HENDERSON CHAMBERS

Alerter
Technology and Data

31 March 2020

COVID-19 is not the only virus business needs to worry about.

Matthew Richardson

As is always the case in times of difficulty and distress there will be those malicious actors who seek to take advantage of the situation by preying on the most vulnerable. The COVID-19 crisis is no different. There has been a noticeable increase in computer misuse and attempted data breaches since the start of the crisis.

Every Crisis is an Opportunity for Malicious Actors

1. COVID-19 presents a number of challenges for companies including maintaining data security and network integrity while workers are remotely accessing their systems. This is weakness is currently being exploited by hackers in a number of sophisticated ways.

2. Companies should be aware they are still obliged, even under these difficult circumstances to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" under article 32 of the General Data Protection Regulation (GDPR).

3. Although the Information Commissioner is likely to give some leeway if a breach occurs, especially given the current circumstances, but she will not give companies carte blanche to ignore security altogether.

4. Many companies and even governments, small and large, have been caught by surprise by COVID-19 and have hastily cobbled together a remote

working strategy that may have ignored basic security in favour of business continuity.

5. Cyber criminals and other malicious actors have begun to exploit this uncertainty. For example, the teleconferencing software Zoom has become very popular very quickly; so too have the scams involving Zoom. In the past three weeks, 170 domains that look a lot like Zoom's domain have been registered, and many of these domains been seen in fake Zoom conference invites. Likewise, fake emails have been reported from HMRC offering relief from tax burden, Microsoft offering free upgrades, and even British Airways offering free flights.

6. These links are used to deploy viruses and malware on to corporate and remote computers that have many and varied purposes none of them good.

How to Avoid Trouble.

7. **Ensure data handling processes are in place.** Having a robust data handling process in place is vitally important and it will be the first document that the Information Commissioner asks to see ensure that you have one. Secondarily, it is worth having such a document to rely on in the event of a breach.

8. **Keep up to date**. This is the refrain of all IT departments, but it is doubly true now. Ensure that all corporate and remote machines accessing the corporate system are up to date with anti-virus and software patches. In most cases these updates are delivered automatically; ensure that this feature is activated. This is only half of the picture, because as fast as updates can be pushed out, cyber criminals can find ways around them and develop new ways of attack that cannot be detected. It is a constant game of "cat and mouse."

9. **Use regularly changing complicated passwords and dual factor authentication.** No remote system should be allowed to access to a corporate system without Virtual Private Network (VPN). This is the most onerous security recommendation; it will slow down access and increase user friction, but it is the most certain to save companies from hacking. Dual factor authentication is incredibly difficult to spoof and will certainly slow down any malicious actor attempted to gain access to systems.

10. **Secure and encrypt all data and restrict access.** Personal Data are the only data with which the Information Commissioner is concerned. However, most companies have valuable non-personal data, too. The loss of this data can be worse, financially, than any other type of breach. Restricting access to all data to only those who absolutely require it removes opportunities for malicious actors to steal data. Keeping logs to track and audit data provides peace of mind if needed.

11. **Conference calls should be treated as non-secure.** It is surprising how many people treat conference calls as secure. They can easily be eavesdropped upon and the contents can be recorded and shared. Although such recordings or covert monitoring would be a criminal offence if the monitoring party was not an intended participant, that doesn't stop valuable business critical information being stolen and used.

12. **Remember there should always be a real person at the end of an email.** It seems strange to say in 2020 but there's usually a real person at the end of an email. If you're suspicious, pick up the phone and call the originator of the email. If nothing else, it will give you chance to speak to a colleague.

What to do if it goes wrong?

13. Despite taking all necessary and prudent steps to prevent breaches they will still happen. Make sure that:

- You have a full log of all breached systems.
- Your Data Processing Procedures are available and accessible.
- Assess the cause of the breach.
- Assess what data was taken.
- Call a lawyer.
- Assess if a report to the ICO or the Police is necessary.
- Determine if a Public Statement or Public Relations Strategy is necessary.

Matthew Richardson
31 March 2020