June 2020

Embracing the new normal

Responding to cyber security challenges during the COVID-19 crisis

pwc

Content

COVID-19 outbreak – a zero-day in reality

The COVID-19 outbreak has resulted in widespread concerns for businesses, clients, consumers and communities worldwide. The COVID-19 pandemic (as declared by the World Health Organization) has mushroomed over an expanding geographic area with a significant impact on the global economy.

In many ways, the outbreak can be compared to a zero-day vulnerability in the cyber world, which is akin to an exploit that software manufacturers have not had a chance to fix yet. Such vulnerabilities are dangerous as threat actors can exploit them and wreak havoc while a patch is being developed.

In times like these, with significant shifts to work from home or off-location operations, businesses worldwide face challenges on continuity with day-to-day operations and need to set up a secure remote working environment within a short duration.

While most organisations have pre-established business continuity and contingency plans to ensure operational effectiveness, such plans may not be enough or effective to deal with the current pandemic that involves many uncontrolled and evolving variables. For example, as already witnessed, many contingency plans had not considered widespread lockdowns or travel restrictions.

Emerging stronger is an important aspect of an effective crisis response strategy. This assumes even more significance when organisations think about life in the new normal, especially around information technology (IT) and cyber security situations.

Organisations have become more vulnerable

Business priorities overtaking cyber security

The COVID-19 outbreak has made it difficult to predict the direction of current and future business disruptions. **It is unclear how this will impact organisations and their ability to operate smoothly.** Organisations would look to balance **business operations and the well-being of their employees** during such a crisis and that may lead to situations where **IT and cyber security functions are temporarily overruled, thus exposing them to exacerbated cyber threats.**

Reduced IT and security support staff

In events during which the **availability of support staff** within an organisation is limited, the **provisioning of critical IT and security infrastructure** to enable smooth remote working **becomes a daunting task and is accentuated by the lack of IT hardware and software resources.**

Technology capacity limitations

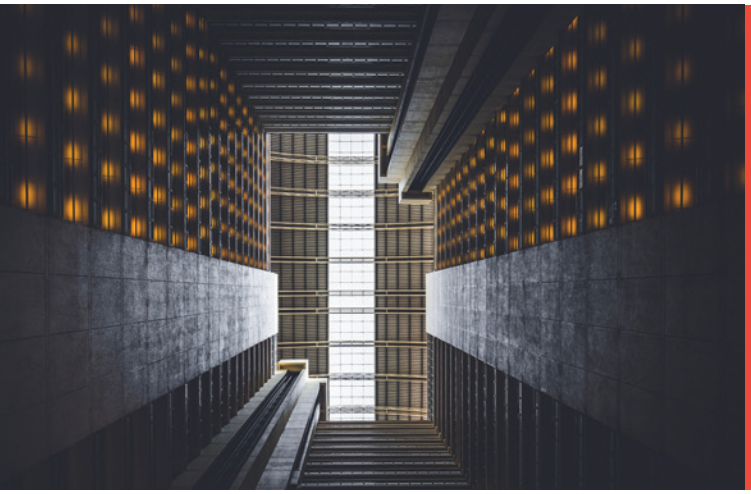
A direct impact of the COVID-19 outbreak has been on the work from home (WFH) model of working. This has triggered an increase in the number of virtual private network (VPN) users. **Small- and medium-sized organisations may currently be facing issues with the availability of VPN licences, thereby restricting parts of their workforce to effectively WFH.**

Further, many organisations may not have adequate devices to support remote working for their entire workforce. Procuring new sets of equipment during such a crisis due to lockdowns and disrupted supply chains is indeed challenging.

Psychological stress and panic

Employees may be under psychological stress due to lesser engagement at work, resulting in issues with their morale. With distractions and potentially impacted concentration, susceptibility of employees to phishing attacks, coupled with advanced threat vectors, may impact business operations.

Rising cyber security challenges amidst the COVID-19 crisis



Hackers are now leveraging a wide spectrum of attack vectors to target end users working remotely. Most common perpetrations include phishing emails offering fake medical advice and counterfeit COVID-19 tracker applications that deploy ransomware on handheld devices.

Sudden spike in hacking attempts

As dependency on digital platforms increases amidst the COVID-19 crisis, and since **majority of the workforce in many organisations is working remotely, hackers have resorted to the following types of cyberattacks:**

- They have launched cyberattacks on staff using **emails containing infected documents with macros that exploit vulnerabilities and are infected with ransomware.**
- Hackers have recently targeted COVID-19 **vaccine test centres and medical centres through a ransomware** and are publishing the data online for ransom.
- Hackers are also **calling gullible users by impersonating law enforcement or medical authority officials** to infiltrate their systems or endpoints for financial gain. They are also posing **as users or employees to trick IT staff to gain network access to** organisations.
- COVID-19 **discount codes** are being shared amongst hackers to **proliferate the spread of malware and exploit security tools.**

Increase in the number of COVID-19 themed phishing attacks

Hackers have gone a step further and are taking advantage of the current crisis situation by targeting employees with **COVID-19 themed phishing attacks to exfiltrate key information and obtain credentials, business data and personal information.**

A three-tiered approach to manage the crisis

Short term

- Secure VPN
- Identity management
- Endpoint security
- Employee awareness
- Frequent patching

Medium term

- WFH guidelines
- Institutionalise insider threat analytics
- Strengthen security operations centre (SOC)
- Privilege user access management

Long term

- Effective crisis response and management

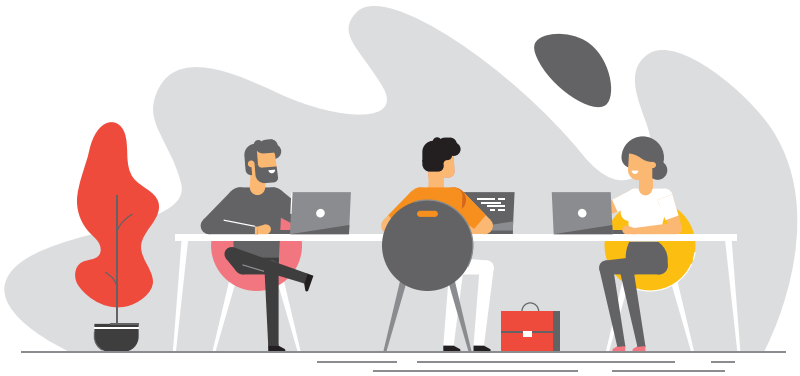
A - Short-term actions on crisis response

As organisations adopt remote working models, there are some short-term actions they can take to secure the information exchange and the critical infrastructure supporting them in crisis.

Establish secure VPN tunnels

Secure VPN tunnels should be established to ensure that employees can access the **organisation's network, applications and utilities from their home network.**

Organisations should have the **adequate bandwidth to support the increase in network traffic** from VPN users to **prevent inadvertent denial-of-services (DoS) attacks.**



Fortify endpoint devices

Since organisations have l**imited control over the remote environment**, it becomes imperative to implement **security controls** on employee and third-party **endpoints**. They should consider implementing **full disk encryption along with an endpoint detection and response (EDR) tool,** that will provide a mechanism to investigate and contain attacks.

There is an **increased emphasis on the use of mobile devices in times like these.** Organisations should evaluate **mobile device management (MDM)** solutions and expand the functionality **to personal devices t**o ensure enterprise data security on personal devices.

Only **approved devices** should be allowed to **connect to the organisation's network** remotely, as the level of security controls and policies on the **personal devices of employees is an unknown variable.**

Improve identity and access management services

Organisations should ensure that only **authorised users** are able to access their services, be it **cloud- or network-based**. Having **adaptive authentication or risk-based authentication mechanisms in place can further help to prevent threat actors** from obtaining access to critical organisational information. Enabling technology that manages identities and access should be aligned with remote working models.

Increase patching frequency of critical infrastructure systems

All **internet-facing and remote access systems of an organisation** should have the **latest critical patches applied and the configurations secured.**

They should **constantly assess and monitor** the **critical systems landscapes** for a**ny vulnerabilities or misconfigurations** by frequently conducting **vulnerability scans and penetration testing.**

Enrich employee awareness campaign

As users spend more time online, they may fall prey to COVID-19 themed phishing emails/scams.

Organisations should improvise the employee awareness campaign aimed at deterring the updated modus operandi of hackers. Key information on **phishing-based cyberattacks, impersonation call attempts and secure practices for remote working** should be conveyed to staff. The users should be made aware of the available authorised technological solutions and tools for remote working. **Organisations should also publish the coordinates of the security desk from where users can seek advice on suspicious activities.**

B - Medium-term actions on crisis response

After tackling the immediate challenges, the focus should be on improving the cyber security posture of organisations to tackle the advancing threat landscape in the medium term.

Enhance remote working guidelines and make them available

Organisations usually have adequate security guidelines. However, it is of utmost importance to ensure that the security guidelines are transformed and available as organisations undergo transition. **They should reiterate to users the security guidelines of remote working.** Policy and procedures should be exercised and updated (if required) to include remote access, layered authentication, remote connection, personal device usage and security of an organisation's crown jewels.

Institutionalise insider threat analytics

The existing cyber security tools lack context of user activity. Organisations should analyse certain user metrics such as system log-on/log-off information, number of emails sent/received, internet/VPN usage and data transfers to profile an insider (employee) for establishing a behavioural pattern. Any deviations to the behaviour should be assessed for suspicion and correlated back with the SOC engine to neutralise an insider threat.

Strengthen SOC capabilities as threat landscape widens

Organisations should implement advanced security operations centre (SOC) capabilities by fine-tuning and redesigning use cases aligned to the remote working model that **impacts access, identities, security, network, servers, information exchange, information storage and dissemination, etc.**

The **existing security solutions** should be reconfigured to **identify, defend, detect and prevent any potential cyberattacks** in times like these.

Effective privilege user access management

Organisations should consider **defining guidelines on how privilege** user access will be provisioned and **monitored, while operating remotely**. While **such privileged activities are performed, they should continuously monitor the actions of the employees to ensure that the activities are appropriate** and well accounted for.

C - Long-term action on crisis response

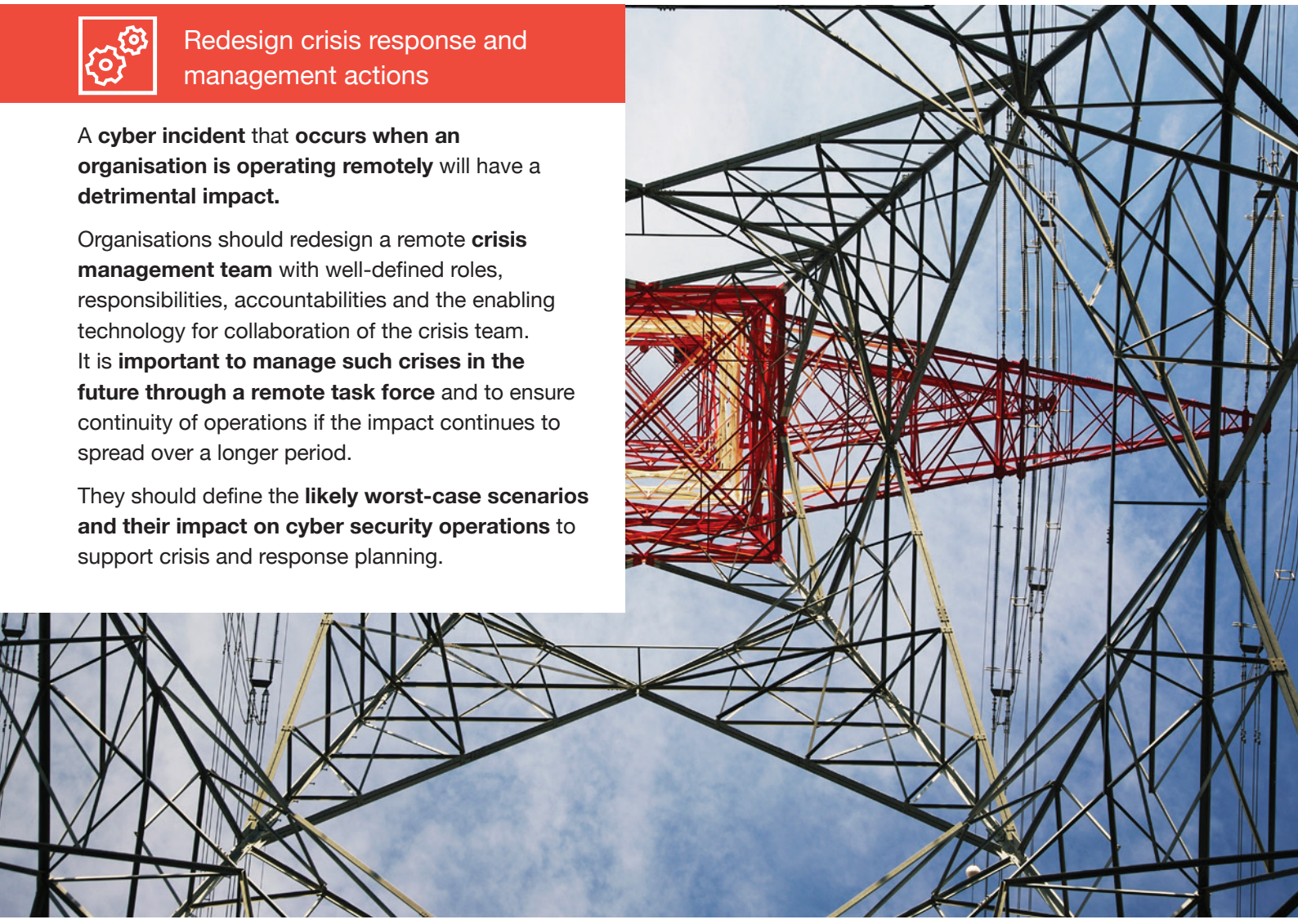
The lessons learnt from any crisis provides a path for improvement. Organisations should plan for long-term action that could hinge on redesigning the crisis response capabilities from the lessons learnt.

Redesign crisis response and management actions

A **cyber incident** that **occurs when an organisation is operating remotely** will have a **detrimental impact.**

Organisations should redesign a remote **crisis management team** with well-defined roles, responsibilities, accountabilities and the enabling technology for collaboration of the crisis team. It is **important to manage such crises in the future through a remote task force** and to ensure continuity of operations if the impact continues to spread over a longer period.

They should define the **likely worst-case scenarios and their impact on cyber security operations** to support crisis and response planning.



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC Channel Islands has offices in these locations: Jersey, Guernsey and Alderney. For more information about PwC Channel Islands service offerings, visit www.pwc.com/jg/en

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

About us

PwC CI's cyber security team has vast experience in working with organisations, law regulators, international bodies and governments worldwide to help them prepare for and respond to cyber security issues during crisis situations and further enhance their cyber security capabilities for secure management of their operations.

Please write to Christopher Eaton, our Cyber Security Director, at **chris.eaton@pwc.com** for further details.

Contacts

Christopher Eaton
Director Advisory, PwC Channel Islands
Mobile: +44 7700 838349
Email: chris.eaton@pwc.com

Volodymyr Kazanskyi
Advisory Senior Manager, PwC Channel Islands
Mobile: +44 7797 776404
Email: volodymyr.kazanskyi@pwc.com

pwc.com/jg/en

Data Classification: DC0

GM/June 2020/M&C-5399