Security Engineering

INFR11208 (UG4) // NFR11228 (MSc)

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

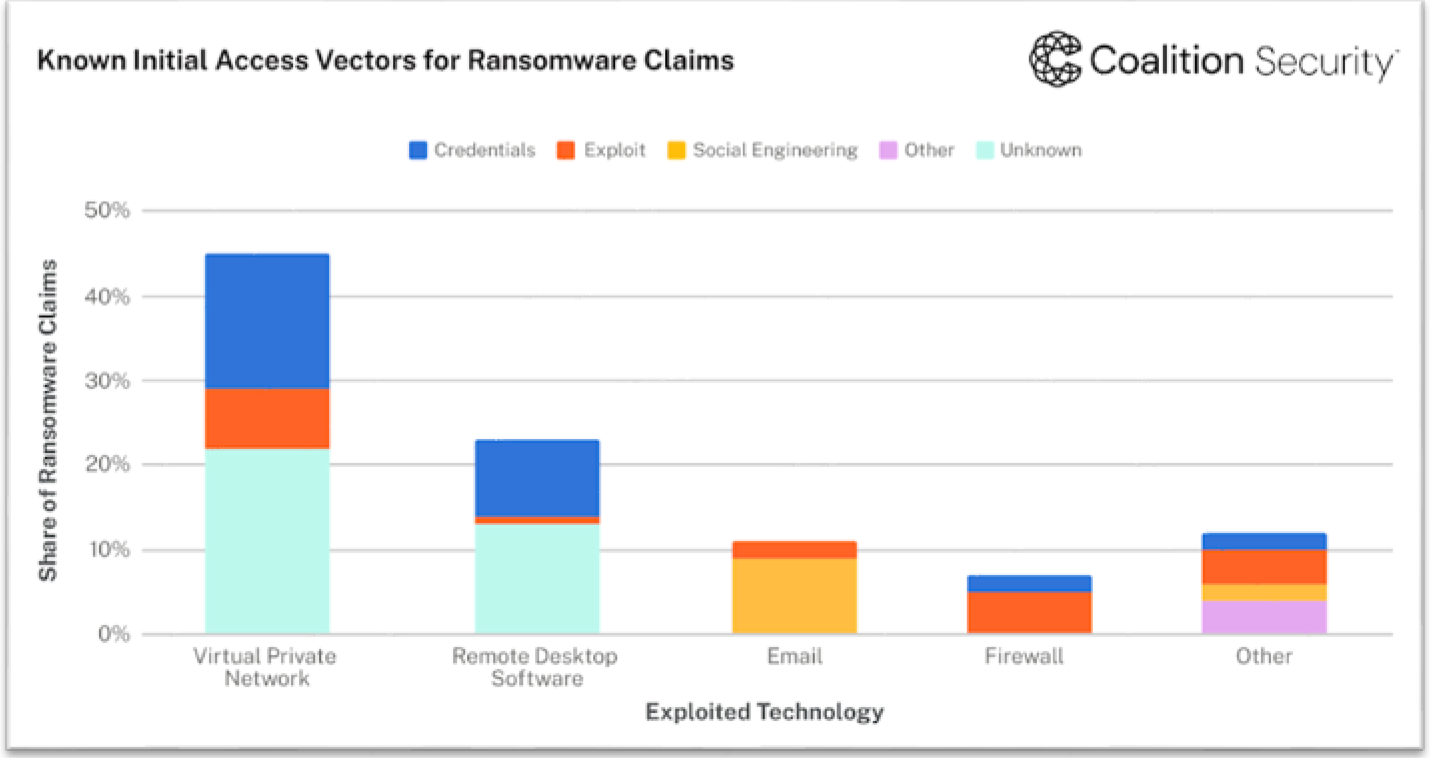
We'll cover three related concepts

- **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.

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

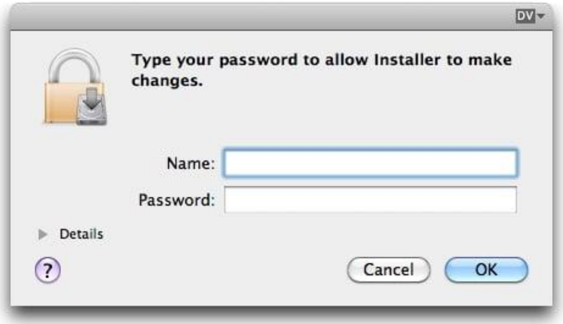
What to verify, test, and monitor

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

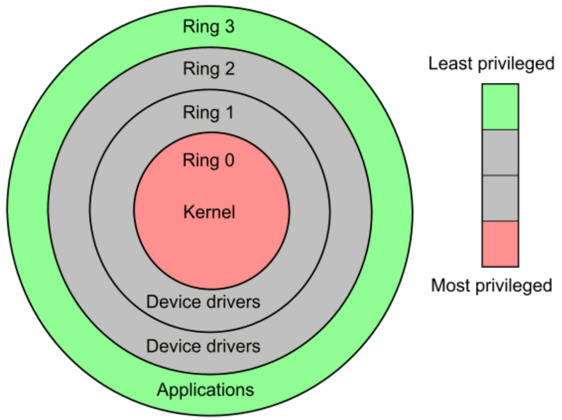


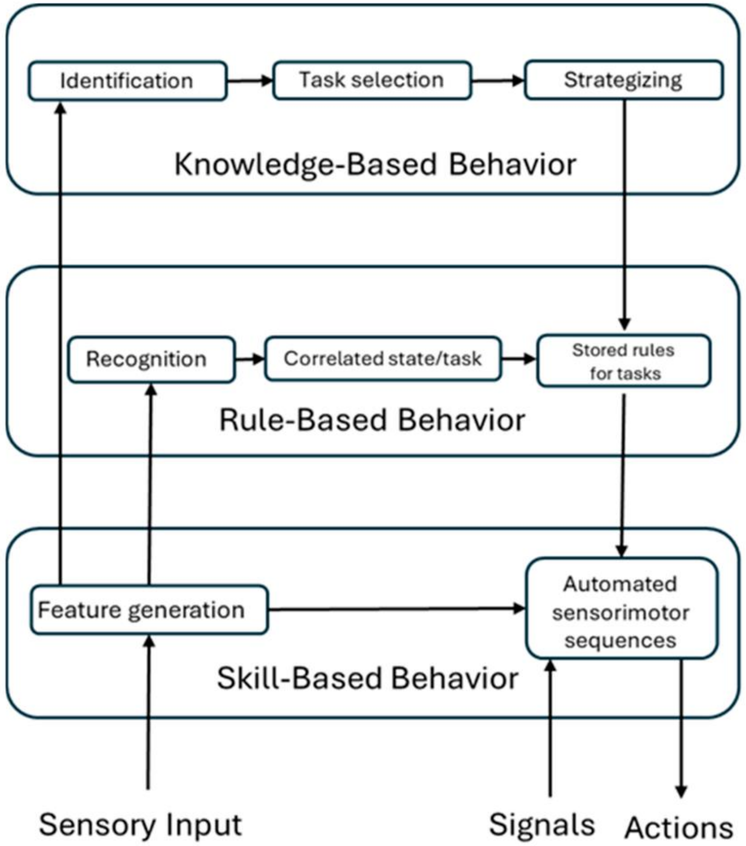
How are you sure about your users?

- 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



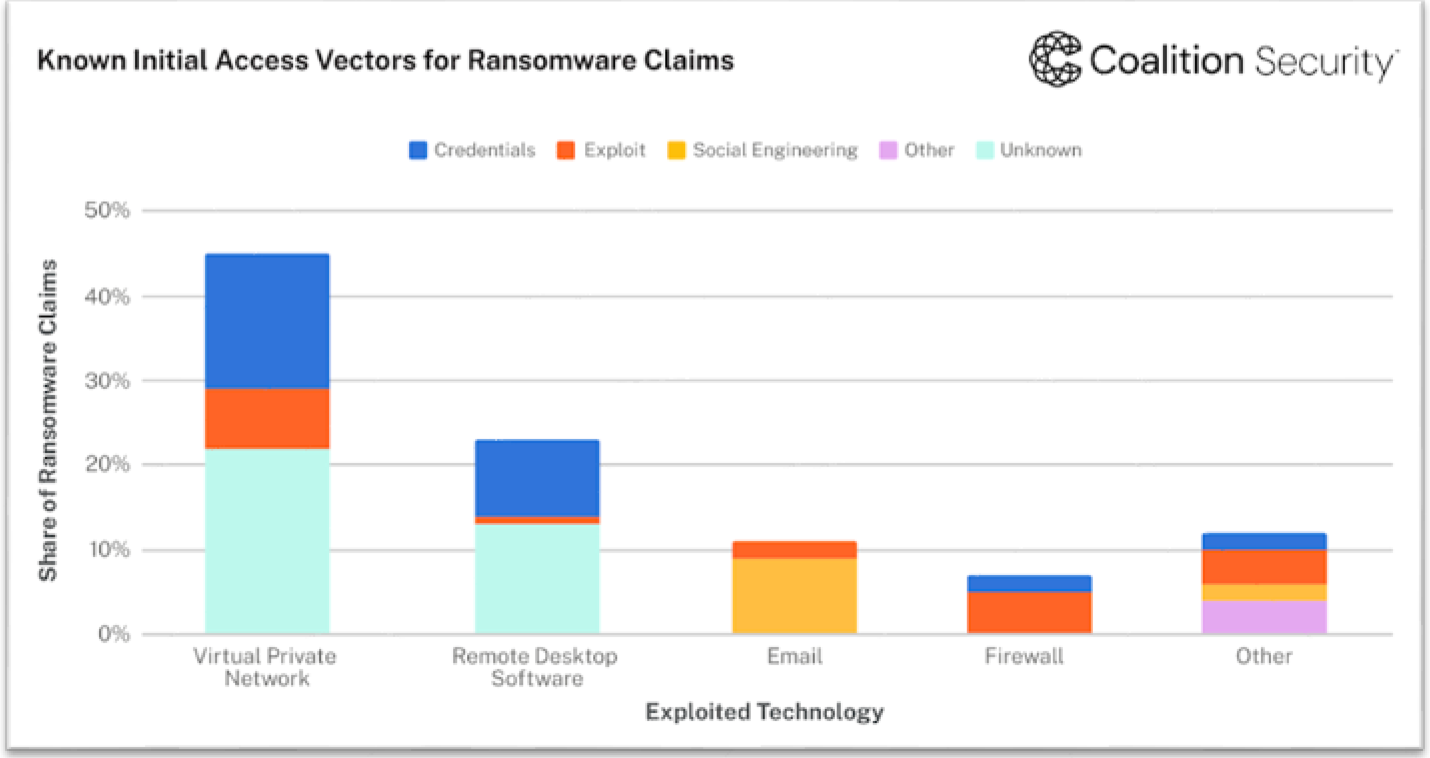
Type your password to allow Installer to make changes.





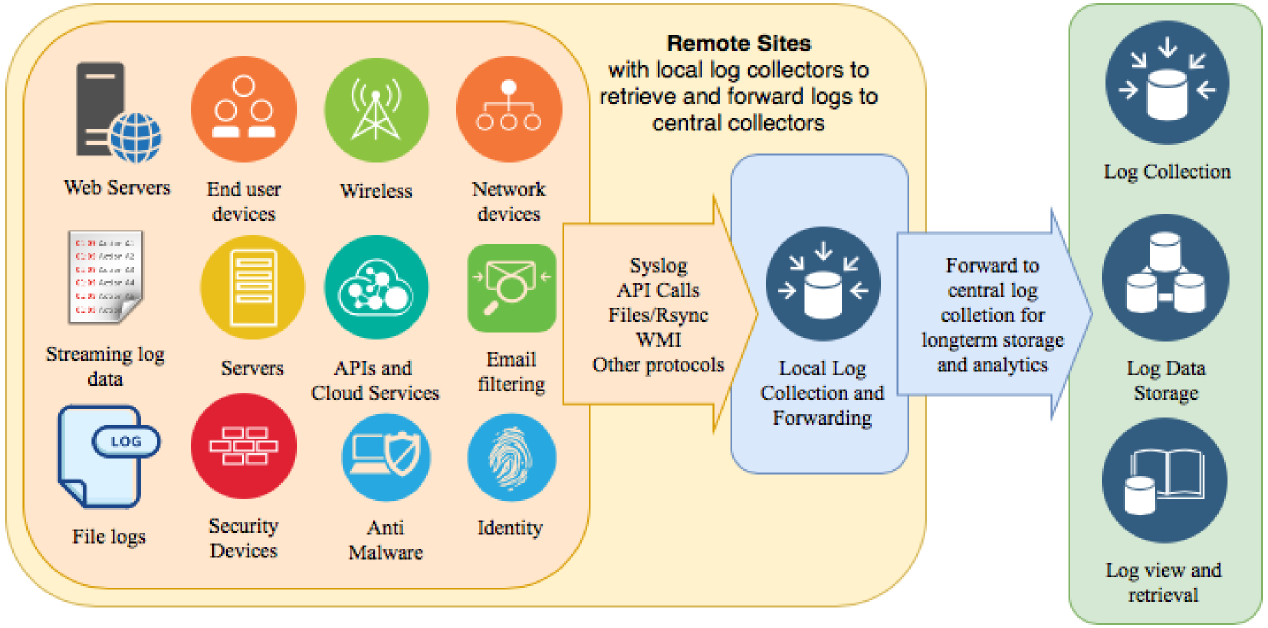
What to verify, test, and monitor

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



Remote Sites
with local log collectors to retrieve and forward logs to central collectors

Web Servers
End user devices
Wireless
Network devices
Streaming log data
Servers
APIs and Cloud Services
Email filtering
File logs
Security Devices
Anti Malware
Identity

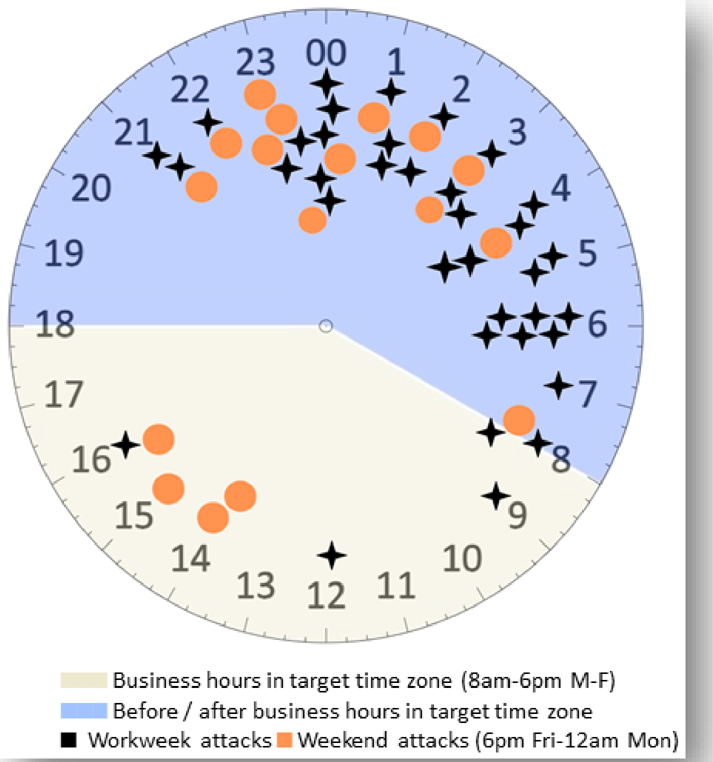
Syslog
API Calls
Files/Rsync
WMI
Other protocols

Local Log Collection and Forwarding

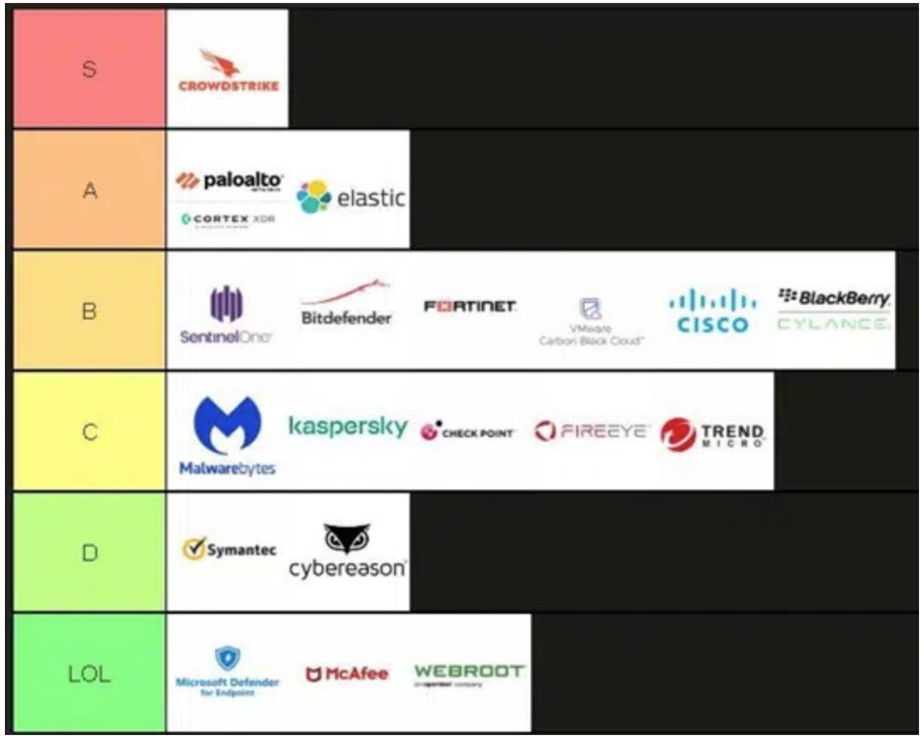
Forward to central log colletion for longterm storage and analytics

Log Collection
Log Data Storage
Log view and retrieval

Evidence that monitoring works



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



S	CROWDSTRIKE					
A	paloalto CORTEX XDR	elastic				
B	SentinelOne	Bitdefender	FORTINET	VMware Carbon Black Cloud	CISCO	BlackBerry CYLANCE
C	Malwarebytes	kaspersky	CHECK POINT	FIREEYE	TREND MICRO	
D	Symantec	cybereason				
LOL	Microsoft Defender for Endpoint	McAfee	WEBROOT			

Attackers discuss EDR tools, and invest in bypasses.

Source: Conti leaks.

MALWARE-FREE ACTIVITY

»

75% 2023

71% 2022

62% 2021

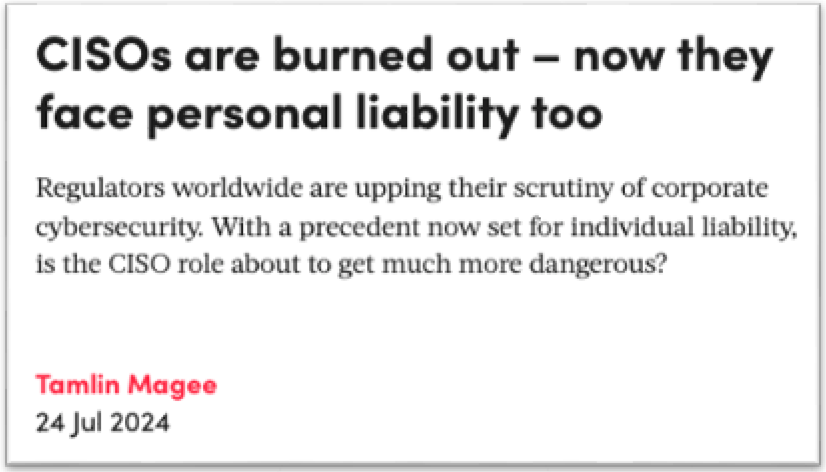
51% 2020

40% 2019

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

Emotional Assurance

The paranoia of a CISO

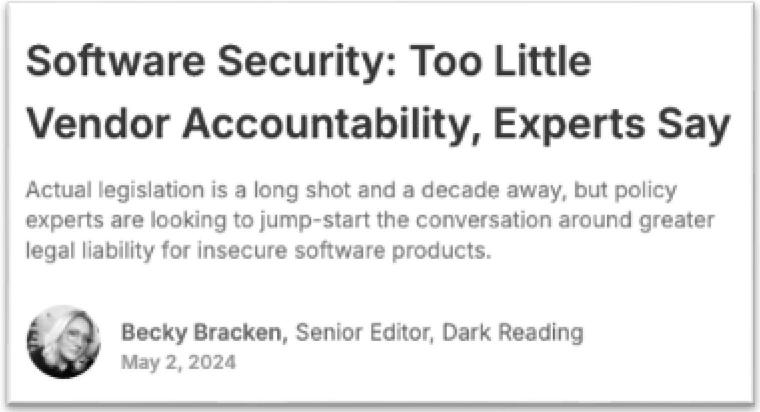


CISOs are burned out – now they face personal liability too

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

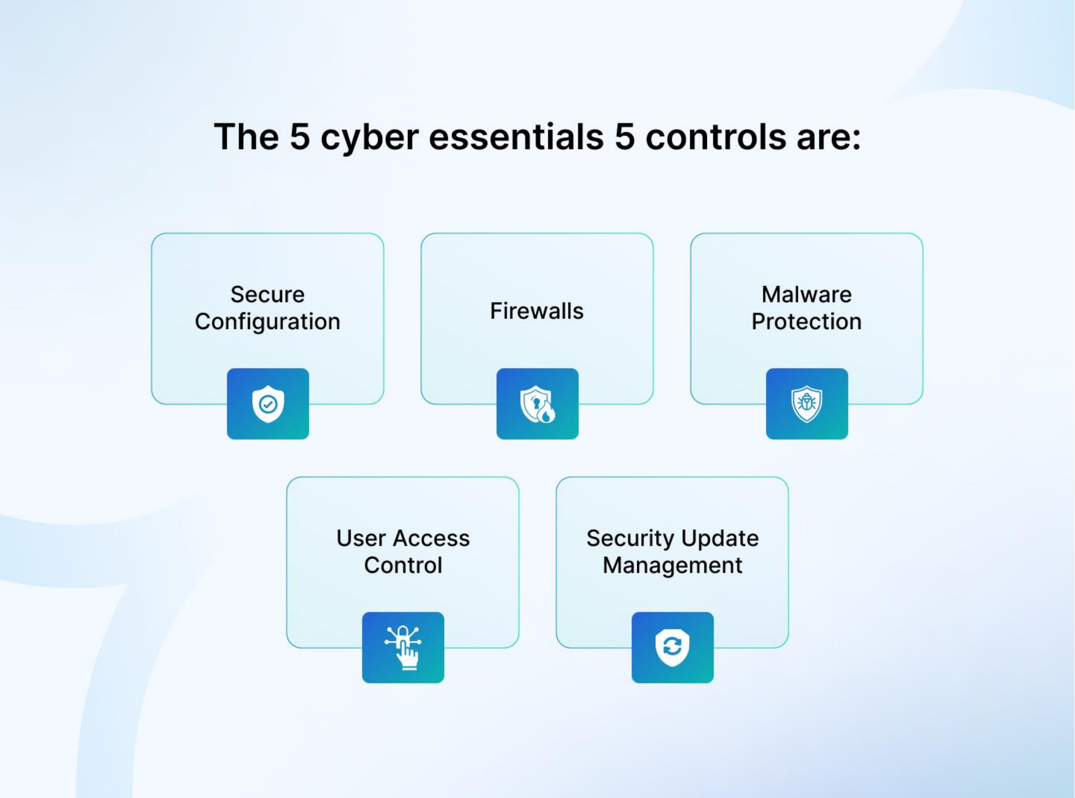
- Pen test and fix
  - Annual, find as many in scope vulns as possible
  - Did you fix what the attacker will exploit?
  - Expensive because it requires human
    - PTaaS?
- Red teaming: employees simulate external attacker
  - Test detection and response
- Attack surface management more "systematic"
  - 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?



The 5 cyber essentials 5 controls are:

Secure Configuration

Firewalls

Malware Protection

User Access Control

Security Update Management

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]

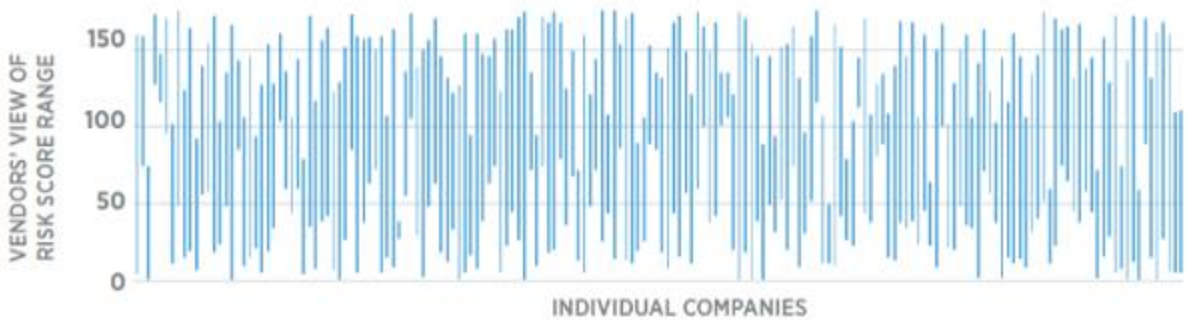
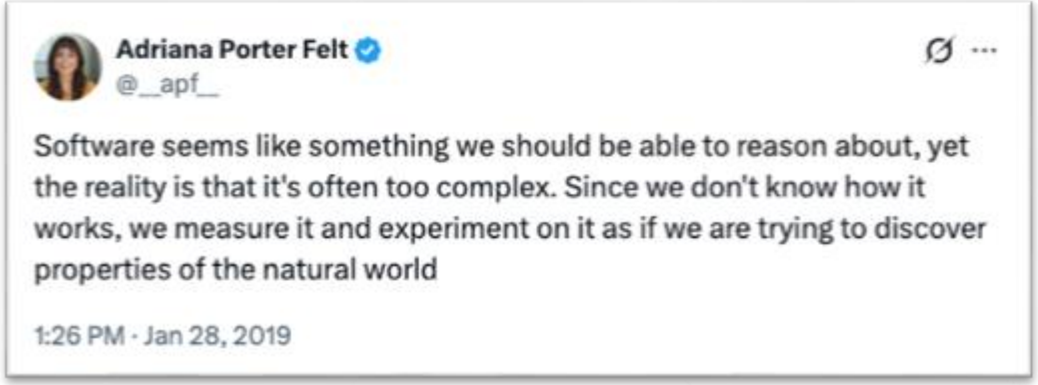


Figure 2: Chart outlining difference between five vendors' view of relative cyber risk presented by companies in a portfolio. The higher the line goes, the more risky the company is considered to be. Each blue line represents one company.

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



Adriana Porter Felt
@__apf__

Software seems like something we should be able to reason about, yet the reality is that it's often too complex. Since we don't know how it works, we measure it and experiment on it as if we are trying to discover properties of the natural world

1:26 PM · Jan 28, 2019

[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?

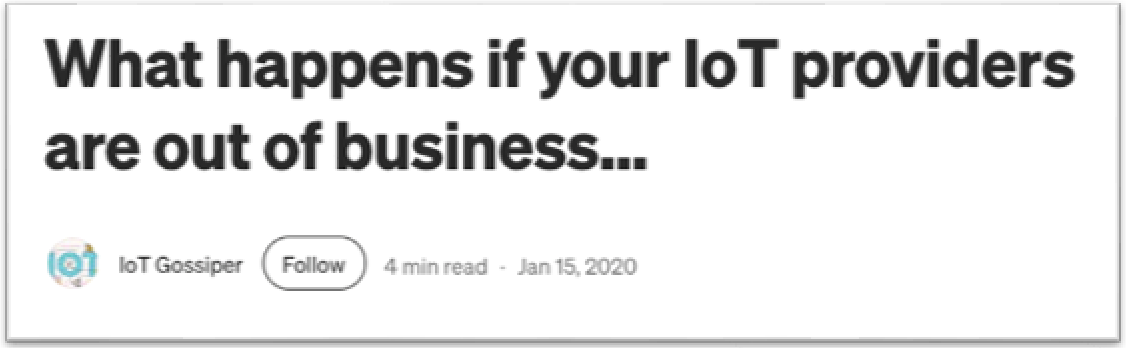
Return on Investment of releasing patches

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



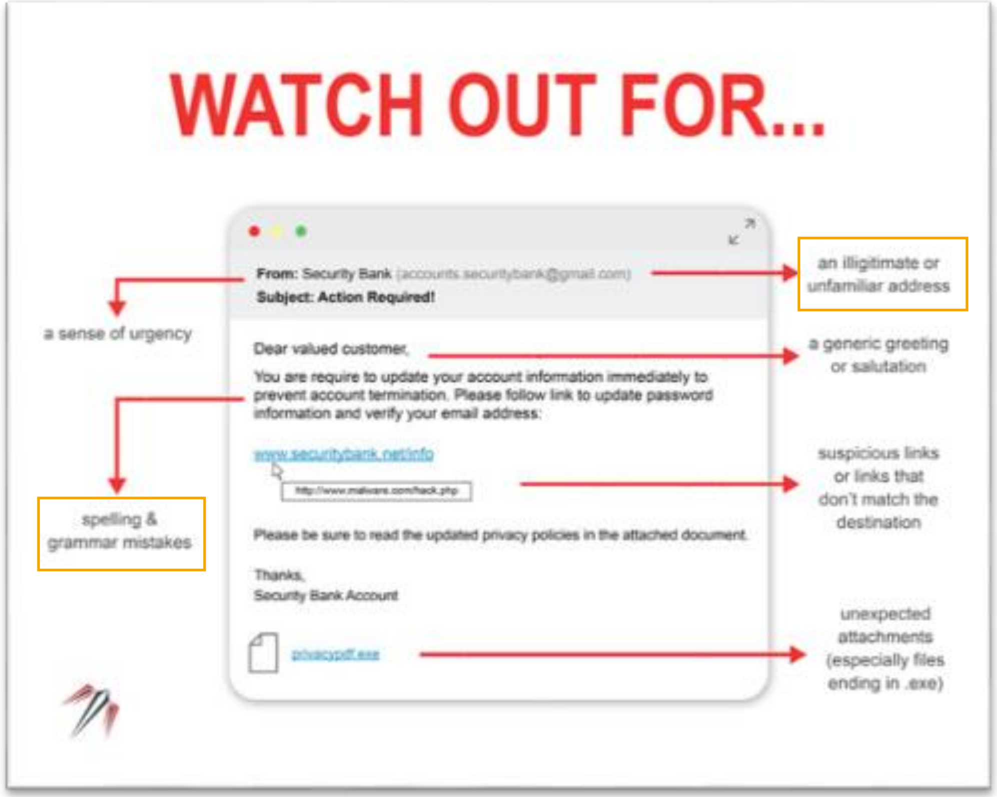
What happens if your IoT providers are out of business...

IoT Gossiper · 4 min read · Jan 15, 2020

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



WATCH OUT FOR...

From: Security Bank (accounts.securitybank@gmail.com)
Subject: Action Required!

Dear valued customer,

You are require to update your account information immediately to prevent account termination. Please follow link to update password information and verify your email address:

www.securitybank.net/info

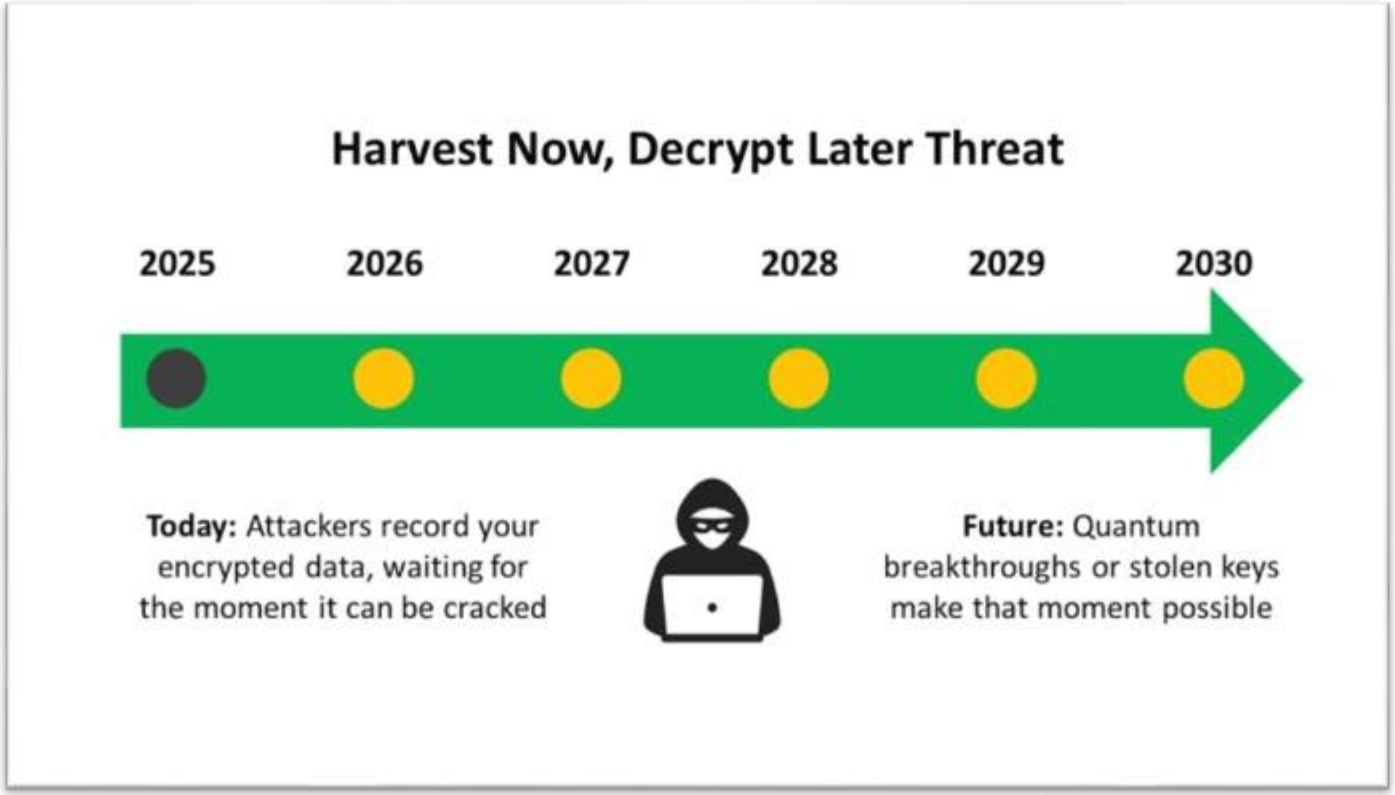
http://www.malware.com/hack.php

Please be sure to read the updated privacy policies in the attached document.

Thanks,
Security Bank Account

privacypdf.exe

an illigitimate or unfamiliar address
a sense of urgency
a generic greeting or salutation
spelling & grammar mistakes
suspicious links or links that don't match the destination
unexpected attachments (especially files ending in .exe)



Harvest Now, Decrypt Later Threat

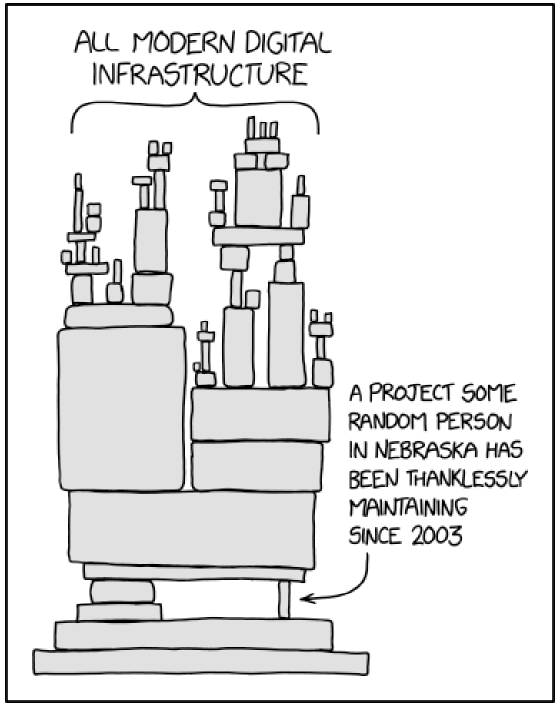
2025
2026
2027
2028
2029
2030

Today: Attackers record your encrypted data, waiting for the moment it can be cracked

Future: Quantum breakthroughs or stolen keys make that moment possible

Ecosystem as strength and vulnerability

Increases the number of stakeholders who can fix an issue.

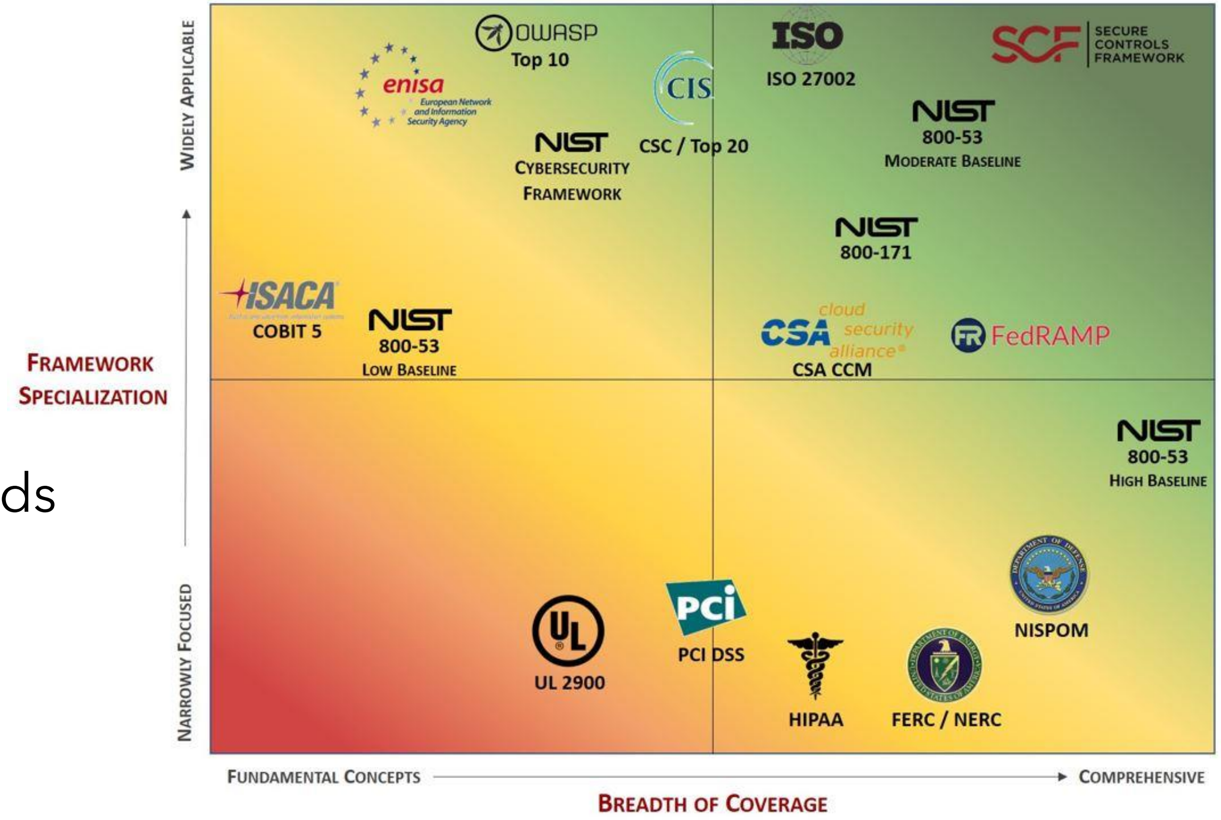

ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

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*?

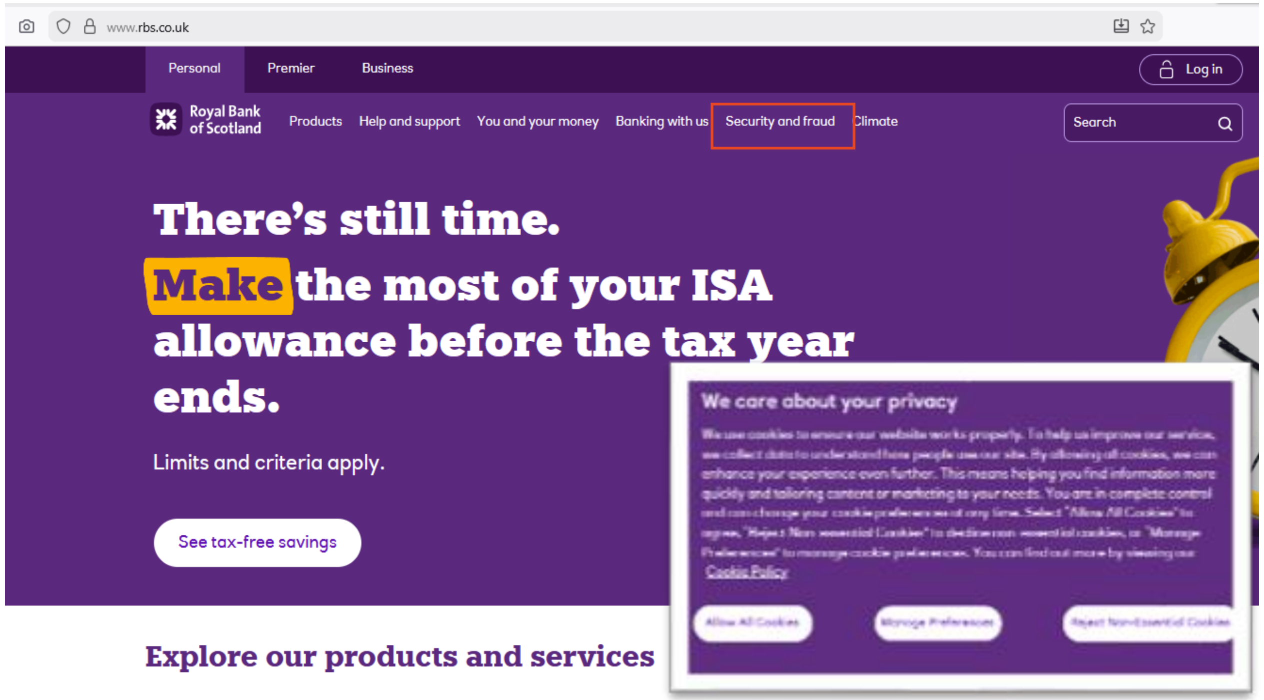
- Customers may require security to do business
  - Individuals for B2C
  - Other organizations for B2B
- Financial institutions
  - Payment Card Industry to process credit cards
  - Insurers to buy a policy
  - Investors or banks to raise capital
- Regulators to avoid penalties, courts to avoid litigation



*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



There's still time. Make the most of your ISA allowance before the tax year ends.

Limits and criteria apply.

Explore our products and services

We care about your privacy

We use cookies to ensure our website works properly. To help us improve our service, we collect data to understand how people use our site. By allowing all cookies, we can enhance your experience even further. This means helping you find information more quickly and tailoring content or marketing to your needs. You are in complete control and can change your cookie preferences at any time. Select "Allow All Cookies" to agree, "Reject Non-essential Cookies" to decline non-essential cookies, or "Manage Preferences" to manage cookie preferences. You can find out more by viewing our Cookie Policy

Banks don't really try to convince you they're secure digitally

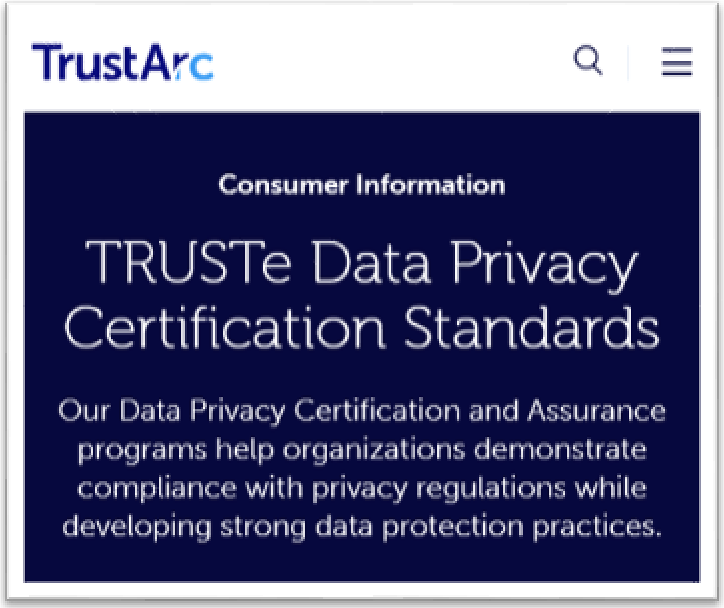
Certifications

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



Consumer Information

TRUSTe Data Privacy Certification Standards

Our Data Privacy Certification and Assurance programs help organizations demonstrate compliance with privacy regulations while developing strong data protection practices.

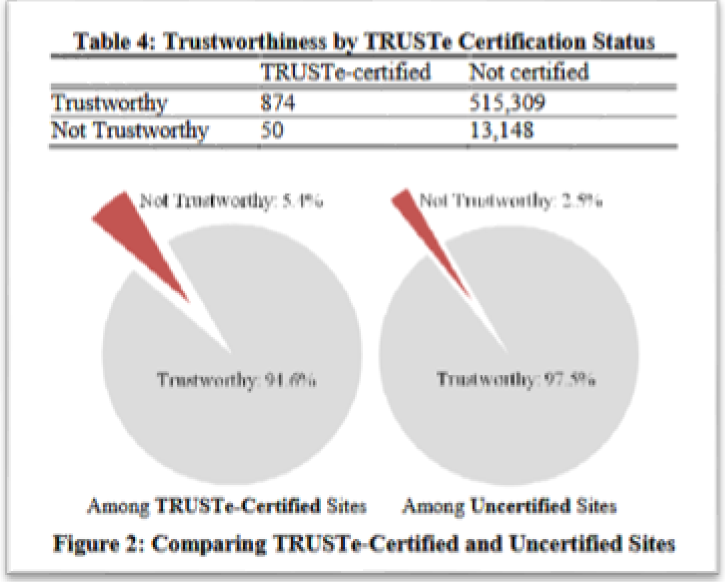


Table 4: Trustworthiness by TRUSTe Certification Status

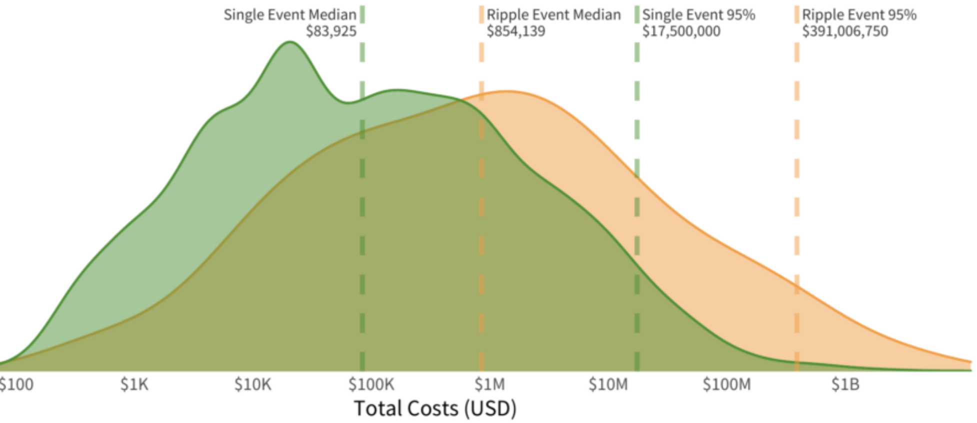
	TRUSTe-certified	Not certified
Trustworthy	874	515,309
Not Trustworthy	50	13,148

Among TRUSTe-Certified Sites Among Uncertified Sites

Figure 2: Comparing TRUSTe-Certified and Uncertified Sites

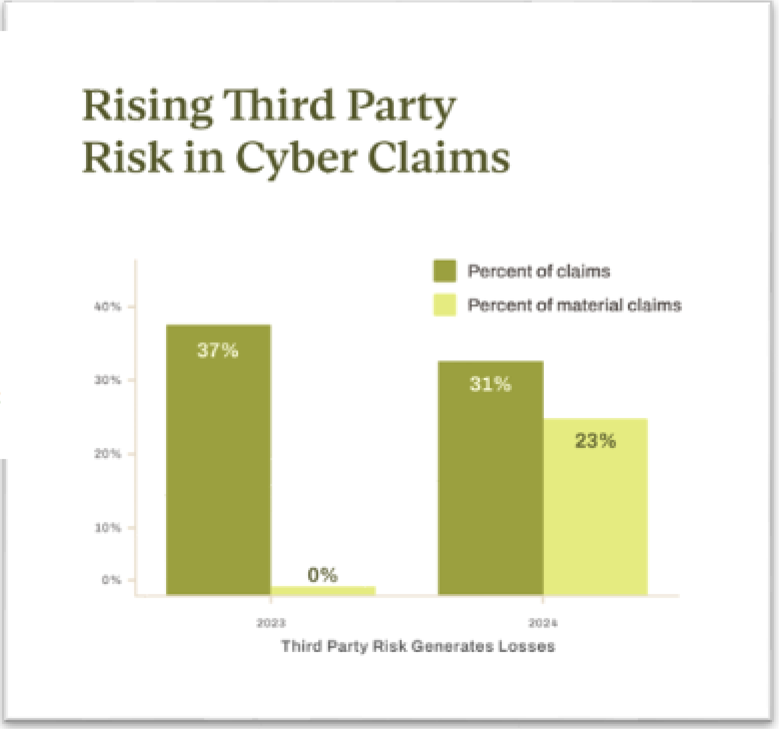
Source: Edelman, Benjamin. "Adverse selection in online" trust" certifications." In *Proceedings of the 11th International Conference on Electronic Commerce*, pp. 205-212. 2009.

Why B2B customers need to be convinced

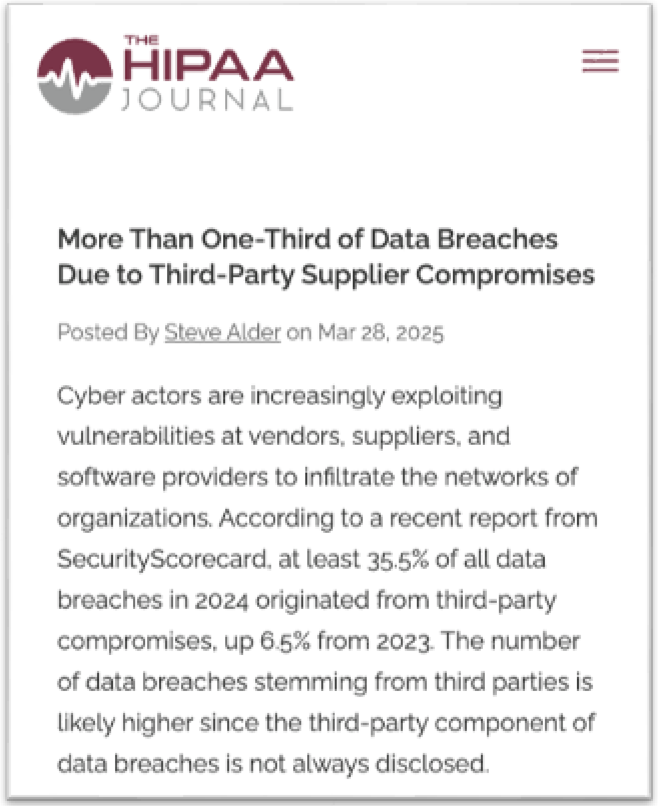


"Ripples are those cyber incidents which have effects (typically financial, legal, or in the form of legal entanglements) beyond the firm initially compromised."

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



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



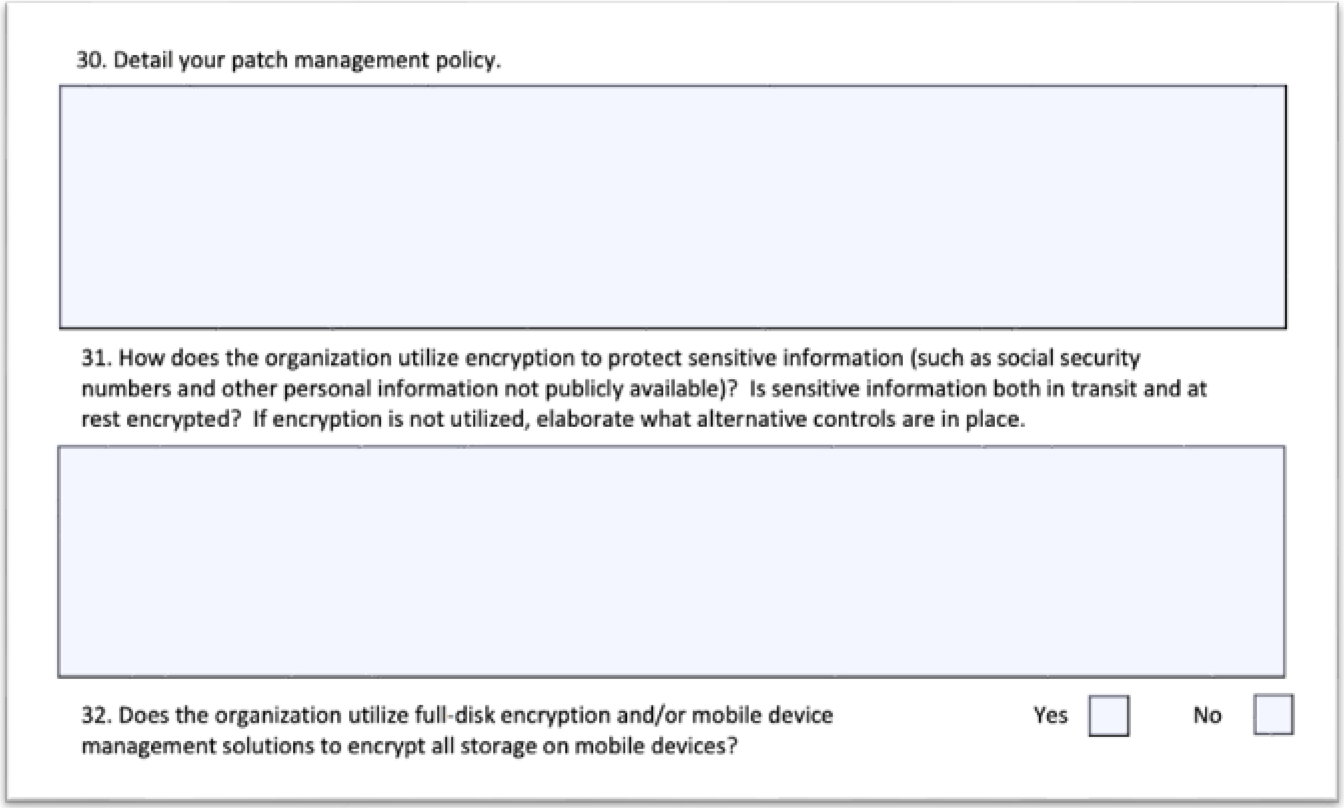
More Than One-Third of Data Breaches Due to Third-Party Supplier Compromises

Posted By Steve Alder on Mar 28, 2025

Cyber actors are increasingly exploiting vulnerabilities at vendors, suppliers, and software providers to infiltrate the networks of organizations. According to a recent report from SecurityScorecard, at least 35.5% of all data breaches in 2024 originated from third-party compromises, up 6.5% from 2023. The number of data breaches stemming from third parties is likely higher since the third-party component of data breaches is not always disclosed.

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.

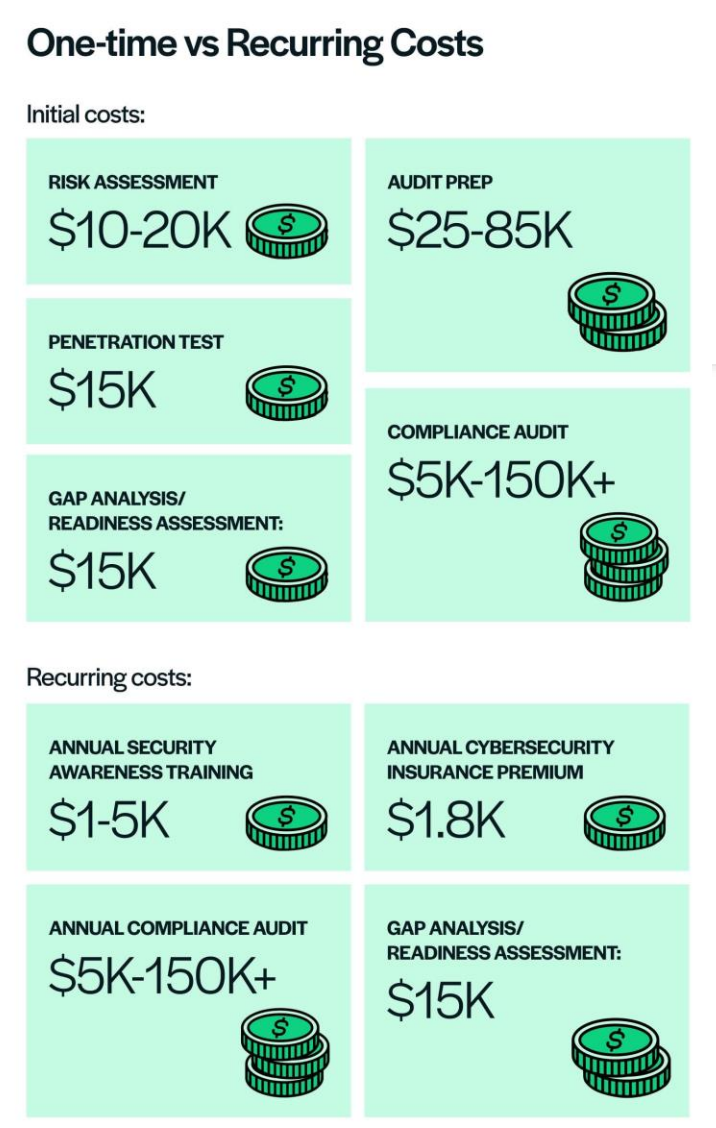
31. How does the organization utilize encryption to protect sensitive information (such as social security numbers and other personal information not publicly available)? Is sensitive information both in transit and at rest encrypted? If encryption is not utilized, elaborate what alternative controls 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
  - o Governments require suppliers to certify to InfoSec standards
    - ▪ UK to Cyber Essentials
    - ▪ USA to FedRamp
    - ▪ DoD to CMMC
  - o Private sector may also require vendors to get certified
    - ▪ SOC2 common for data security
- Economic pressures
  - o Expensive, but motivated by sales
  - o External auditors "maintain" standards



One-time vs Recurring Costs

Initial costs:

RISK ASSESSMENT $10-20K	AUDIT PREP $25-85K
PENETRATION TEST $15K	COMPLIANCE AUDIT $5K-150K+
GAP ANALYSIS/ READINESS ASSESSMENT: $15K	

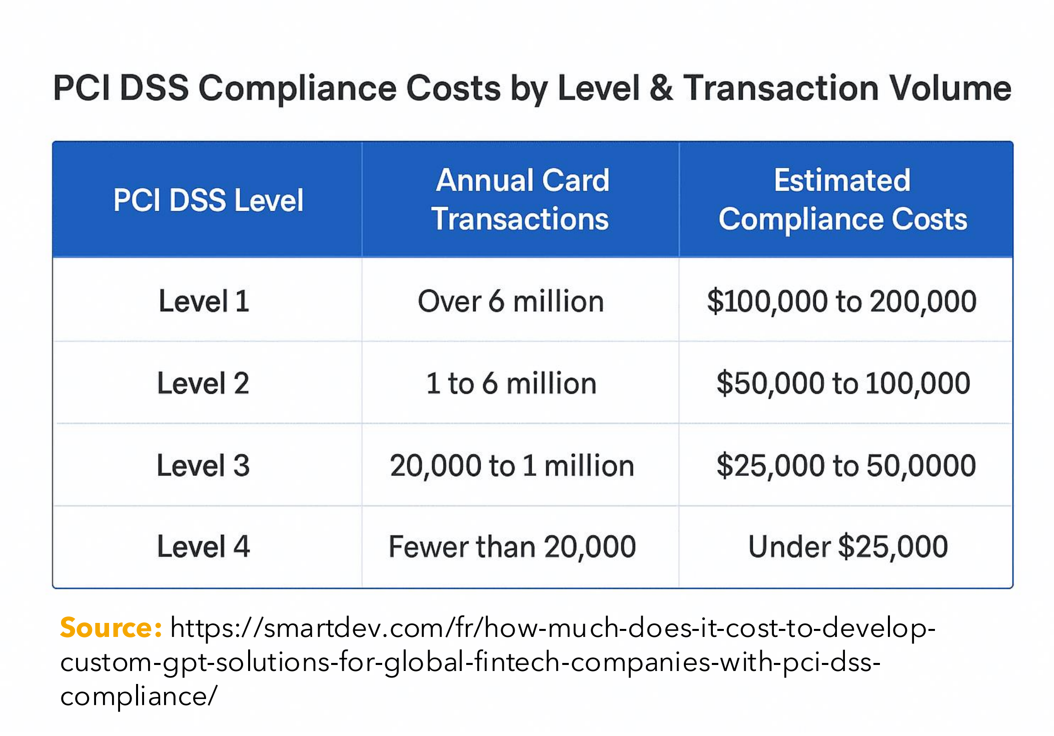
Recurring costs:

ANNUAL SECURITY AWARENESS TRAINING $1-5K	ANNUAL CYBERSECURITY INSURANCE PREMIUM $1.8K
ANNUAL COMPLIANCE AUDIT $5K-150K+	GAP ANALYSIS/ READINESS ASSESSMENT: $15K

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.

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, 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
- Ultimately, compliance is better than nothing

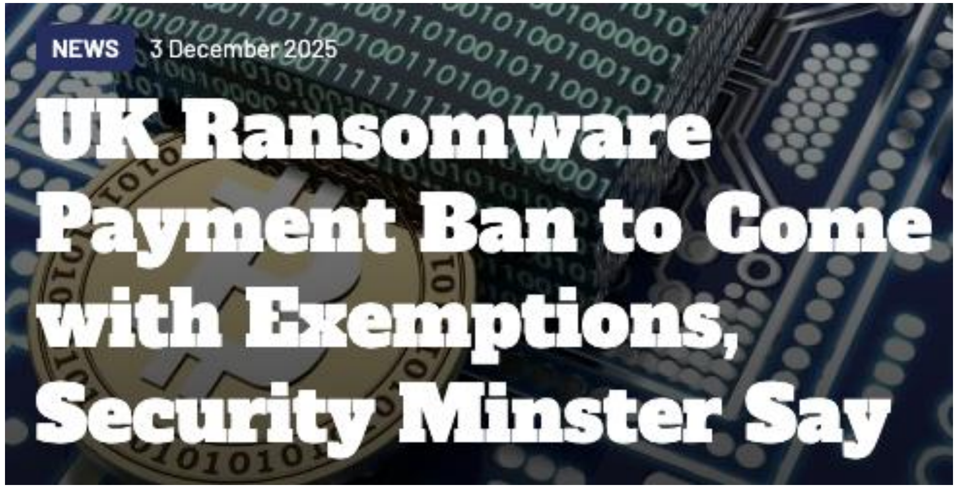
Regulatory capture

- 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 with backdoors for intel access
    - Dual_EC_DRBG

Regulating beyond ex-ante security

Ex-post regulation of incident response

- Mandatory data breach notification to consumers
  - First in California in 2003
  - Truly could not have been done by B2B relationships
- Mandatory notification of authorities
- Direct support for victims
  - FBI helped Colonial Pipeline get their crypto payments back
- Ransomware payment sanctions and bans



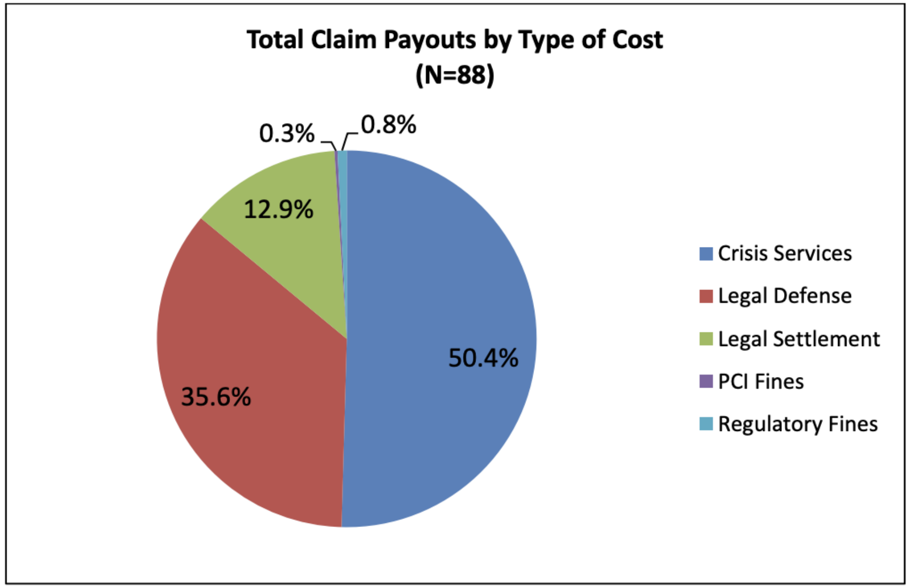
NEWS 3 December 2025

UK Ransomware Payment Ban to Come with Exemptions, Security Minster Say

Costs of security failures

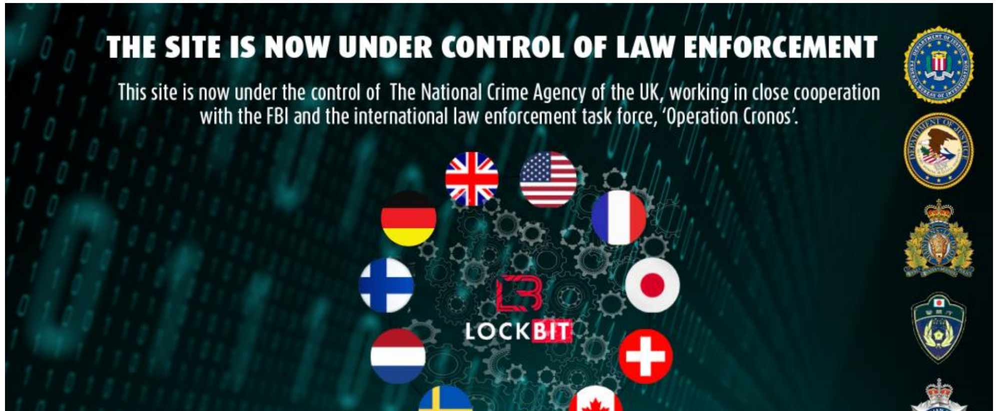
- Set costs for security failures
  - Fines and investigations
  - Create liability regimes by legislation
- Decide who is to blame
  - The hospital who didn't patch in time?
  - The vendor who released insecure software?
- Mandatory data breach response inadvertently added costs to breaches

NetDiligence® 2013 Cyber Liability & Data Breach Insurance Claims
A Study of Actual Claim Payouts



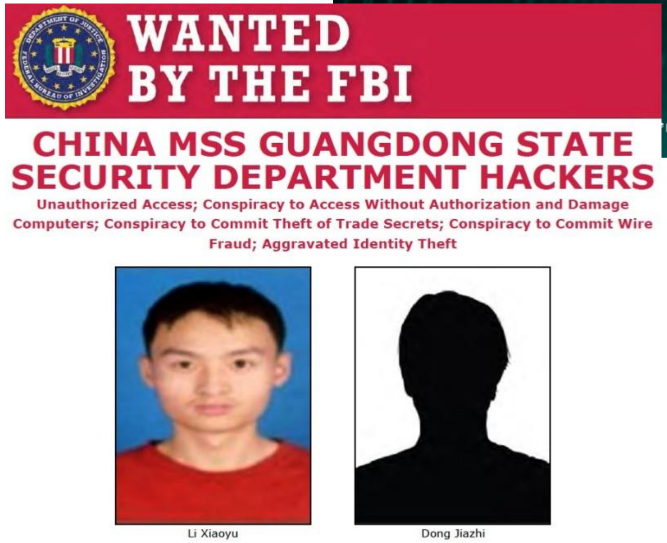
Law enforcement

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



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.



WANTED BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Li Xiaoyu

Dong Jiazhi