

Cyber Crime



Introduction

The integration of the internet into our daily lives has been a continuous trend in the 21st century. Individuals, businesses, charities, and government all rely on digital technology and online capability, including in the delivery of essential and public-facing services.

The COVID-19 pandemic has emphasised our reliance on digital technologies, both through personal communication and through business and government's ability to work remotely in support of the national response.

While there are huge opportunities and benefits for individuals and businesses, our vulnerabilities become greater as we increasingly rely on cyberspace.

Cyber criminals engage in criminal activity, from the sending of malicious emails to hacking to steal data, by exploiting weaknesses in online systems, and a lack of personal security, usually for financial gain.

Interesting Facts

According to the *Cyber Security Breaches Survey*, almost half of businesses (46%) and one-quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses (68%), large businesses (75%) and high-income charities (57%). Among the 46% of businesses that identify breaches or attacks, more are experiencing these issues at least once a week in 2020 (32% vs. 22% in 2017).

Local Risk Rating

Cyber Crimes are assessed as 'Very High' on our Community Risk Register

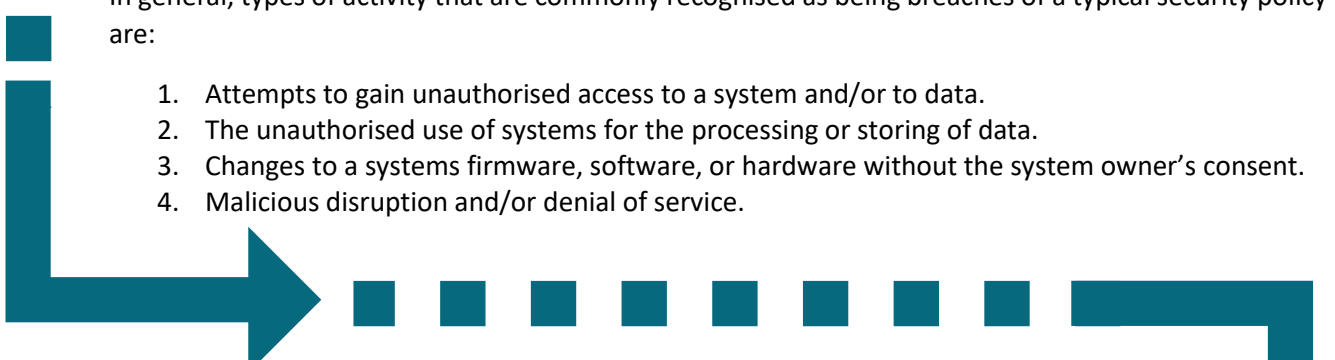
Impact	Significant (4)	Likelihood	Medium/High (4)	Rating	Very High
---------------	-----------------	-------------------	-----------------	---------------	-----------



What is it?

The National Cyber Security Centre (NCSC) defines a cyber incident as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).

In general, types of activity that are commonly recognised as being breaches of a typical security policy are:

1. Attempts to gain unauthorised access to a system and/or to data.
 2. The unauthorised use of systems for the processing or storing of data.
 3. Changes to a systems firmware, software, or hardware without the system owner's consent.
 4. Malicious disruption and/or denial of service.
- 

History


The internet as we know it came into being following Research at CERN in Switzerland by the British computer scientist Tim Berners-Lee in 1989–90 which resulted in the World Wide Web.

We now use the 'web' in every aspect of our lives from personal banking, shopping online, communicating via email or instant messaging or running our businesses, both big and small.

Criminal activity has similarly kept pace and operates in the cyber space alongside more traditional crimes such as theft.

Cyber activity varies from crude 'phishing' emails that encourage you to 'click' on a 'link' that will release malware onto your computer, social media accounts being hacked or cloned, through to state actors that seek to influence the outcome of national elections.

Governments have responded to these threats by establishing, in the case of the UK, the National Cyber Security Centre, that monitors and counters threats and provides advice and support to individuals and businesses to make the UK the safest place to live and work online.





What are we doing about it in the LRF?

The LRF has assessed the risk of a cyber attack as very high. It has created a cyber guide for partner organisations to use in response to a cyber-attack, which includes arrangements to secure partner and wider support to mitigate the effects of the attack.

Consideration of cyber activity is built into our major incident guide and is the subject of monitoring across all partner agencies.

We promote cyber security across and within our partner agencies and provide opportunities to test our preparedness through training and exercising.

What can you do?

The National Cyber Security Centre (NCSC) provides a range of resources to help protect you from cyber attack and this is tailored to individuals and families, through to corporations and government.

Basic and obvious steps everyone can take include:

- Use a strong and separate password for your email.
- Install the latest software and app updates.
- Turn on 2-Step Verification (2SV).
- Password managers: using browsers and apps to safely store your passwords.
- Backing up your data.
- Three random words: Combine three random words to create a password that's 'long enough and strong enough'.

Further support, guidance and advice can be found at: [National Cyber Security Centre - NCSC.GOV.UK](https://www.ncsc.gov.uk)