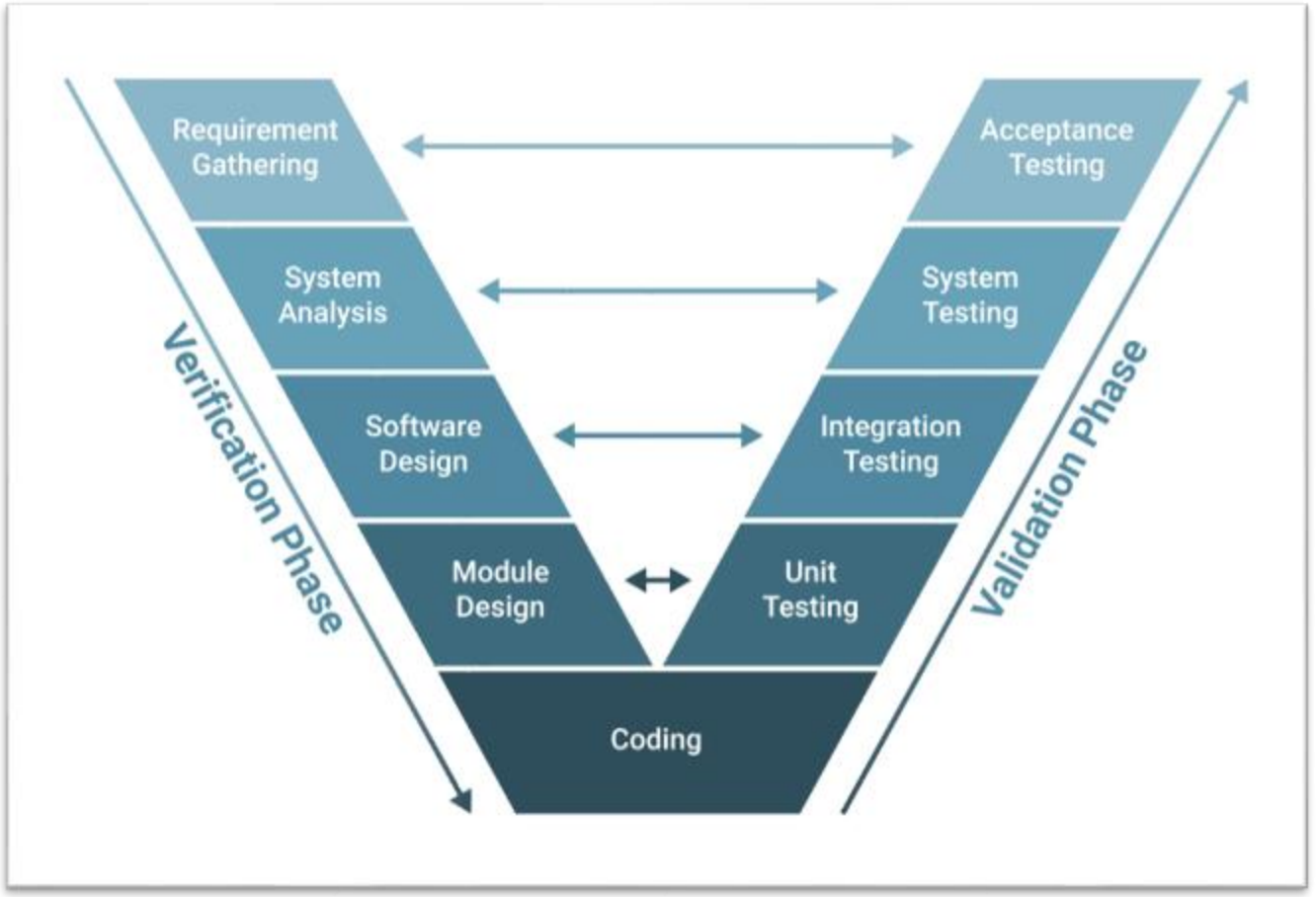
- Both share heavy investment in initial design
- Formally represent design and verify security properties
  - Focus on specification
- Used in safety and military systems
  - Also for security protocols (TLS)



Testing

- Unit testing for reliability, fuzzing for security
- Static/dynamic analysis
- Internal security audits
- LLM code reviews??
  - See Anthropic
- Finally, user testing

What goes wrong??

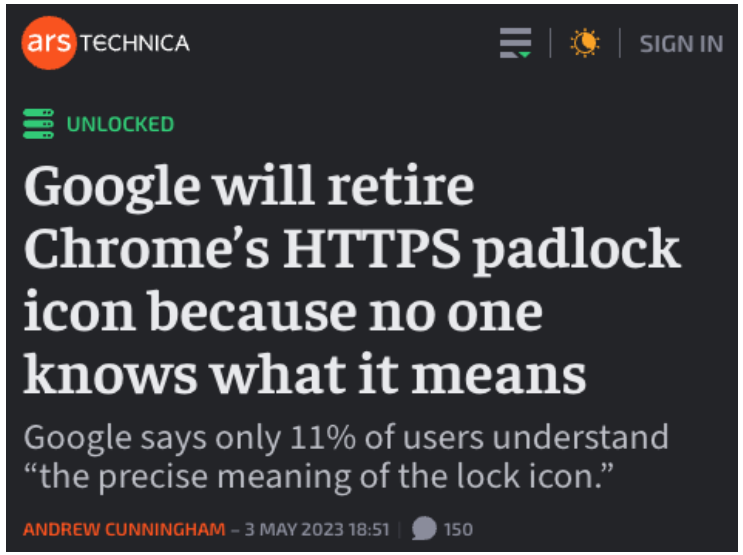


Verification and validation model

User Testing







"Our research in 2021 showed that **only 11% of study participants correctly understood the precise meaning of the lock icon**. This misunderstanding is not harmless — nearly all phishing sites use HTTPS, and therefore also display the lock icon."

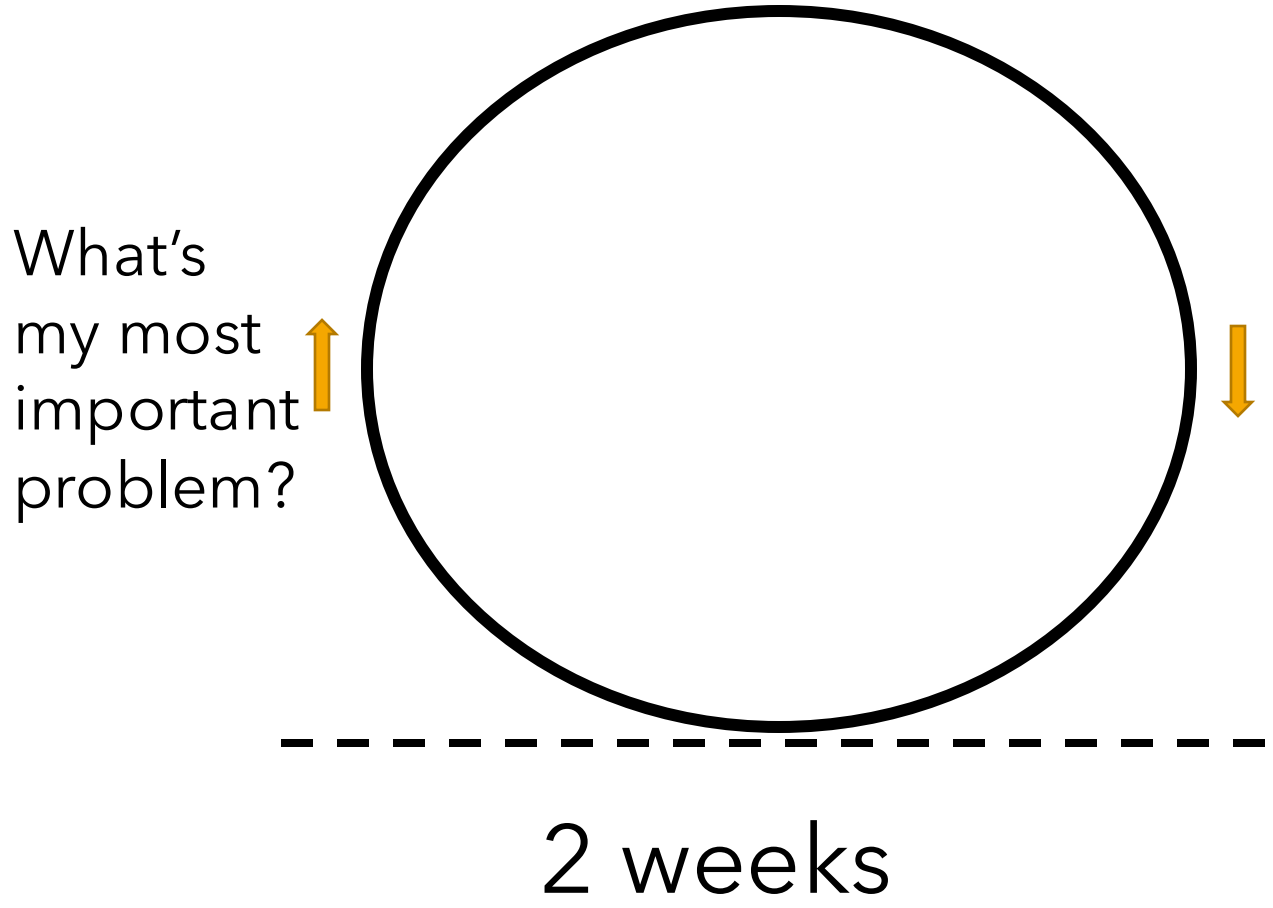
Assurance in agile developments

Cons

- Past assurance breaks as you add new requirements
- Hard to maintain verification and validation
  - Need automation

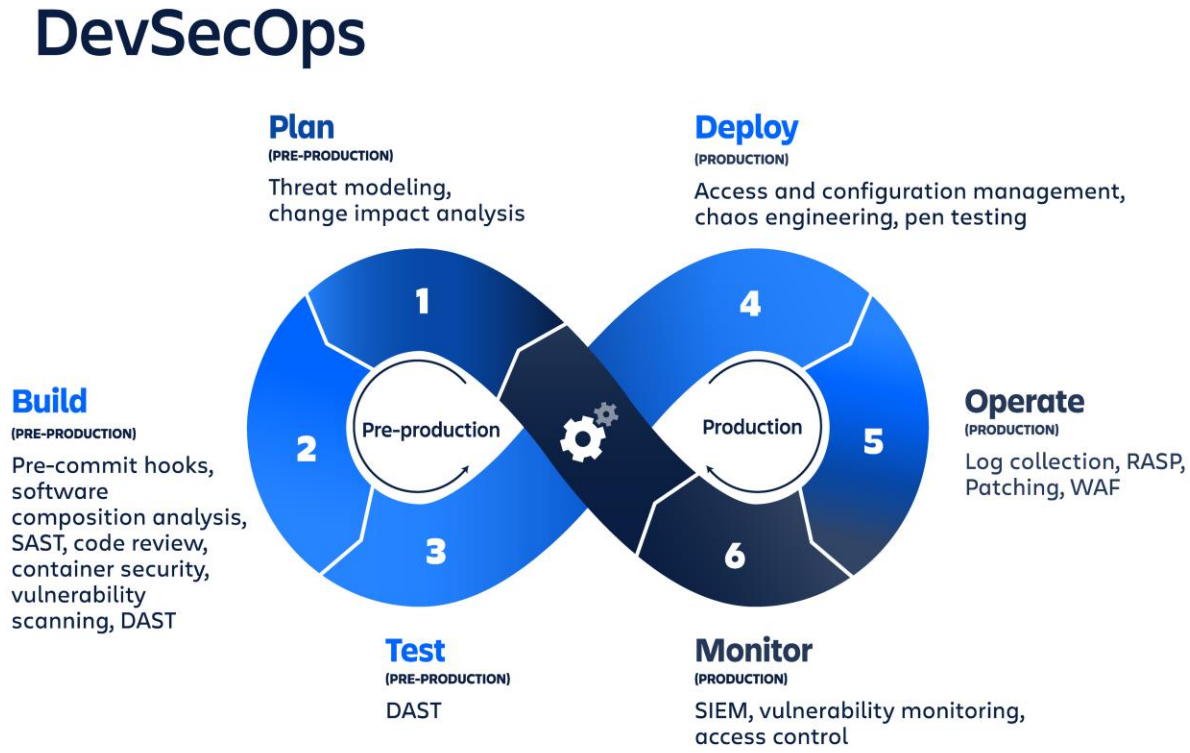
Pros

- Easier to integrate feedback
  - Vulnerabilities reported to you!
  - Insights from user testing

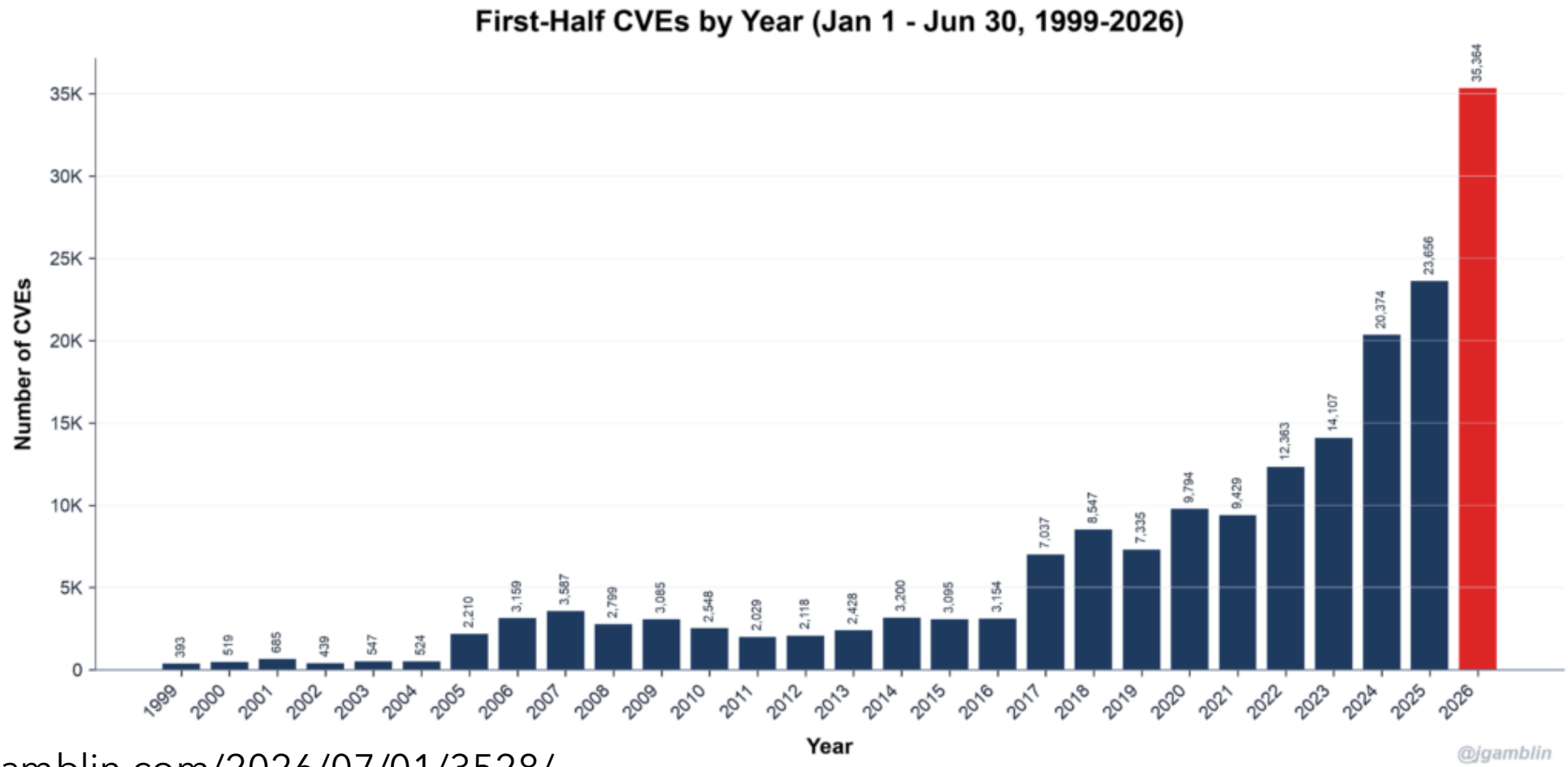


"Shift left" in secure software development

- Secure by design
  - Memory safe languages, secure templates
  - Train developers on secure coding
- Automated code review
  - SAST scans for patterns like creds or SQL injection
  - SCA generate Software Bill of Materials and check for CVEs
- Continuous monitoring
  - DAST & fuzzing to identify run-time issues
  - Vulnerability scanning, SIEM etc
- Test deployment
  - Cloud security scans, patch management etc
- Vulnerability disclosure policy



The challenge of bug reports



https://jerrygamblin.com/2026/07/01/3528/

Patching is non-trivial

"17 out of the 41 in-the-wild 0-days from 2022 are variants of previously reported vulnerabilities."

Did you fix the root cause?



Source: https://security.googleblog.com/2023/07/the-ups-and-downs-of-0-days-year-in.html

Getting Your Disclosure Policy Right

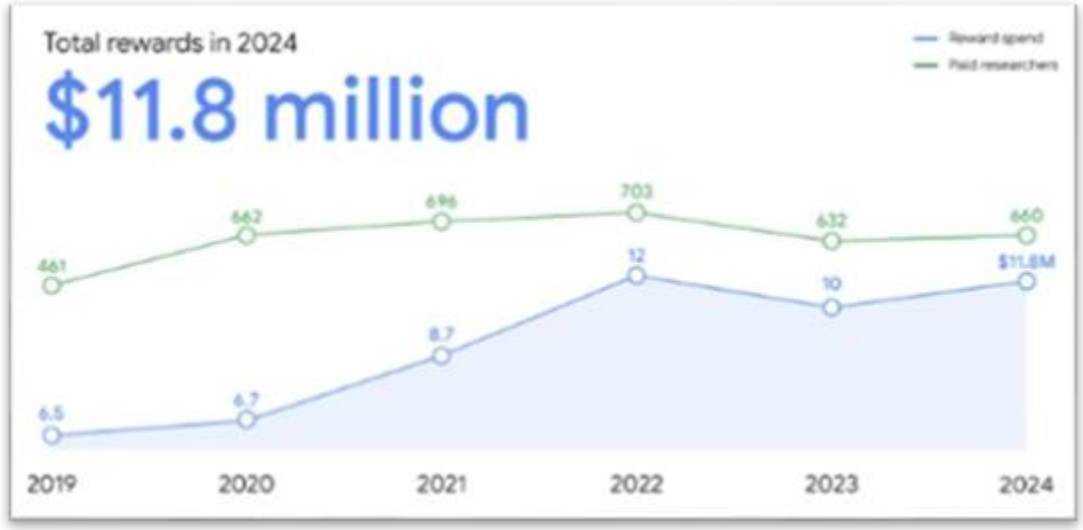
- How do you get people to report bugs to you before they disclose publicly?
- How do you avoid researchers selling your bugs to someone else?
- How do you get your CEO to not deny/deflect?

Types of Disclosure Policies

- Bug bounty policy
  - offer financial rewards
- Vulnerability disclosure policy
  - offer legal guarantees you won't sue
- Security contact via security.txt

Empirical Study of AI Vendors:

- 40% have BBP
- 16% have VDP
- 8% have security contact
- 36% have no policy

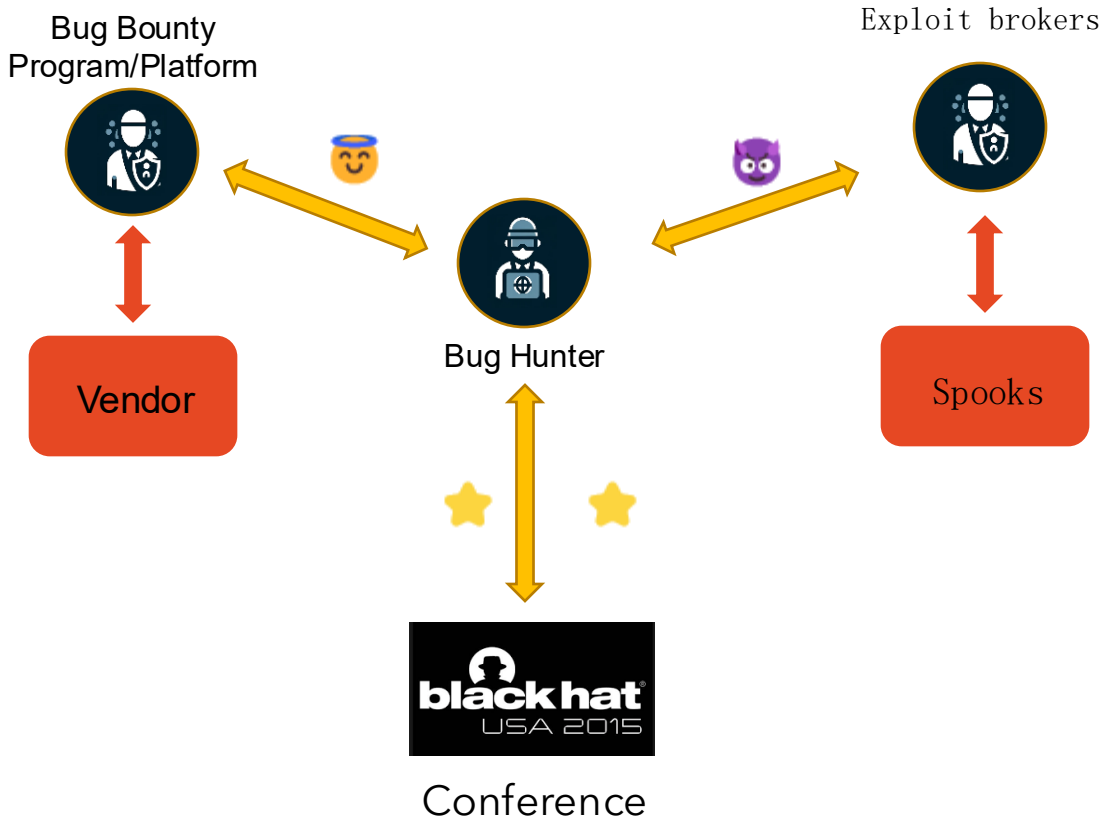


Source: https://www.mediapost.com/publications/article/404028/google-paid-118m-in-bug-bounties-in-2024.html

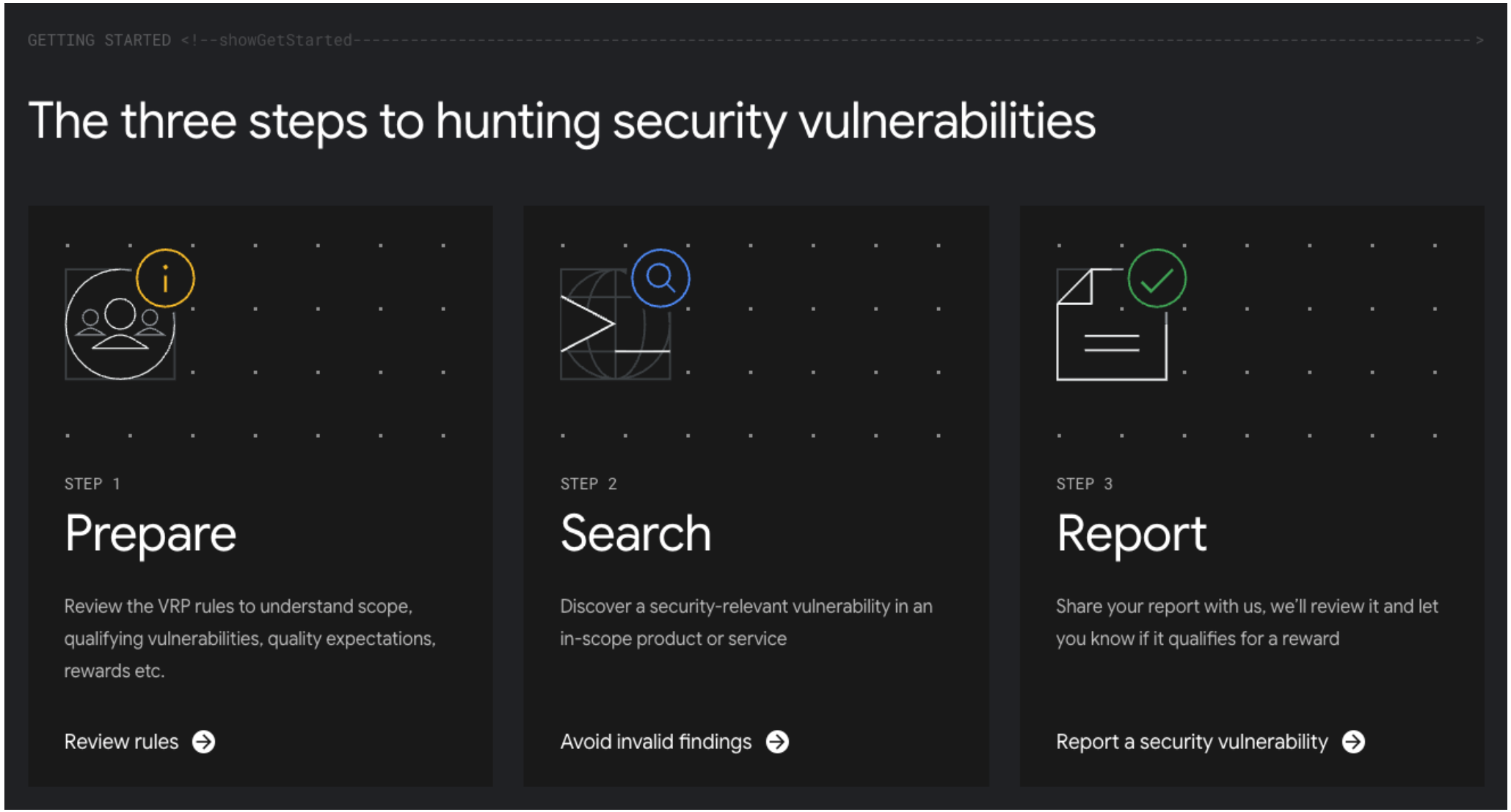
Source: Piao, Yangheran, Jingjie Li, and Daniel W. Woods. "" Abuse Risks are Often Inherent to Product Features": Exploring AI Vendors' Bug Bounty and Responsible Disclosure Policies." arXiv preprint arXiv:2509.06136 (2025).

How to make sure the report comes to you

- Pay enough
- Give them credit too
- Don't require a working exploit
- Reduce legal risk



https://bughunters.google.com/



Tip: Not sure which program to report the issue you've discovered to? When in doubt, report to the Google and Alphabet Vulnerability Reward Program (VRP).

Android & Friends

Program name	Scope	Where to report
Android and Google Devices Security Reward Program (rules)	Security issues affecting Pixel, Smart Home, Google Nest, Home APIs, Pixel Watch, and Fitbit devices and their latest operating systems	Use the standard form (report to *Android & Devices VRP*)
Google Mobile Vulnerability Reward Program (rules)	Security issues affecting first-party Android applications	Use the standard form (report to *Mobile VRP*)

"In general, we reward critical and high severity vulnerabilities ...
A few classes of vulnerabilities exist that generally do not qualify for a reward:
- Phishing attacks that involve tricking the user into entering credentials.
- Issues that only affect userdebug builds.
- Bugs that simply cause an app to crash.
- Issues with negligible security impact, as described in Bug Hunter University, with some exceptions."

Managing bug reports is hard

"In ride sharing, the task is clear (drive the customer from location A to location B), and the driver can reliably estimate the time to completion. In contrast, ambiguity in bug bounty policies—like the description of qualifying bugs—leaves hackers uncertain about how long it will take to find a specific vulnerability or how much they might receive"

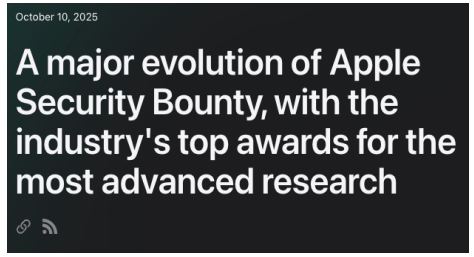


Source: Piao, Y & Woods, DW 2025, The Bug Bounty Manifesto: Collectivization and Fairness. in Security Protocols XXIX: 29th International Workshop. Lecture Notes in Computer Science, Springer, Twenty-ninth International Workshop on Security Protocols, Cambridge, United Kingdom, 26/03/25.

So then what is assurance for builders?

- System is so complex you know there are vulnerabilities
- … maybe it's enough to say exploits are getting more expensive?
- Most vendors fall a long way short
  - Lots of room for improvement here!
- What does it matter if your users will be spear phished anyway





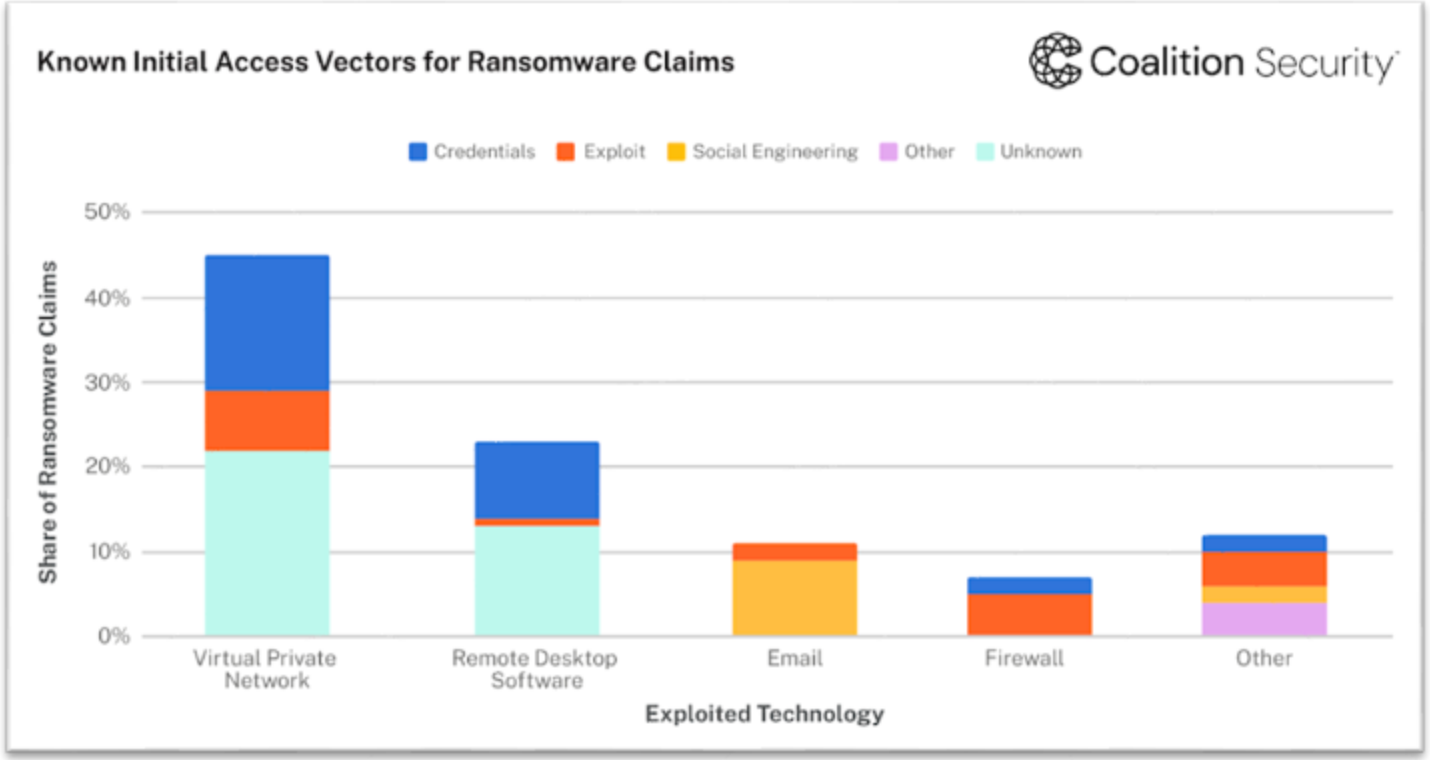
"We're doubling our top award to **$2 million** for exploit chains that can achieve similar goals as sophisticated mercenary spyware attacks."

Follows announcement of Memory Integrity Enforcement.

Deploying Assurance

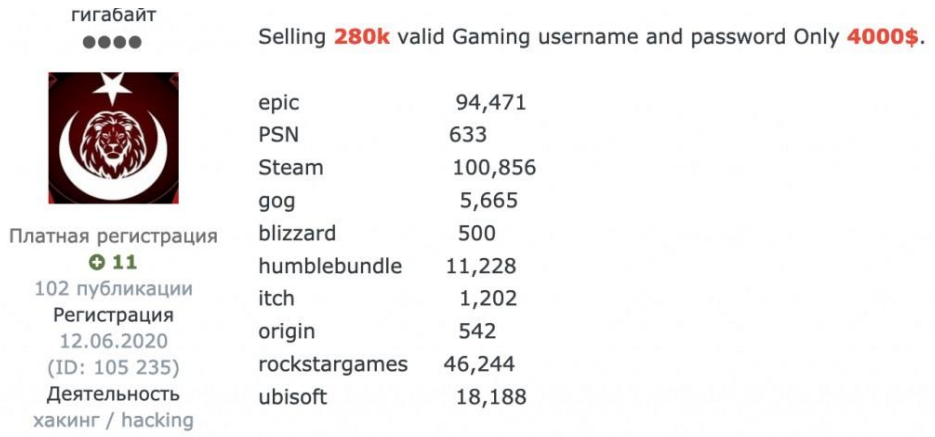
What to verify, test, and monitor

1. **Credential security**
2. Vulnerabilities
3. User awareness
4. Signs of intrusion
   - Malware
   - Data exfiltration
   - Access requests
   - Etc



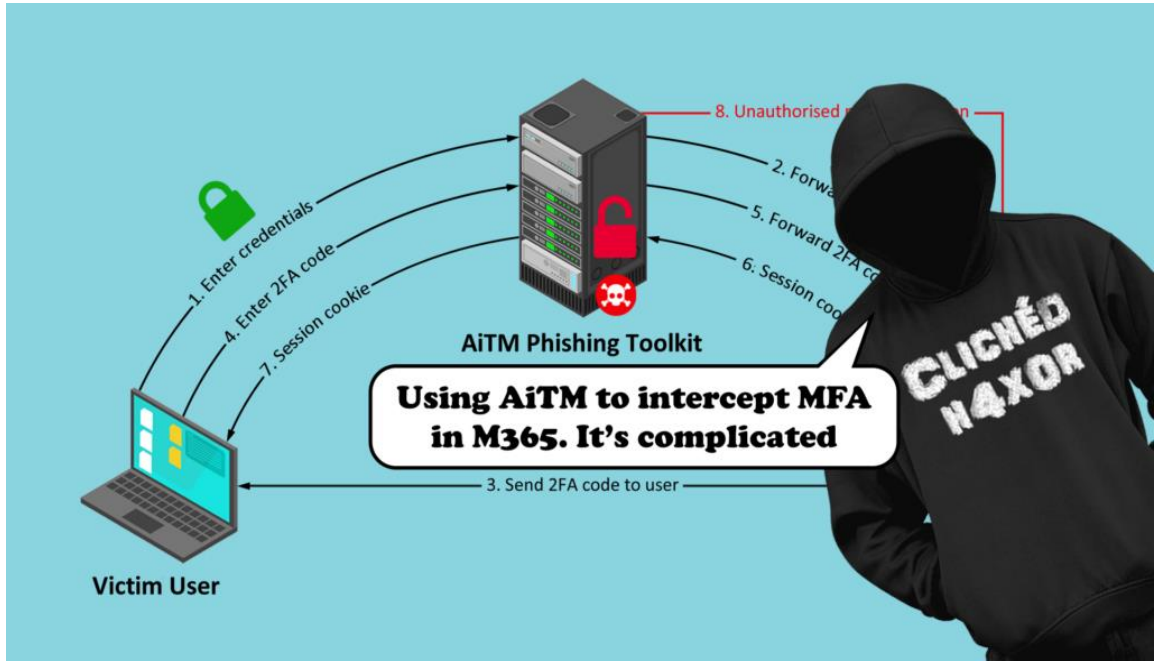
How to be sure passwords are secure

- Passwords are inherently **hard to control**
  - Set and "stored" by the user
  - Could be re-used on other insecure apps or on personal devices
  - Could be leaked
- Policies try to address often lead to **unintended consequences**
  - Write down passwords
  - Re-use same password on multiple services



How to be sure 2nd factors are secure

- SMS-based better than passwords
  - Fresh codes better than stale passwords
  - … maybe the code is phished or SIM swapped
- App-based is better still
  - At least you don't rely on a Telecomm firm
  - … maybe the code was phished
- FIDO designed to avoid this
  - Tied to a device
  - If user logs into go0gle.com, won't auth
- **Better MFA tends to be costlier**
  - Onboarding + credential reset



Source: https://www.pentestpartners.com/security-blog/intercepting-mfa-phishing-and-attackers-in-the-middle/

Configuring identity security is hard

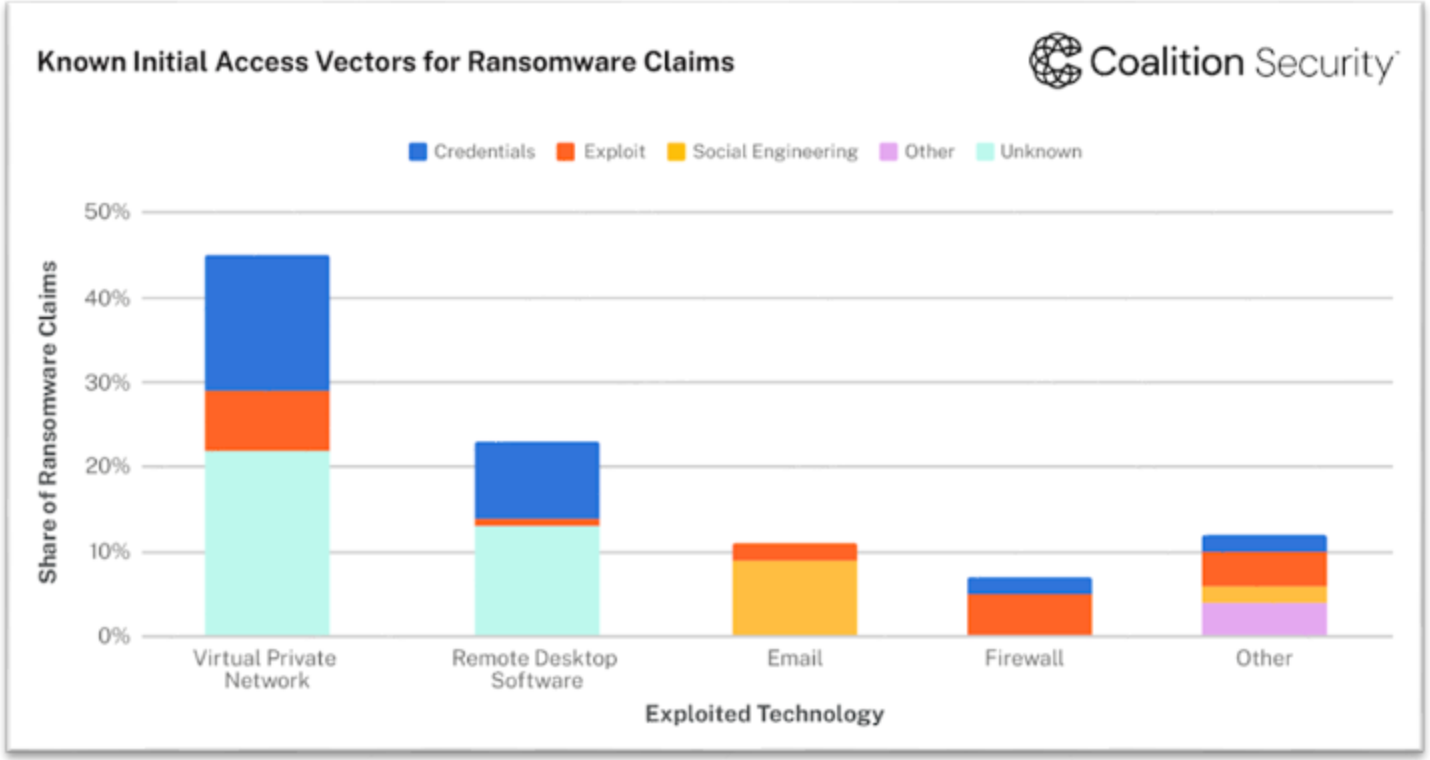
- Not every service has MFA enabled
  - "63% of organizations that stated they used MFA for protecting privileged access were still impacted by a ransomware event linked to coverage gaps in MFA configuration/installation method"
- Not every account enforces MFA
  - Service accounts
  - Users who refuse
  - Before users enrol



Source: Identity Has Become the Prime Target of Threat Actors

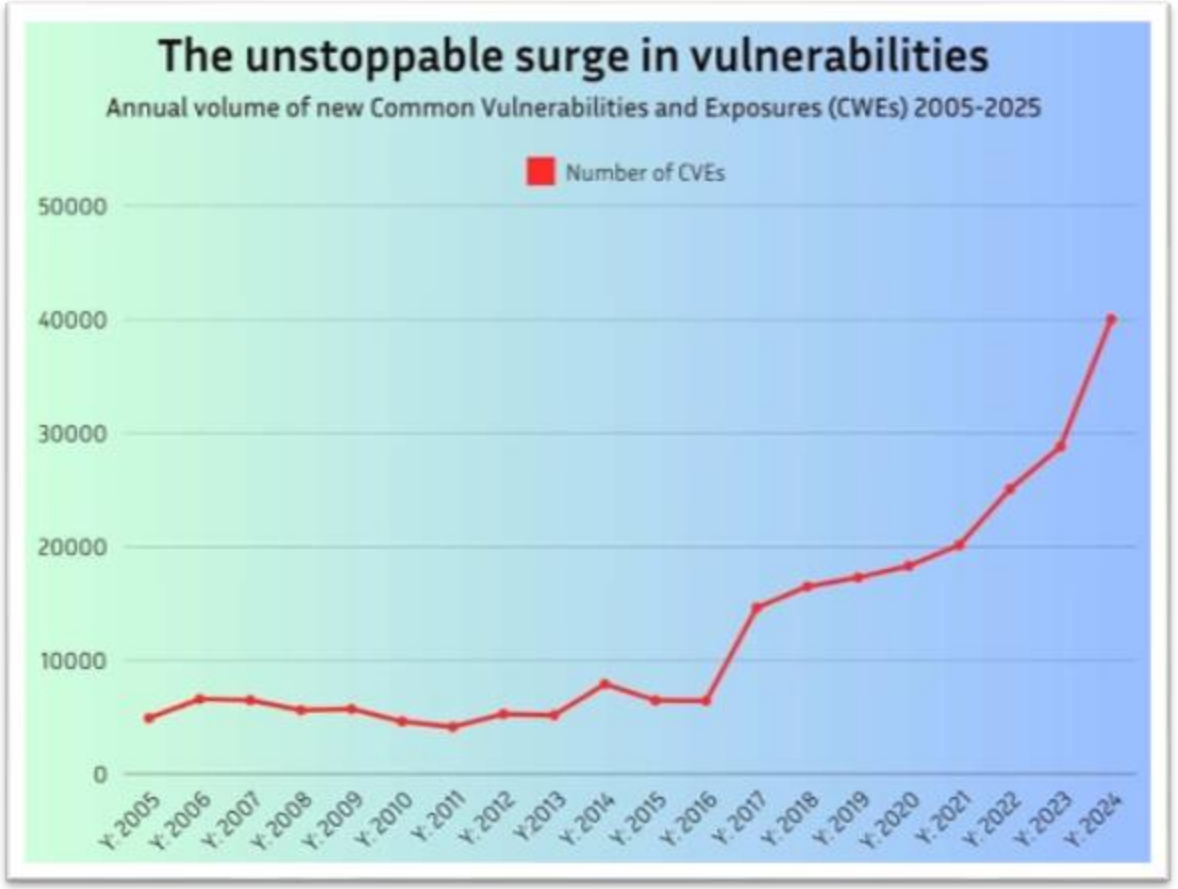
What to verify, test, and monitor

1. Credential security
2. **Vulnerabilities**
3. User awareness
4. Signs of intrusion
   - Malware
   - Data exfiltration
   - Access requests
   - Etc



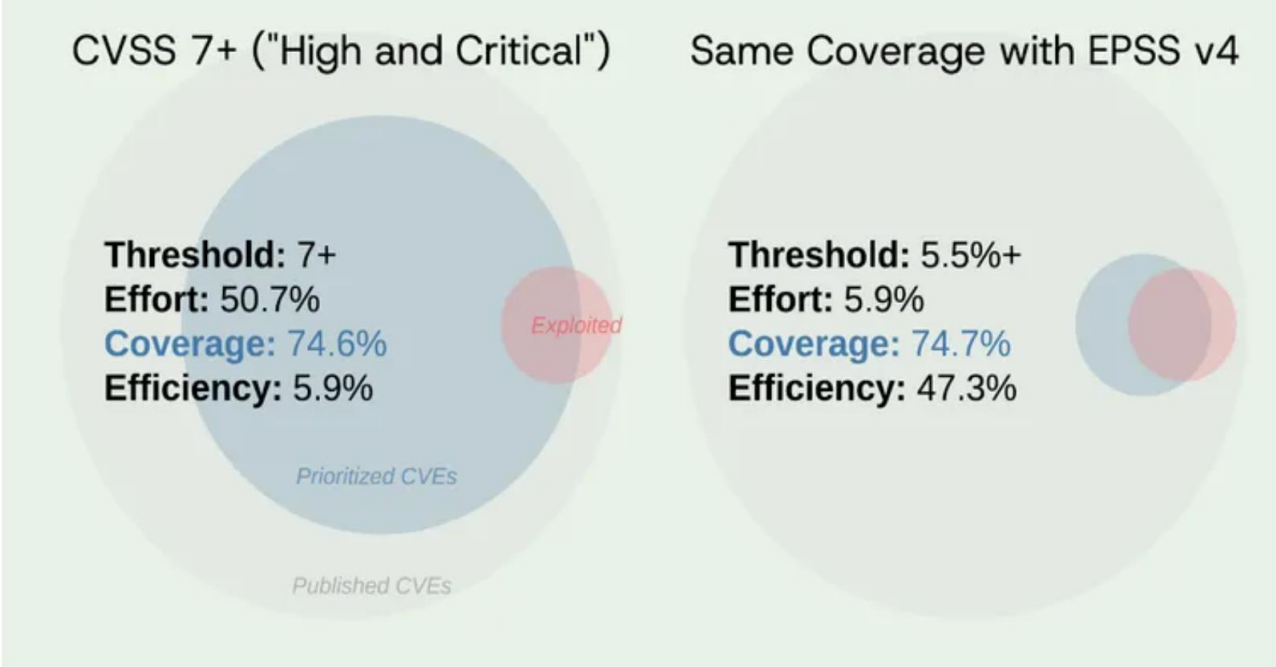
Patch Management

- If vulnerability reports are bad for vendors, they're even worse for customers
  - Most use **far more** products than they build
  - Microsoft produces 1 patch, and 1 billion plus customers need to apply it



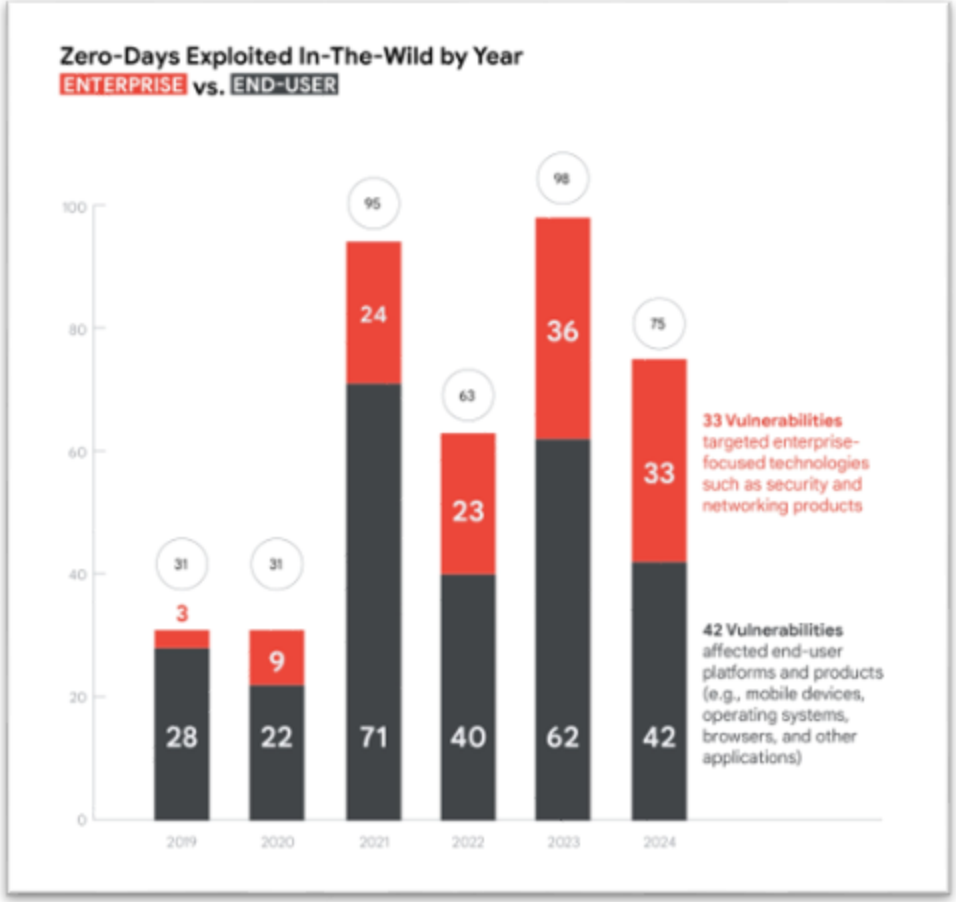
How sure are you about your patch strategy

1. **PCI DSS:** Update high and critical vulnerabilities (according to CVSS) within one month of release
   - Miss many exploited vulns
2. **EPSS:** Patch what ML says is most likely to be exploited.
   - Miss less exploited vulns, maybe patch before n-day exploits.
3. **KEV:** Patch what has already been exploited.
   - Efficient but maybe you are the threat intelligence!
4. **Cloud infra:** Rely on professionals.
   - Until there's an 0day



Uncertainties in patch management

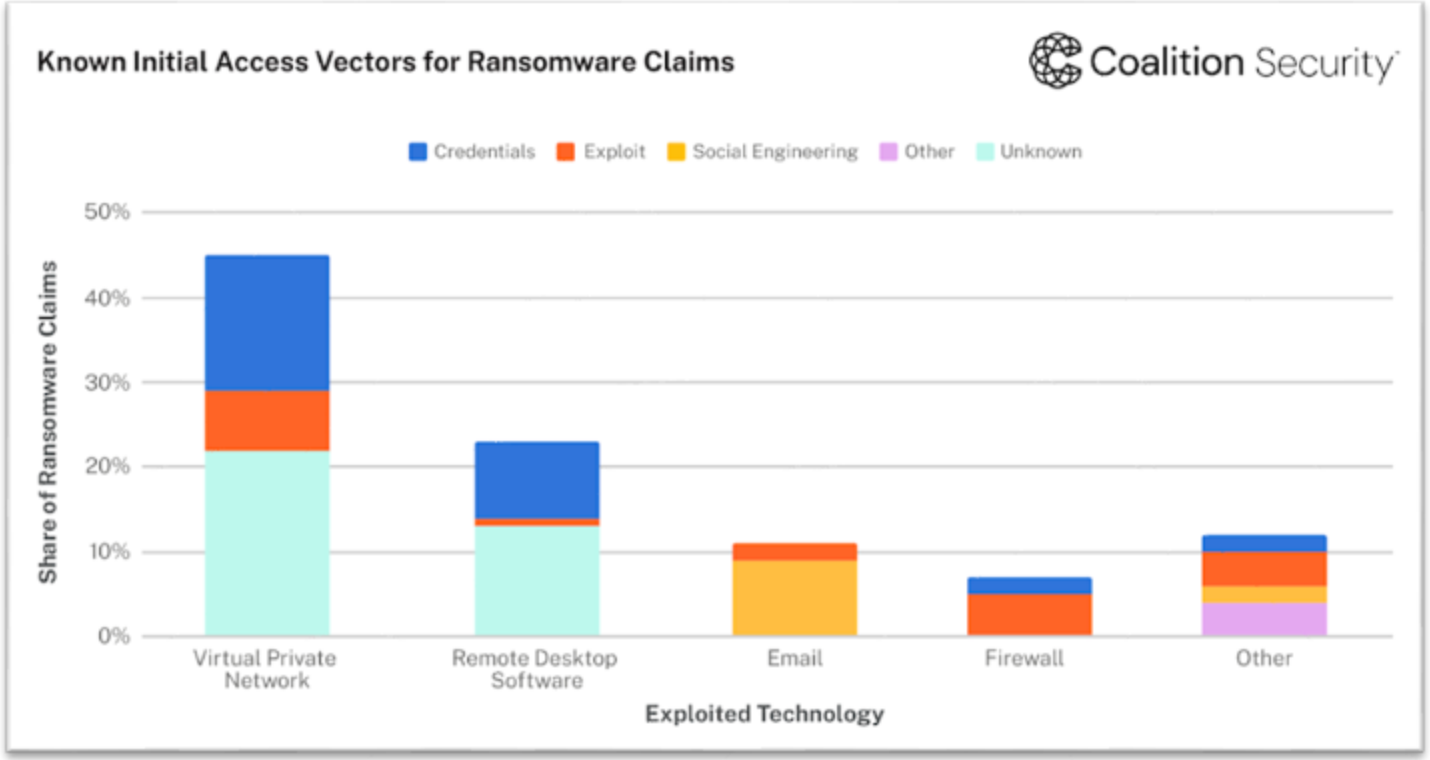
- 0-days
  - Google Project Zero are tracking
- The patch doesn't work
  - 41% of 0days in 2022 were variants on known vulns
- Shadow IT + user-managed devices
  - ASM and vulnerability scanning



Source: https://security.googleblog.com/2023/07/the-ups-and-downs-of-0-days-year-in.html

What to verify, test, and monitor

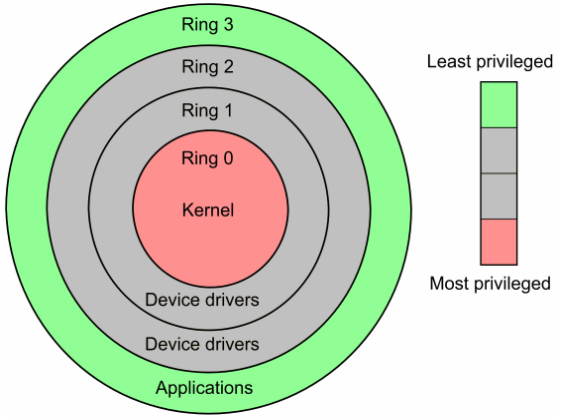
1. Credential security
2. Vulnerabilities
3. **User awareness**
4. Signs of intrusion
   - Malware
   - Data exfiltration
   - Access requests
   - Etc

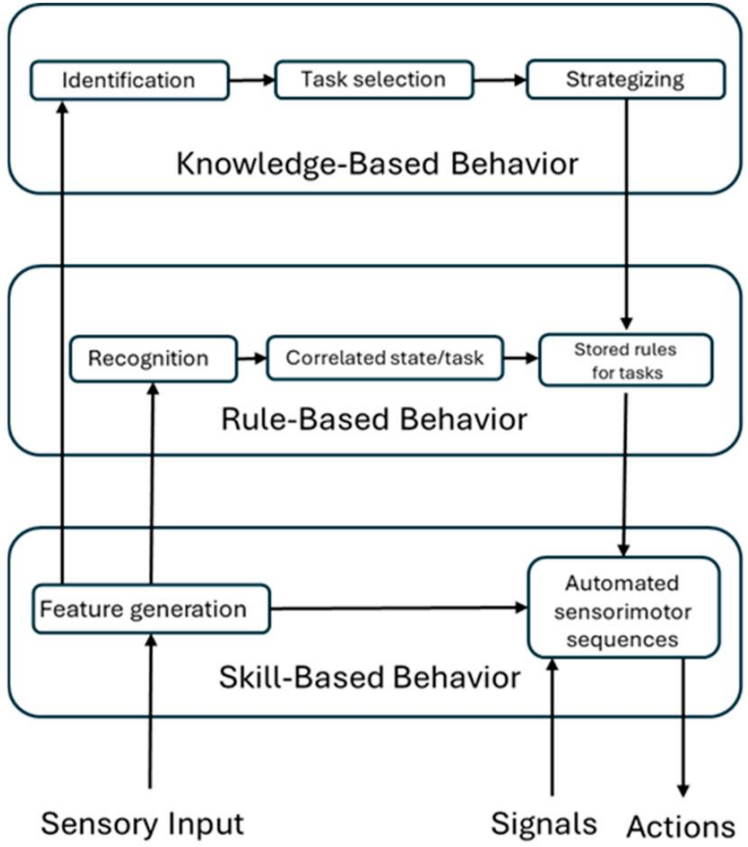


How are you sure about your users?

- You can't be!
  - Errors at every point of the stack!
  - Training helps with knowledge-based behaviour
- Reduce the "blast radius"
  - Application white lists
  - Disable autorun
  - Principle of least privilege
  - Phishing resistant MFA
  - Etc etc

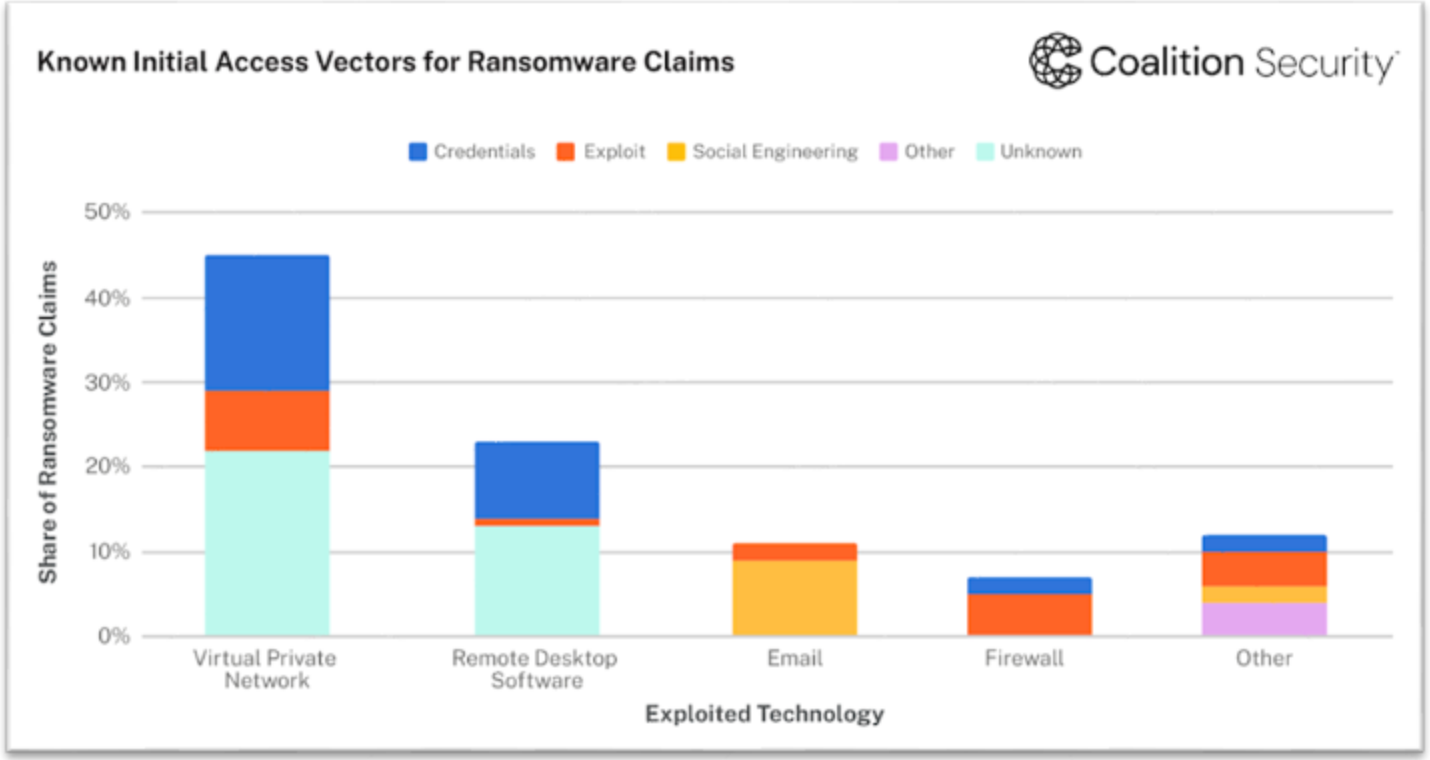






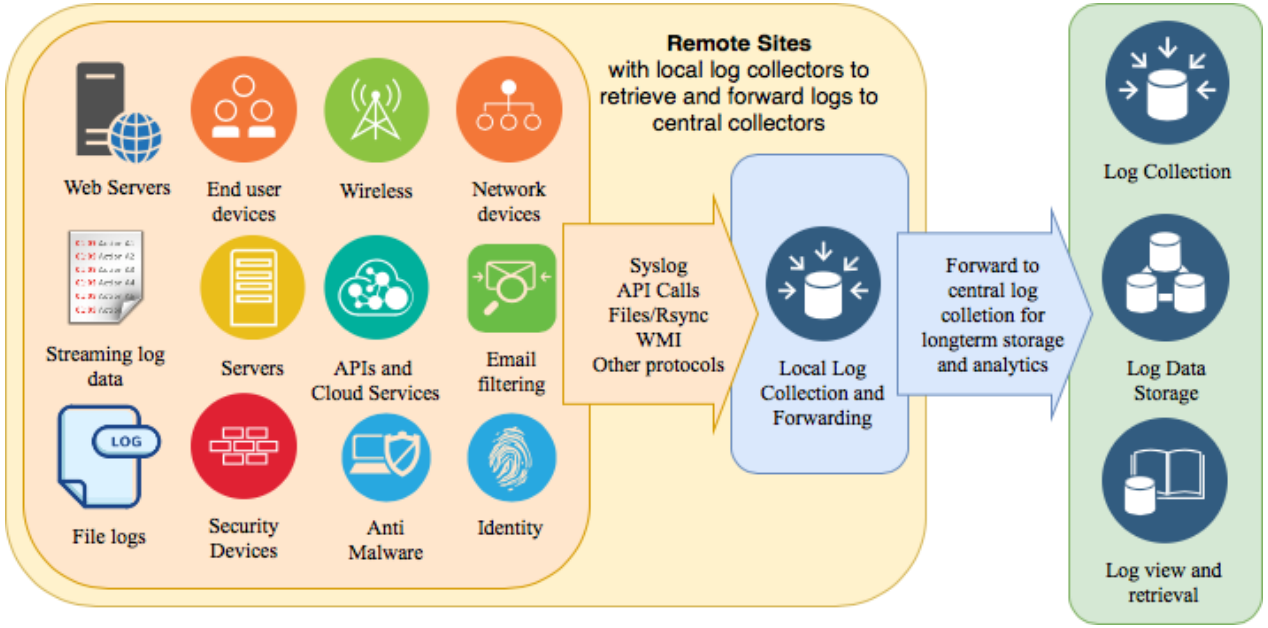
What to verify, test, and monitor

1. Credential security
2. Vulnerabilities
3. User awareness
4. **Signs of intrusion**
   - Malware
   - Data exfiltration
   - Access requests
   - Etc

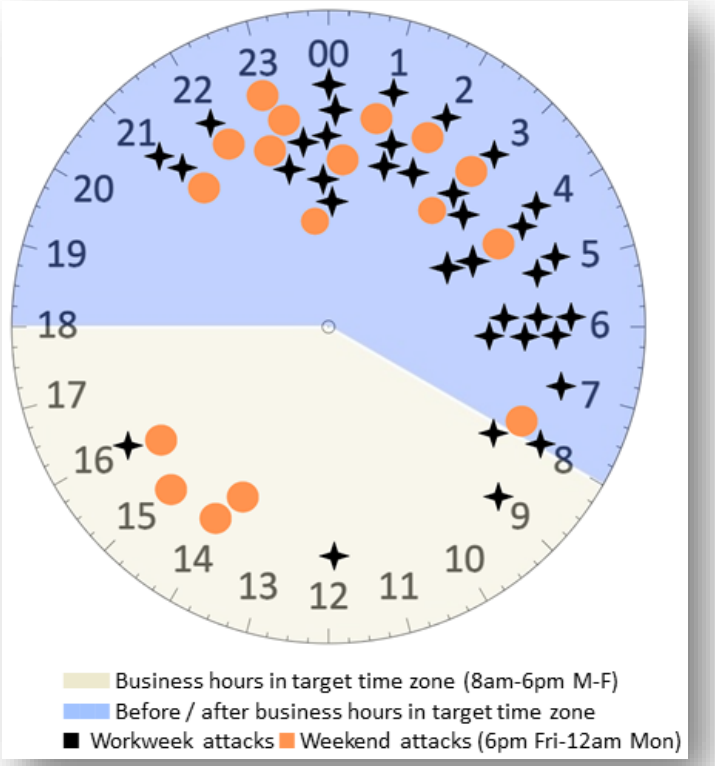


Monitoring and Response

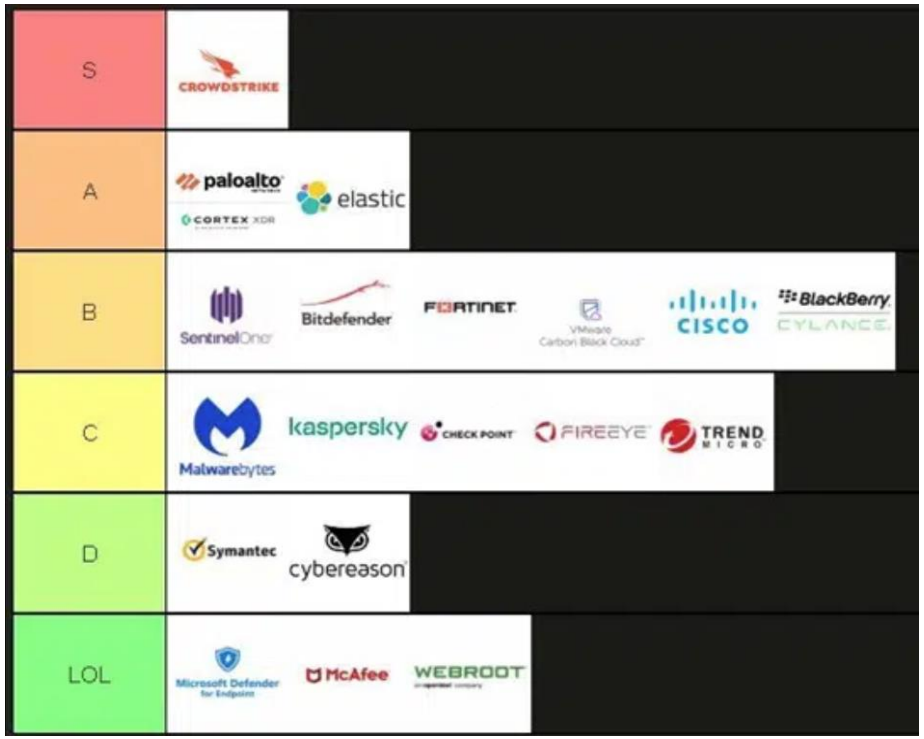
- HUGE amount if InfoSec focuses on **monitoring logs**:
  - Security Operations Centre
  - Endpoint Detection & Response
    - MDR, ITDR etc
  - Data loss prevention
  - Threat Hunting
- Huge cat and mouse game
- Provides an **extra "safety net"**
  - In addition to assurance in prevention controls, you can detect and contain compromise



Evidence that monitoring works

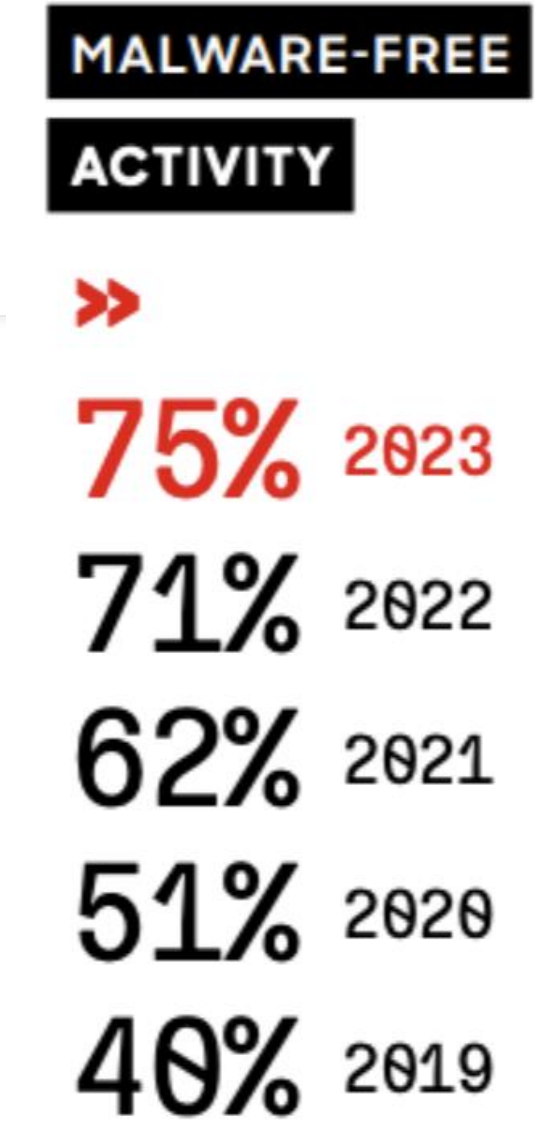


Source: https://www.darktrace.com/blog/im-sorry-were-closed-why-most-ransomware-attacks-happen-out-of-hours



Attackers discuss EDR tools, and invest in bypasses.

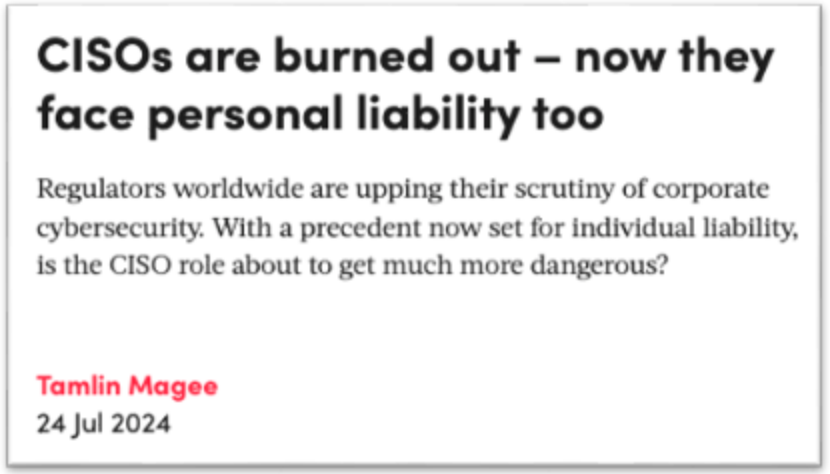
Source: Conti leaks.



Source: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

Emotional Assurance

The paranoia of a CISO



CISOs are burned out – now they face personal liability too

Regulators worldwide are upping their scrutiny of corporate cybersecurity. With a precedent now set for individual liability, is the CISO role about to get much more dangerous?

Tamlin Magee
24 Jul 2024

The SEC brought charges against SolarWinds, and for the first time an individual security executive – the CISO.



Software Security: Too Little Vendor Accountability, Experts Say

Actual legislation is a long shot and a decade away, but policy experts are looking to jump-start the conversation around greater legal liability for insecure software products.

Becky Bracken, Senior Editor, Dark Reading
May 2, 2024

Meanwhile, vendors face little accountability.

Critical Perspective: Do InfoSec products serve the company, or the budget holder?

External assessment

- Pen test and fix
  - Annual, find as many in scope vulns as possible
  - Did you fix what the attacker will exploit?
  - Expensive because it requires human
    - PTaaS?
- Red teaming: employees simulate external attacker
  - Test detection and response
- Attack surface management more "systematic"
  - Scan external infra
  - Find shadow IT and unpatched vulns
  - Most valuable InfoSec startup (Wiz) does cloud configuration scans

"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 Cyber Security Framework
- But does checking off quick wins lead to better security?



Dashboards and measurement

- Dashboards fit the philosophy of boards and e-teams
  - Minimal context needed to track progress via KPIs, metrics etc
- 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]

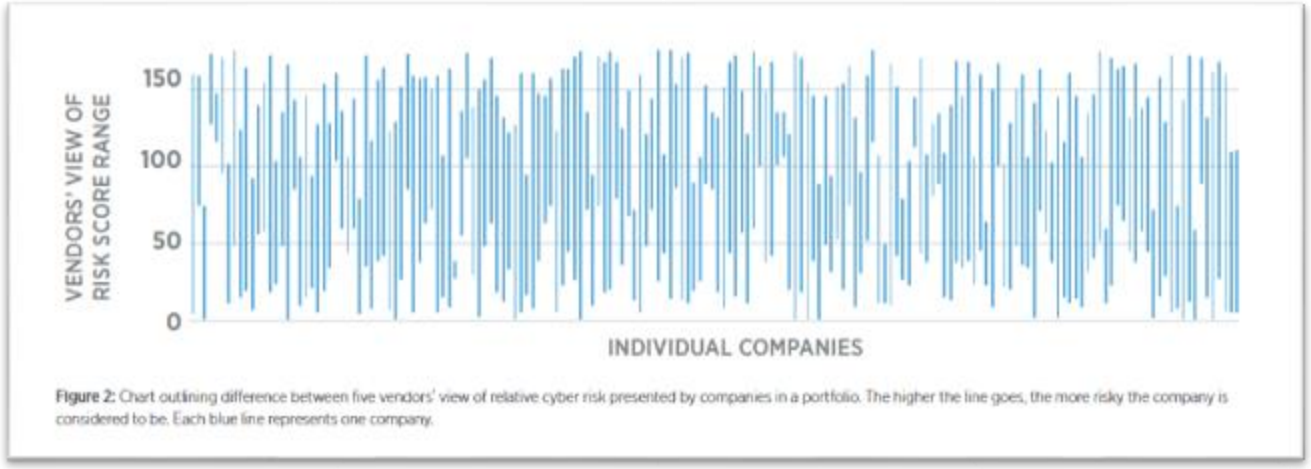


Figure 2: Chart outlining difference between five vendors' view of relative cyber risk presented by companies in a portfolio. The higher the line goes, the more risky the company is considered to be. Each blue line represents one company.

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



[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.

Sustainability: **how long** will the system be secure for?

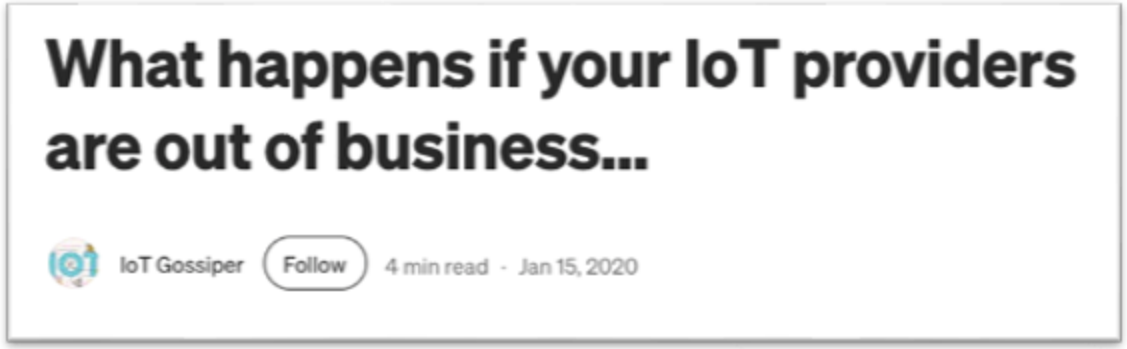
Return on Investment of releasing patches

Why vendors release patches

- Your customers demand security updates
- May be reputation backlash

Why they might not

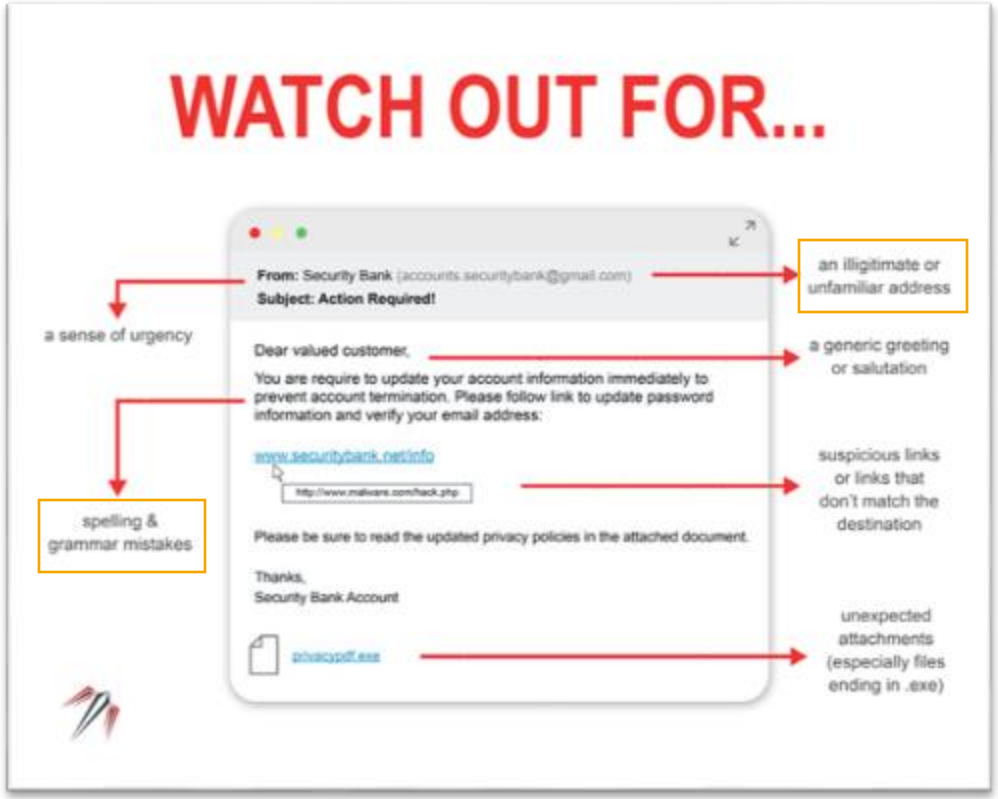
- Planned obsolescence helps business
- Running a patch program is expensive
  - Triage takes time
  - Paying researchers ($10m+ a year for main vendors)
  - Developers need to work on security patches

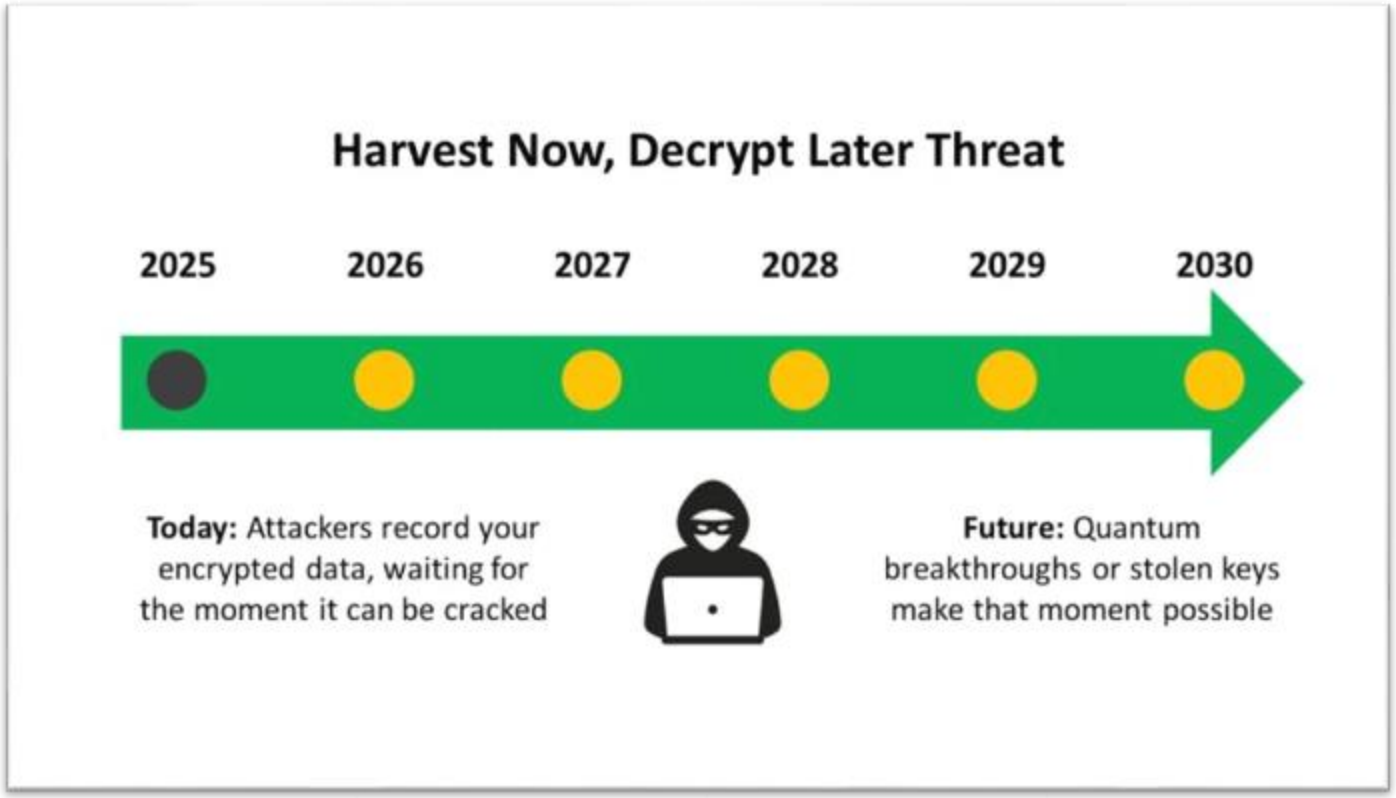


Windows 10 Case Study

- Windows 10 used by 42.8% of all Windows computer users worldwide.
- Windows 8 ended in Jan 2016, only 3.7% of Windows users were still using it.
- Only 2.2% were still using Windows 8.1 when support ended in January 2023.
- Many of the computers still running Windows 10 can't upgrade to Windows 11.

Changing Threat Actor Capabilities

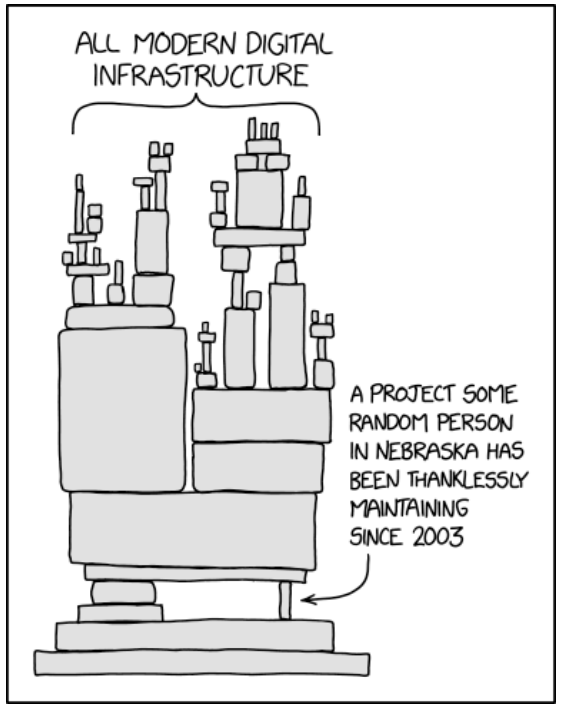




Ecosystem as strength and vulnerability



Increases the number of stakeholders who can fix an issue.

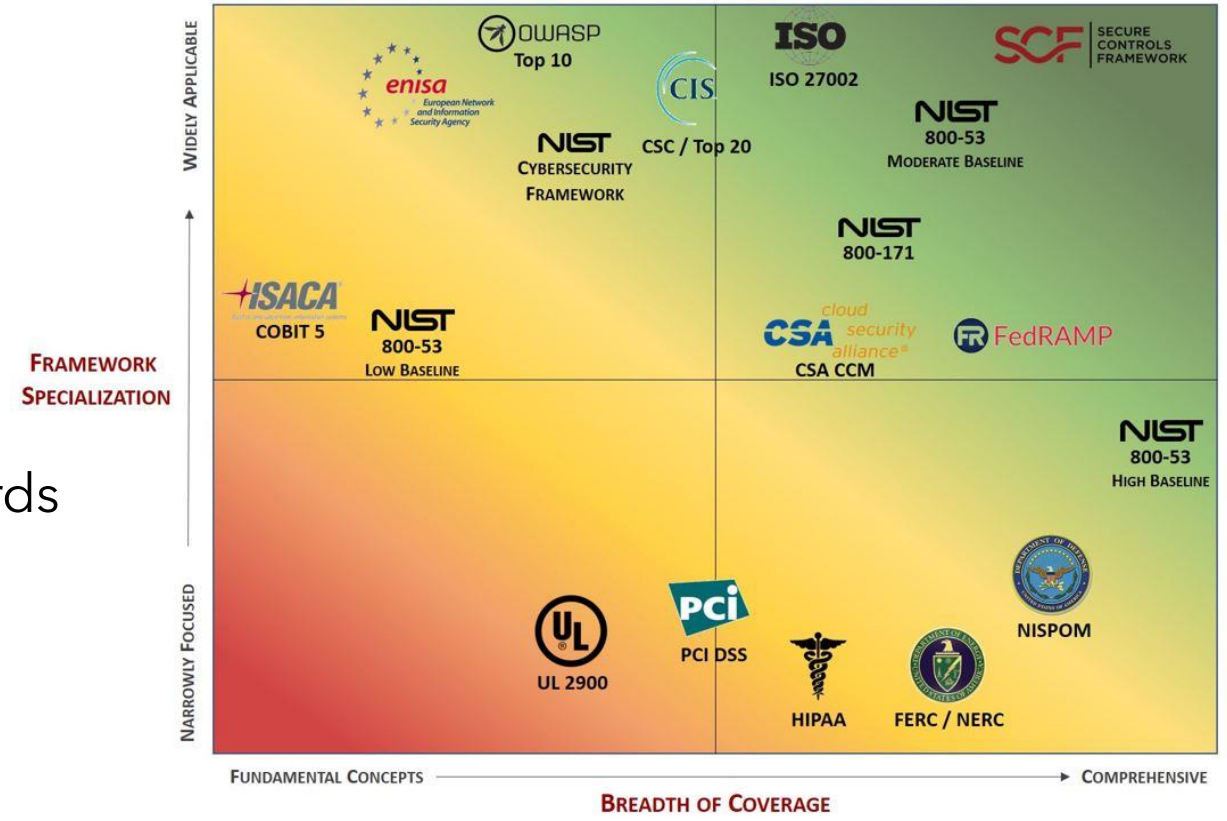


But can you rely on stakeholders you don't control to fix an issue?

Compliance: how you can **convince others** that your system is secure.

Who do you need to convince? And how*?

- 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



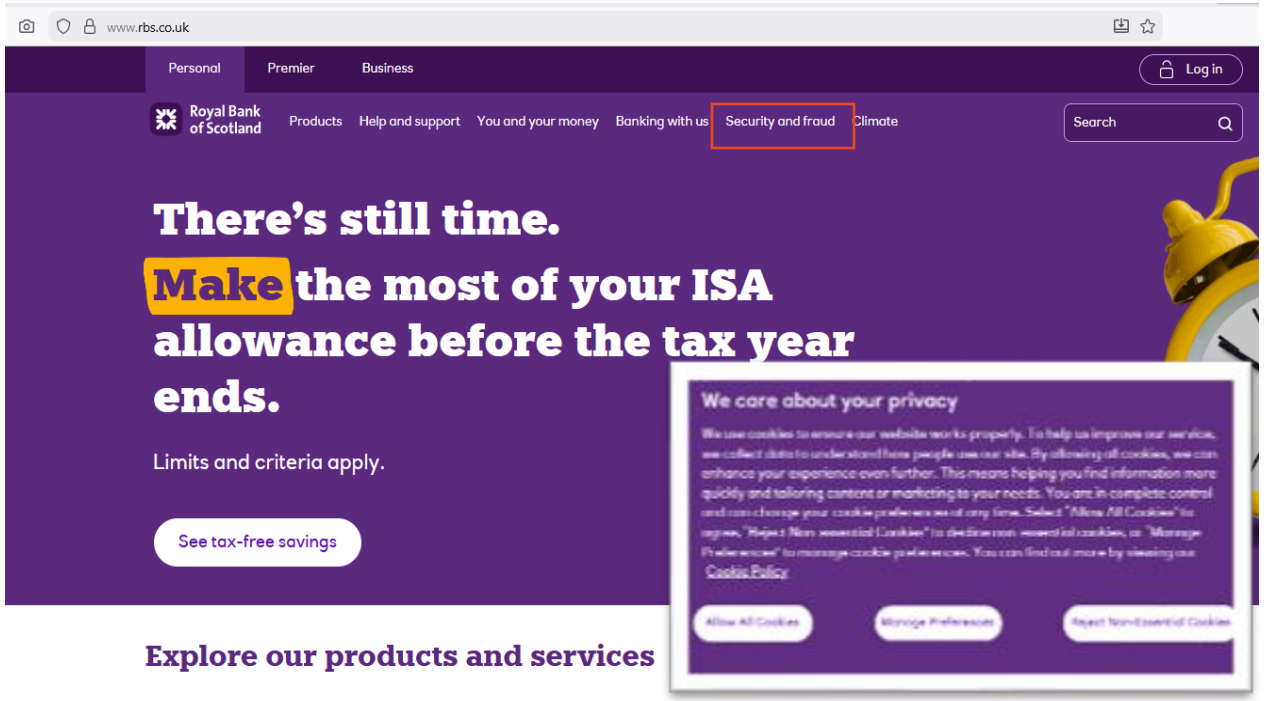
*All require "security", but we're not going to track what is required by each in this course.

Convincing B2C customers





How banks used to convince customers they could reliably store money



Banks don't really try to convince you 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



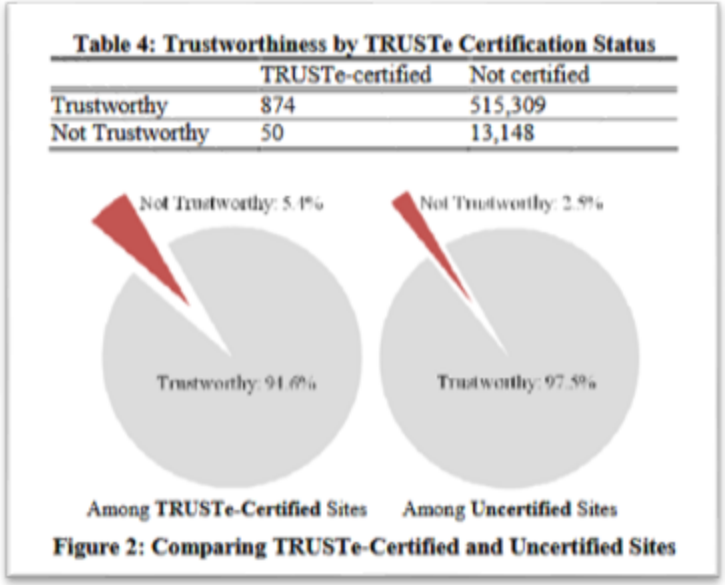


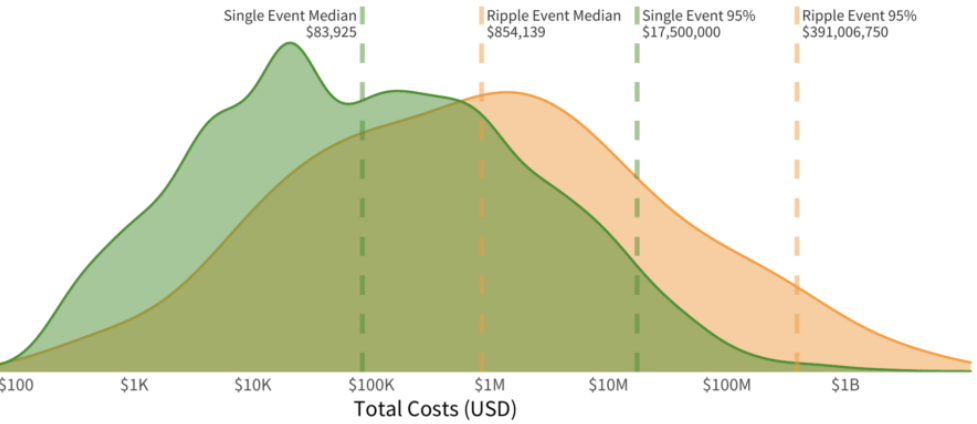
Table 4: Trustworthiness by TRUSTe Certification Status

	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.

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

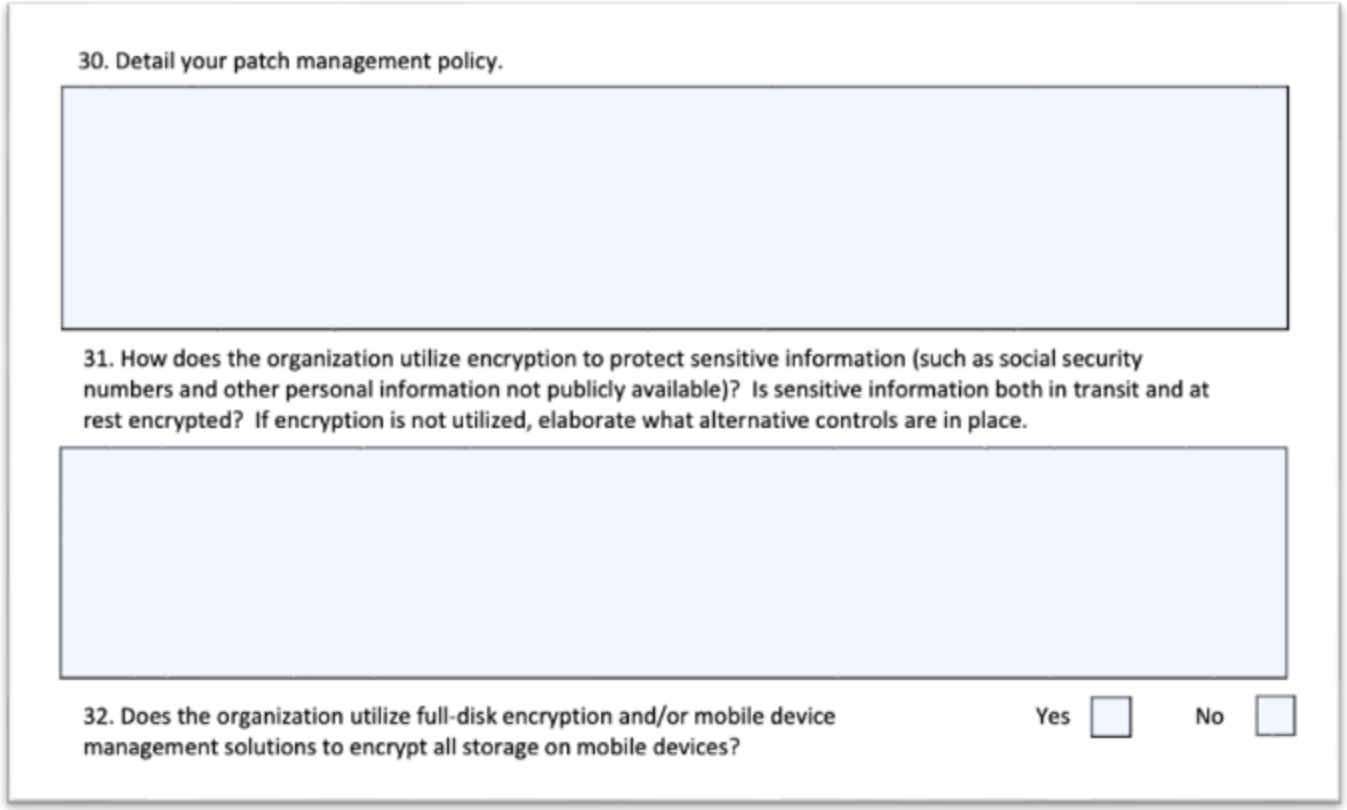


Source: https://cyberresilience.com/blog/2024-cyber-risk-year-in-review/



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
- Certifications
  - ISO 27000, SOC2 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

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 common for data security
- Economic pressures
  - Expensive, but motivated by sales
  - External auditors "maintain" standards



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 Thursday

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/

Regulatory Compliance in the EU/UK

Law / Regulation	Scope
NIS2 Directive	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	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.

Regulatory Compliance in the US

Law / Regulation	Scope
CMMC 2.0 (similar to NIS 2 in the EU)	Defense & Critical Infra: 300k+ 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)	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.

How governments scale regulation

- Incident reporting requirements
  - Mandatory breach notification, ransomware payment bans
- Set costs for security failures
  - Fines and investigations
  - Create liability regimes by legislation
- Law enforcement, cybercrime takedowns etc
- Support other mechanisms
  - Formalize and define best practice
  - Mandate + backstop insurance insurance
  - Build workforce pipelines





Does compliance decrease risk?

- What determines compellence power
  - Governments, customers, and payment card industry have the most power
  - Insurers and banks are weak due to competition
- How to ensure requirements are effective
  - Reducing risk vs jumping through hoops
  - Need engineers to help draft requirements
- Ultimately, compliance is better than nothing

