Part 5

Inform Report

Cyber risk - the challenge for local government

Cyber risk futures

March 2019

Socitm inform

Table of contents

Introduction 03

Future IT cyber risks 04

Internet of Things (IoT)

Biometrics

Artificial Intelligence (AI), Automation

and Machine Learning (ML)

Cloud Computing

Virtual Reality (VR)

The Future is today 10

Conclusion 12

Introduction

One of the biggest challenges in dealing with cyber threats lies in their ever-changing nature. If only technology didn't change so much, the job of cyber protection would be so much easier!

With every new technology that offers new business and social value, there are inevitably downsides that can be exploited by those with malicious intent. And, as the rewards from online crime rise and detection rates remain low, it is not surprising that huge investment is made to take advantage of the illicit pickings.

For IT leader in any organisation this poses a dilemma: to stick with what you know or to be an innovator and take the greater risks that often accompany adoption of emerging technologies. For IT leaders naturally concerned about risk, this is a real problem, especially given the growing demands coming from digital programmes to exploit the well-publicised advantages of new technologies such as Cloud and Artificial Intelligence.

Part of this is about understanding the nature of changing risks and their mitigation. But part is also about ensuring that the advocates and the enthusiasts also take some of the responsibility for the managing these risks.

This last in our series of cyber reports looks at how IT leaders in the public sector and councils, in particular, should approach this dilemma.

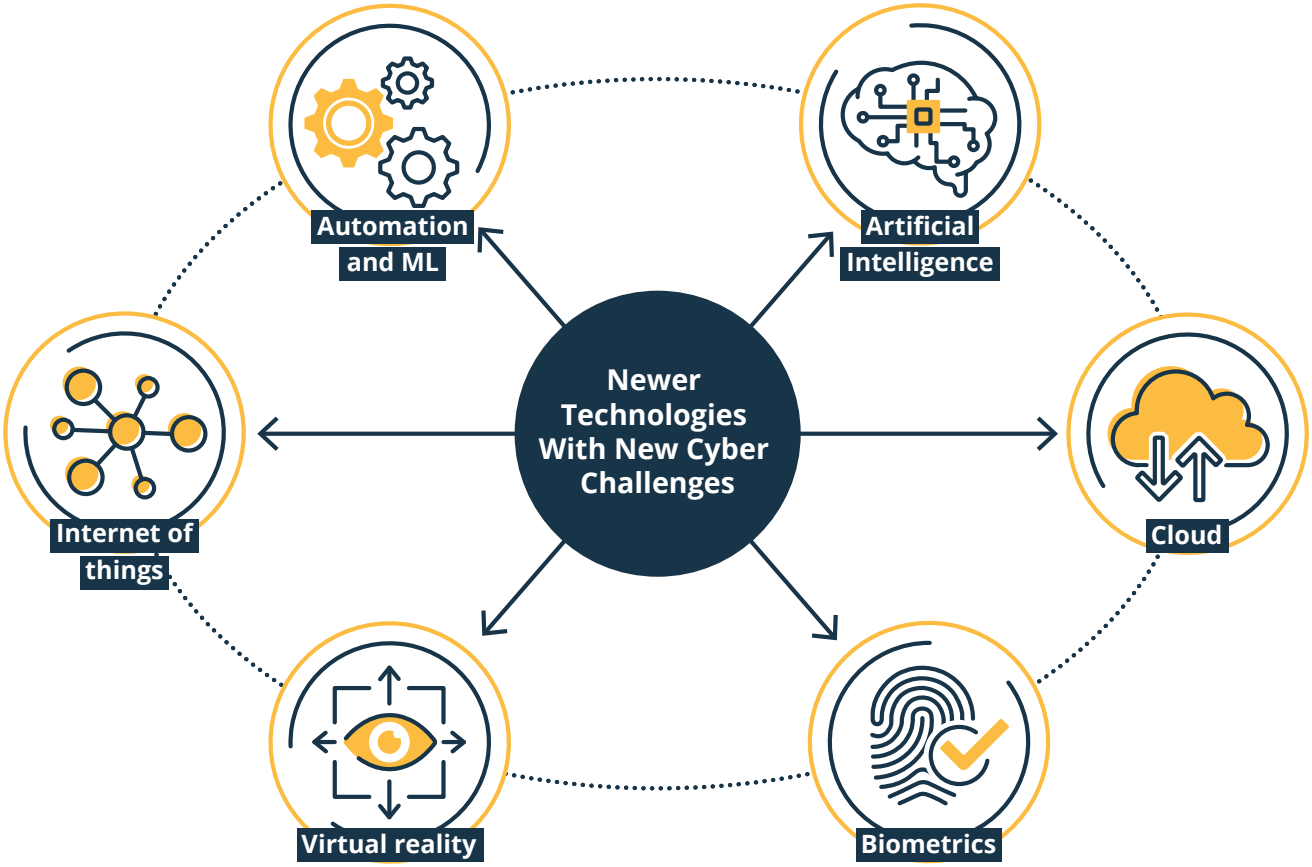
Future IT cyber risks

Many of the issues and challenges facing councils in the use of new technologies lie as much in the culture, process and governance needed to exploit their potential, as in managing the technology itself.

This is especially true of the cyber risks associated with new technologies, where wider working practices, understanding and willingness to adopt are crucial factors in safe and secure deployment. As new technology methods and tools are implemented in digital programmes, IT leaders need to be aware of the inherent cyber risks and be able to advise their council on how to manage these risks effectively.

Balancing risks and benefits and ensuring business-focused IT reporting, good governance and effective communications have been covered in previous reports in this series and have an essential part to play.

There is a variety of newer technologies that pose significant and new cyber challenges and that are already finding their way into use in councils:



Each of these new technologies offers opportunities to strengthen cyber protection, not just to create new risk, and councils should consider how they can be deployed in the armoury of cyber protection.

The following tables describe in more detail some of these new tools and associated cyber issues, with guidance for councils' IT leaders planning their use. But it is the role of IT leaders to take time to keep abreast of new technologies. Any report such as this will only be partial in its assessment, and probably quickly out of date.

Internet of Things (IoT)

The cyber issue:

Embedded sensors create a whole new opportunity for the management of assets. This includes everything from equipment, transport, roads, buildings and raw materials, to the way that linked data can reduce asset loss and maximise productivity. As IoT moves from 'things' to being about 'people', it will also revolutionise services such as care, protection and mobility.

But these low-cost, linked and integrated sensors create new security challenges. Some will use wireless connections from outside secure zones to connect to devices linked to corporate infrastructure. A simple security light or CCTV camera, or even a connected coffee machine in the office can create a backdoor into a more secure system through that connection, if care is not taken. They can also be targeted for distributed denial of service attacks (DDoS) to disable corporate networks or services.

Attackers can usually easily find and access these devices and their signals, and then break through a secure network perimeter if configuration and security practices are not undertaken with care. They can therefore become soft targets for those with malicious intent.

Perhaps even more challenging is that these consumer devices are built for cheapness and ease of implementation, not on-going security compliance. They will often lack the power or technology capability to be future-proof, as security threats change, and IT infrastructure matures. Future security systems may simply not be able to manage these devices, which could become isolated or hidden devices to be used or even adapted for malicious purposes.

There is also debate about the risk of the mass production of IoT devices in foreign states being used to harbour sleeping vulnerabilities, which could be exploited at a later date to access government networks or to disrupt western society and democracy. This lies at the heart of recent international concerns about some commonly used Chinese embedded technologies.

What to do:

It is important to know about every device linked directly to a corporate network. This is a challenge in the explosion of IoT devices, but automated tools can be used to disable network access, where required, in response to access moving from a low to high security zone.

More critically, IT leaders need to ensure that policies, protocols and procedures exits for IoT deployment, especially where sensors wirelessly connect to internal networks. Where personal data is being collected (such as in safeguarding, health monitoring, movement tracking, etc) even greater care is needed to manage and control data - for GDPR compliance as a minimum.

IT leaders are therefore advised to factor IoT into technology strategies, planning and technology architecture design, rather than allowing IoT deployment to be sporadic, organic and unchecked in its inevitable growth. This can include creating an IoT integration platform, a secure interface, which protects data, access and also tracks devices and assets.

A structured approach will also assist with the essential vulnerability patching. Unfortunately, many cheap consumer IoT devices were never built with this in mind. So, IoT devices that fail to keep up with the required security patching and management policies should be isolated in terms of their access or replaced.

Finally, IT leaders need to ensure that, as part of their cyber protection planning, there is constant monitoring and probing for IoT weaknesses. Tools exist to do this, seeking out IoT devices on networks and in buildings, such as www.shodan.io . Tools can also be used to find and deal with sensors that begin to exhibit uncharacteristic behaviour which could indicate a risk or a threat.

Biometrics

The cyber issue:

The use of biometrics in IT is growing, largely for identity management where it offers greater authenticity of the party seeking access, for example in health and safety and tracking personal well-being.

Fingerprint, voice and facial recognition are today commonplace, reliable and quick to use. These also offer much greater levels of security on mobile personal devices than traditional passcodes.

Challenges for IT leaders include whether and how to allow these newer technologies to be used to access credentials on corporate networks and their cost (in terms of design, migration, adoption and on-going management).

There are also questions about PSN compliance and whether biometrics on mobile devices such as smartphones are sufficiently secure in themselves to span both personal and corporate use.

Public confidence and concerns are also relevant here. Citizens need to feel comfortable with using biometric technologies to access public services and their personal data.

What to do:

For IT leaders, biometric recognition could enable wider adoption of 'bring your own device' (BYOD).

But this depends on reconfiguration of security practices and technical architectures and does not necessarily overcome any challenges about using personal devices to access sensitive corporate data. Adoption should be coupled with a review of HR policies, since there are specific responsibilities falling on employees using any equipment to access sensitive data.

Given the likelihood that the explosion of biometrics for consumer devices will gradually spread to infrastructure access, IT leaders should begin planning for how this might work in practice, perhaps in conjunction with smartphones.

Part of this will be about tracking public confidence and adoption led by the private sector and ensuring a holistic approach to access management design rather than an ad hoc approach to exploiting specific technologies, such as biometrics

"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 (now part of Jisc)

Artificial Intelligence (AI), Automation and Machine Learning (ML)

The cyber issue:

Whilst they are not the same, AI and ML are often linked because they have common cyber characteristics. In particular their power to detect cyber vulnerabilities and breaches as well as their potential to create them.

In the future, it will be increasingly difficult to detect whether an attack on a computer system comes from a human or a machine. AI malware can already mimic human behaviour to hide or disguise itself. It uses this to exploiting human habits in order to penetrate systems, adapting along the way. It can also sit in an 'infected area' after an initial, perhaps low-level penetration, learning about internal security systems, practices and physical infrastructure, for example, keeping data stealing below discovered detection thresholds.

To assist with protection, automated tools can trawl and monitor networks for new cyber risks, advising security administrators of vulnerabilities, risks and attempted penetration.

Those services range from virus protection to defence against a wide range of cyberattacks from within and outside an organisation. Coupled with AI and machine learning technologies, these services can increasingly adapt to the habits of an organisation and its users to be become more alert to unusual patterns of behaviour that would be impossible to spot by manual means alone.

What to do:

In recognising that these powerful new technologies are a risk as well as a counter measure to cyber risk, this latter capability should be exploited as part of their adoption and to help enable methods of keeping networks safe from attack.

Councils will already be using penetration testing, network mentoring, virus and phishing protection from external sources (or should be). IT leaders should ensure that they are equipped with intelligence tools to keep pace with cyber risks and the activities of those with malicious intent.

But in addition, councils should be considering some of the new and specialist tools that can be used to monitor threats as new technologies (such as IoT and AI) are deployed. These will gradually help to mitigate the risks of cyber exploitation from abuse of data to the misappropriation of assets.

IT leaders need to understand the ramification of AI and ensure that their organisation's deployment of AI for business benefit is matched by AI that detects and prevents new cyber risk.

"Walsall council is investing in migration to the cloud to address the risks associated with an aging on premise data centre. Cloud computing is giving greater flexibility to our employees helping them to be agile workers, improving service delivery and addressing cyber risks."

Carol Williams, Head of ICT, Walsall MBC

Cloud Computing

The cyber issue:

Far from a new technology, the growth in cloud options, variations and their widespread adoption require a reassessment of cyber planning in councils. In this respect, Cloud is still an emerging technology, so included here.

Cloud computing is a central part of most council's IT architectures today and this adoption is increasing. Even those councils with a highly cautious cloud adoption policy will be using cloud – even if the IT department doesn't know about it.

Many cloud platforms from major suppliers are highly robust and secure – more secure and protected from incidents than an in-house solution would be able to afford - as well as highly accessible. However, with the myriad of cloud services available on the market, this is not always the case.

Many cloud providers subcontract the provision of data processing and some take advantage of their role as processors and data handlers, selling on customer data. Small print in contracts will often surprise.

Public services must be concerned also about where data physically resides. The ability to access, track and recall data will be important. Moreover, transitioning to a cloud model requires careful handling of the change and appropriate due diligence. Working with a reputable partner to assist in this can be beneficial.

Above all, councils need to avoid creating a patchwork of different cloud solutions in response to business demand. This can result in a range of standards, access methods, identities for users, security methods and data interchange problems.

In moving to a cloud model, the focus must be on the data:

- The disparate systems holding the data
- The classification and sensitivity of the data
- The various locations where processing takes place

What to do

Cloud presents a range of new challenges for councils. Unlike on-premise IT, it is not feasible to 'secure the cloud' – a new approach is needed that encompasses:

- Being clear about where your data is being held
- Not putting sensitive data in the cloud unless you trust the provider and their security methods
- Having strong information management policies in place, with clear accountability
- Ensuring that any department or teams using cloud services understand the data risks.

It is not enough to ensure that each cloud service is safe and secure, for example with individual firewalls. A holistic approach is required that recognises the variety and changeability of cloud solutions, which are often free to use, and invisible to the IT department.

Cyber risk planning for cloud therefore needs to encompass a multi-supplier approach, including platforms and systems, internal and external. The approach needs to be layered, with rigorous automated reporting tools that inform IT about what is happening across the whole network, regardless of where any threat originates and within which cloud domain. Cloud computing cannot be avoided. It often offers low cost, flexible, agile, scalable and often more robust IT solutions than conventional IT. It is also becoming the default, as many suppliers move away from on-premise delivery of core services.

IT leaders should therefore plan for cloud adoption holistically and strategically, determining policies, practices and architecture principles that ensure the right cloud solutions are implemented in a consistent fashion. This will help to avoid a piecemeal approach of a disparate array of cloud services simply being 'bolted on' to the existing IT infrastructure, with little thought given to cyber protection, longer-term support, data management or hidden costs.

The cyber planning for cloud adoption should consider factors such as:

- The many devices and device types accessing the data
- The identity and authorisation of the individual accessing the data.

- Data security in general, from access to recovery
- Cloud adoption policies to ensure appropriate platforms are used and only suitable data/functions are run in the cloud
- Identity management, access controls and federated identity management for users
- Monitoring and tracking tools to detect risks
- Disaster recovery planning, testing and exit planning
- Change control planning and practice
- 'Critical application' status, data sensitivity/location
- The cloud supplier's responsibilities and liabilities relating to cyber and their credibility as a trusted data processor.

Virtual Reality (VR)

The cyber issue:

Virtual Reality is largely associated with gaming, but its deployment is growing rapidly in areas such as design, retail and health.

For councils, there are many potential applications of VR in civic planning, transport, buildings controls and design, social care, environmental health, training, new services scenario simulation, leisure services and more. As VR grows it will be important that the cyber risks are considered.

VR systems are likely to hold large amounts of data, both about assets and about people. Potentially, they will hold high intellectual property value, and have privacy concerns, as well as vulnerability exposure (such as in civic infrastructure or systems design). Protecting personal data, physical security and assets will become more important, especially where VR links to IoT and AI.

VR tools will also be embedded or at least linked to corporate networks, and often span partner and public access, creating new risks.

What to do:

Many of the risks are no different from any connected system, but for VR it could be easy to overlook the connection as something isolated, limited to scope or just different and less risky.

In addition to the usual network security from new connected devices and systems, there are some specific aspects of VR to consider in terms of privacy and the rights of VR users. VR headsets can be dangerous if hackers take over the device, both in influencing the wearer, or in exploiting the data they contain.

These ethical and privacy issues are equally important in terms of cyber planning as network protection. Policies in councils on data ethics and digital standards to protect the individual will be key requirements here.

The Future is today

In general, councils are already taking cyber risks seriously. Many of the risks are well understood and there is much good practice. At the same time, the rate of growth of cyber incidents and 'near misses' is increasing across all organisations. For those that have so far avoided a serious breach, cyber resilience may not always get the priority or visibility that it deserves. Excitement over the opportunities presented by emerging technologies will sometimes outweigh or obscure the risk.

The degree of sophistication of cyber threats seen today, and their variety, requires an equally sophisticated response, if councils are to protect services, systems, data, and the very communities which they serve and support. Meanwhile, the trend towards more cyber-attacks, using more sophisticated IT and human-like methods, is increasing. The challenge for Heads of IT is to keep pace – with knowledge, protection and adoption.

New technologies offer councils huge opportunity in tackling cost reduction, service improvement and complex problem-solving. But as the IT landscape becomes more complex, all councils need a comprehensive plan of action if they are to keep pace. IT strategies, policies and methods will need revising, with new architectures for emerging technologies such as IoT, AI, RPA, Cloud, VR and more. Simply 'bolting on' emerging IT to legacy IT won't do.

This should include consideration of changing risks, modelling technology defences as part of wider business continuity plans and emergency planning. It is almost inevitable that a cyber incident will occur at some point and that an organisation-wide response will be needed.

However, the majority of successful cyber-attacks are not sophisticated. They are the result of simple mistakes, such as mishandled data, falling for a phishing attack or poor patching of systems, leaving the organisation vulnerable. Maintaining good cyber hygiene requires cross-organisation coordination, not just IT protection.

Service leaders and staff need to understand the new technologies that they are using. Cyber protection should feature regularly as a topic at board level.

Political leaders too need to be aware of the risks and implications of cyber threats in how future digital services are designed and delivered, in how policies are set, in the impact of adopting emerging technologies and in how transformation programmes are enacted. These are all issues for today, not for the future.

This requires some basic practice to be in place, led by IT with service leaders, including:

- a clear, agreed and broad definition of cyber risk and how new technologies offer both new risks and new solutions
- an understanding of where emerging technologies should sit in IT and digital planning, based on a balance of risks and benefits
- clear governance and reporting on new technology adoption, including the involvement of third party suppliers and other partner organisations
- regular testing, audit and adjustment of cyber mitigation plans, using tools to keep pace with the new IT.

IT leaders need to be experts in their field and lead corporate advisors on technology futures and IT risk. There are plenty of sources of current technology predictions and vision to assist, including those from Socitm.

"Our experience in dealing with a sustained cyber-incident highlighted a handful of key learnings. Quick decision-making was crucial in ensuring that we were agile and responsive as the threat evolved. The Chief Executive was involved from the outset (as were political leaders and service directors). Communication channels were established at operational, strategic and political levels, with regular scheduled updates throughout the incident. In parallel, we put in place regular and transparent messages to our citizens explaining the difficulties that we were experiencing and advising of alternative ways to contact us."

Ed Garcez, Chief Information Officer, LB Camden

"Many colleagues will remember when IT security risks moved out of the basement into the board room in the run up to the Y2K bug. Today, digital technology is the foundation for all business and commerce, public and private. If we worried about Y2K, it was only because we had a deadline to focus on. But our next massive security event could happen at any point and most of us aren't ready! The platform for highly efficient public services is digital. The security around that platform is fragmented and federated across cloud platforms, communications providers, hardware manufacturers and systems vendors. It's never been more important, more difficult and yet it will probably never be this easy. Cyber security needs now to be number 1, 2 and 3 on my list."

Glyn Peach, Director of Digital Services & Transformation, Swindon Borough Council

Conclusion

Technology is not going to stop evolving , offering new opportunity to transform organisations, to improve services and to improve people's lives. The pace of change shows no abatement, and resistance is futile, especially for public service organisations struggling with the dual effects of growing demands and reducing resources, for which digital transformation is crucial to future service sustainability.

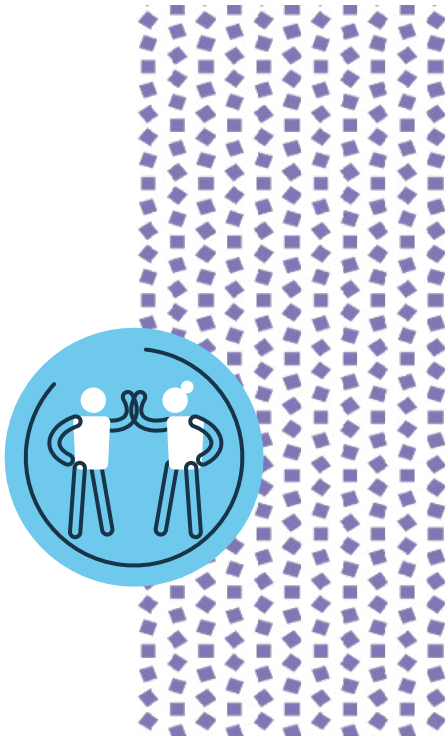
Yet in the rush to adopt new and exciting technologies that promise amazing benefits (usually promoted by pundits and the suppliers offering them), organisations need to be mindful about the new cyber risk that they bring, and how these can best be managed and mitigated.

IT leaders need to be at the forefront of technology change, advising their business colleagues on the benefits and the risks, in a clear balance of argument, to guide investment and to align innovation with the organisations appetite for risk and its business ambition. Positioning IT as an internal auditor, a policing function, or corporate cyber owner is a big mistake, usually resulting in IT being seen as slow, resistant to change and a barrier to business improvement.

This is not to say IT leaders should be blasé about cyber risk, leaving it to the SIRO and others. IT needs to be able to articulate cyber risk in business terms related to service aims and with mitigation plans to allow appropriate adoption of new technologies.

Particular areas are summarised in this report, but IT leaders need to keep abreast of technology change, especially through networks of peers such as Socitm.

> *"As our world transforms at pace to "digital" it is vital that digital resilience and cyber security is secured across all systems and services within the public sector. This series is a priceless reference highlighting that the breadth of responsibility in securing our data, as well as ensuring we use optimal methods to secure resilience and ownership, extends beyond traditional IT departments. A must read for all across the public sector, but in particular those with senior responsibilities in local authorities."*
>
> **Huw McKee,**
> *Head of IT and Digital Transformation, and Socitm Vice President, Conwy County Borough Council*



This series of reports is proudly sponsored by:

FORTINET®

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organisations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 350,000 customers trust Fortinet to protect their businesses.

Learn more at www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

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®