CGI

Experience the commitment®

COVID-19 and Cybersecurity

A quick reference guide for business and security leaders

COVID-19

Coronavirus (COVID-19) pandemic is having a significant impact on businesses and their employees working remotely. Threat actors are actively exploiting these uncertain and confusing conditions through a variety of means.

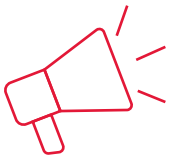
IDEAL CLIMATE FOR THREAT ACTORS

The COVID-19 pandemic has forced organizations to ask their employees to work remotely to safeguard their health and safety while ensuring continuity of day-to-day operations. Employees are using text messaging and collaboration platforms to be able to communicate while their organization is dealing with Virtual Private Network (VPN) licensing shortage or bandwidth issues. This unprecedented measure forces everyone “outside the firewall” creating an added burden to reliable cybersecurity measures such as preventing Distributed Denial of Service (DDoS) attacks, security awareness, data leakage, network availability and monitoring.

We have seen a sharp increase in exploitation such as phishing scams, malware hidden in COVID-19 tracking maps, and increased ransomware attacks. We will take a quick look at the things you should be doing to take control of the situation from a cybersecurity 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 files or phishing scams. Read “Cybersecurity 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)

Implementing diligent monitoring so that you can identify the indicators of attack as quickly as possible

Ensuring all endpoints are up to date on antimalware and antivirus

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

Any endpoints that can’t be patched or secured should have its own endpoint protection to mitigate the risk

Verify that DDoS protection is working as intended (certain organizations are DDoS’ing themselves with legitimate traffic because their systems cannot handle the increased demands)

If your organization does not already have 24/7 incident response, you should consider it now – at least for the coming weeks

Extending traditional controls such as Endpoint Detection and Response (EDR) and Windows log collection to employee home computers to offset the risks. Alternatively, Virtual Desktop Infrastructure (VDIs) could be of benefit here too, to better control the risk of inadvertent disclosure of sensitive data

For any questions around cybersecurity reach out to **globalcybersecurity@cgi.com.**