Part 3

Inform Report

Cyber risk - the challenge for local government

Taking advantage of external cyber resources

March 2019

Socitm inform

Table of contents

Introduction

Few organisations, if any, can be self-sufficient in their internal cyber resources. Apart from relying on specialist external services, such as penetration testing and virus filtering, councils are likely increasingly to be using other service providers for a wide range of cyber activities, from independent testing to routine monitoring software. In addition to internal auditors, external cyber specialist advisors can bring a level of knowledge and current expertise that it is hard to retain in-house, to check on the robustness and appropriateness of cyber resilience planning and implementation.

Not all of these services need be costly. Many, such as the advice and support from local WARPs and the NCSC are freely available. There is also a variety of basic network and systems tools that can be acquired at no or low cost and that can be used to target particular cyber risks, perhaps complementing, if not replacing, the more sophisticated technologies required to protect digital infrastructures.

Other services come at a price, especially the more sophisticated managed security services and tools. Methods too take resources to implement and to sustain them, and there is a need to consider the internal cyber roles necessary to oversee good practice.

Councils need to make adequate provision in their plans, processes and practices for the insurance and protection demanded in this modern digital age, since skimping on cyber protection can have serious consequences for the organisation and for citizens.

This requires the necessary prioritisation of cyber investment, with the CIO or Head of IT working with colleagues, including the CFO and emergency planners, to ensure an understanding of its value and importance in digital developments and in ensuring resilience of legacy IT services. A cyber strategy should harness the skills, tools and processes needed to anticipate changing cyber risks and should ensure strong governance to manage and mitigate them.

This is also an area where there is justification for sharing and pooling resources, best practices and methodology across public services. Benefits lie not only in economies of scale in staff and technologies, but also in sharing best practice and intelligence, and in protecting mutual interests.

This third in our series of cyber investigative reports looks at some of the common cyber standards, methods, technologies, and resources that are available to public service organisations as they plan their cyber strategies.

Taking advantage of external cyber resources

There are a variety resources available to councils externally to assist with cyber security:

- free services and resources – such as guidance, advice and tools
- local intelligence networks, providing a collaborative cyber intelligence hub
- a range of external paid-for services, some low cost, others very costly and sophisticated.

The choice of which to use lies with individual councils and will depend on the scope, scale and sensitivity of their activities, amongst other factors. However, no councils can (or should) attempt complete cyber protection without using external help, especially free services and the essential basic tools and services.

Where councils are in IT shared service arrangements, or with IT outsourcing in place, or if they rely on largely cloud provided IT solutions, care is needed to ensure that intelligence gathering and collaboration still occurs, and that IT suppliers are fulfilling their duty of cyber protection. For these third parties, in particular, councils need to ensure integrity of their cyber practices and that they are not creating gaps in cyber protection collectively that need addressing to ensure that the council or citizens are left unintentionally vulnerable.

Doing this effectively requires careful planning, and as a minimum, appointing an IT security officer (ITSO) internally with the responsibility to devise and oversee the plan, how resources can be used in concert, and to manage the relationship with external providers.

The National Cyber Security Centre

The The National Cyber Security Centre (NCSC) was created as part of a £1.9b UK Government strategy launched in 2017. Since then it has defended the UK from over 10 malicious international cyberattacks every week.

> *"We are calling out unacceptable behaviour by hostile states and giving our businesses the specific information they need to defend themselves. We are improving our critical systems. We are helping to make using the Internet automatically safer. As we move into our third year, a major focus of our work will be providing every citizen with the tools they need to keep them safe online."*
>
> **Ciaran Martin,**
> *Chief Executive of the National Cyber Security Centre*

The NCSC provides local not just national services support to protect the UK, and its function includes engagement with local government and local business. It offers a range of tools, services and advice, often at low or no cost. Indeed, it sees its local role as being critically important in its overall question to protect UK interests in what an increasingly inter-connected society.

NCSC advice covers the full range of common cyber protection measures that councils can take, along with guidance in areas such as IT disaster recovery testing scenario exercises, methods to keep equipment safe (especially removeable media), and systems access and authentication advice, such as password policies. Details can be found on the NCSC web site, where a growing range of solutions are offered and summarised below:

The NCSC's range of solutions offered:

What it offers	What it Does	How to use it
Active Cyber Defence (ACD)	Active Cyber Defence (ACD) initiative aims to protect the UK from high-volume cyberattacks that affect people's everyday lives. Since its launch, the ACD programme has reduced the UK's share of visible global phishing attacks by 50%, including removing 138,398 phishing sites hosted in the UK.	Councils should maintain an awareness of the ACD programme and support its activity, including how businesses and local organisations can protect themselves and how councils can make use of NCSC guidance, products and services.
Mail Check	Mail Check is the NCSC's platform for assessing email security compliance. It collects, processes and analyses DMARC reports from across the public sector, as well as checking the security of other organisations. It gives information on how email is being sent from a council domain, without affecting delivery. This then allows implementation of policy to block spoofed emails, leaving legitimate email unaffected and reducing the risk of council email addresses being used by attackers.	With a public sector email address, any council can sign up for an NCSC account and access the Mail Check tool. It processes DMARC reports for the council, checks for encryption use and implements the DMARC policies.
Public Sector DNS Service	The UK Public Sector Domain Name System (DNS) Service is one of the NCSC's most widely deployed ADC services. On average, the service actively blocks 70,000 attempts to access known malicious sites each week. There are two NCSC DNS services for the public sector: a simple Internet service and a PSN DNS service soon to be launched.	The Internet DNS service can be used without needing to move your existing Internet DNS records. The Public Services Network (PSN) DNS provides greater protection as both a resolver and an authoritative name server for PSN. 'Free at point of use' - the service is centrally funded by the NCSC. Councils can register for both the Internet and PSN DNS services
CiSP	The Cyber-security Information Sharing Partnership (CiSP) is a joint industry and government initiative to share cyber threat and vulnerability information. Part of the NCSC, it seeks to increase cyber threat awareness and so reduce the impact of cyber risk on UK business. CiSP members come from across sectors and organisations to exchange cyber threat information in real time, in a secure environment.	Membership is free, and as a CiSP member, councils can also sign up to receive network monitoring reports as a free service from the UK's national Computer Emergency Response Team (CERT-UK), covering any malicious activity found on the council's network.

Web Check	Web Check is a free to use website configuration and vulnerability scanning service from the NCSC, available to all UK public sector organisations, currently scanning 1,200 government websites every day. It checks on a continual basis that data is protected in transit and in the user's web browser, as well as classifying risks (e.g. urgent, advisory, informational and best practice).	Local councils and emergency services in particular, are likely to benefit from using Web Check, according to NCSC. Councils can create a local 'watch list' of managed website URLs, then Web Check runs a non-intrusive scan, providing shareable reports of risks.
Cyber Essentials	Cyber Essentials was developed by NCSC to help organisations protect themselves against common cyber threats. It is backed by industry including the Federation of Small Businesses, the CBI and a number of insurance organisations. From 2014, Government requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information and providing certain ICT products and services, to be certified by the Cyber Essentials scheme. Cyber Essentials [BASIC] provides a route to self-certification. Cyber Essentials [PLUS] involves an independent external vulnerability scan (which carries a cost).	Councils can gain certification in one of two Cyber Essentials schemes, both suitable for councils of any size. Cyber Essentials certification gives evidence of good practice and the process for securing certification is simple and can be completed entirely online. It is also a useful step to GDPR compliance.

(1) DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

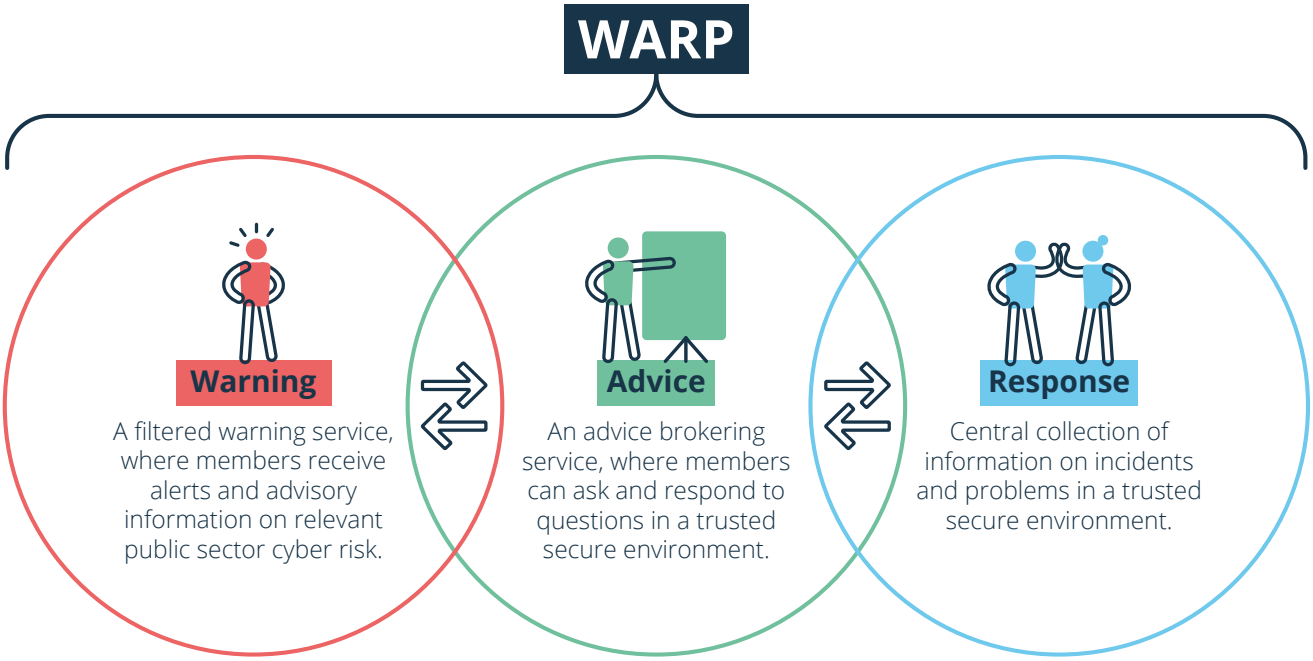
(2) A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases, serves to resolve, or translate, those common names to IP addresses as requested. DNS servers run software to communicate with each other using protocols.

Warning, Advice and Reporting Points

A Warning, Advice and Reporting Point (WARP) is (typically) a community-based service to share advice and information on computer-based threats and vulnerabilities.

UK councils and other locally-based public sector organisations have access to regional WARPs across the UK and have the opportunity to play an active part in attending meetings, contributing ideas, and sharing information about threats and counter-measures.

The WARPs typically provide:



It may not be clear in a council who should attend WARP meetings – for example, in an IT outsourced model or a shared service, or where there is no full time IT Security Officer.

It is recommended that the council does appoint a lead for cyber security in the IT team or domain, who would be responsible for retaining WARP (and other) links, even if they are represented by a partner of the service provider who reports back. They should be able to ensure the council can use the 'warning, advice and reporting' received to inform the council's approach to cyber protection and IT disaster recovery.

Being part of a WARP will increase knowledge and alerts regarding serious threats to information security and be a source of advice on preventative measures. More importantly, it is usually a free resource, attended by peers with common interest.

Circumstantial evidence provided for this research suggests that the regional WARPS vary in their scope and intensity of activity. Currently, the focus of Socitm, the LGA and MHCLG is on helping councils to invest the time and support to improve WARPs for the sector, as they are all supportive of the WARP model.

Socitm advice to councils' IT security teams is to be an active player in your nearest WARP and invest a bit of time and energy to help it to develop and improve, emulating best practice across the UK network of WARPs.

"Cyber is a growing challenge and priority for us all. Although fully aware of the need to address this challenge properly, it can feel like drinking from a firehouse to keep up! Our chosen approach is to put in place a clear and structured plan, with tools, resource and methods, which embraces both legacy and future IT and digital platforms."

Jason Tillyard, Shared IT Manager, Breckland and South Holland District Councils

Local Resilience Forums and emergency planning

Local Resilience Forums (LRFs) are multi-agency partnerships covering regions of the UK. They include representatives from local public services, including the emergency services, local authorities, Police, the NHS, the Environment Agency and others. These agencies are known as 'Category 1 Responders', as defined by the Civil Contingencies Act.

The LRFs are also supported by 'Category 2' responders, such as the Highways Agency, charities, military, and public utility companies, creating a network of information sharing and collaboration to protect against and respond to a civil emergency, including a cyber-attack.

In the past, LRFs would have had little to do with cyber matters, but the increasing risks to community resilience from a sustained cyber-attack means that the topic is now high on the agenda, and some LRFs have run cyber-related scenario exercises.

Typical risks for local cyber emergencies that LRFs would consider include:

- **Failure of civil infrastructure** and services, such as power, water or telecommunications services, as a result of a cyber attack or systems failure
- **Targeted attacks**, such as ransomware on public services on which people depend, causing hardship or even panic
- **A new computer virus** is highly infectious and contaminates linked systems in an area, bringing businesses, homes, and public services to a standstill
- **A non-cyber incident** that causes major community disruption (such as terrorism), which is then used by cyber criminals to mount a cyber attack while resources are stretched.

"...the increasing risks to community resilience from a sustained cyber-attack means that the topic is now high on the agenda..."

These are all reasons why emergency planning officers in councils need to take on cyber responsibilities as part of their roles. To do this, given few will be technology specialists, they need to work with IT experts and security officers to help to understand the risks, their mitigation and likely threat impacts.

Emergency planners also need to work with politicians, service leaders, and local partner organisations, such as the Police, in raising awareness and preparedness for a cyber incident, as well as maintaining strong links with national bodies and peer groups in other LRFs, NCSC and MHCLG.

Using a Managed Security Services Provider

A Managed Security Services Provider (MSSP) works with the internal IT security lead to take on much of the management of a council's IT security processes remotely, typically from the cloud. They may design and implement security infrastructure, as well as responding to incidents and offering access to specialist services such as forensic analysis, cryptoanalysis, and malware reverse engineering.

By providing up-to-date and deep security expertise and capacity, an MSSP allows a Head of IT or CIO to focus on security governance, rather than maintaining the integrity of operational security administrative tasks.

In deciding to work with an MSSP, determining the services you seek to contract, and the nature of that partnership, and implementation planning require care:

Step 1: Getting your house in order

As with selecting any external IT service provider, it is important to sort out any internal IT security management issues first, since not doing so and passing problems on unassessed is often a recipe for disaster, leading to high costs, supplier delivery issues and failure to meet expectations. Good preparation includes:

- Internal maturity and understanding of the management of information risk
- An inventory of where information and other digital assets lie and their ownership
- A Stocktake of good and weak cyber practice, methods and tools
- Clarity on the corporate appetite for risk and cyber aspect of the corporate risk register
- Effective internal cyber governance that leads to clear prioritisation for the MSSP.

Step 2: Choosing the right MSSP

Selecting an MSSP for cyber security requires care in what is a relatively new market providing critical services. Key considerations should include:

- Understanding the range of services and products on offer and how they would be used
- Determining MSSP credentials: recognition, awards, references and track record
- Assessing capacity, skills and capability of the MSSP – including as technologies evolve
- The MSSP's understanding of the public sector and council challenges in particular
- The incident response practices and processes of the MSSP
- The MSSP's own internal practices, processes, training, external audits, etc.
- Their partnership style and expectations of the council in providing a tailored service
- Their dependence on other third parties in how they provide managed services.

Methods and Tools

Every council needs an appropriate cyber ecosystem to manage the risks and opportunities of technology, including protecting and exploiting data and information.

This ecosystem combines methods and tools, procured or externally run. These need to be complemented by the governance and wider organisational awareness and employee practices that together ensure good cyber protection in a council.

There is a huge amount of material and advice which already exists on the Web, and Socitm has previously produced two essential briefings for members, on the practical steps to be taken to help to protect digital channels.

This new report does not seek to provide a comprehensive list of such resources (which would

in any case be quickly dated). IT Security managers in councils need to consider for themselves the right combination of methods and tools for their organisations.

This includes reviewing the resources and methods that councils can deploy such as recommended methodologies, standards, policies, procedures and frameworks, from the NCSC and others. Some of the most common are listed below.

ISMS

An Information Security Management System (ISMS) is a framework of policies and procedures that includes all legal, physical and technical controls involved in a council's information risk management processes, within IT and beyond.

For example:

- Information use, governance, tools and monitoring
- IT use policies for all employees
- IT procurement policies to ensure supplier and product conformity
- Cyber security responsibilities embedded throughout the council
- Polices for device management and mobile working technologies and tools
- ID management, access security linked to role and HR practices
- Systems monitoring methods and practices – firewall, intrusion detection and prevention, virus protection etc.

An ISMS typically addresses employee behaviour and practices, as well as data and technology. It can be targeted towards a particular type of data, such as citizen data, or it can be implemented in a comprehensive way that becomes part of the organisation's culture.

ISO27001

For most councils the overall approach to an ISMS will be developed in-house, or in partnership with an external provider. ISO 27001 (previously known as ISO/IEC 27001:2005) is set of auditable and recognised security management processes and standards that effectively specify the basis for creating an ISMS.

ISO27001 does not mandate specific actions, but it provides a basis for good practice internal IT security practices, including documentation, internal audits, continual improvement, and corrective and preventive action.

Whilst the majority of councils do not have full ISO27001 accreditation, many use it partially – either as a tool to check and guide ISMS development or in a specific part of their activities, perhaps where cyber risks are higher.

Achieving accredited certification to ISO 27001 provides an independent, expert assessment that information security is managed in line with international best practice and business objectives. This can be a valuable approach for councils operating at scale, those with serious security issues to address, or where a council is seeking to develop commercial credibility as an IT shared services partner or provider.

For smaller councils, full ISO27001 is probably an unnecessary overhead, although following its pattern of checks and auditable procedures can be helpful, even if final accreditation is not sought.

PCI compliance

If there is a growing commercial function in the council, perhaps selling services and products (leisure, parking, events booking, hiring equipment or venues), there will be a need to either contract a PCI compliance payment hosting partner or demonstrate internal PCI compliance.

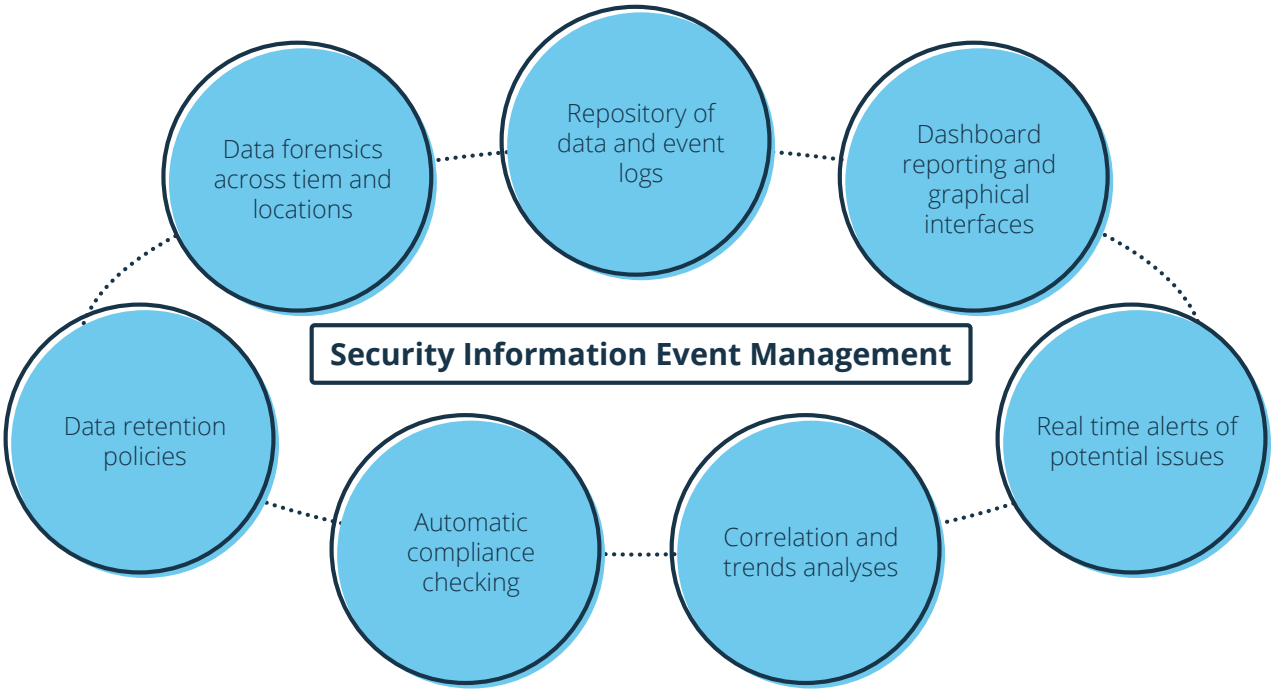
The Payment Card Industry Data Security Standard (PCI DSS) applies to organisations of any size that accept credit card payments, whether on the Web, face to face, or over the telephone.

SIEM

Security Information and Event Management (SIEM) is an approach to security management and cyber incident (event) management. Having a SIEM in place is a good way of preparing for how to act should a cyber incident occur.

A SIEM system brings together relevant data from multiple sources, to target anomalies, create system alerts and to initiate actions to prevent a cyber incident occurring or spreading. The challenge in this is to be able to detect abnormal behaviour and data from the 'white noise' of network traffic and avoid having to use a mis-match of ad hoc tools that create unnecessary cost or potential 'blind spots' in cyber protection.

For some councils, SIEM will be a service from a supplier partner, collecting data and using tools from different sources in one coherent approach to security tracking and reporting. The below illustration outlines the SIEM approach:



Cyber tools in general

Many specialist cyber tools exist to support full SIEM practices, from simple checks in data logs and correlation of cyber risk in related systems, to more sophisticated tools that learn behaviour and create automatic response, for example to surreptitious data 'leakage'.

There are free tools such as 'Open Vast' antivirus, which provides a basic cover, although not necessarily sophistication or elegance, compared with the more complex (and expensive) tools.

The choice of tools and level of investment that councils need to make depends on the nature of the risks, the technology environment, and how cyber is managed overall. A partner or shared service provider may bring a range of tools and services, perhaps as part of a shared SIEM.

Whilst every council needs to consider its security risks and cyber protection requirements individually, a completely bespoke approach is not advisable. Commonly used methods, tools and policies should be adopted to save time and effort and also to maximise the protection afforded by importing best practice. Complete tailoring will carry risks with a dependence on retained local knowledge and skills, in keeping up with cyber trends and in the potential for unintentional cyber 'bloodspots'.

The challenge for councils is to ensure these are kept up to date and that interdependencies are tracked in maintenance activities, such as systems patching.

There are many external services and tools that can assist councils with their cyber challenge. It is not necessary to invent bespoke security checks. Neither is it true that these tools are only affordable by the larger councils with greater IT spending power.

Some of the most common examples are:

Tool	What is it?	When to use
STIX	Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analysed in a consistent manner.	STIX, Taxii and CybOX™ are free to use and internationally recognised technical specifications designed to enable automated information sharing for cybersecurity situational awareness, and real-time network defence. Their use would be typically overseen by a Security Operations Centre.
Taxii	Trusted Automated eXchange of Indicator Information defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organizational, product line and service boundaries. TAXII enables organisations to share the security information they choose with the partners they choose.	
CybOX™	Cyber Observable eXpression. Cybersecurity relies on information such as event management and logging, malware characterisation, intrusion detection, prevention, incident response, and digital forensics. CabOX aims to provide a common structure and content types for addressing cyber observables across this wide range of areas to improve consistency and interoperability.	
CVSS	Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS seeks to assign severity scores to vulnerabilities, allowing prioritisation of responses and resources according to threat levels. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe. While many utilize only the CVSS Base score for determining severity, temporal and environmental scores also exist, to factor in availability of mitigations and how widespread vulnerable systems are within an organisation, respectively.	This is a useful method for councils to adopt to standardise the assessment of risk priorities, as part of a wider armoury of prioritisation, recovery planning and risk prevention.

There are plenty of cases reported of systems fraud, in all sectors and types of organisations, from internal systems abuse (such as the recent case of the Westminster interim manager defrauding the council of £1m) to external abuses, such as benefit claimant fraud.

These fraudulent attacks on council assets can be hard to detect by manual means, as they are typically hidden in the system or lie below threshold alarm levels. But modern audit tools and automated pattern analysis that cross-link data sets can assist in detecting even the most complex and sophisticated fraud. These should form 'part and parcel' of a councils' cyber armoury.

It is also not acceptable simply to rely on external suppliers and service providers to be responsible in the way they process and handle council (public) data in their care, assuming that they will apply good practice and the necessary level of cyber planning, protection and testing. Councils have a duty of care to protect assets and ensure suppliers use appropriate cyber protection tools in their public service duties.

Whatever tools and methods a council chooses, it needs to have technology tracking in place to track and to categorise risk. This includes insight into who is on the network, what data is being access and by whom, how data is being linked and shared, the devices connected and if these conform to security standards.

Strong authentication (two-factor authentication, biometrics and tokens) can all help. Where there are federated or shared identities, there must remain central visibility and control, should authentication and access control methods become compromised in any way, intentionally or by accident.

"Digital technologies underpin the delivery of the council's essential services; therefore strong security standards are imperative to protect data and maintain business-as-normal. Cyber resilience features strongly in our business continuity and emergency plans, ensuring we are able to respond and recover from cyber-attacks."

Steve Makin, ICT Contracts Officer, Folkestone and Hythe District Council

Conclusion

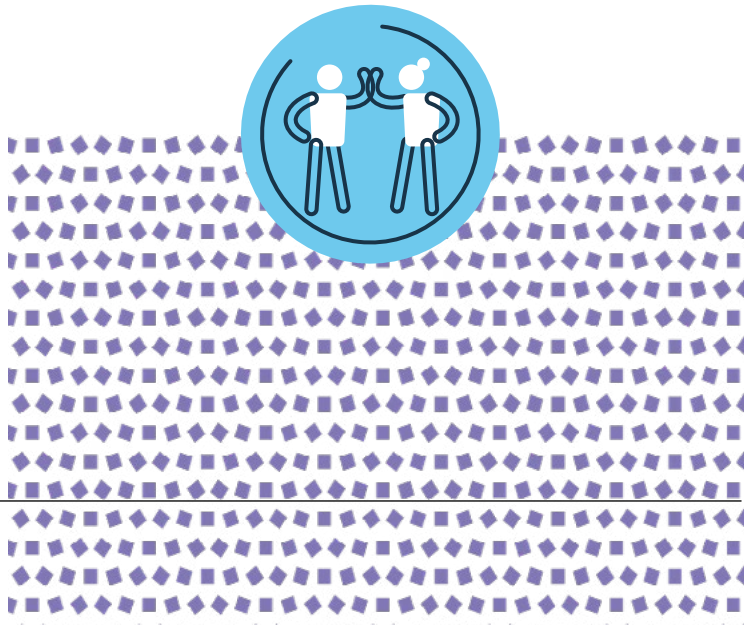
This report is not intended to provide a full exposition of all the technologies and cyber services available. It does seek to give a simple update on some of the approaches that can help ensure awareness of common methods, standards and resources.

Some of these are freely available and every council should be making the maximum use of these. Examples include the WARPs, the NCSC and the Local Resilience Forums. Many tools are also low cost or free, although often basic in their nature.

Others have significant cost, although some of these can be emulated (such as using ISO27001 as a test base of good practice, without necessarily applying for full accreditation).

Where services are required from external providers, councils need to ensure their integrity, as well as their value for money, preparing the ground carefully before committing. This can partly be achieved by collaboration and sharing, perhaps a single contract with an MSSP. There should be a clear expectation on suppliers to play their part, especially in outsourced IT arrangements.

Overall, the most important starting point is to have a plan for the methods used to track and deal with cyber threats as they change, and to determine where services can best be run in-house or where external support and expertise is needed.



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®