

SECURING SOCIAL HOUSING

Cyber Security for Housing Associations: A Practical Guide

What a ransomware outage means for tenants, repairs and rent, and how to be ready for it

Housing associations hold some of the most sensitive data in any sector: tenancy and benefit records, vulnerability flags, safeguarding notes and bank details, alongside the repairs and compliance systems that keep homes safe. Cyber security and IT management was the most common risk theme in the annual reports of 100 housing associations for the third year running[1], and the Regulator of Social Housing now says boards must understand and manage growing cyber security, data protection and operational resilience risks[2]. The question for most boards is no longer whether an attack is plausible, but how long the organisation could keep serving tenants without its core systems.

84%
of 100 housing associations named cyber as a concern in their 2024/25 annual reports[1].

28%
of UK charities identified a breach or attack in the last 12 months[3].

19%
of charities have a formal cyber incident response plan[3].

45%
of ransomware victims had not fully recovered within a week[4].

INSIDE THIS GUIDE

PAGE 2
Week one of an outage
Day by day, what tenants, repairs and rent collection experience, and why Awaab's Law clocks keep running.

PAGE 3
Where you are exposed
The systems, suppliers and devices attackers use, and what the regulator expects of boards.

PAGE 4
A 90-day plan
Cyber Essentials, penetration testing and a rehearsed recovery, with questions for the board.

WHAT TENANTS WOULD NOTICE FIRST

A Ransomware Outage, Day By Day

This illustrative timeline is drawn from what happened at Clarion, Bromford, Connexus, Flagship and the London councils whose shared IT was attacked in November 2025[5–9]. The detail will differ for every landlord. The pattern rarely does: phones and email go first, appointments are missed, payments stop matching accounts, and recovery is measured in weeks.

DAY	TENANTS	REPAIRS AND SAFETY	RENT AND INCOME
Day 1 Discovery	Systems are shut down as a precaution. Phone lines and email fail; tenants are asked to call only for emergencies[5,6].	Job schedules, operative apps and contractor portals go dark. Emergency calls are logged by hand.	Direct debit runs and payment allocation stop with the housing management system[6].
Days 2 to 3 Containment	Data theft is suspected, so the ICO must be told within 72 hours of discovery[10]. Scam calls and phishing aimed at tenants begin[7,9].	Appointments are missed and gas and electrical safety visits slip[6,7]. Awaab's Law timescales are still running[11].	Payments arrive but cannot be matched to rent accounts, so arrears and statements become unreliable[9].
Days 4 to 7 Recovery	Complaints grow and vulnerable tenants are hard to identify without case records.	A backlog builds in damp and mould investigations, voids and planned works.	Arrears action pauses; income teams cannot tell who has paid. Clarion later made extra provision for rent arrears linked to its attack[12].
Weeks 2+ Long tail	Flagship was still in recovery more than three weeks on[8]; Clarion tenants reported disruption after seven weeks[13].	Repairs satisfaction and timeliness, both Tenant Satisfaction Measures, take the hit[14].	At the London councils, Housing Benefit payments were unavailable for around six months[9].

WHY REPAIRS CANNOT WAIT

Awaab's Law Clocks Keep Running

Since 27 October 2025, social landlords in England must meet fixed timescales for emergency hazards and significant damp and mould, with further hazards phased in during 2026 and 2027[11]. The only defence is that delay was for reasons genuinely beyond the landlord's control. The government's examples are access, contractor and material problems; an IT outage is not among them, and the courts will decide. Plan on the assumption that a ransomware attack will not stop the clock.

24 hrs
to investigate and make safe an emergency hazard

10 days
working days to investigate a significant hazard

5 days
working days to start safety work after investigating

THE SECTOR RECORD

- **Flagship Group, 2020.** REvil ransomware; most systems shut down and some customer and staff data compromised[15].
- **Clarion Housing Group, 2022.** England's largest association; phones and email hit, emergency repairs only[5].
- **Bromford, 2022.** Systems shut down; direct debits initially affected[6].
- **Albyn Housing Society, 2024.** Around 10GB of staff and tenant data posted on the dark web[16].
- **Choice Housing, 2025.** Northern Ireland's largest association; precautionary shutdown and significant disruption[17].

Have These Ready Before Day One

TENANTS

Offline contact and vulnerability lists

A printed or offline copy of key contacts and tenants with priority needs, refreshed monthly.

REPAIRS

A manual job log and contractor call tree

So emergency and Awaab's Law cases are recorded, timed and evidenced while systems are down.

INCOME

A rent receipting workaround

Bank, payment provider and benefits contacts, plus a way to record payments for later matching.

COMMUNICATIONS

Pre-approved messages

Templates for tenants, staff, the regulator and the ICO, with a phone and SMS route that does not rely on email.

WHERE HOUSING ASSOCIATIONS ARE EXPOSED

Six Routes In, And What Each Puts At Risk

Most housing incidents start the same way as in any other sector: a phishing email, a stolen password, an unpatched internet-facing system or a supplier. What makes housing different is how much depends on a small number of systems, and how many people and partners have access to them.

01 · CORE SYSTEMS

Housing management and asset data

Tenancies, rent accounts, stock condition and compliance records. Lose them and you lose the evidence the Safety and Quality Standard expects you to hold[18].

02 · IDENTITY

Email and Microsoft 365 accounts

Phishing, stolen passwords and fake MFA prompts give attackers a foothold. Phishing remains the most common attack charities report[3].

03 · REMOTE ACCESS

VPNs, firewalls and remote desktop

Internet-facing devices that are unpatched or lack MFA are a leading ransomware entry point across all sectors.

04 · MOBILE WORKFORCE

Repairs teams and contractor devices

Operative tablets, DLO apps and contractor portals widen access well beyond the office and are often the least managed devices.

05 · SUPPLIERS

Platforms and managed service providers

When repairs platform Plentific was breached in 2021, residents of L&Q, Peabody and Notting Hill Genesis received phishing emails[19].

06 · CONNECTED HOMES

Sensors, door entry and building systems

Damp sensors and smart building technology add devices the regulator now expects boards to understand[2].

What The Regulator Expects

> "Boards must also ensure they understand and manage growing cyber security, data protection and operational resilience risks."
>
> Regulator of Social Housing, Sector Risk Profile 2026[2]

- **Governance.** Effective governance, staff awareness, clear accountabilities and robust controls, with business continuity and recovery regularly reviewed and tested[2].
- **Safety and quality.** An accurate, up to date and evidenced understanding of the condition of homes and a timely repairs service[18].
- **Data protection.** Report a qualifying personal data breach to the ICO within 72 hours of discovery, and tell affected tenants without undue delay when the risk to them is high[10].
- **Repairs timescales.** Awaab's Law duties continue during an incident[11].

WHERE THE SECTOR STANDS

The Gaps Most Boards Should Close First

13%
of charities have technical controls in all five Cyber Essentials areas[3].

9%
of charities review the cyber risks posed by their immediate suppliers[3].

30%
of charities have a board member responsible for cyber security[3].

4%
of housing associations felt the sector was fully ready for ransomware in a 2023 survey[20].

Most housing associations are registered societies or charities, so the charity figures are the closest national benchmark. They point to the same priorities: basic controls, supplier assurance, board ownership and a tested response.

SUPPLIER ASSURANCE

Five Questions For Every Critical Supplier

- **Which of our systems and data can you reach,** and from which accounts and devices?
- **Do you hold Cyber Essentials Plus or ISO 27001,** and when were you last independently tested?
- **How quickly will you tell us** about an incident that affects our tenants' data or services?
- **Is MFA enforced** on every remote connection into our environment?
- **What is your recovery time** for the service we depend on, and when did you last prove it?

A MEASURABLE 90-DAY PLAN

Ninety Days To Prepare, Test And Prove

DAYS 1 TO 30 · PREPARE

Know what matters and who decides

- Name a board lead and an executive owner for cyber risk.
- List the systems that support repairs, rent and tenant contact, and the suppliers behind them.
- Turn on MFA for email, remote access and every admin account.
- Work towards Cyber Essentials; the government reports 92% fewer insurance claims from organisations with it[21].

DAYS 31 TO 60 · TEST

Find the gaps before attackers do

- Commission a CREST penetration test of internet-facing systems, the housing management system and tenant portals.
- Test a full restore of the housing management system from an offline or immutable backup[22].
- Ask key suppliers for their certifications, incident contacts and notification commitments.

DAYS 61 TO 90 · PROVE

Rehearse the first week

- Run a tabletop exercise built on the week-one scenario on page 2. NCSC Exercise in a Box is a free starting point[23].
- Write manual workarounds for emergency repairs, Awaab's Law cases and rent receipting.
- Pre-draft tenant, regulator and ICO communications.
- Report results and remaining risks to the board.

Questions The Board Should Ask

1. If our housing management system were encrypted tonight, how would we log an emergency repair tomorrow morning?
2. How quickly could we restore it, and when did we last prove that?
3. Which suppliers could take our services down, and would they tell us within hours?
4. How would we identify vulnerable tenants without our case records?
5. Who decides whether to shut systems down, and who tells tenants, the regulator and the ICO?
6. When was our last independent penetration test, and are its findings closed?

TWO PLACES TO START

Certify the Basics, Then Test Them

Cyber Essentials and Cyber Essentials Plus cover the five controls that stop the most common attacks, and give boards, funders and insurers independent evidence that they are in place.

CREST penetration testing shows how far a real attacker could get from a phishing email, an exposed VPN or a contractor device to your housing management system and tenant data.

Cyber Essentials Plus | CREST Penetration Testing

Talk Through Your Housing Cyber Priorities

Cybergen is a CREST-certified cyber security partner combining experienced practitioners, threat intelligence and next-generation technology. If this guide has raised questions about your estate, we would welcome a conversation about where to start.

Speak to an Expert
+44 (0) 1865 950 828
sales@cybergensecurity.co.uk
cybergensecurity.com

SOURCES

1. Risk Register Survey 2026: Key insights from UK housing associations (Inside Housing survey), Capsticks, 13 Feb 2026. capsticks.com/insights/risk-register-survey-2026-the-key-insights-from-uk-housin
2. Sector Risk Profile 2026, Regulator of Social Housing, Oct 2026. assets.publishing.service.gov.uk/media/6ad62b2749ba86d6c953cc20/261015_2026_SRP_
3. Cyber security breaches survey 2025/2026, DSIT and Home Office, 30 Apr 2026. gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-secur
4. The State of Ransomware 2026, Sophos, 2026 (55% fully recovered within a week). assets.sophos.com/X24WTUEQ/at/jbww7pmb8n3gp99wr6hfq4/sophos-state-ransomware-rep
5. Country's largest housing association hit by cyber attack, Inside Housing, 24 Jun 2022. insidehousing.co.uk/news/countrys-largest-housing-association-hit-by-cyber-attac
6. Cyberattack forces 40,000-home landlord to shut down systems, Inside Housing, 27 Jul 2022. insidehousing.co.uk/news/cyberattack-forces-40000-home-landlord-to-shut-down-sys
7. West Midlands association hit by cyberattack, Inside Housing, 30 Jan 2024. insidehousing.co.uk/news/west-midlands-association-hit-by-cyberattack-84897
8. Update on Flagship Group cyberattack, Flagship Group, 24 Nov 2020. flagship-housing.co.uk/news/article/update-on-flagship-group-cyberattack
9. Cyber security attack FAQs, Royal Borough of Kensington and Chelsea, updated 3 Jul 2026. rbkc.gov.uk/cyber-security-incident-faq
10. 72 hours: how to respond to a personal data breach, ICO. ico.org.uk/for-organisations/sme-web-hub/72-hours-how-to-respond-to-a-personal-d
11. Awaab's Law: guidance for social landlords, MHCLG, updated 16 Jul 2026. gov.uk/government/publications/awaabs-law-guidance-for-social-landlords/awaabs-l
12. Cyber-attack and inflation hit Clarion's surplus, Housing Today, 2022. housingtoday.co.uk/news/cyber-attack-and-inflation-hit-clarions-surplus/5120088.
13. Clarion Housing's computer system still broke after cyber attack (tenant reports), Fitzrovia News, updated 5 Aug 2022. fitzrovianews.com/2022/07/14/clarion-housings-computer-system-still-broke-four-w
14. Tenant Satisfaction Measures 2024/25: Headline Report, Regulator of Social Housing, 2025. gov.uk/government/statistics/tenant-satisfaction-measures-202425/tenant-satisfac
15. Staff and tenants' data compromised in cyber attack at 32,000-home housing association, Inside Housing, 5 Nov 2020. insidehousing.co.uk/news/staff-and-tenants-data-compromised-in-cyber-attack-at-3
16. Staff and tenants' data splashed on dark web as cyberattack targets Scottish housing charity, FutureScot, 30 Aug 2024. futurescot.com/staff-and-tenants-data-splashed-on-dark-web-as-devastating-cybera
17. Cyber security incident, Choice Housing, 19 Feb 2025. choice-housing.org/news/2025/february/cyber-security-incident
18. Safety and Quality Standard, Regulator of Social Housing, Apr 2024. assets.publishing.service.gov.uk/media/65f8250c78087a001a59ebac/April_2024_-_Saf
19. Housing association residents hit by phishing emails after Plentific cyber attack, Inside Housing, 1 Sep 2021. insidehousing.co.uk/news/housing-association-residents-hit-by-phishing-emails-af
20. Only 4% of UK housing associations feel sector is fully prepared for ransomware attack, Scottish Housing News, 27 Nov 2023. scottishhousingnews.com/articles/only-4-of-uk-housing-associations-feel-sector-i
21. Businesses urged to lock the door on cyber criminals, DSIT and NCSC, 17 Feb 2026. gov.uk/government/news/businesses-urged-to-lock-the-door-on-cyber-criminals-as-n
22. Mitigating malware and ransomware attacks, NCSC. ncsc.gov.uk/guidance/protecting-your-organisation-ransomware
23. Exercise in a Box, NCSC. ncsc.gov.uk/section/exercise-in-a-box/overview