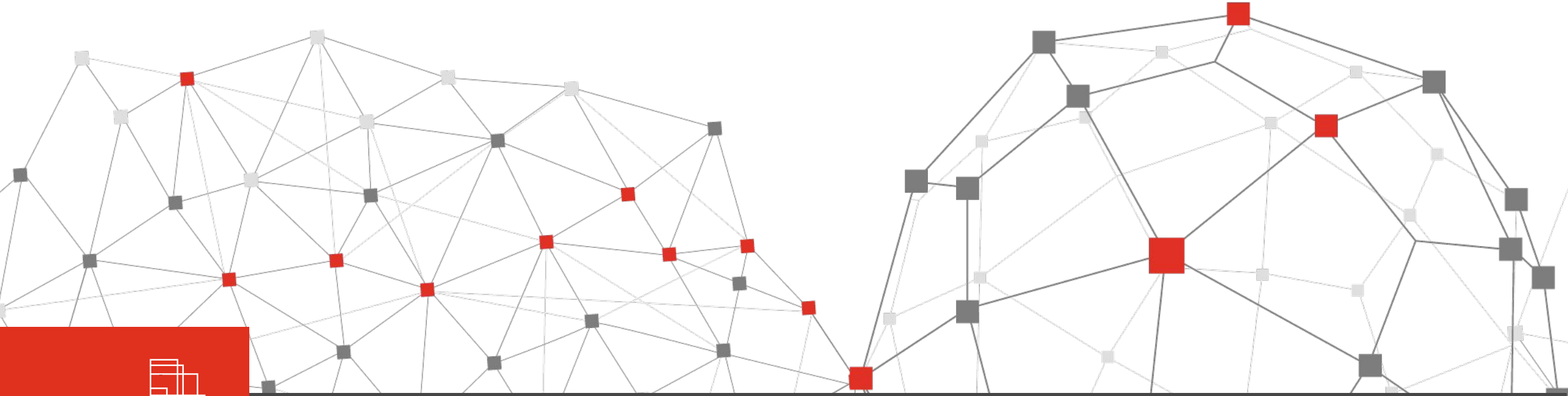
COVID-19

Impact on cyber security



pwc

30 March 2020

The emerging cyber security risks as a result of COVID-19

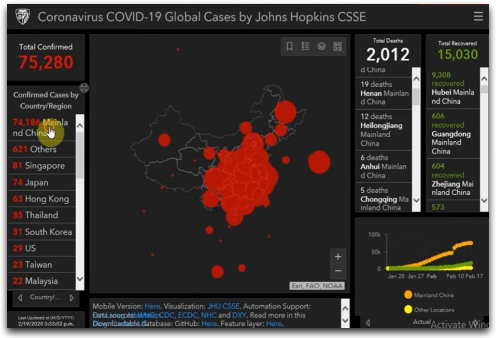
The COVID-19 outbreak has been declared a pandemic by the World Health Organization, causing huge impact on people's lives, families and communities.

As a result we are seeing both the likelihood and impact of cyber attacks increasing.We are also beginning to see the nature of the threat changing, as attackers exploit uncertainty, unprecedented situations, and rapid IT and organisational change.

Threat actors are always quick to identify new ways to exploit vulnerabilities, whether these are technical or psychological. PwC's Threat Intelligence research has uncovered a mixture of espionage and cyber crime activity from a variety of threat actors capitalising on the COVID-19 situation.

Cyber criminals and espionage threat actors have begun using COVID-19 based phishing lures as part of their efforts to infect victims with malware and gain access to their infrastructure.

At a time when people are more likely to be susceptible to social engineering techniques, most lures and malicious apps are copying legitimate content to enhance their authenticity. We've also seen hundreds of COVID-related domains being created everyday, some of which may be malicious infrastructure for use in future campaigns.



Map from John Hopkins is being used to market a phishing kit and downloader

Mobile malware variants are appearing on download sites

Some phishing campaigns are using legitimate documents to cover malware downloads

We see three key emerging cyber security risks as a result of COVID-19

As the international response continues to develop, we know that organisations are facing potentially significant challenges to which they need to respond rapidly.

Many organisations and employees are needing to rethink ways of working in light of considerable operational and financial challenges. Without appropriate considerations, this could fundamentally increase the risk of cyber security attacks.

With organisations going through a period of rapid unplanned change, we expect that many initial responses to COVID-19 will have a net-negative impact on the cyber security position of the business.

We see three key emerging cyber security risks as a result of COVID-19:

A shift to remote working and prioritising business operations will bring immediate risks

Disruption to the workforce and suppliers will increase vulnerability to old risks

Going forward this will change organisations' cyber security risk landscape

Organisations should focus on mitigating these three cyber security risks in the short term

Secure their newly implemented remote working practices

- ✓ Monitor for shadow IT and move users towards approved solutions.
- ✓ Ensure remote access systems are fully patched and securely configured.
- ✓ Ensure on-premise security controls still apply to systems when they are not on the internal network.
- ✓ Monitor remote access systems, email and Active Directory for anomalous logins.
- ✓ Monitor and react to issues encountered by employees with remote working.
- ✓ Support your people to work safely and securely from home.
- ✓ Review tactical actions and retrospectively implement key security controls which may have been overlooked.
- ✓ Ensure remote access systems are sufficiently resilient to withstand DDOS attacks

Ensure the continuity of critical security functions

- ✓ Identify and monitor critical security activities to ensure continuity.
- ✓ Confirm patching processes are functioning, including for laptops connected remotely.
- ✓ Secure Internet-facing applications and services.
- ✓ Implement IT change freezes on high-risk systems if normal processes cannot be followed due to workforce shortages.
- ✓ Review how privileged users perform administration and ensure that alerting is in place for any high risk activities.
- ✓ Ensure you have the people, process and technology capability to detect and respond to cyber attacks.
- ✓ Update incident response plans and playbooks to ensure they function with a workforce primarily working remotely.
- ✓ Deploy asset management tooling to ensure continued visibility as systems are moved away from the internal network.

Counter opportunistic threats looking to take advantage of the situation

- ✓ Target additional awareness and communications where emerging threats arise.
- ✓ Provide specific guidance to employees to be extra vigilant when it comes to requests for personal or financial information, or requests to transfer money.
- ✓ Mitigate the increased risk of insider threats in the event of redundancy or termination.
- ✓ Mitigate the increased risk of phishing with technical controls.
- ✓ Apply quick-win technical controls across the IT estate where possible.

How might business change as a result of COVID-19

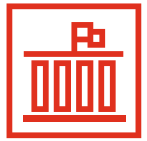
Expansion of ecosystem business models

Ecosystem business models that encompass a network of third parties are able to adapt and change to rapidly evolving risks more effectively than traditional supplier-customer models. Digital transformation has predominantly focused on business to consumer change, but greater benefits could be realised by extending the definition of digital transformation.

Accelerated adoption of Cloud

Whilst most organisations have adopted Cloud for a variety functions, applications and services, there is likely to be a broader reassessment of how Cloud can help to alleviate some of the recent challenges related to remote working, running business critical operations and enabling access to key business systems.

Redefined meaning of a resilient business

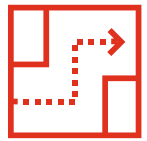


Disaster recovery and business continuity planning have for many years had some degree of focus on pandemic scenario planning. However, as this is the first time that we have lived through such a widespread event there will doubtless be a need to revisit plans, apply lessons learnt and consider what makes a business resilient.

Augmented reality / virtual operations functions

The use of new technology could change the way businesses and users interact with each other by extending location agnostic services and capabilities and by maximising virtual experiences. Such technology is already being adopted to address health and safety challenges in dangerous environments, but with the roll out of 5G there will be potential for much wider adoption and application.

Cross business industry resilience



The definition of business and industry boundaries seems less applicable during periods of large scale crisis. Assessing how businesses work together during these periods could influence the way in which cross business and industry resilience is addressed in the future.

To find out how PwC UK is responding to COVID-19, please visit:
www.pwc.co.uk/COVID19businesscontinuity

For our latest insights, please visit:
www.pwc.co.uk/COVID-19

pwc.com