CGI

Experience the commitment®

COVID-19 and Cyber Security

A quick reference guide for business and security leaders

COVID-19

The Coronavirus (COVID-19) pandemic is having a significant impact on businesses around the world and their employees. Threat actors are using this against us and actively exploiting these uncertain and confusing conditions through a variety of means.

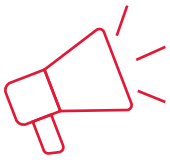
IDEAL CLIMATE FOR THREAT ACTORS

The COVID-19 pandemic has forced organisations to react rapidly, often asking their employees to work remotely in order to safeguard their health and safety. This all done while ensuring the continuity of day-to-day operations. In order to cope, employees are using a variety of collaboration methods, many of which may not have had a thorough security assessment ranging from text messaging, video conferencing or cloud based tools in order to "get the job done". Meanwhile, their organisation is dealing with Virtual Private Network (VPN) licensing shortage or bandwidth issues. This unprecedented situation forces everyone “outside the firewall”, creating new complexity and hidden dangers which existing cyber security operations are struggling to handle.

We have seen a sharp increase in exploitation such as phishing scams, malware hidden in COVID-19 tracking maps, and increased ransomware attacks. Overleaf, we take a quick look at the things you should be doing to take control of the situation from a cyber security standpoint to defend against threat actors.

WHAT SHOULD YOU DO

When your employees are “outside the firewall”, there are certain security measures you should factor in, such as:



Increased awareness so people do not fall for clicking on malware infected maps or phishing scams. Read “Cyber security hygiene during COVID-19 – A dos and don’ts guide to share with your employees”

Data leakage prevention (establishing or reinforcing rules of conduct while communicating via unlicensed versions of chat and collaboration platforms)

Diligent monitoring so that you can identify the indicators of attack as quickly as possible, particularly these new collaboration services

Where possible only use devices authorised by your organisation and ensure they are all patched and are up to date on antimalware and antivirus

Ensuring all internet-facing endpoints are patched and undergo vulnerability scanning

Ensure your backups are Working and include and necessary data being processed locally while people are working from home

Verify that Network defence and DDoS protection is working as intended (certain organisations are creating their own DDoS because they can’t sustain the increase In traffic)

If you don’t have 24/7 incident response, you should consider it now – at least for the coming weeks

Extending traditional controls such as Endpoint Detection & Response (EDR) and log collection to newly leveraged services in order to gain visibility Virtual Desktop Infrastructure (VDIs) could be of benefit here in order to better control the risk of inadvertent data leak disclosure

For any questions around cyber security reach out to **enquiry.uk@cgi.com**.