Welcome to our Seminar
Empowering the Future of Housing

chess® Making it Easy to work **Securely, Anywhere, Anytime**

Protecting Housing Associations

Empowering the Future of Housing

Protecting the nation, business and people

Gavin Wood

CEO, CyberLab

Worked in IT industry since 1999

UK CNI Architect

Specialised in Cyber Security 2015

Started CyberLab 2023

cyberlab

Protecting the nation, business and people

Meet the Speakers

Gavin Wood

CEO, CyberLab

Adam Myers

Sales Director, CyberLab

cyberlab

Protecting the nation, business and people

Agenda

- Introduction
- What are the Trends inc. Government Research
- Ransomware & Housing Associations
- Protecting Housing Associations
- Q&A

Protecting the nation, business and people

Awards and Accreditations

SOPHOS Partner Award Winner 2025

EMEA Partner of the Year

SOPHOS Partner Award Winner 2025

UKI Partner of the Year

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

THE CYBER SCHEME

IASME CONSORTIUM

SOPHOS Partner Award Winner 2025

UKI Public Sector Partner of the Year

FORESCOUT

National Cyber Security Centre

CREST

Vendor Partners

SOPHOS Forcepoint FORESCOUT /logpoint

proofpoint. SecurEnvoy vicarius mimecast

Island cisco Microsoft egress

State of Cyber Security 2025

43%

Over four in ten UK businesses (43%) reported cyber security breach or attack in the last 12 months.

1

Source: Gov.Uk

$1.5m

The average cost to recover from a ransomware attack dropped, excluding the ransom payment.

Source: The State of Ransomware 2025, Sophos

4%

Of housing associations feel the sector is prepared for a ransomware attack.

Source: Housing Digital, 2024

1: Cyber Security Breaches Survey 2025, Gov.UK 2: 2025 Ransomware Trends & Proactive Strategies, Veeam 3:The State Of Ransomware 2025, Sophos

cyberlab

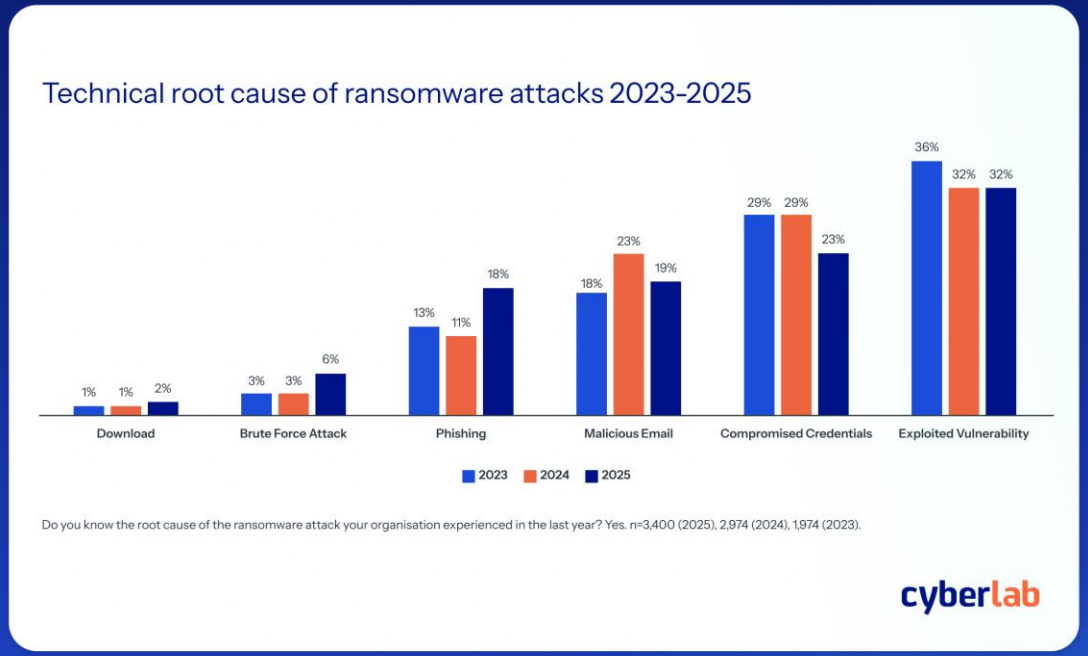
Protecting the nation, business and people

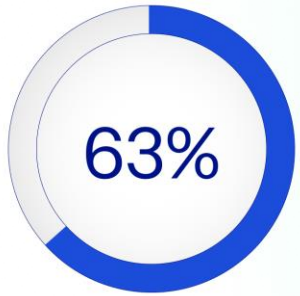
Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.

NCSC

Why Organisations Fall Victim to Ransomware

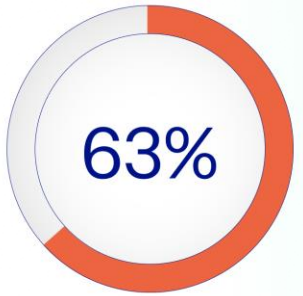
Operational root cause





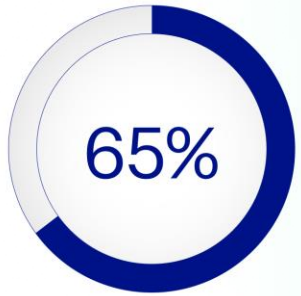
Protection Issue

(lack of or poor quality protection solutions)



Resourcing Issues

(lack of expertise or people/capacity)



Security Gap

(known or unknown)

The State Of Ransomware 2025, Sophos

Risks to Your Organisation

Biggest Risks

- Exploited Vulnerabilities
- Compromised Credentials
- Visibility
- Phishing & Malicious Emails
- Legacy Systems
- Resource
- Supply Chain

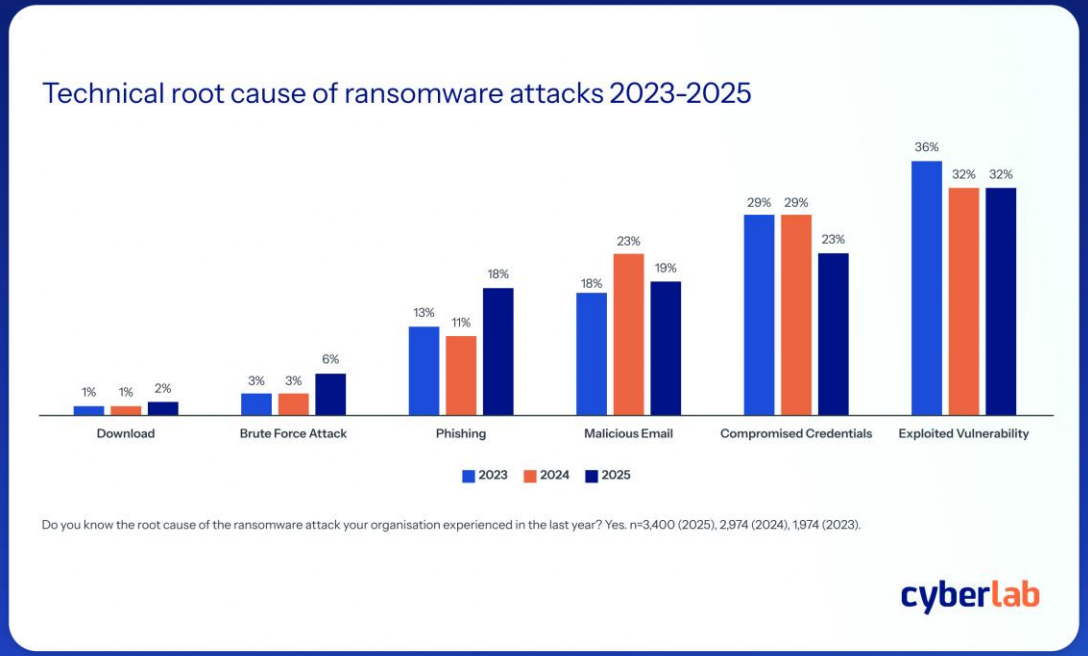
Security Testing Results

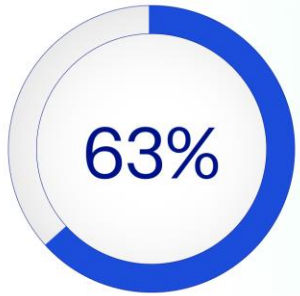
- Outdated Software - including:
  - Missing Windows Patches
  - Vulnerable Network Device Firmware
  - Vulnerable and/or Unsupported 3rd-Party Software
  - Unsupported Operating Systems
- Web Application Component Vulnerabilities
- Weak Passwords on Domain User Accounts
- Wireless Pre-Shared Key in Use

CyberLab Penetration Test Team Analysis

Why Organisations Fall Victim to Ransomware

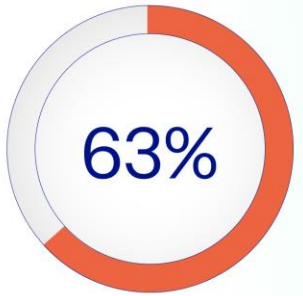
Operational root cause





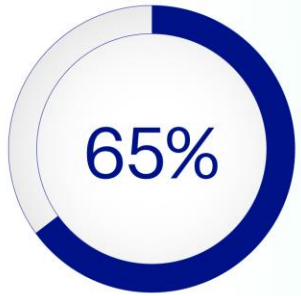
Protection Issue

(lack of or poor quality protection solutions)



Resourcing Issues

(lack of expertise or people/capacity)



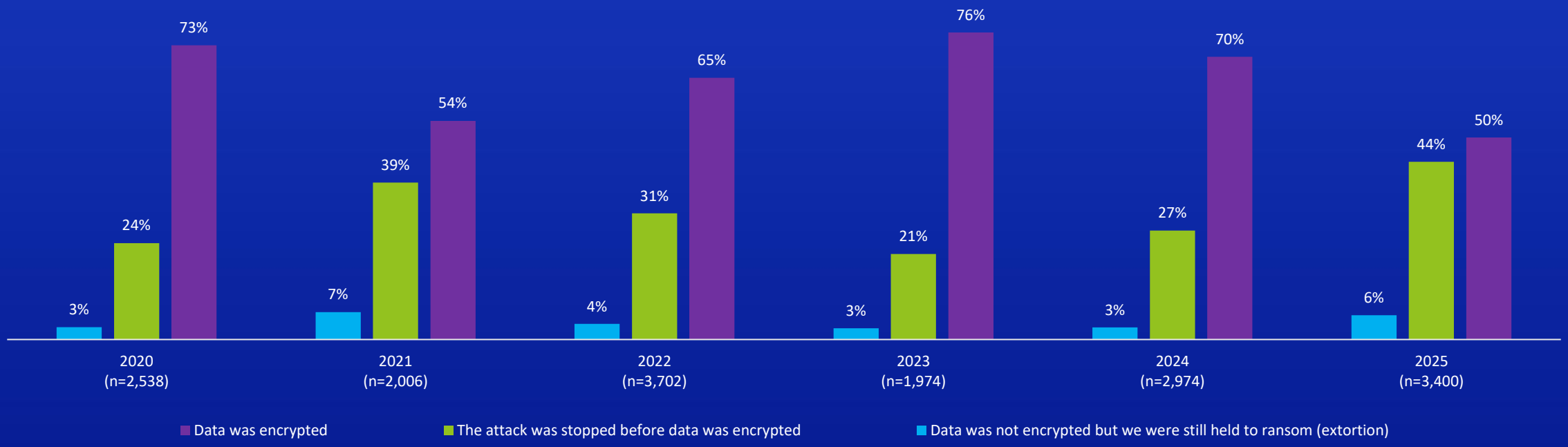
Security Gap

(known or unknown)

The State Of Ransomware 2025, Sophos

Encryption: What Happens to Your Data

Data encryption is at the lowest rate in six years. At the same time, the percentage of organisations whose data was not encrypted but they were held to ransom anyway (extortion) doubled in the last year.



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.

Cyber Attacks in Housing Associations

Recent News

Why housing associations are lucrative to cybercriminals

So it's no wonder that cybercriminals have been targeting the industry for years. Some successful cyber-attacks have been made public, with high-profile cases reaching the press as well as technology and cyber security trade publications. Accounts usually tell of successful break-ins where criminals have stolen the data of thousands of citizens, or, equally maliciously, ransomware attacks where housing providers have been locked out of their systems until they pay up. And while exact figures aren't always made public, it's well-publicised that cybercriminals can charge millions of pounds at a time.

Clarion Housing: Anger over landlord silence since cyber attack

2 September 2022

Unexpected Cyber Threats Put Housing Associations and Tenants at Risk

06.07.24

News > South London News > Housing

Tenants 'bombarded with phishing scams' beg government to step in after housing association hack

Tenants have reportedly been left in the dark and unable to request for repairs, report anti-social behaviour, enquire about rent or service charges or get help with finances since Friday, June 17

Connexus cyber security incident update FAQ

21st February, 2024 R.Goodwin + Company

In December 2023, Connexus experienced a cyber security incident, which involved unauthorised access to its systems. The IT team at Connexus worked quickly to contain the situation, switching off systems to protect customer data. All relevant authorities, including the ICO and the Regulator of Social Housing were informed.

CASE STUDY

Moat Homes

Challenge: Moat had already laid strong foundations for cyber security. Their internal IT team was efficient and knowledgeable but lacked the capacity for round-the-clock coverage.

Solution: The combined delivery of MDR, penetration testing, and hands-on support has significantly strengthened Moat Home's cyber resilience. With 24/7 monitoring and expert guidance in place, the organisation has reduced its risk exposure without adding pressure to internal resources.

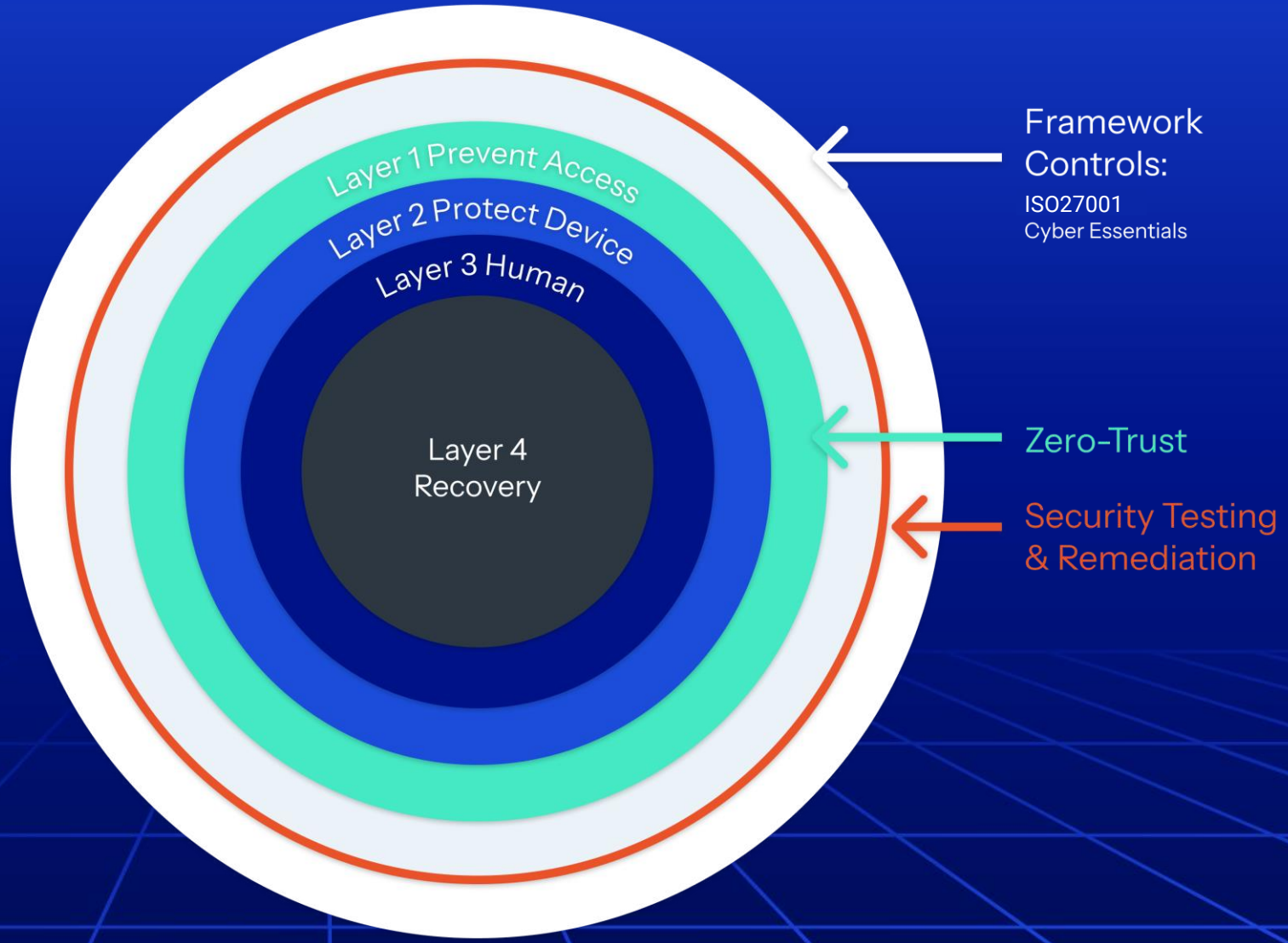
"CyberLab's deep technical knowledge and proactive support have been instrumental in helping us navigate complex threats with confidence. Their team of experts have become a trusted extension of our IT function."

– Warren Yeo, Head of IT Services at Moat

cyberlab

Protecting the nation, business and people

Layers of Security



cyberlab

Protecting the nation, business and people

Recommendations

Prevention

Secure your organization by controlling your attack surface, prioritizing patching, implementing MFA, and providing ongoing training on how to detect and respond to phishing emails.

Protection

Robust security demands strong foundations. Focus on effective foundational controls and tools that are easy to ensure optimal configurations.

Detection and response

Detecting and neutralizing an adversary inside your environment before they can compromise your backups or encrypt your data will improve your outcomes.

Planning and preparation

An incident response plan is essential for mitigating the impact of a major attack. Practicing data restoration from backups ensures swift and effective execution during a crisis.

Detect Your Hack Risks

Introducing HackRisk.AI

AI-powered cyber risk monitoring with secure dashboard and shareable reports, delivered by security experts.

cyberlab

Protecting the nation, business and people