Brought to you by Socitm Ltd | *Reference: 19007*

Part 2

Inform Report

Cyber risk - the challenge for local government

People, teams and cyber roles

March 2019

Socitm inform

Table of contents

Introduction

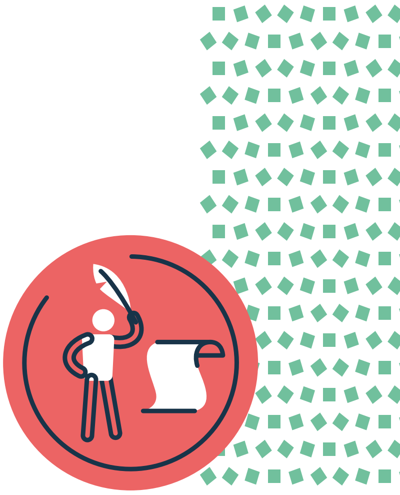
Effective cyber management requires effective leadership, and not just in IT. This is the second of five cyber reports. It looks at the role of IT leadership and specific cyber technical functions, set alongside other key roles that play a part in cyber management, from the Senior Information Risk Owner (SIRO) to local councillors.

For IT itself, there are recognised methods for good cyber management – protecting data and IT assets from abuse, misuse or just reducing human error. Systems patching, risk tracking and penetration testing regimes, coupled with strong asset management and data controls, go a long way to protecting councils from common threats such as phishing, viruses and ransomware attacks.

But more needs to be done to create strong resilience in critical digital infrastructure. This includes growing the awareness of the responsibility that rests with IT suppliers. Gone are the days (if they ever existed) when outsourcing IT included outsourcing risk management. With the growth in cloud adoption, IT partnerships and shared services, IT supply chains are often opaque and complex. The inherent cyber risks of these new delivery models, coupled with the growth in emerging technologies, such as the Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), Robotic Process Automation (RPA) and Virtual Reality (VR), must be understood, visible and controlled.

Today's IT architectures typically comprise a web of inter-connected digital components and linked data. These bring huge benefits, such as data mining and insight, but also bring new risks. It is essential that councils are able to retain a good grip on how and where data handling and processing is undertaken by others, especially when external suppliers and agencies need access to sensitive or secure infrastructure and systems. This goes beyond vetting IT service providers, to include all contractors and suppliers involved in public service delivery.

Everyone in the organisation has a responsibility for cyber, and that requires wide training, awareness and accountability, with appropriate support and advice from IT itself.



The role of IT leadership

Whilst it is not the job of IT professionals to decide on the balance of risks or the risk appetite of the organisation, it is the task of IT to help organisations to understand cyber risks in the context of their wider portfolio of risks, in order for the council to be able to take informed decisions about cyber protection measures.

IT leaders need to balance their attention between the technology measures for cyber protection and the time they need to work with colleagues outside IT in improving cyber risk understanding and resilience:

IT leadership - technology

- **A rigorous patching regime** exists so that all systems holding sensitive information or supporting critical services are patched and run on supported and protected operating systems. This requires classification of supplier updates according to their importance and risk, planning and grouping their implementation.
- **Classification of system risks** and removing any systems or suppliers that do not conform to cyber risk criteria.
- **Firewalls are being properly managed** and maintained, especially where they face the internet to guard against infection.
- **A comprehensive and tested response plan** in the event of a cyberattack occurring, with clear responsibilities and mobilisation processes, communications and internal and external reporting.
- **Specific cyber responsibilities** are clearly defined and rehearsed, such as the Emergency Planning Officer, IT Security Officers, SIRO, CFO and CEO.
- **All virus, phishing and other security services** are in place, and that these keep pace with a changing threat landscape.
- **Involvement and communications with external bodies** and partners takes place routinely, including the National Cyber Security Centre (NCSC) and Warning and Reporting Point regional groups (WARPS) for the interchange of intelligence about threats and best counter-measures.
- **All staff and third parties on the network take cyber threats seriously**, understand the direct risks to front-line services and are working proactively to maximise their resilience and minimise impacts on services.
- **Inventories exist** of devices, systems and other hardware assets with network access.
- **Secure configurations of hardware and software** exist (maybe by third party security partners).
- **Continuous vulnerability assessments** and tests are undertaken of central and local IT, from typical user to privileged access.

> *"CEOs are increasingly involved in a debate about cyber security and cyber threat. It is essential that they provide leadership to maintain public sector preparedness should a cyber event happen. The CEO must set the 'tone' and priority for their organisation on cyber issues."*
>
> *Stephen Baker, Chief Executive, Suffolk Coastal and Waveney Councils, and Spokesperson on Civil Resilience and Community Safety, SOLACE*

IT leadership - influencing and involving others

- **Regular cyber and IT risk reporting** takes place using language and descriptions based on business impacts.
- **Business colleagues outside IT are helped** to understand the changing nature of cyber risk and the extent of technology protection.
- **IT suppliers and third parties are challenged** for their cyber credentials in contracts, services and products.
- **HR leaders are involved** in cyber planning and employee responsibilities for cyber are clear in HR policies.
- **Finance leaders are involved** in asset risk management, changing cyber threat assessment and auditing priorities.
- **Digital leaders are involved** in cyber planning, ensuring that transformation programmes take full account of cyber risk.
- **Emergency planning officers understand their role on cyber protection** and testing, giving them technical support as required.
- **Service leads are helped** in aligning and testing IT Disaster Recovery planning with Business Continuity plans.
- **Members are briefed** on cyber planning – for example in terms of risk scrutiny, information governance and IT planning.
- **Specific IT responsibilities and accountabilities** are assigned for protecting infrastructure and IT services as part of the internal team.

In order to protect councils from cyber risk, IT leaders need to ensure that relevant controls should are embedded in policies, practices and procedures, and review how these relate to business policies, practice and procedures.

For example, however good IT policies are for access and data protection, unless these are backed by HR policies for employees then protection against attack will always be at a greater risk of compromise. Moreover, IT protections may be too rigid – often seen in limitations in how mobile and flexible working operates, such as 'bring your own device' (BYOD).

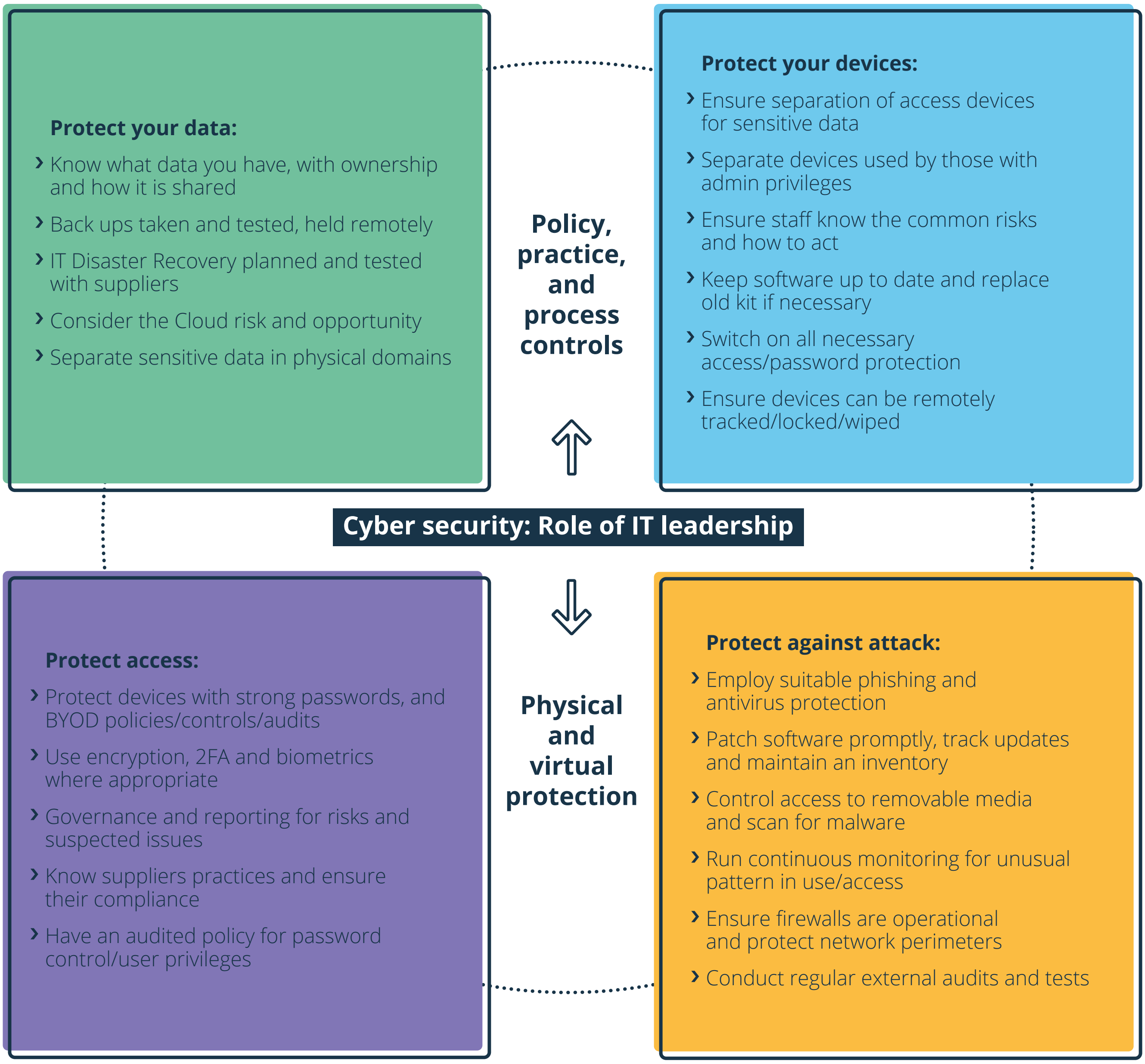
Within IT itself there may also be multiple cyber roles – even if a number of these are held by one individual in smaller organisations such as district councils. These roles require specific support and training to ensure their responsibilities are understood and carried out as part of their accountable performance in the design and delivery of digital solutions and infrastructure:

- CIO or head of IT
- IT Security Manager
- CTO
- Network manager
- Software developers
- IT contracts manager
- Business analysts
- Project managers
- Systems testers
- Systems managers.

Those responsible for cyber risk in councils, with whom the IT management must liaise, include (amongst others):

- CEO – as overall head of service
- Senior Information Risk Owner (SIRO)
- Head of Legal (contracts)
- HR director (employee risks)
- Caldicott Guardian (for health and social care)
- Chief Digital Officer (CDO)
- Auditors (assurance)
- Chief Finance Officer (assets)
- Politicians (governance and risk)
- Suppliers of IT solutions and services.

The following diagram shows the connections for council IT leaders to consider across policy and practice, and physical or virtual cyber protection:



Protect your data:

- Know what data you have, with ownership and how it is shared
- Back ups taken and tested, held remotely
- IT Disaster Recovery planned and tested with suppliers
- Consider the Cloud risk and opportunity
- Separate sensitive data in physical domains

Policy, practice, and process controls

Protect your devices:

- Ensure separation of access devices for sensitive data
- Separate devices used by those with admin privileges
- Ensure staff know the common risks and how to act
- Keep software up to date and replace old kit if necessary
- Switch on all necessary access/password protection
- Ensure devices can be remotely tracked/locked/wiped

Cyber security: Role of IT leadership

Protect access:

- Protect devices with strong passwords, and BYOD policies/controls/audits
- Use encryption, 2FA and biometrics where appropriate
- Governance and reporting for risks and suspected issues
- Know suppliers practices and ensure their compliance
- Have an audited policy for password control/user privileges

Physical and virtual protection

Protect against attack:

- Employ suitable phishing and antivirus protection
- Patch software promptly, track updates and maintain an inventory
- Control access to removable media and scan for malware
- Run continuous monitoring for unusual pattern in use/access
- Ensure firewalls are operational and protect network perimeters
- Conduct regular external audits and tests

Do you need a Security Operations Centre?

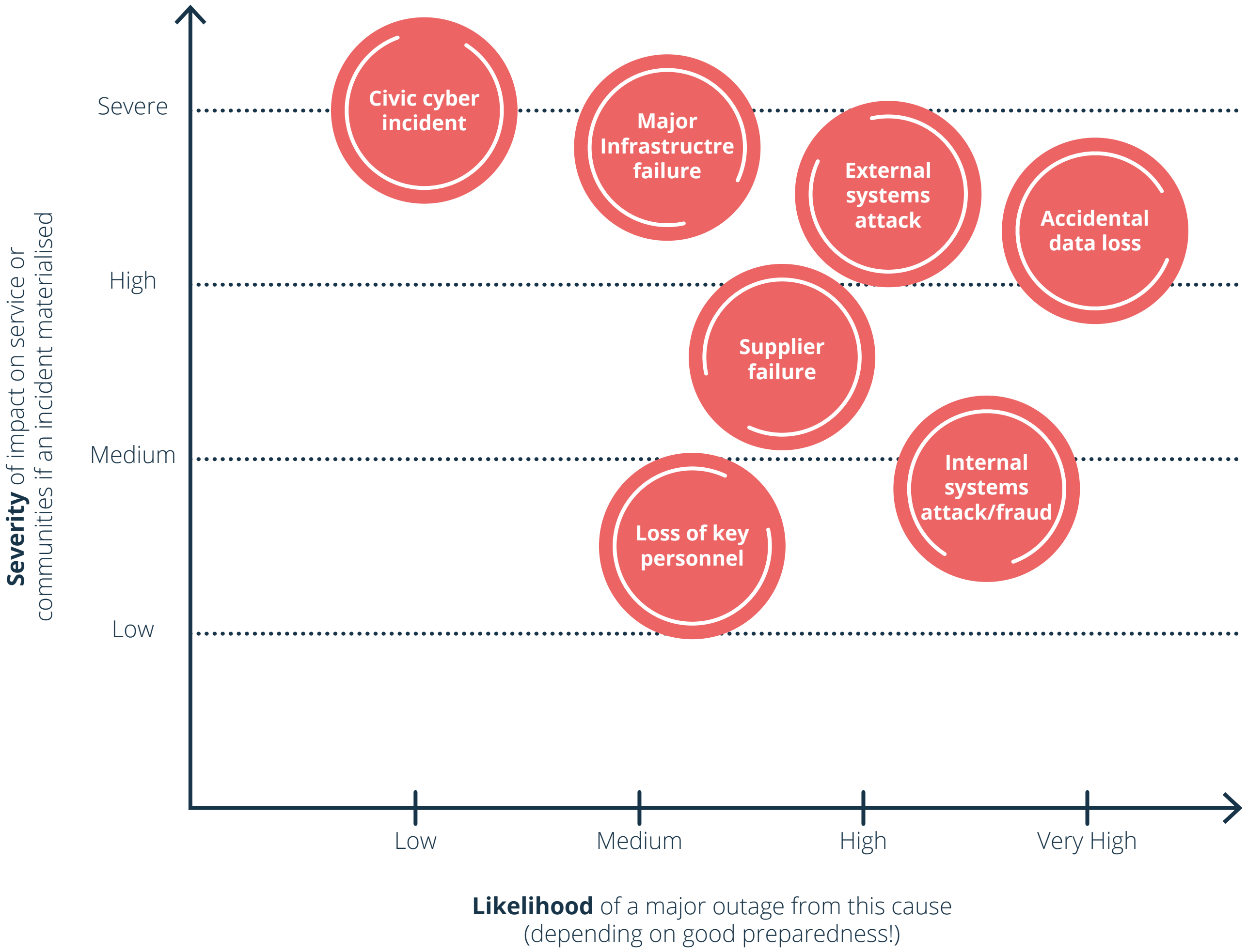
A Security Operations Centre (SOC) is the industry term for an internal team responsible for monitoring and analysing IT security on an ongoing basis. The job of the SOC is to prevent, detect and respond to cybersecurity threats and incidents, using a combination of technology solutions and processes.

A SOC team of security analysts ensures continuous monitoring, analysis and reporting of activity on networks: systems, servers, endpoints, databases, applications, and websites, seeking out anything that could be indicative of a security incident or potential compromise.

They also ensure compliance with industry and government regulation, such as ISO27001 or, the Public Services Network, overseeing the integrity of the IT security architecture (e.g. firewalls, breach detectors and the use of a SIEM - Security Information Event Management system).

In a smaller organisation, such as a district council, a SOC team is likely to operate on a matrix management format, with external as well as internal expertise or on a shared service basis to reduce costs. External agencies such as the NCSC and WARP, IT auditors and IT suppliers can provide up to date threat intelligence, continuous monitoring tools and advice, perhaps with a third party Managed Security Services Provider (MSSP).

Amongst other activities, the SOC can help with categorising risk and explaining the priorities for protective measures, as illustrated below.



The role of members

Local councillors are elected to represent the interests of their communities. Increasingly, they depend on digital methods in order to:

- carry out what is often a mobile role
- communicate with those who represent them and with the council officers
- access essential information, which is often only available online
- manage case work for their portfolio interests
- ensure they are accessible and representative – for example by using social media.

Council's democratic processes lend themselves to digital operation, because of costly administration (reports, briefings, consultation, elections, decision-making processes), but they are also at risk of interference, intrusion and bias, if digital methods are compromised or poorly designed.

In addition, with on-line fraud being a growth industry and the biggest source of crime in the UK, councillors have a duty of care to their communities, especially vulnerable people, who can be at great risk from malicious online activity.

> *"Cyber has continued to rise up the agenda for us at Rugby. We already have senior level involvement for what is a major corporate risk area, and we continuously focus on reflecting new and changing technology threat areas in our IT infrastructure protection"*
>
> *Raj Chand, Head of Communities and Homes, Rugby Borough Council*

For all these reasons, councillors have the important duty of cyber oversight and scrutiny, which includes:

- **Protection of the council's assets**, such as buildings, money and people, from cyber-attack, fraud, and abuse, including internal misuse of systems
- **Ensuring effective management of IT resources**, so that they are safe, secure and resilient
- **Protection of personal data**, including GDPR compliance and the handling of sensitive data relating to vulnerable people
- **Assessing the appropriateness of cyber risk** in transformation programmes, design of new systems and digital services, information governance and critical IT infrastructure availability
- **Setting cyber risk appetite** in the context of wider risks, including channel shift to 'digital only' self-service, development of commercial services and business continuity planning
- **Ensuring that digital solutions are designed for inclusion and equality**, not just for efficiency and ease of operation or to protect past practice
- **Validating risk models for transformation programmes**, with specific regard to data, money, time, reputation and other resources
- **Tracking changing threats** to community safety, well-being, resilience and local infrastructure vulnerabilities, such as broadband and mobile access
- **Managing relationships with third parties** on whom the council depends for digital (and other) services
- **Ensuring that democracy is never compromised** by technology methods, in elections, decision making, public consultation or in the equality of citizen representation and interest
- **Supporting communities to be safe on line**, through advice, guidance and the way the council sets an example in good cyber practices.

As council services become increasingly digital in nature, there is also a broader role for members in ensuring that digital policy development and service strategy represent the interests and priorities of the communities they serve (e.g. in digital inclusion). For example, risks, including those that are cyber-related, will need to be considered for each of the priorities set out in Leeds City Council's Plan (illustrated below).

In practice, many members are not always close to their councils' digital programmes. This can lead to issues and tensions with them feeling out of touch with associated risk, supporting digital policies, new contracts and programmes without fully understanding the risks, or become risk averse to 'be on the safe side'.

Recruiting and retaining cyber expertise

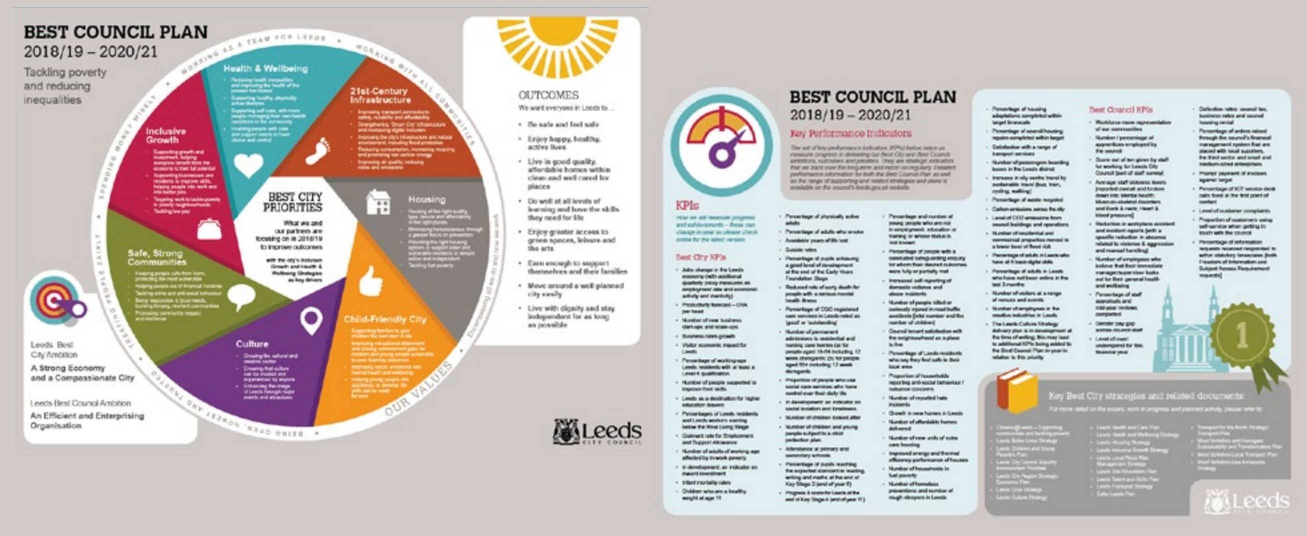
Every council should have a senior nominated lead on IT cyber security, even if this is primarily a role to ensure others take responsibility for ensuring cyber security e.g. management of suppliers, outsourcers, shared service partners, specialist security agents.

Recruitment and retention in this area can be tough, with a shortage of skilled cyber and information governance professionals and massive growth in global demand.

IT security decision makers across all sectors say their teams lack the staff and skills needed to combat sophisticated cyberattacks, according to a new report from Osterman Research, and 57% just to recruit and retain the IT security staff they need. The same research found that 60% of businesses said they lack the in house cyber skills they needed to address complex security problems. In another study, the Information Systems Audit and Control Association (ISACA) predicted that there will be a global shortage of two million cyber security professionals by 2019.

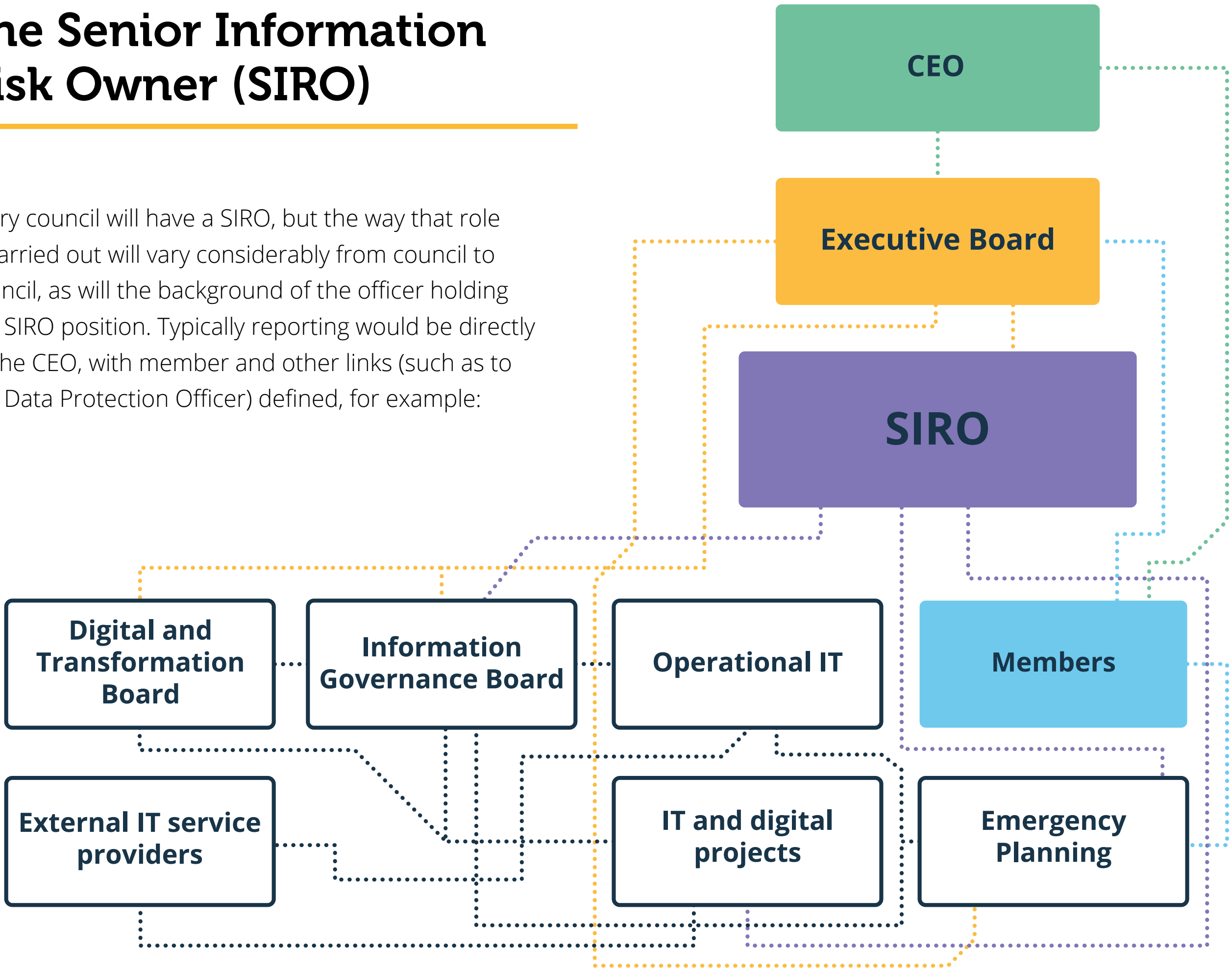
With the growing demand for cyber skills globally outpacing talent availability, the UK public sector faces particular challenges, where pay constraint becomes an added factor by limiting the available talent pool of cyber specialists. This may require councils to review HR policies and remuneration packages to ensure they can attract skills in this area, alongside the necessary investment in cyber training and development to build potential future cyber capability.

For councils with major IT outsourcing contracts, for whom the main IT presence there may only be an IT procurement client. This is an area where attention will be needed, since retaining a level of inhouse cyber skills could wrongly be viewed as an avoidable cost overhead.


BEST COUNCIL PLAN
2018/19 – 2020/21
Tackling poverty and reducing inequalities
Health & Wellbeing
21st-Century Infrastructure
Inclusive Growth
Housing
Safe, Strong Communities
Culture
Child-Friendly City
BEST CITY PRIORITIES
What we and our partners are focusing on in 2018/19 to improve outcomes
with the city's Inclusive Growth and Health & Wellbeing Strategies as key drivers
WORKING AS A TEAM FOR LEEDS
WORKING WITH ALL COMMUNITIES
SPENDING MONEY WISELY
TREATING PEOPLE FAIRLY
BEING OPEN, HONEST AND TRUSTED
OUR VALUES
Leeds Best City Ambition
A Strong Economy and a Compassionate City
Leeds Best Council Ambition
An Efficient and Enterprising Organisation
OUTCOMES
We want everyone in Leeds to...
Be safe and feel safe
Enjoy happy, healthy, active lives
Live in good quality, affordable homes within clean and well cared for places
Do well at all levels of learning and have the skills they need for life
Enjoy greater access to green spaces, leisure and the arts
Earn enough to support themselves and their families
Move around a well planned city easily
Live with dignity and stay independent for as long as possible
Leeds CITY COUNCIL
BEST COUNCIL PLAN
2018/19 – 2020/21
Key Performance Indicators
KPIs
Best City KPIs
Best Council KPIs
Key Best City strategies and related documents
Leeds CITY COUNCIL

The Senior Information Risk Owner (SIRO)

Every council will have a SIRO, but the way that role is carried out will vary considerably from council to council, as will the background of the officer holding the SIRO position. Typically reporting would be directly to the CEO, with member and other links (such as to the Data Protection Officer) defined, for example:


CEO
Executive Board
SIRO
Digital and Transformation Board
Information Governance Board
Operational IT
Members
External IT service providers
IT and digital projects
Emergency Planning

The SIRO is a strategically important role, with some serious accountabilities should a significant information risk materialise. The nominated SIRO should be an Executive or Senior Manager on the Executive Board, who is familiar with information and wider cyber risks and the organisation's response to risk in general.

Overall, the role of the SIRO is to take ownership of the organisation's information risk policy, act as an advocate for information risk on the executive team and to members and provide written advice on information risk as part of an annual audit statement. By ensuring good information governance and data consistency, cyber risk is much better managed overall, since it is data and information protection that lies at the heart of cyber risk management.

The SIRO can also take a broader role for cyber risk, working with others – such as the head of IT, business continuity managers and emergency planning, bringing together risk owners and risk functions to ensure a single and coherent perspective on cyber risk on behalf of members and the executive team.

The SIRO's responsibilities can be summarised as:

- **Leading** and fostering a culture across the council that values, protects and uses information for the organisation and to deliver benefit of citizens
- **Owning overall information risk** management and risk assessment processes and ensuring they are implemented consistently
- **Owning information incident management** and advising the Chief Executive, the executive team and members on information risk and internal controls, ensuring that mitigation plans are robust

- Ensuring that the council has **Information Asset Owners (IAOs)** who understand their roles and are supported by cyber risk management specialists that they need
- Initiating and overseeing an **information risk awareness and training** programme of work to communicate importance and achieve GDPR compliance
- Acting as the **focal point for information risk management**, including resolution of escalated risk issues raised by IAOs, Information Security Officers, Auditors, IT Security Officers, etc
- Developing and implementing an **Information Risk Policy** covering all areas, setting out how compliance will be monitored, including Privacy Impact Assessments
- Overseeing a programme of work to **identify, prioritise and address risk** and system accreditation, with particular regard to systems that process personal data
- Ensuring that i**nformation risk assessments are completed** on a regular basis to understand the information risks faced by the council and its partners
- **Signing off an annual assessment** of information risk performance, including material from the IAOs and specialists, as part of the annual Audit letter
- **Investigating and reporting of cyber information incidents** to conform with national guidance.

The following five areas warrant being assigned a specific council lead, to ensure a comprehensive approach, coming together as part of a cyber or information management group chaired by a SIRO:

Leadership

Ensure regular CEO, CMT, member briefings and reporting on cyber matters with clear lines of accountability to Executive and Member level. This includes cross-organisation training and awareness of cyber matters.

Governance

Ensure a triage of cyber roles from IT security matters through to information governance and wider cyber risk to the corporate risk register, coordinated by a single officer (e.g. SIRO). This includes prioritisation of systems recovery.

Ownership

Ensure ownership for cyber includes specific reference to emergency planning, CEO, SIRO, audit, HR, all staff, members, procurement, legal, CFO, as well as IT contracts and all employees accessing data and systems.

Risk planning

Ensure risk planning includes joined-up testing and design of business continuity plans with IT disaster recovery plans, with the appropriate involvement of third parties and emergency planning officers.

Technology

Ensure a single IT cyber security lead in the council, working with third party IT suppliers, defining IT standards, policies and practices such as IT DR. This includes links to WARPs, use of specialist services and external technical resources.

Third party suppliers

Suppliers in general

A growing area of cyber vulnerability and risk is not the organisation's own networks and systems, but the third parties that provide services, including IT. Suppliers and partners are increasingly processing data and accessing systems on behalf of councils in a number of ways:

1. Providing **cloud** systems and services.
2. **Partners and shared service delivery agents** who are processing and sharing data between one another.
3. **Outsourcers** and service managing agents.
4. **Specialist services**, such as auditors, consultants and contractors.
5. **Team members** who are not employees, but need to access councils systems and data.

Councils hold and harvest a significant amount of sensitive and personal data. GDPR compliance, the growing value of personal data to criminals, and the distributed nature of how such data is processed, all mean that councils need to be careful to ensure they know how third parties manage and use data.

Even simple and free online cloud-based services, such as a public or employee survey, can create risk. For example, in July 2018 Fortnum and Mason suffered a data breach affecting 23,000 customers as a result of a commissioned third-party online survey form.

Not only is it important to be sure that suppliers, partners and other third parties are being professional in their data management practices, but to recognise that they could also be a 'backdoor' to council systems. Specific care is needed where access is given to council networks:

- Any supplier staff given **IDs and logon** credentials
- Specialist IT support **accessing secure system areas** to provide support
- **Penetration testing** and other automated tools used to probe and test
- **Financial payments** to third parties checked against legitimate purchase orders
- Data processing activity **remotely in cloud or outsourced systems.**

The recent problems faced by Cambridge Analytica and Facebook in how they used public data to impact democratic processes, are a more general example of risk, and it is a small step from these global examples to an abuse of data that affects a local council's reputation or political processes in elections or procurement.

These newer cyber risks lie alongside the more traditional IT systems and data security threats. Whilst the likelihood of a data breach is low, whether caused deliberately or otherwise, it will become more a common threat.

> *"GDPR compliance, the growing value of personal data to criminals, and the distributed nature of how such data is processed, all mean that councils need to be careful."*

> *"Hyperscale public cloud providers have a significant amount of money to invest in the cyber security of the cloud – far more than any individual customer, or even a national cloud provider, could invest. They also have a massive incentive to make such investments because their whole business model rests on their ability to prevent any cyber-attacks or other security incidents. Furthermore, all customers of hyperscale public cloud providers benefit from the investments made to satisfy the most security conscious of customers – including banks and fintech, the military, government, healthcare, retail, pharma and large media companies. That said, all public cloud providers operate under what is known as a shared security model – they protect the physical estate, their cloud platforms and any connectivity but customers are responsible for protecting their own deployments on that cloud platform. The providers make available default configurations, tooling and automation to streamline this activity but that doesn't remove the responsibility for implementing it from the customers or their partners."*
>
> **Andy Powell**
> *Cloud CTO, Eduserv*

In 2017 Opus & Ponemon Institute undertook a 'Third Party Data Risk Study' of global private sector organisations. They found that 56% of survey respondents had experienced a third-party data breach in 2017, a 7% increase on the previous year. Yet many did not know who their third-party partners were, and more than half did not know whether the third party policies would prevent a data breach. Fewer than one in five respondents felt their organisations effectively managed third party risk and less than half said that managing outsourced relationship risks is a priority in their organization.

There is no reason to assume councils would be different from private sector organisations and, given their diversity (in terms of scale and function), they could find third party access management more challenging. The LGA cyber stocktake in 2018 has indicated weaknesses in supplier management regarding cyber risk.

Councils increase reliance on cloud services mean that it is important to be confident in cloud vendors' security policies and practices if any sensitive data or processing is being undertaken. There are also risks that malicious parties will seek to copy or 'spoof' third-party cloud services that have been legitimately commissioned.

Protecting against these risks depends on some simple preliminary steps:

- **Knowing who your third party vendors** are, what they provide, and the cyber risk profile associated with those services
- **Checking that the third party has effective policies** in place to prevent cyber incident
- **Confirming whether the third-party has had a data breach** or suffered a cyber incident and how that was dealt with
- **Reviewing how a third party is using and managing council data**, for example whether they are sharing it with other services in their delivery practice
- **Testing a third party's internal detection, prevention and recovery policies** and practices, alongside the councils practices
- **Having strong supply management policies and practices**, from procurement to service level management, that includes the third party's cyber responsibilities
- **Ensuring that supplier and council IT activity align**, including disaster recovery, business continuity and appropriate data policies are being maintained in tandem.

These are general supplier issues – not just IT service providers.

IT service suppliers

Every council IT department depends on third party suppliers, even if the majority of IT delivery is run in-house. Typically, bought-in technology services cover a range of areas, both short-term (such as consultancy or on-off support) and the longer-term provision of hardware, software, cloud solutions and a mix of support functions. These external IT services create specific cyber risks for IT leaders to manage, whether large or small councils, insourced or largely outsourced.

In an outsourced environment, developing a cyber protection strategy must involve IT suppliers in a range of ways, to ensure effective and transparent protection including:

- **Designing IT policies and procedures** which work end-to-end across the IT supply chain
- Requiring **supplier contracts to include cyber practice** and policy (not just in IT)
- Establishing **cyber compliance polices for IT contractors** accessing internal systems
- **Automated audit checks on payments** to suppliers from councils' systems
- **Monitoring where networks are accessed** and for what purposes
- **Testing suppliers practices** where cyber resilience is dependent
- **Developing and jointly testing IT disaster recovery plans**
- Addressing **cyber awareness, training and processes** for key IT supplier activity
- **Prioritisation of cyber practice** and tackling technical vulnerabilities.

Contracts, especially with IT suppliers, need to be explicit about the expectations of high levels of information and systems cyber housekeeping and integrity:

- Adherence to the same levels of cyber protection, awareness and employee practice in the supplier's teams as in the council's client teams, especially where access to internal networks is permitted
- Supplier IT Disaster Recovery plans, including any client dependencies, are understood and tested where they affect council services. This should cover how plans are tested, recent incident, and reports on adjustments to reflect client business continuity priorities
- Transparent cyber practices, where a supplier is providing IT and data processing services. This includes routine reporting about testing and incident management, and how data is stored and protected (this needs to be audit-able)
- GDPR compliance and practice in the supplier organisation, including any reported weaknesses, how responsibilities and accountability are managed. and specifically, how personal data is handled and transmitted safely, including how the council's data is to be returned securely once a contract is ended
- Any downstream agencies, suppliers or delivery partners who are involved in processing council data, ensuring these comply with the same good cyber practice
- How changes will be managed by the supplier to keep up to date with changing threats, technologies, regulation or business requirements. This would include processes, policies, staff awareness, disaster recovery and incident management
- How physical network connections are securely contained, where the supplier and councils' networks link, and how data is used and protected if remote support is provided.

Keeping cyber security high on the agenda in IT supplier service review meetings can help, coupled with making specific references in contracts as they are let. But ultimately, if a supplier fails to adhere to good levels of cyber protection, it should be possible to apply sanctions or even end a contract.

> “The reality of cybercrime is increasingly affecting all of us, irrespective of how digitally engaged we chose to be. All organisations have a duty to protect data, in particular to ensure sensitive data is secure; however, the pervasive use of technologies together the evolving sophistication of attacks makes the need for strong security standards imperative. Socitm’s research project on cyber security and the public sector provides insight on the wider context of managing cyber risks, and the responsibility we all have in fighting it. This series of reports provides practical guidance on how to raise the profile of cybercrime at senior levels, as well as emphasising the need for this to be accepted as an organisational risk rather than simply the responsibility of IT. “

Sandra Taylor, Head of Digital and IT Services
and Socitm Vice President, Dudley MBC

Citizens' access to systems

It is easy to conceive a future where all council transactions and many other more complex interactions with the public take place on-line. This will depend on well-designed systems, enabled by artificial intelligence (AI) and machine learning to aid personalisation. Suitable 'safety nets' will be required for intervention when digital services fail, coupled with a digitally-savvy and technologically-equipped population.

Whilst this may be some way off, the direction of travel is clear, and many councils are already seeking to minimise face-to-face and telephone contacts. The challenge is to ensure the necessary professional support is there when required, to complement what can better be delivered by intuitive, personalised and well-designed digital systems.

One of the implications of voice activated and automated systems for public use, delivering complex transactions requiring personal or financial data, is a new level of cyber risk. Not only is there a risk of new threats from public access systems (e.g. people masquerading as benefits claimants), but systems are also more complex, making attacks harder to trace.

There is also the secondary cyber risk of the public being exploited by criminals through such systems, hiding modern slavery, domestic violence, usurping credentials or just defrauding. Poor quality data and checks can also lead to the wrong judgements being made in highly automated systems.

Being able to support, protect and track vulnerable service users, such as those with mental health issues, is vital, as problems with the rollout of Universal Credit have shown.

It is in the interests of local councils to ensure that citizens are aware of digital risks and are able to take care of themselves when on-line. There is, arguably at least, a duty of care resting on councils to protect the public accessing digital public services, especially those who are more vulnerable in society, or those who are digitally excluded and therefore more likely to depend on public services.

There are also a growing number of risks that need to be considered in the design of externally facing services, including ensuring that they are 'hard wired' separately from internal and sensitive systems:

1. Many websites have not been designed with security at the forefront, having grown organically from the early days of the World Wide Web and internet.
2. More sensitive systems are being moved to the Web, such as employee self-service, creating new 'backdoors' to internal systems.
3. There are transactions available which make systems calls to sensitive system data in order to fulfil end to end service provision.
4. With the increased adoption of cloud services and mobile, the Web and internet become transport layers for highly sensitive data.

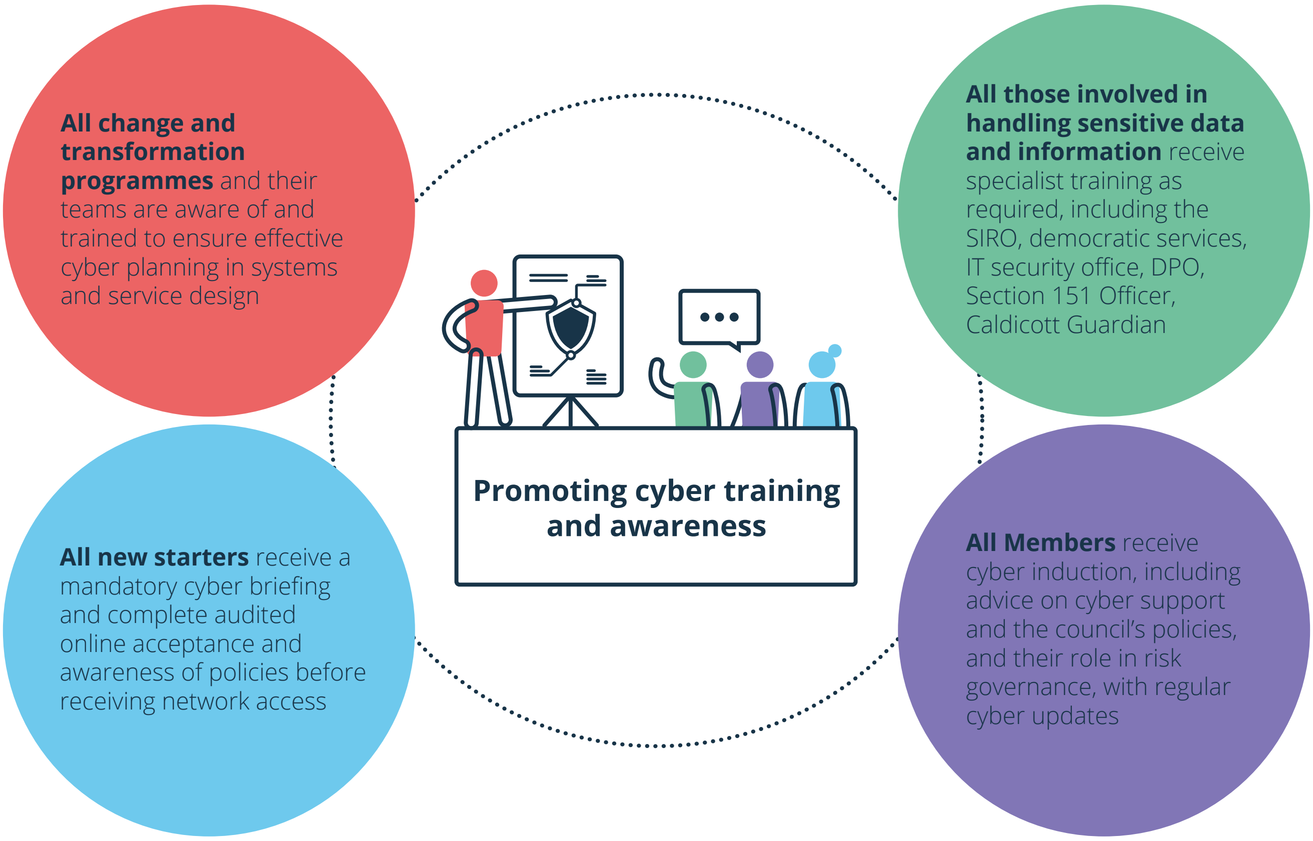
> *"Today's society is facing a whole range of new surveillance and cyber intrusion threats. Councils have a special role not only in protecting the data and other assets they look after, but also in protecting their local communities and civic digital infrastructure from attack. This, alongside changes in the law such as the new Data Protection Act, places growing responsibilities on councils for how they handle and process data, and work with partners. Embracing new consumer technologies, embedded sensors, artificial intelligence, robotic process automation and smart city management systems must go together with effective cyber management, beyond traditional IT security. This report is therefore welcome and timely."*
>
> *Dylan Roberts, Chief Digital and Information Officer, City Digital Partnerships Team, Leeds City Council and NHS Leeds Clinical Commissioning Group and Chair, Local CIO Council*

Improving cyber training and awareness

From all this analysis, advice and best practice examples, it is clear that good cyber practice comes from awareness and, to a lesser extent, training. Everyone, from employees to the delivery partners they work with, and from members, to the citizens they protect, has a role to play.

Often, the topic of cyber is neglected within councils, because it is seen as too 'technical' or the role of IT to protect, so is limited to basic IT security awareness. Of course, any training and awareness is better than none, but ideally it should:

- Relate IT risks and the tasks to mitigate those risks to the **practical actions everyone can take** on a day-to-date basis
- **Use real examples** that reflect the business of the council and its activities, maybe from other councils,
- **Explain the role of IT** as it works 'behind the scenes', its limitations and the support it needs from everyone to carry out technology protection effectively
- **Provide specific advice and guidance** in areas such as emergency planning, business continuity planning, and the role of third parties in wider IT Disaster recovery
- **Run simulated scenario exercises** to test and to raise awareness, involving partners and suppliers as necessary
- **Target tailored training and awareness** for IT specialists, service leaders, SIRO, DPO, politicians, auditors, those handling sensitive data, front line staff in general and citizens
- **Reserve the technology descriptions, jargon and complex descriptions for the IT people** who need to know and ensure the language and descriptions for everyone else brings cyber as a topic to life.



All change and transformation programmes and their teams are aware of and trained to ensure effective cyber planning in systems and service design

All those involved in handling sensitive data and information receive specialist training as required, including the SIRO, democratic services, IT security office, DPO, Section 151 Officer, Caldicott Guardian

Promoting cyber training and awareness

All new starters receive a mandatory cyber briefing and complete audited online acceptance and awareness of policies before receiving network access

All Members receive cyber induction, including advice on cyber support and the council's policies, and their role in risk governance, with regular cyber updates

Delivering training and awareness – and this does not have to be 'classroom based' - and cyber training and awareness needs to constitute more than running a few optional briefings on IT security or some self-help e-learning modules available to staff.

Examples include:

- Internal **social media and poster campaigns**, promoting good cyber practice and pointing staff towards their IT security office, SIRO, tools, policies and resources, as well as how they can personally be alert to cyber risks
- Running **scenario exercises** in specific areas of risk and in service areas, with involvement of business continuity leads and emergency planning officers
- **Working groups** looking at how information risks are changing and how to reduce them, with DPO, SIRO, IT, and others, cascading findings and recommendations
- **Briefing sessions for staff and members** on a regular basis, including IT cyber and wider business risk updates
- **Routine cyber reporting** designed to keep senior managers aware of cyber practice, changing threats and current cyber risk profiles
- **Risk profiling exercises**, with those leading on corporate risk and the corporate risk register, or in the most vulnerable and critical service areas
- **Simulated phishing and other tests**, to spot and probe for risks, maybe in teams or generally across the council
- **E-learning modules for staff**, members and citizens, to use in their own time, but also as part of induction and qualification for network or systems access, with activity tests and self-help
- **Post incident wash-up activities** on 'near misses', failed changes, experiences from others, feedback from WARPs, Local Resilience Forums, and NSCS, and continual learning to improve practice
- **Specific training and briefing for democratic service officers and members**, to be alert to risks associated with digital practice in decision making, democratic processes, policy formulation, consultation and information provenance
- **'Safe on-line' guidance for citizens**, linked to existing material from agencies helping the digitally excluded or those most at risk

In practice, a combination of these will help to ensure wider awareness and on-going vigilance, and there are a range of services available to councils, such as the CC2i Dojo training, which offers 60 minutes of animated video-based e-learning. Dojo is available in 12 modules and is accessible on any device, and in a variety of formats, covering the full range of cyber threats, as well as two specific modules on GDPR.

> *"The traditional approach to IT or cyber security is to see it as something that IT does to the business (be that patching PCs or trapping email viruses). I don't see it that way. For me it's all about the data and how to protect it, whilst making sure its accessible when needed. Information management and governance colleagues are a key part of this. We work closely with them in an approach that includes collaboration on developing, writing and setting policy, project and bid funding, and training, as well as combined presentations to our senior officers."*
>
> *Sam Smith, Head of Strategy & Architecture LGSS, Socitm Vice President*

Conclusion

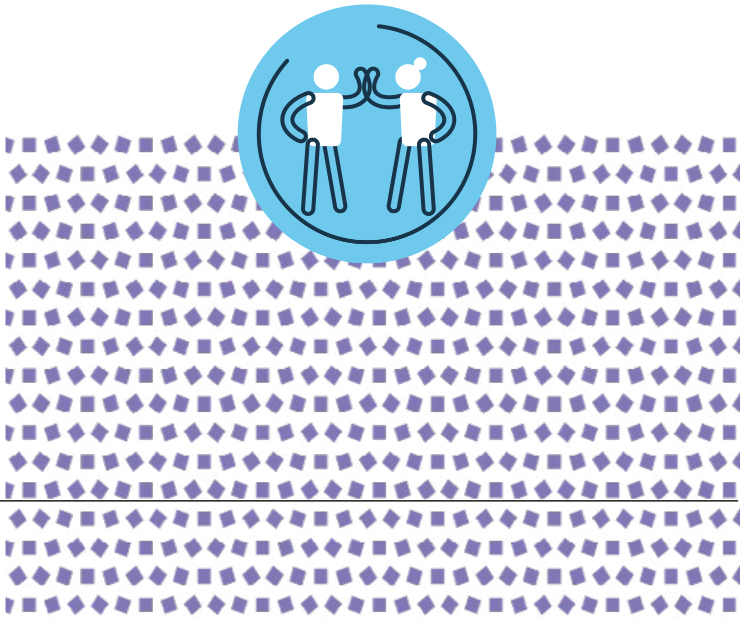
As important as having effective IT methods, change control, IT tools and testing regimes to protect against cyber risk, it is the wider cyber maturity of an organisation that defines its technology risk profile.

This is particularly true in the public sector. Local councils, for example, have responsibility for a vast number of disparate services, each depending on IT systems in different ways. Trying to eliminate cyber risk through technology methods alone is infeasible.

An organisation that treats cyber risk as a corporate responsibility, with broad, clear and effective governance, accountability and reporting, is more likely to be able to protect high-risk assets and digital services, and also to be adaptable and alert to an ever-changing landscape of cyber threats.

This means that cyber security planning and management cannot be left to IT alone, but the specific part that IT leadership must play in defining and managing cyber risk needs to be carefully defined.

Ideally, members, the chief executive, service leaders, SIRO, emergency planning, delivery partners, suppliers, the IT team and ultimately all employees have a part to play and to know what is their role. Only then can a council adequately adopt true digital working in ways that protect the public, whilst exploiting the power of technology opportunity.



Have your say

We welcome comments and discussion on the ideas presented in this guidance report.

Martin Ferguson
Director of Policy & Research, Socitm

About this report

Author
Jos Creese, Socitm Associate Director and Researcher

Editor
Martin Ferguson, Director of Policy & Research, Socitm

Production
Christopher Doyle - Designer
Magdalena Werner - Senior Creative Designer

Socitm Inform programme

Tel: 01604 709456
Email: inform@socitm.net
Website: www.socitm.net
Linkedin: Socitm
Twitter: @Socitm
KnowledgeHub: khub.net/Socitm

Sponsored by:

FORTINET®

hello@socitm.net | 01604 709456

Reference: 19007