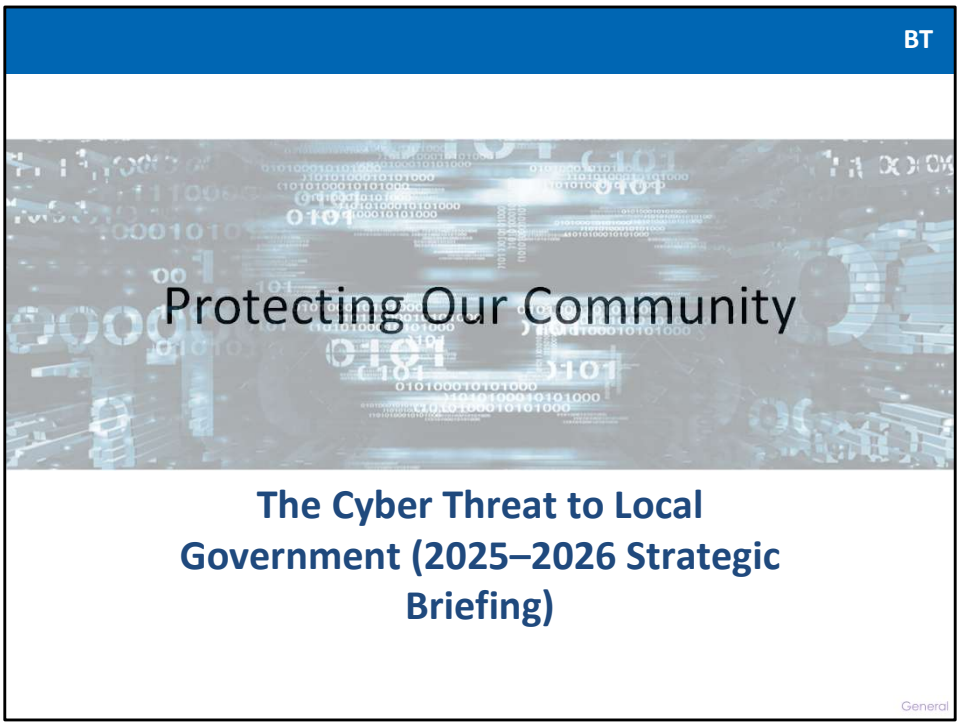


Protecting Our Community, The Current Landscape, Financial & Operational Consequences, Why Local Councils?, Strategy & Compliance, The Councillor's Role

BT

Protecting Our Community

Cybersecurity as Civic Duty

Cybersecurity is a core responsibility of local government leadership, linking cyber resilience to public safety and trust.

Impact of Cyber Attacks

Cyber attacks disrupt essential services, erode public confidence, and put vulnerable citizens at risk.

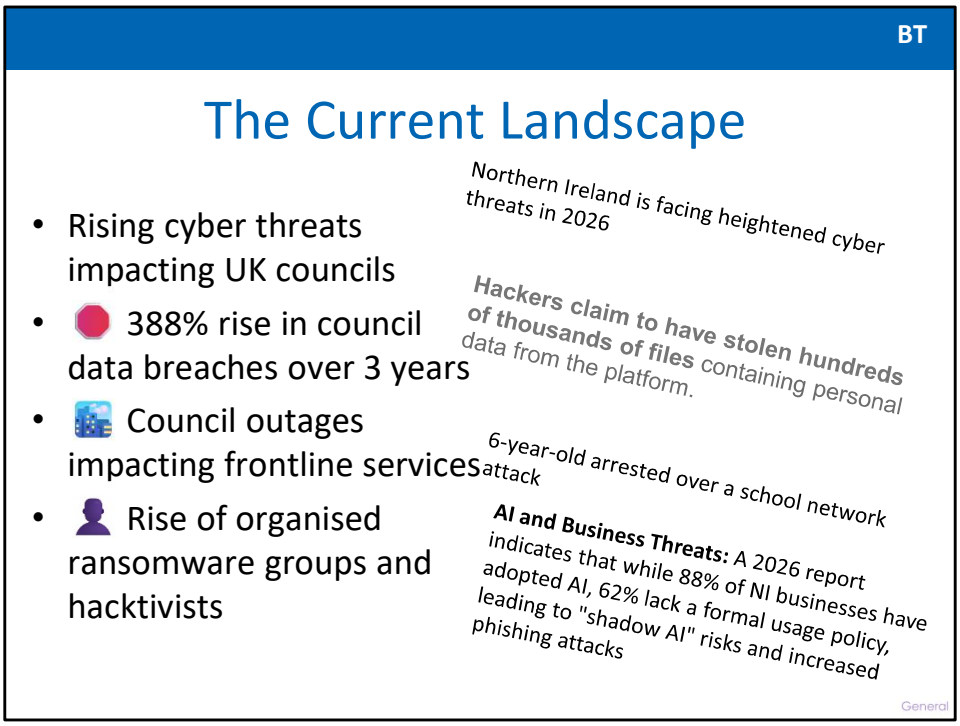
Strategic Governance Focus

Cybersecurity requires leadership attention, investment, and cultural change beyond IT, ensuring democratic legitimacy.

General

This opening slide sets the strategic and civic context for the briefing by framing cybersecurity not as a purely technical concern, but as a core responsibility of local government leadership. The title, “Protecting Our Community,” deliberately aligns cyber resilience with public safety, continuity of services, and trust in democratic institutions. Councils today are custodians of essential services that residents rely on daily, from housing and benefits to social care and planning. A successful cyber attack can therefore have consequences comparable to physical emergencies, disrupting lives, eroding confidence, and placing vulnerable citizens at risk. The subtitle, “The Cyber Threat to Local Government (2025–2026 Strategic Briefing),” positions the presentation as forward-looking and decision-focused, aimed at councillors and senior leaders who must govern through an increasingly hostile digital environment. The visual language of a modern UK town hall or digital network overlay reinforces the message that traditional civic institutions now operate within a highly connected, technology-dependent landscape. The inclusion of a shield icon incorporating national or council symbolism emphasises collective defence, accountability, and stewardship of public assets. This slide should encourage the audience to recognise cyber security as a strategic governance issue that demands leadership attention, investment, and cultural change, rather than being delegated solely to IT teams. It establishes the tone for the remainder of the briefing: practical, risk-focused, and centred on protecting communities, services, and democratic legitimacy in an era of

escalating cyber threats.



This slide explains the scale, pace, and nature of the cyber threat currently facing UK local authorities. The headline statistic of a 388% increase in council data breaches over a three-year period illustrates a dramatic and sustained escalation rather than a temporary spike. This trend reflects both increased attacker capability and greater targeting of the public sector as a whole. **Health Sector Data Breach:** A recruitment platform used by Northern Ireland health trusts, Healthdaq, was targeted by hackers who accessed sensitive files, including CVs, qualifications, and potential health data for employees.**School Network Attack:** A 16-year-old boy was arrested in County Armagh following a cyber attack on the C2K system used by schools across Northern Ireland during the Easter break, which locked pupils out of their accounts.**AI and Business Threats:** A 2026 report indicates that while 88% of NI businesses have adopted AI, 62% lack a formal usage policy, leading to "shadow AI" risks and increased phishing attacks.**Economic Impact:** While the cyber sector in Northern Ireland remains strong—supporting over 2,700 roles and generating £258m GVA—hiring has slowed, making the 2030 target of 5,000 roles challenging.The slide also highlights an important shift in threat actors. Where councils were once primarily targeted by opportunistic or lone hackers, they are now facing organised ransomware gangs with commercial business models, as well as ideologically motivated hacktivist groups. These actors are more

persistent, better resourced, and more willing to cause prolonged disruption to achieve financial or political objectives. The suggested visual of a rising curve reinforces the trajectory of risk, while the warning icon over the UK contextualises the threat as national and systemic rather than isolated. Overall, this slide is intended to create urgency and shared understanding among decision-makers that cyber risk is accelerating, increasingly professionalised, and already impacting councils similar to their own.

BT

Financial & Operational Consequences

- The true cost of cyber incidents
- 💰 Recovery costs often exceed £1M–£12M
- ⏳ Recovery can take 10 weeks to 12+ months
- 🛠️ Disruption to critical public services

General

This slide focuses on the tangible costs and long-lasting operational damage caused by serious cyber incidents in local government. Financially, recovery costs frequently reach seven-figure sums, with high-profile cases such as Hackney reportedly exceeding £12 million. These costs extend far beyond IT remediation and include emergency response, specialist consultants, legal advice, regulatory action, system rebuilds, and long-term transformation programmes. Importantly, many of these expenses are unplanned and place immediate pressure on already constrained council budgets. Operationally, recovery is rarely quick. Full restoration of systems and data can take anywhere from ten weeks to more than twelve months, during which time staff may be forced to revert to manual processes or suspend services altogether. This creates backlogs, errors, and reputational damage. The most serious impact is service paralysis, where core functions such as housing benefits, council tax processing, and adult or child social care systems become unavailable. These disruptions directly affect residents, particularly the most vulnerable, and can attract intense media and political scrutiny. The visual metaphor of a broken chain or locked currency symbol reinforces the idea that cyber incidents break operational continuity while draining financial resources. This slide is designed to help councillors understand cyber risk in terms they regularly govern: money, service delivery, and public accountability.

BT

Why Local Councils?

Valuable Sensitive Data
Local councils hold extensive sensitive data valuable for extortion and resale on criminal markets.

Pressure to Maintain Services
Councils face intense political and public pressure, making disruptions costly and increasing ransom risks.

Resource Constraints and Legacy Systems
Budget cuts have led to legacy IT, complex supplier environments, and limited cyber capabilities increasing vulnerabilities.

Systemic Cybersecurity Challenge
Cybersecurity is a structural issue shaped by funding, policies, and historic investments, not isolated failings.

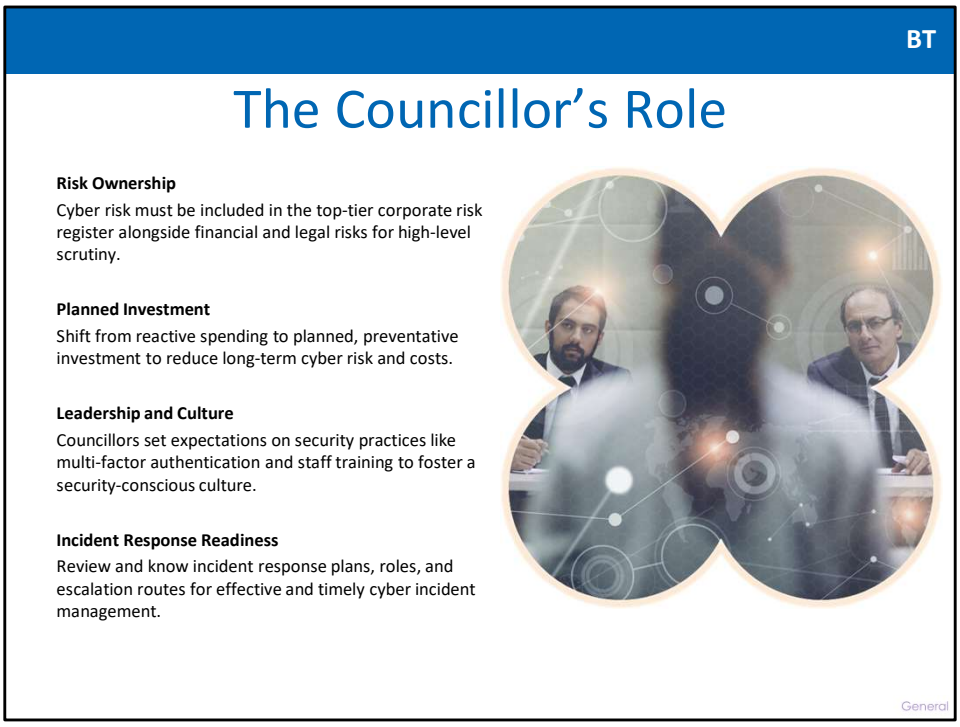
This slide explains why local councils are particularly attractive targets for cyber attackers. First, councils hold vast quantities of sensitive and high-value data, including financial records, health information, housing data, and child protection files. This data is valuable both for extortion and for resale on criminal markets. Second, councils operate under intense political and public pressure to maintain services. Attackers understand that prolonged disruption to benefits, social care, or housing creates strong incentives for rapid decision-making, including the consideration of ransom payments. Third, many councils face a significant resource gap. Years of budget constraints have resulted in legacy IT systems, complex supplier environments, and limited in-house cyber capability. These factors increase attack surfaces and slow response times. The “honey pot” or treasure chest visual reinforces the perception of councils as data-rich but resource-constrained organisations. By articulating these drivers clearly, the slide helps shift the narrative away from blame and towards structural risk. It enables councillors to see cyber security as a systemic challenge shaped by funding, policy, and historical investment decisions, rather than isolated technical failings.

BT

Strategy & Compliance

- Strengthening cyber resilience
- 📋 CAF standards introduced Oct 2024
- 💸 Leveraging £19.9m resilience funding
- 🚀 Move to secure-by-design infrastructure

This slide outlines the strategic and regulatory response now expected of local authorities. Central to this is the Cyber Assessment Framework (CAF), with updated standards introduced by MHCLG in October 2024. These standards set clearer expectations for governance, risk management, resilience, and incident response across the sector. Compliance is no longer optional or purely advisory; it is increasingly tied to assurance, funding, and reputational standing. The slide also highlights the availability of national support, including the £19.9 million cyber resilience fund, which is intended to help councils uplift capability, address critical weaknesses, and invest in modern security controls. Importantly, the slide frames cyber strategy as a shift from reactive “patching” to a secure-by-design approach. This means embedding security into system architecture, procurement, and transformation programmes from the outset, rather than attempting to bolt it on after incidents occur. The checklist and green checkmark imagery reinforces progress, accountability, and assurance. For councillors, this slide clarifies that there is a defined national direction of travel, practical support available, and a clear expectation that councils move towards more mature and proactive cyber governance.



The final slide translates cyber security into concrete leadership actions for councillors. It begins with risk ownership, emphasising that cyber risk should sit on the top-tier corporate risk register alongside financial, legal, and safeguarding risks. This ensures regular scrutiny and informed decision-making at the highest level. Investment is the next theme, encouraging a shift from reactive, post-incident spending to planned, preventative funding that reduces long-term exposure and cost. Leadership and culture are equally important. Councillors play a key role in setting expectations around practices such as multi-factor authentication, staff training, and secure ways of working. Visible support from elected members helps normalise security-conscious behaviour across the organisation. Finally, the slide calls for immediate readiness by prompting a review of the council's incident response plan. Knowing roles, escalation routes, and decision-making authority before an incident occurs is critical to effective response. The boardroom visual reinforces collective responsibility and governance. This slide leaves the audience with a clear message: cyber resilience is a leadership issue, and councillors have a direct and meaningful role in protecting their communities in the digital age.