Colne Parish Council

Cyber Security

Adopted by the Council on the 26th June 2018, reviewed annually in June

Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the council, the delivery of local public services and ultimately have the potential to compromise national security. Additional costs will be incurred by the council to rectify any cyber security or cybercrime event.

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.

The scale of targeted attacks, coupled with the difficulty of monitoring all possible attack methods requires the public sector to work together to both reduce the likelihood and the impact of such a threat succeeding.

Criminals may try to compromise public sector networks to meet various objectives that include:

- 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

Council employees can also be targets for criminal activity.

Cyber Security Risks

The following types of cyber security all pose risks to the council:

- Cybercrime:

The most common form of cyber-attack against public bodies is the use of stolen or false customer credentials to commit fraud.

The uptake in online services means this form of crime can now be undertaken on a much larger scale and can be international.

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.

There are several types of malware (malicious software) that have been written to specifically steal banking and log in information.

The council secures its network with up to date antivirus and malware protection and manages the use of personal USB devices on council computers.

- Hacktivism:

Hacktivists seek to cause embarrassment or annoyance to the owners of high-profile websites and social media platforms that they may deface or take off line.

When targeted against local government websites and networks, these attacks can cause reputational harm both locally and nationally.

The council has third party availability monitoring tools in place to alert key team members of the websites status.

The council's web site's content management system conforms to the councils ICT Policy with regards to password enforcement.

- Insider threats:

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 judgment 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. Technology advances have created opportunities for staff at all levels to access information.

The council enforces the use of strong passwords for access to systems.

The council only allows corporate USB devices to be written to. All personal USB devices are read only.

The council uses mobile device management tools to secure corporate information on personal devices (smart phones and tablets).

The council periodically reviews access to key IT systems.

- 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 could impact upon local government IT systems.

- Terrorists:

Some terrorist groups demonstrate intent to conduct cyber-attacks but 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 an opportunity for escalations and the hiring of Hacktivists.

The council's approach to Cyber Security:

As with most local authorities, the council relies heavily on access to the internet and to information held in its systems. There are several IT systems that have an internet presence (website, webmail homeworking), and there are several different access mechanisms to information (Wi-Fi, physical networking, smartphones, tablets). All present threats to cyber security. It is widely acknowledged that it is not currently possible to keep out all attacks all of the time, but the council employs a range of tools and good practice to minimise the risk to its information and systems.

The council employs a range of technology and processes to help it achieve a good security platform. These range from up to date firewalls and core networking equipment, through antivirus controls and a secure wireless configuration, to encrypted devices.

Reporting Data Breaches and Security Incidents – See councils Breach of Security Policy

This policy will be reviewed annually.