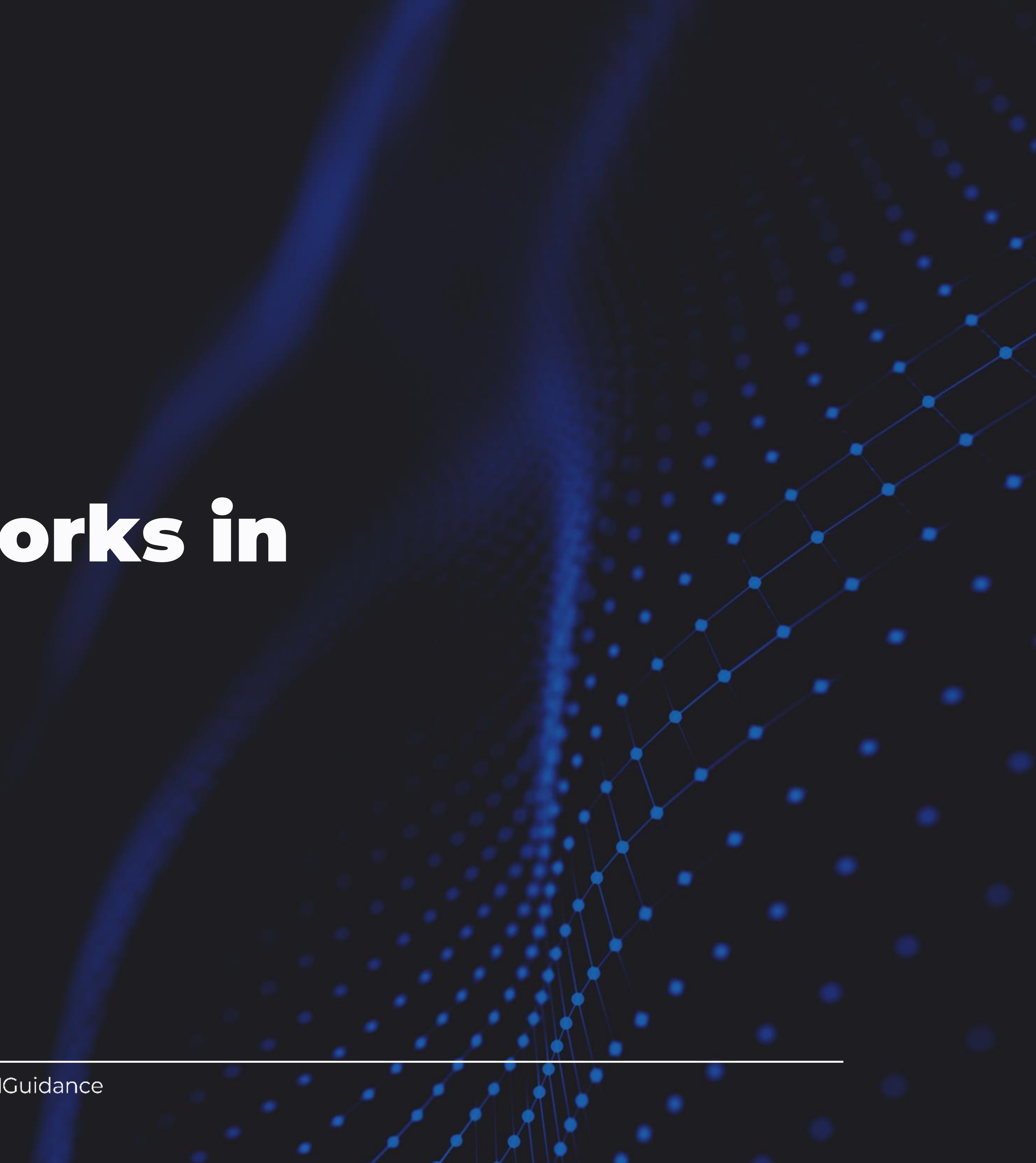
STORMGuidance

The Evolution of Regulatory Frameworks in Risk Management

Harley Morlet



STORM Guidance

Full service offering for reinsurers, insurers, brokers and clients

Assess

Lightweight cyber risk assessments to enable clients to learn and improve their cyber security and to help insurers and reinsurers manage book risk

Plan

Helping insured clients to create, learn (through training) and exercise / test their plans in dealing with different types of cyber incidents in the context of their business.

Respond

Delivering a fully coordinated and Integrated Cyber Incident Response Team (I-CIRT)

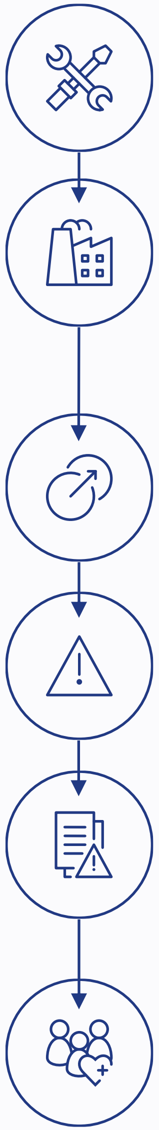
ReSecure: full-service offering for insured clients

CyberCare: retainer and subscriber for direct cyber crisis response

The Evolution of Regulatory Frameworks

1. **History of Health and Safety**
2. **The state of Cyber Security and Regulation**
3. **Regulatory next steps**

A brief history of health & safety regulation



Pre-Industrial Revolution

Guilds defined health practices for various trades, but implementation was limited.

Industrial Revolution

The rise of the poor working conditions in factories led to early legislation for specific industries, such as the Health and Morals of Apprentices Act 1802 and the Factory Act of 1833, which protected apprentices and set age limits for child workers.

Broadening Scope

Legislation expanded to cover mines, railways, and construction.

Aberfan disaster

116 children and 28 adults killed in a coal tip collapse.

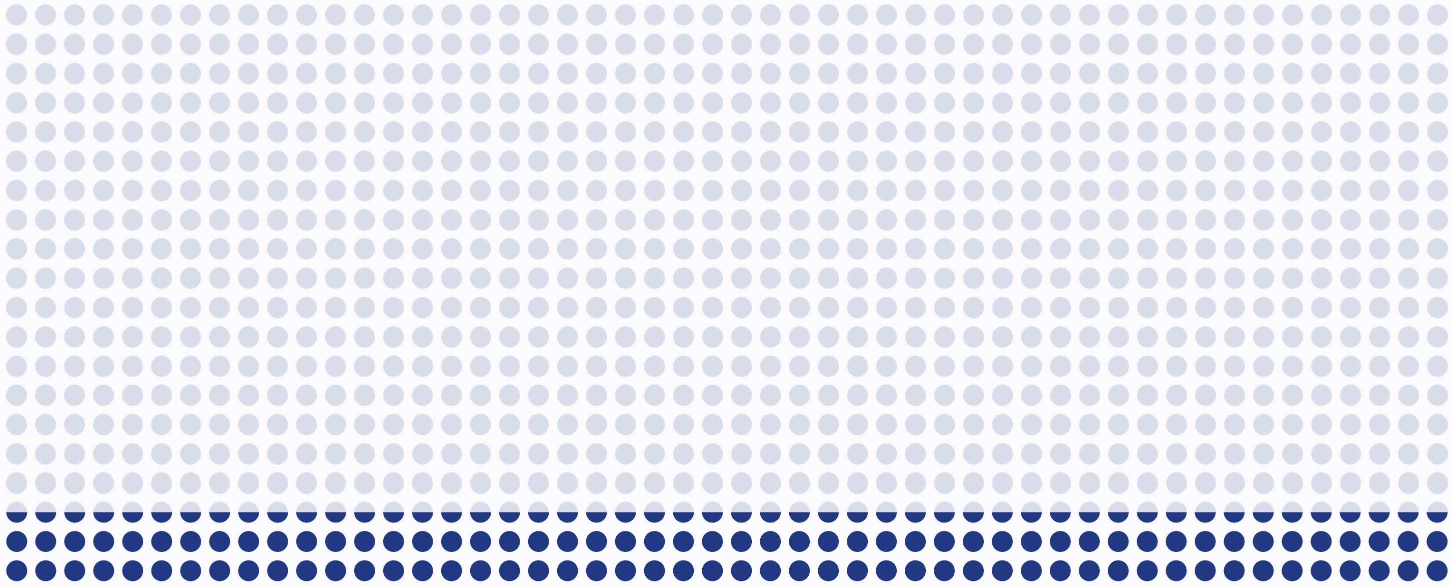
Robens Report

By the late 1960s, health and safety laws in the UK were fragmented and outdated, leading to the Robens Report's recommendations.

Health & Safety at Work Act 1974

Created the Health and Safety Executive (HSE) and emphasized the responsibilities of both employers and employees in maintaining safe workplaces, setting the stage for modern health and safety standards.

Result of the Health & Safety at Work Act 1974



Fatal injuries at work have dropped by 85% from more than 1000 a year in 1974 to less than 150 today.

Before the act, there were around 1,000 work-related deaths each year, half a million injuries, and 23 million working days lost each year due to industrial injury and disease. We are now down to less than 150 deaths a year.

Where are we with cyber regulation?

Pre-Industrial Revolution

Guilds defined health practices for various trades, but implementation was limited.

Industrial Revolution

The rise of the poor working conditions in factories led to early legislation for specific industries, such as the Health and Morals of Apprentices Act 1802 and the Factory Act of 1833, which protected apprentices and set age limits for child workers.

Broadening Scope

Legislation expanded to cover mines, railways, and construction.

Aberfan disaster

116 children and 28 adults killed in a coal tip collapse.

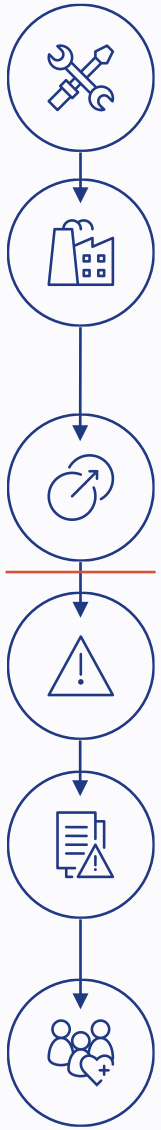
Robens Report

By the late 1960s, health and safety laws in the UK were fragmented and outdated, leading to the Robens Report's recommendations.

Health & Safety at Work Act 1974

Created the Health and Safety Executive (HSE) and emphasized the responsibilities of both employers and employees in maintaining safe workplaces, setting the stage for modern health and safety standards.

Where are we with cyber regulation?



Pre-Industrial Revolution

Guilds defined health practices for various trades, but implementation was limited.

Industrial Revolution

The rise of the poor working conditions in factories led to early legislation for specific industries, such as the Health and Morals of Apprentices Act 1802 and the Factory Act of 1833, which protected apprentices and set age limits for child workers.

Broadening Scope

Legislation expanded to cover mines, railways, and construction.

We are here.

Aberfan disaster

116 children and 28 adults killed in a coal tip collapse.

Robens Report

By the late 1960s, health and safety laws in the UK were fragmented and outdated, leading to the Robens Report's recommendations.

Health & Safety at Work Act 1974

Created the Health and Safety Executive (HSE) and emphasized the responsibilities of both employers and employees in maintaining safe workplaces, setting the stage for modern health and safety standards.

The state of cyber security

1. Companies are unaware of their risk
2. We have a patchwork of frameworks and regulation
3. We have very little enforcement

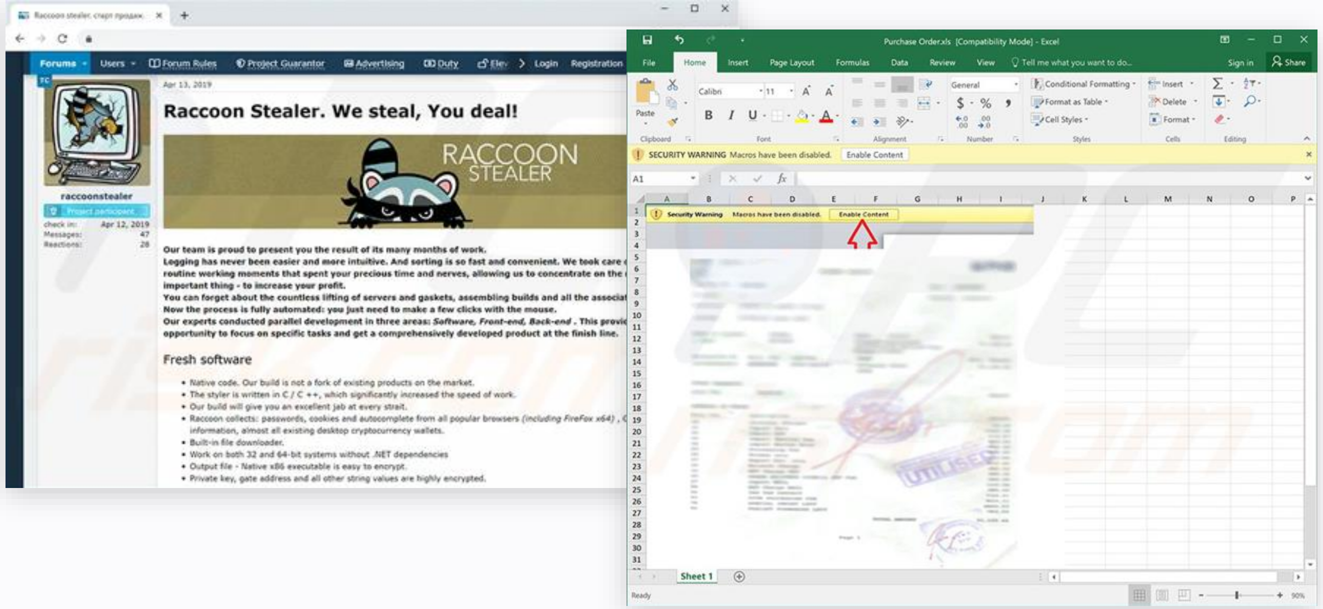
Cybercrime ecosystem

Off the shelf malware tools to help extract credentials from your victims

Malware as a service

Raccoon stealer – first seen in April 2019 — was a popular infostealer because of its low price (USD$75 per week and $200 per month) and rich features.

Racoon is used to steal sensitive and confidential information including login credentials, credit card information, cryptocurrency wallets and browser information (cookies, history, autofill) from almost 60 applications.



Apr 13, 2019

Raccoon Stealer. We steal, You deal!

Our team is proud to present you the result of its many months of work.
Logging has never been easier and more intuitive. And sorting is so fast and convenient. We took care routine working moments that spent your precious time and nerves, allowing us to concentrate on the important thing - to increase your profit.
You can forget about the countless lifting of servers and gaskets, assembling builds and all the associat
Now the process is fully automated: you just need to make a few clicks with the mouse.
Our experts conducted parallel development in three areas: *Software, Front-end, Back-end* . This provid opportunity to focus on specific tasks and get a comprehensively developed product at the finish line.

Fresh software

- Native code. Our build is not a fork of existing products on the market.
- The styler is written in C / C ++, which significantly increased the speed of work.
- Our build will give you an excellent jab at every strait.
- Raccoon collects: passwords, cookies and autocomplete from all popular browsers *(including FireFox x64)* , C information, almost all existing desktop cryptocurrency wallets.
- Built-in file downloader.
- Work on both 32 and 64-bit systems without .NET dependencies
- Output file - Native x86 executable is easy to encrypt.
- Private key, gate address and all other string values are highly encrypted.

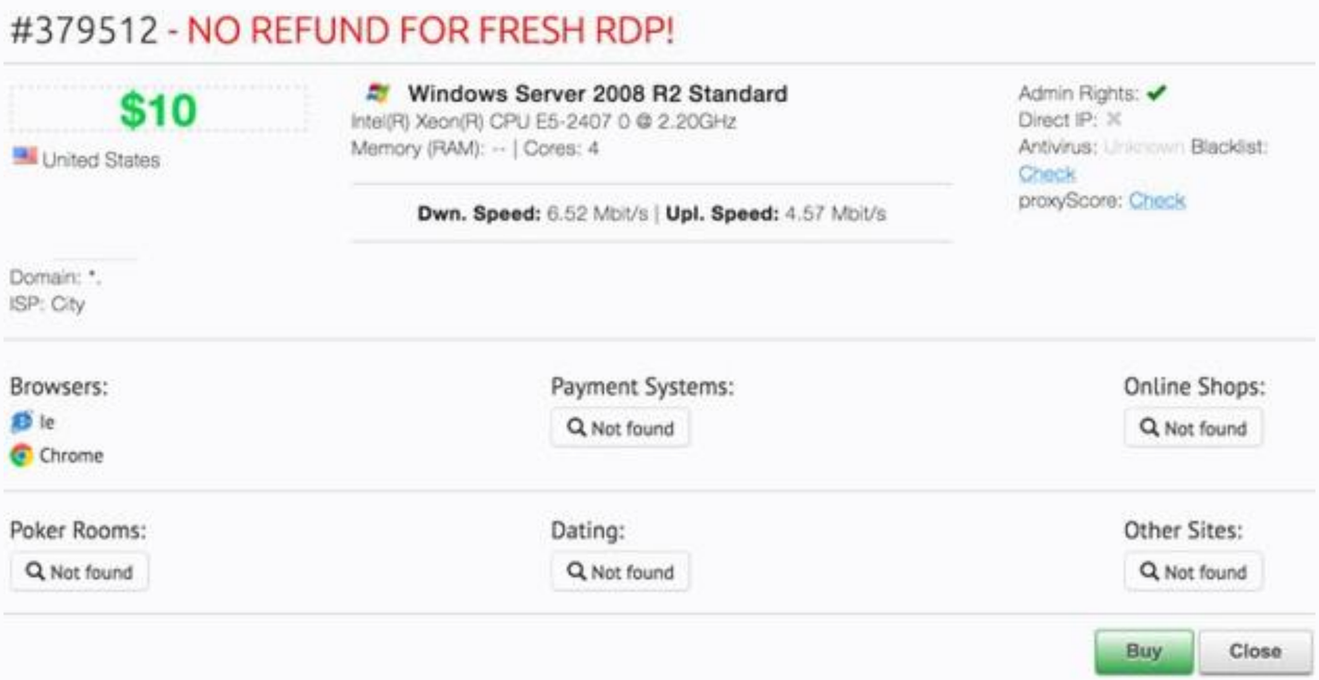
SECURITY WARNING Macros have been disabled. Enable Content

Source: https://www.cyberark.com/resources/threat-research-blog/raccoon-the-story-of-a-typical-infostealer, https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/#:~:text=The%20cybercrime%20group%20behind%20the,in%20the%20invasion%20of%20Ukraine.

Cybercrime ecosystem

Cybercrime business vertical: Access brokers

How much is network access is being sold for on the dark web



#379512 - NO REFUND FOR FRESH RDP!

$10

United States

Windows Server 2008 R2 Standard

Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz

Memory (RAM): -- | Cores: 4

Dwn. Speed: 6.52 Mbit/s | **Upl. Speed:** 4.57 Mbit/s

Admin Rights: ✓

Direct IP: ✗

Antivirus: Unknown Blacklist: Check

proxyScore: Check

Domain: *.

ISP: City

Browsers:

Ie

Chrome

Payment Systems: Not found

Online Shops: Not found

Poker Rooms: Not found

Dating: Not found

Other Sites: Not found

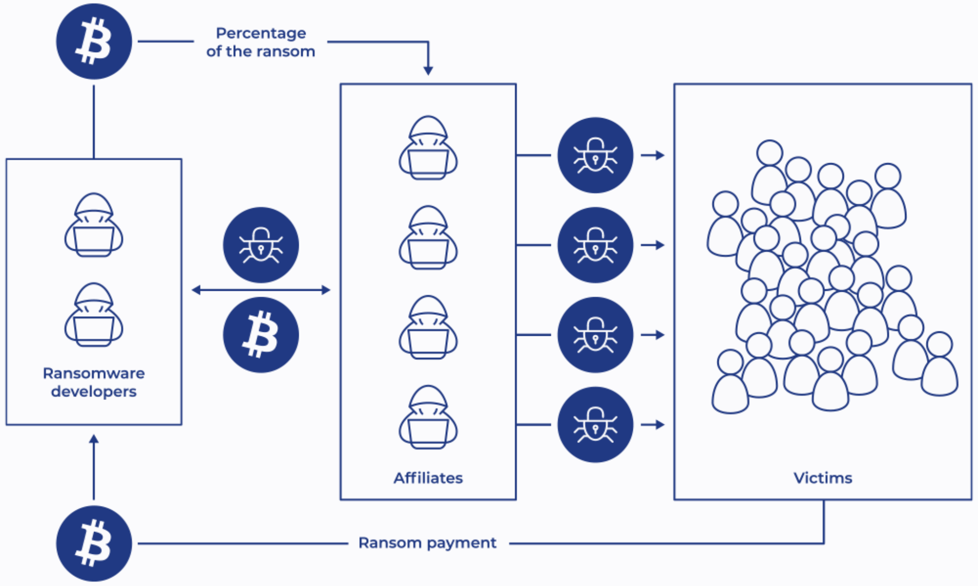
Source: https://thehackernews.com/2018/07/rdp-shop-dark-web.html

Cybercrime ecosystem

Cybercrime business vertical: Ransomware as a service (RaaS)

These services include:

- A “build your own ransomware package” panel, with setup and technical support
- The ability to set your own ransom, and custom post-compromise message
- A command and control panel to manage your demands, and victim communication
- Payment portal and negotiation support
- Dedicated leak site



Sources: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ and https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac?t=1653301902242

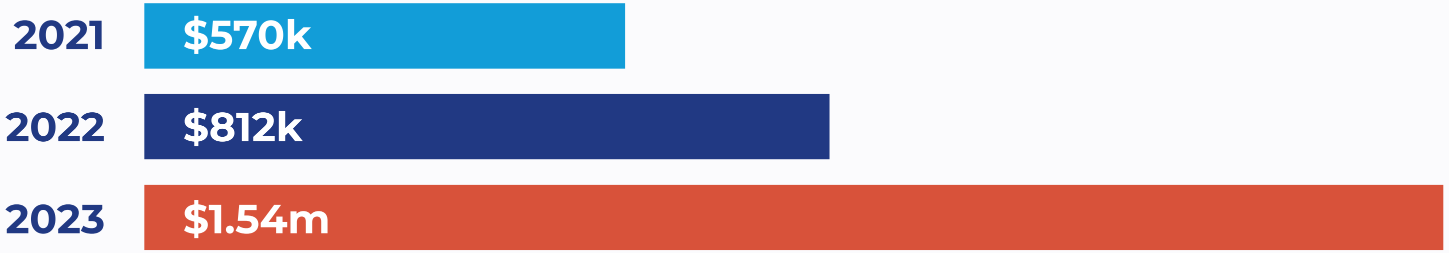
The state of cybersecurity

Growing frequency of attacks:

Nearly half (48%) of SMEs have experienced at least one cyber incident in the past year. (Source – Infosecurity Magazine).

“Our own trend data reveals more organisations than ever are experiencing cyber security breaches” (Source – ICO)

Extortion growth:



The average ransom by year. (Source – GRC world forums, Source – Sophos)

No prosecution:

“cyber enforcement efforts are so scattered that less than 1% of malicious cyber incidents see an enforcement action taken against the attackers.” (Source – Third Way)

The Cyber Regulation Landscape

Regulations

- Payment Card Industry Data Security Standard (PCI DSS)

For companies that process, store, or transmit credit card information.

- DORA (Digital Operational Resilience Act)

Ensures that financial institutions can withstand, respond to, and recover from ICT-related disruptions and threats.

- GDPR

Data protection law enacted by the European Union to safeguard individuals' personal data and privacy

Frameworks and certifications

- Cyber Essentials / ISO 27001/ NIST/ NCSC codes of practice

Challenges with GDPR enforcement

There has been a lack of enforcement from the ICO regarding security breaches.

- 1/3 of 5443 incidents reported were ‘unassigned’ over five years (based on our own freedom of information act request)
- The ICO has approximately 680 staff, however less than 10 of these work in their investigation unit. (Source – Irvings Law)
- The ICO has levied 18 fines in 2023 – 0 were for security breaches. Almost all fines issued by the ICO are for illegal processing of personal data, and breaches of electronic marketing rules (PECR fines). (Source – ICO)

What needs to be done

Businesses need a sobering assessment of their risk

We need to dispel the myth that a cyber incidents won't happen. Risk assessments will help organisations appreciate their security posture.

Implement financial repercussions for negligence

Implement small fines for visible vulnerabilities, utilising scanning technology to detect and enforce compliance, thereby encouraging better security practices.

STORMGuidance

Thank you for your attention