Appendix 2

Department for
Communities and
Local Government

Understanding Local Cyber Resilience

A guide for local government on cyber threats and how to mitigate them

March 2015
Department for Communities and Local Government

This document/publication is also available on our website at www.gov.uk/dclg

If you have any enquiries regarding this document/publication, complete the form at http://forms.communities.gov.uk/ or write to us at:

Department for Communities and Local Government
Fry Building
2 Marsham Street
London
SW1P 4DF
Telephone: 030 3444 0000

For all our latest news and updates follow us on Twitter: https://twitter.com/CommunitiesUK

March 2015

ISBN: 978-1-4098-4619-2

Contents

Introduction

This paper, commissioned by the Department for Communities and Local Government and prepared in collaboration with the Cabinet Office, outlines the key cyber resilience threat to Local Government. This is a persistent threat that, if left unchecked, could disrupt the day-to-day operations of councils, the delivery of local public services and ultimately has the potential to compromise national security.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services. However, these also present more opportunities for attackers. The networks and public-facing websites of every local authority are threatened. On average, 33,000 malicious emails are blocked from accessing public sector systems every month and this is just one of the many different types of attack government and wider public service systems must defend against. The scale of the targeting, coupled with the difficulty of monitoring all possible attack methods, means some attacks will get through but our collective responsibility is to both reduce the likelihood and the impact of such a threat succeeding. Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threat. They may try to compromising public sector networks to meet various objectives that include:

- Stealing sensitive information to gain an economic, diplomatic or military advantage over the UK
- Financial gain
- Attracting publicity for a political cause
- Embarrassing central and local government
- Controlling computer infrastructure to support other nefarious activity
- Disrupting or destroying computer infrastructure

Whilst the level of threat will vary across local authorities they all possess information or infrastructure of interest to malicious cyber attackers. Council employees can also be targets for criminal activity. Across the country local government IT departments are working hard to reduce these threats every day and the support of senior officers and councillors is vital to ensuring the continued focus and profile of this work. This guide is intended to help the non-technical reader understand the threats and what can be done to reduce their organisations' vulnerability to security incidents and cyber-attacks.

Cybercrime

Cybercriminals’ principal goal is to monetise their attacks. The most common form of cyber-attack against public bodies is the use of false or stolen customer credentials to commit fraud. The uptake in online services means this form of crime can now be done on a much larger scale and foreign nationals as well as onshore criminals can defraud local authorities from outside the UK. Cybercriminals also seek to steal data from government networks that has a value on the black market, such as financial information or data that can be used for ID theft. Several types of malware have been specifically designed by cybercriminals to exploit e-banking details or log-in information. These include Shylock, Gameover Zeus and Citadel. Such malware is sometimes found on public sector networks, but financial and commercial organisations are more likely to be targeted.

Cybercriminals often want to control computer infrastructure and use it as a platform for carrying out other activity such as sending spam and phishing emails. Government networks are an attractive target. These groups also launch ransom attacks, locking victims out of their data and only providing the key once money is paid. Although the victims are usually members of the public and sometimes small organisations, the criminals often purport to come from a public agency leading to the potential for reputational damage.

A recent E-Government Bulletin survey highlighted the concerns amongst Councils of being exposed to risks of losing website traffic, and even blackmail, through 'cybersquatting' of internet domain names. Cyber squatters use these domains to draw traffic away from council sites to their own commercial information services, and perhaps to publish material attacking the council or to imply an endorsement which does not exist.

Despite the continued success of National Crime Agency (NCA) and FBI operations in the USA, cybercriminals adapt their methods and tools to counter law enforcement action. It therefore takes a sustained campaign to keep cyber-security standards up to date. Removing malware from a network is a complex and time-consuming task that would have a significant impact on the running of an organisation, especially if a network needs to be shut down – so prevention is better than cure. Public bodies that fail to secure personal data will be investigated by the Information Commissioner and can expect a fine if found negligent.

Hacktivism

Hacktivists crave publicity. For them, success is for example causing embarrassment or annoyance to the owners of high-profile websites and social media platforms that they deface or take offline. When targeted against local government websites and networks, these attacks can cause reputational damage locally and to the UK at home and abroad. Hacktivist groups have successfully used distributed denial of service (DDoS) attacks to disrupt the websites of UK local authorities. A DDoS is when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable. If targeted at online public services (such as UK visas, Universal Credit, Council Tax payments) this kind of attack would cause financial, as well as reputational harm.

> In July 2014 a Council member’s Twitter account was hacked. A hacktivist group claimed responsibility and posted political statements. The council involved shut down its entire email system while it investigated.

A May 2014 global survey commissioned by BT showed, on average, organisations take 12 hours to recover fully from an especially powerful DDoS attack. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Lone hacktivists can pursue their own personal agenda. They do not require detailed technical know-how to achieve their goal. There are many commercially available hacking tools which have easy, step-by-step guides providing motivated but low-skilled individuals with the opportunity to gain illegitimate access to networks. The social media accounts (Facebook, Twitter and LinkedIn) of local authorities and individuals can be hijacked and misleading information posted.

> The website of a major unitary authority in the Midlands was taken down by online attackers in 2012. As a result outside browsers wishing to check on services like council tax details, report service issues, pot holes or find out about library times or council committee meetings were unable to do so for up to 48 hours after the initial attack.

Insiders

An insider is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include:
Unauthorised disclosure of sensitive information
Facilitation of third party access to an organisation's assets
Physical sabotage
Electronic or IT sabotage

Not all insiders deliberately set out to betray their organisation. An unwitting insider may compromise their organisation through poor judgement or due to a lack of understanding of security procedures. The insider threat is not new, but the environment in which insiders operate has changed significantly. Technological advances have created broader opportunities for staff at all levels to access information. These advances have also made it easier for insiders to collate, remove and circulate vast volumes of sensitive data and local authorities are at risk. Although the number of potential insiders within an organisation is proportionately very small, the potential impact on government and wider public sector is significant.

A clerk at a Magistrates Court was jailed for seven years in 2011 after taking bribes for using privileged access to court systems to help offenders avoid prosecution.

A council worker based in a unitary authority in North East England had been working with information held on a USB stick while using a laptop that was connected to the council's networked computer system. When logging off the system and leaving the office for the day, the user forgot to remove the USB stick. When the employee realised the mistake and tried to retrieve the USB stick, it was gone. As a result the council was subject to a significant fine from the Information Commissioner for the data loss.

Physical threats

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that impact upon local government IT systems. Authorities take a range of approaches to mitigating threats in this area ranging from accepting the risk (for low impact services), to ensuring information is backed up off site (for medium impact services), having plans in place to recover services in an alternative location (for high impact services), to full resilience across more than one location (for very high impact services). Many local authorities are starting to share services and locations to provide resilience in a cost effective way.

In 2013 a council in the north of England suffered a second fire in a data centre in the space of 24 months so took the decision to invest in a fully resilient solution that now enables them to recover their services in a very short space of time and alternative location in the event of a fire, flood or terrorist event.

Terrorists

Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could acquire improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

Terrorist propaganda hacks occur across local public sector on an ad hoc basis such as the case of a town council in the south east that was hacked; viewers accessing the councils' web pages were confronted with the image of a hooded combat figure dressed in black.

So whilst many hacktivist groups do not pose a significant threat to the UK, they do possess skills and capabilities which are desired by some terrorist groups. Terrorists may learn from large-scale data deletion attacks – such as the attack against the Saudi Arabian national oil company, Saudi Aramco, in which data on 30,000 computers was lost – and aspire to have the same impact in the UK.

Espionage

Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily. In a recent case a hostile, state-sponsored group gained access to a system administrator account on the Government Secure Intranet. Fortunately this attack was discovered early and dealt with to mitigate any damage but it and the example below from Canada illustrates the potential threat from cyber-espionage in this way to both central and local government.

> Hackers, believed to be linked to a foreign state, gained control of a number of Canadian Government computers belonging to senior officials. The hackers, then posing as the officials, sent emails to administrators, conning them into providing key passwords that unlocked access to government networks. At the same time, the hackers sent other staff seemingly innocuous memos as attachments. The moment a recipient opened the attachment, malware infected the network. The malware looked for specific kinds of classified government information and sent it back to the hackers over the internet. Once the compromise was detected, access to the internet was shut down for thousands of public servants.

The internet's global nature enables hostile foreign intelligence agencies to conduct espionage on an ever-increasing scale with the added benefit of using deniable infrastructure to keep their activity hidden. This technical infrastructure allows sophisticated state actors to obfuscate their location, making Government networks an attractive target for state cyber programmes. Rmployees are also a target for hostile foreign intelligence agencies.

What you can do and who can help

As well as localised threats such as flood or fire the global nature of the internet and its potential for deniability makes it fertile ground for all kinds of cyber-attack. The UK, as one of the world's most internet-dependent nations, is particularly vulnerable. Attackers can use multiple methods to steal your organisation's information or disrupt its systems and it is not currently possible to keep out all the attacks, all the time. Inevitably disasters occur and some attackers will get through, which makes a robust cyber incident management plan essential for all public sector organisations. Advice on protective security is available on the websites of Centre for the Protection of the National Infrastructure (www.cpni.gov.uk) and Communications-Electronics Security Group (www.cesg.gov.uk).

Adopt the 10 Steps to Cyber Security approach

A good starting point is adopting the basic cyber-security measures, set out in CESG's the 10 Steps to Cyber-security, is highly effective at preventing most attacks. A more detailed guide around how to brief board-level corporate and business decision making can be found at
http://www.cpni.gov.uk/highlights/cyber-advice-businesses/

- **Information Risk Management Regime -** Assess the risks to your organisation's information assets with the same vigour as you would for legal, regulatory, financial or operational risk. To achieve this, embed an Information Risk Management Regime across your organisation, supported by the Board, senior managers and an empowered information assurance (IA) structure. Consider communicating your risk management policy across your organisation to ensure that employees, contractors and suppliers are aware of your organisation's risk management boundaries.

- **Secure configuration -** Introduce corporate policies and processes to develop secure baseline builds, and manage the configuration and use of your ICT systems. Remove or disable unnecessary functionality from ICT systems, and keep them patched against known vulnerabilities. Failing to do this will expose your business to threats and vulnerabilities, and increase risk to the confidentiality, integrity and availability of systems and information.

- **Network security -** Connecting to untrusted networks (such as the Internet) can expose your organisation to cyber-attacks. Follow recognised network design principles when configuring perimeter and internal network segments, and ensure all network devices are configured to the secure baseline build.

Filter all traffic at the network perimeter so that only traffic required to support your business is allowed, and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack (or attempted attack).

- **Managing user privileges -** All users of your ICT systems should only be provided with the user privileges that they need to do their job. Control the number of privileged accounts for roles such as system or database administrators, and ensure this type of account is not used for high risk or day-to-day user activities. Monitor user activity, particularly all access to sensitive information and privileged account actions (such as creating new user accounts, changes to user passwords and deletion of accounts and audit logs).

- **User education and awareness -** Produce user security policies that describe acceptable and secure use of your organisation's ICT systems. These should be formally acknowledged in employment terms and conditions. All users should receive regular training on the cyber risks they face as employees and individuals. Security related roles (such as system administrators, incident management team members and forensic investigators) will require specialist training.

- **Incident management -** Establish an incident response and disaster recovery capability that addresses the full range of incidents that can occur. All incident management plans (including disaster recovery and business continuity) should be regularly tested. Your incident response team may need specialist training across a range of technical and non-technical areas. Report online crimes to the relevant law enforcement agency to help the UK build a clear view of the national threat and deliver an appropriate response.

- **Malware prevention -** Produce policies that directly address the business processes (such as email, web browsing, removable media and personally owned devices) that are vulnerable to malware. Scan for malware across your organisation and protect all host and client machines with antivirus solutions that will actively scan for malware. All information supplied to or from your organisation should be scanned for malicious content.

- **Monitoring -** Establish a monitoring strategy and develop supporting policies, taking into account previous security incidents and attacks, and your organisation's incident management policies. Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate attacks and the compromise of data. Monitor all ICT systems using Network and Host Intrusion Detection Systems (NIDS/HIDS) and Prevention Systems (NIPS/HIDS).

- **Removable media controls -** Produce removable media policies that control the use of removable media for the import and export of information. Where the use of removable media is unavoidable, limit the types of media that can be used together with the users, systems, and types of information that can be transferred. Scan all media for malware using a standalone media scanner before any data is imported into your organisation's system.

- **Home and mobile working -** Assess the risks to all types of mobile working (including remote working where the device connects to the corporate network infrastructure) and develop appropriate security policies. Train mobile users on the secure use of their mobile devices for locations they will be working from. Apply the secure baseline build to all types of mobile device used. Protect data-at-rest using encryption (if the device supports it) and protect data-in-transit using an appropriately configured Virtual Private Network (VPN).

Join the Cyber-security Information Sharing Partnership (CiSP)

In addition to these resources, the Cyber-security Information Sharing Partnership (CiSP) **www.cert.gov.uk/cisp** (part of and Computer Emergency Response Team CERT-UK), allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information. It is a joint industry/government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on the UK. CiSP members benefit from:

Engagement with industry and government counterparts in a secure environment
Early warning of cyber threats
Ability to learn from experiences, mistakes, successes of other users and seek advice
An improved ability to protect their corporate business network

CiSP is free to join and a dedicated forum for local authorities exists on the CiSP platform, this is specifically to enhance the ability of organisations to share sensitive information in a safe and trusted environment. An increasing number of local authorities are joining CiSP to help become better equipped to deal with such new and emerging threats. Working with others in this way is enabling them to fully utilise the benefits of working at a network defending level - to secure local authorities against the online threats to both their operations and the data held in their care.

The ability of CISP members to deal with the recent Heartbleed vulnerability incident illustrated of the benefit of being a member; a dedicated group was established allowing members to easily access the latest information and mitigation advice, including privileged information that had a direct impact on members' ability to update their firewalls in a timely fashion.

It is important to remember however, that should a local authority fall victim to a cyber-attack it should report the incident to GovCertUK in the first instance.

To find out more

The application process to join CiSP is straightforward with details available **at** www.cert.gov.uk/cisp In addition for further details about the CiSP please contact CERT-UK at **https://www.cert.gov.uk/contact-us/contact-form/**

Conclusion

This guide is intended to provide the basis for non-technical senior managers and leaders to gain a better understanding of the potential threats from cyber-attack and how local authorities can reduce their vulnerability to threats. Getting cyber resilience right has never been more important as public services continue to modernise and improve our ways of working and as we deliver more and more services online.

Ultimately being cyber resilient is about having the right resilience, appropriately tailored to take proper account of the very wide range of different activities councils undertake, the assets they handle and environments they work in. Focus in this area will help ensure that local authorities can gain and develop the public's trust that they will handle their information properly and protect the public, commercial and financial interests they are responsible for on behalf of their local communities.