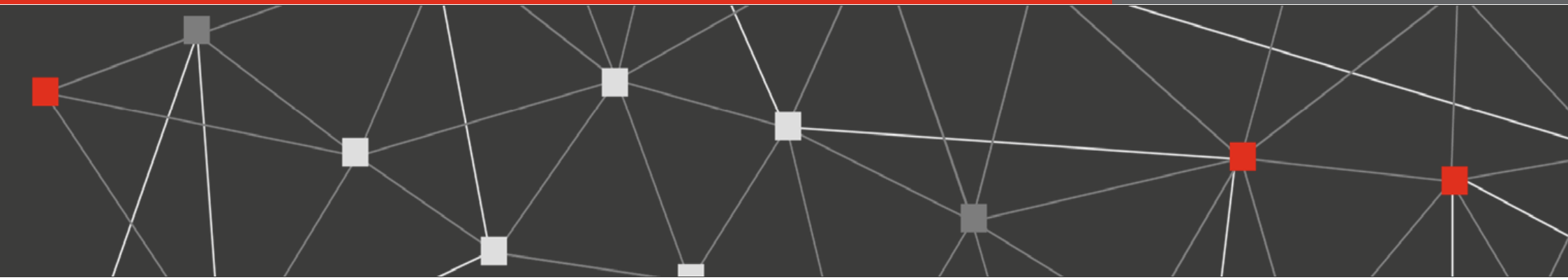
COVID-19 Outbreak

Impacts on Organisations – Cyber Security Considerations

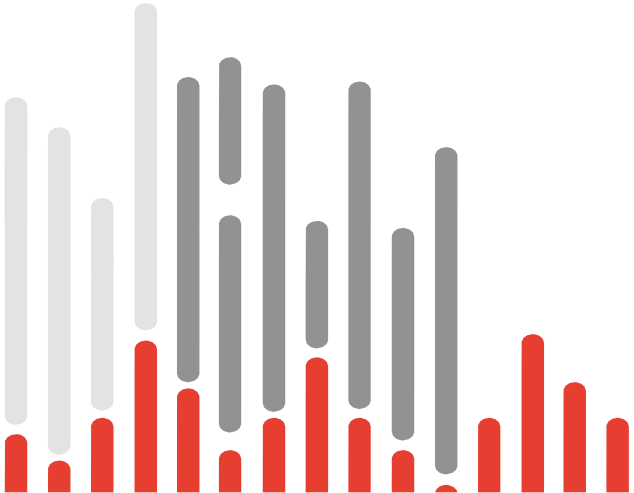
June 2020



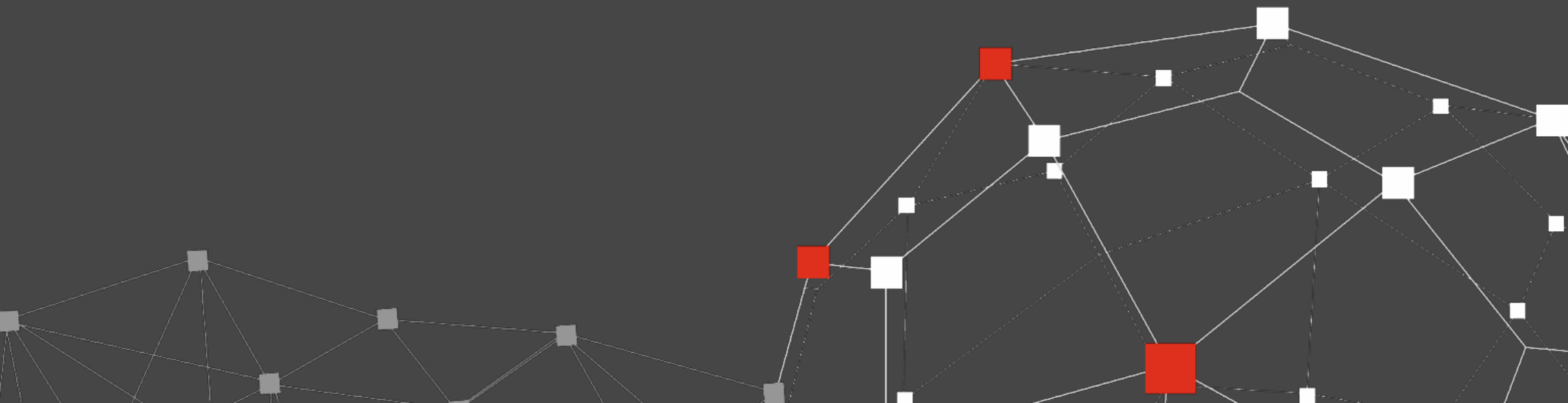
pwc

A·F·FERGUSON&Co.

Contents



1 Cyber Security Risk(s)



Cyber Security Risk(s)

Background

"We expect that many initial organisational responses to COVID-19 will have a net-negative impact on the cyber security posture of the business. This will be both as a result of existing risks being left unaddressed as security expenditure is cut and IT changes are frozen, and as we see new risks emerging. Going forward this will change Organisations' cyber security risk(s) landscape globally"

Business Challenges

A shift to remote working and prioritising business operations will bring immediate cyber security risks for organisations operating in Pakistan. Security controls may not be applied to new systems or tools hastily stood up to support employees with remote working that 'just works'. Security teams may not be consulted on systems before they are deployed, or exceptions will be put in place for assurance activities normally carried out (e.g. vulnerability assessment and penetration testing).

Existing processes and good practices may be sidestepped by, or not available to, employees when they encounter obstacles to normal ways of working. For example, workers finding their normal secure method of sharing files is unacceptably slow when working from home, may resort to using free and unsanctioned services as an alternative.

Reliance on remote access systems may make organisations more vulnerable to distributed denial of service (DDOS) attacks seeking to disrupt business operations or to extort money. Employees will be required to work with technologies (e.g. remote collaboration tools) they are not familiar with, potentially resulting in new security risks being introduced.

Vulnerabilities may be introduced as security basics such as patching are neglected, due to resources being refocused elsewhere.

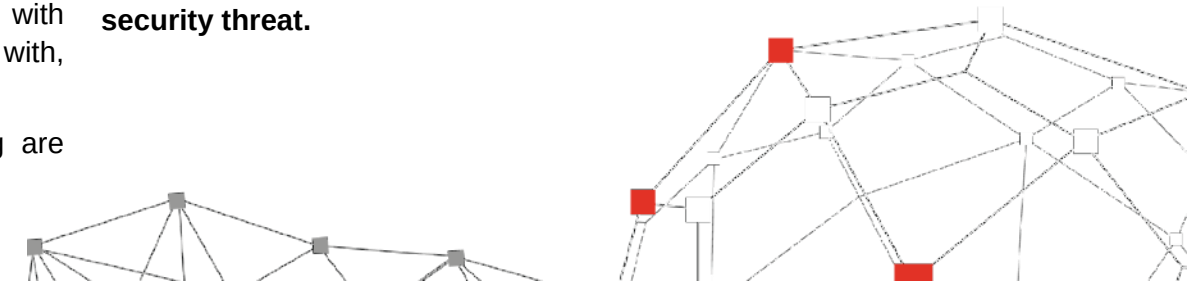
Employees may be more susceptible to social engineering attacks as attackers take advantage of employees' increased workloads, unfamiliar ways of working and heightened stress levels. Phishing attacks crafted to exploit potential alarm around COVID-19 have already been seen in action. For example, in the recent times Google reported millions of phishing and malware scams related to COVID-19 every single day.

Insider threats may increase as organisations face the prospect of having to make portions of their workforce redundant, or having to reduce working hours. Disgruntled employees facing redundancy may look to remove intellectual property, gain financially or otherwise cause reputational or financial damage to their employers.

Organisations may not effectively detect cyber attacks as security teams are short-staffed or repurposed to support other activities, leaving security alerts uninvestigated. Organisations are also likely to struggle with detection as their Managed Security Service Providers will be unavailable as they manage disruption to their own workforce.

Organisations may not be able to effectively respond to and recover from cyber security attacks as key employees from security, IT service providers, and the wider business may not be available immediately to support decision making and cyber incident response efforts. This is likely to be especially true for organisations with lower maturity who rely on key individuals, rather than having fully documented and widely rehearsed processes.

However, we also expect that some cyber security risks are likely to be decreased as a result of changes. For example, a workforce operating from primarily home and travelling less will have a decreased physical security threat.



Cyber Security Risks (contd.)

Top Management Priorities

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 corporate boards and CEO's fight the battle of their lives to keep their organisations alive amongst the COVID-19 crisis, they've also had to stiffen their lines of defense against cyber criminals who look to take advantage of the situation.

Businesses face significant challenges and disruption. The ability to navigate through crises and unforeseen events is an essential aspect of operational resilience; particularly through a public health crisis. Cybersecurity risk(s) is on the rise, defenses are being challenged, and weaknesses are being exposed through widespread work-from-home practices. As organisations become more technology dependent than ever, we are also beginning to see the nature of the threat changing, as attackers exploit uncertainty, unprecedented situations, and rapid IT and organisational change.

To ensure continuing business operations through uncertain times, top management need to ensure build and rehearse a holistic capability to respond to cyber attacks, increased demand for remote working, and increasingly complex governance. Make it easy for employees to comply with security requirements while investing in strong safeguards.

Management should ensure following key areas to mitigate these emerging risk(s)s:

Culture & awareness

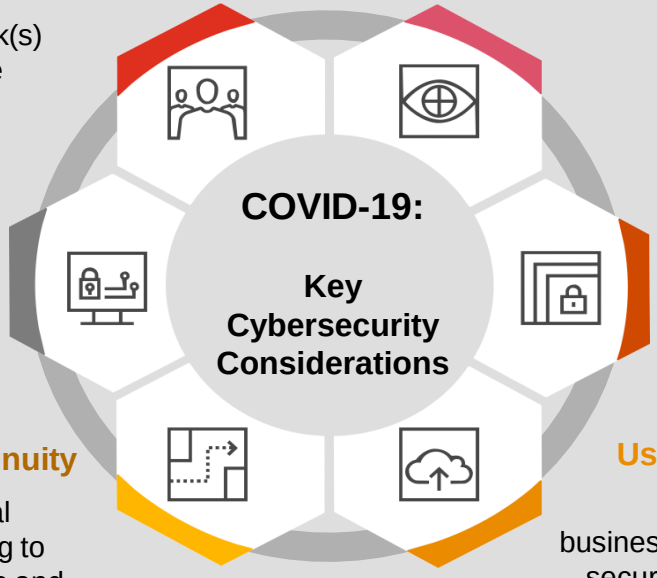
Instilling a cyber secure culture in end user behavior during a time of heightened cyber risk(s) supported through dedicated programs, online articles and training and awareness sessions.

Tools and Controls

Identify and record mission critical information assets (crown jewels), secure these assets by implementing rights tools and use efficiently by maintaining effective monitoring, detection and protection controls.

Incident management & business continuity

Develop contingency plans to address residual deficiencies in the operating model. Continuing to operate incident management, crisis response and business continuity capabilities during a period of increased organizational stress



Governance

Operating an effective level of governance structure in an uncertain environment to maintain an appropriate security posture

Data security

Protecting sensitive information whilst implementing and operating different working practices

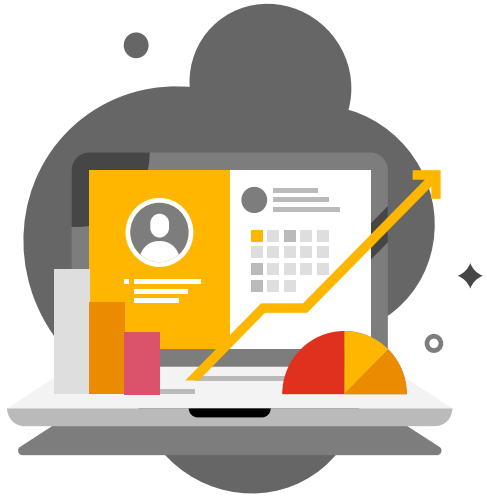
Use and Security of emerging technologies

Consider emerging technology to enhance the businesses ability to manage resilience and harden the security of actively deployed new technologies (cloud services, remote access, video conferencing etc.)

Cyber Security Risks (contd.)

How could organisations mitigate these risks?

Organisations should take three key actions to mitigate these emerging risk(s)s:



1

Secure their newly implemented remote working practices.

2

Ensure the continuity of critical security functions.

3

Counter opportunistic threats that may be looking to take advantage of the situation.

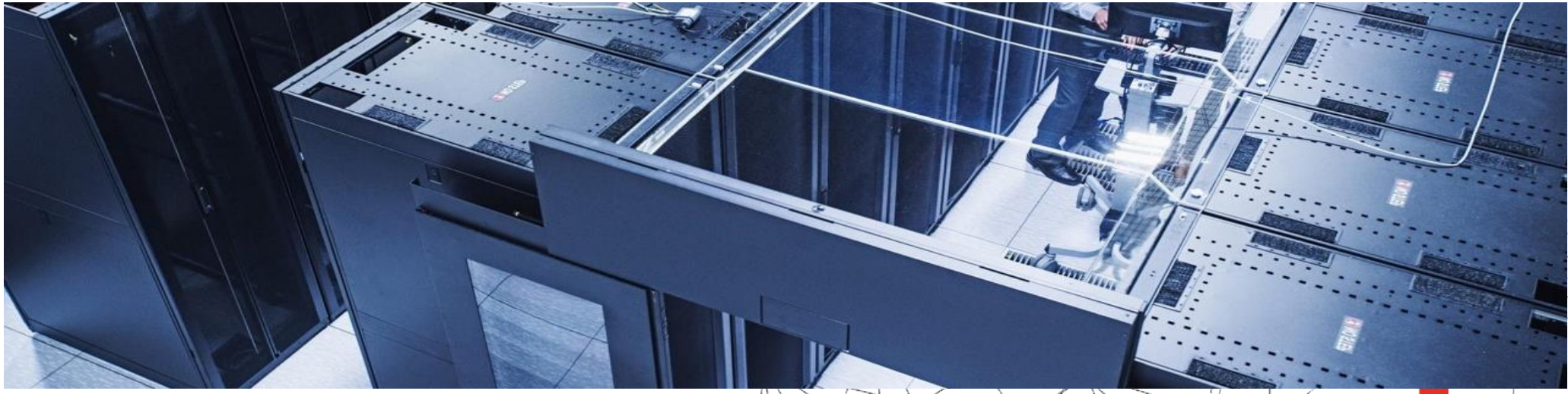
1 - Secure Organisation's newly implemented remote working practices

- Review web traffic logs to monitor for the use of shadow IT (e.g. file sharing, video conferencing, and collaboration tools), and work to implement and move users towards business-approved and secured solutions (e.g. using access security brokers and web proxy filtering).
- Review all remote access systems to ensure critical security patches have been applied and secure configurations have been used.
- Identify any vulnerabilities or mis-configurations using vulnerability assessment and penetration testing or red teaming.
- Secure configurations should also be applied to email, identity management (e.g. Active Directory) and conferencing systems used by remote workers, for example by disabling legacy authentication protocols.
- Organisations' employees working remotely should be required to use multifactor authentication (MFA) to access Organisation's internal networks and critical applications specially for users who have elevated privileges (administrators) and business users who work with critical financial applications.
- Organisation' should implement stringent controls for third-party service providers and connections. Should any third parties fail to demonstrate adequate security controls and procedures, consider limiting or even suspending their connectivity until they remediate their weaknesses.
- Map out the network-centric border security controls that apply to devices when they are on the internal network and evaluate whether a similar control set still applies to network traffic from systems not on the internal network.

Cyber Security Risks (contd.)

1 - Secure Organisation's newly implemented remote working practices (contd..)

- Confirm web browsing is secured by web filtering when working remotely and, if not, consider deploying a cloud-based web filtering solution to detect and prevent malicious web traffic. Configure this to restrict the types of websites that can be accessed, restrict file types users can download and block access to newly registered or untrusted domains.
- Configure remote access solutions, email systems and Active Directory to log all authentication events. Preserve logs and analyse these for anomalous activity, including brute force attempts, logins from unfamiliar locations, and logins that indicate impossible travel.
- Confirm tools related to Data Leakage and other security controls on laptops perform as expected when devices are removed from the internal network for extended period of time.
- Monitor the IT help desk to identify complaints from employees about processes, controls or technology limitations that are preventing them from working remotely.
- Organisations' training providers should be able to push out a short 'working from home' security awareness module to help the workforce understand the potential threats and safeguards they may need to take when working remotely. If not, try creating a short fact sheet or guidance note.
- Review any laptops or servers deployed to allow employees to work remotely, and ensure that they have key security controls including full disk encryption, anti-malware protection, data loss prevention, automated backup solutions and endpoint detection and response tooling applied.
- Information Security teams should work with IT to understand the resilience of remote access systems to DDOS attacks, including reviewing bandwidth available, limitations of remote access software and whether any DDOS protection services can be added in front of them.
- In order to ensure resilience, organisations' should also consider implementing a backup remote access system for privilege and critical business users to access critical internal systems in the event that the primary remote access systems are taken offline or having denial of service.



Cyber Security Risks (contd.)

2 - Ensure continuity of critical security functions

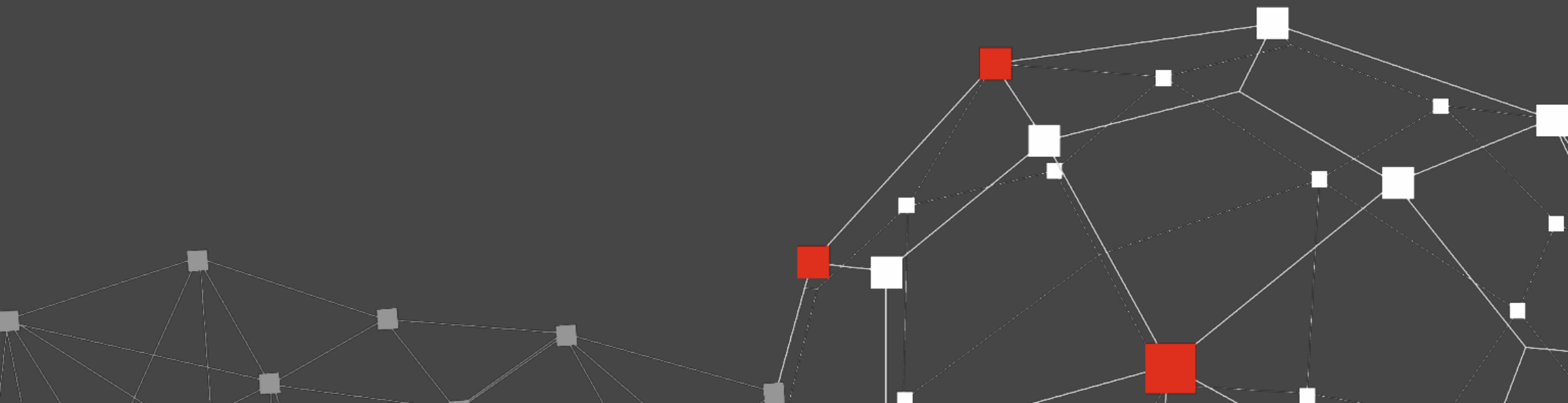
- Identify which activities are crucial to manage cyber security risk(s) e.g. patching security vulnerabilities, security monitoring, identity management and backing up key systems.
- Implement asset management tool to provide visibility and full coverage of assets wherever they are and, crucially, shows whether they are compliant with security controls (e.g. whether systems are patched and running an updated version of the remote access client).
- Confirm patching processes still work when systems are not on internal networks and test that patches or updates applied will not impact on remote workers.
- Perform continuous external and internal vulnerability scanning on publicly exposed systems and internal production infrastructure to confirm patching processes are functioning and all critical vulnerabilities have been patched or mitigated.
- Regularly review and document Internet-facing systems and services, and ensure that any exposed systems and services are required.
- Configuration changes to high-risk or commonly misconfigured systems (e.g. firewall access around cloud-hosted databases) should be restricted. Alternatively, additional approval processes should be put in place to ensure that changes are not made with insufficient consideration or in error.
- Organisations should use privileged access management solutions to securing and segregating privileged access to prevent attackers from compromising high-value accounts and the wider network.
- Ensure teams have the people, processes and technology necessary to monitor and respond to alerts, with appropriate levels of redundancy. Consider augmenting Security Operations teams with additional resources (e.g. SIEM) or managed service using Endpoint Detection and Response technology.
- Review incident response processes (including frameworks, playbooks and runbooks) to ensure they are up to date, and function with a remote workforce. There may be need to enhance cyber incident response capability to investigate and create a defensible record if challenged later.
- Due to increased network traffic, validating remote communications and collaboration tools, organisations might have to adjust their incident-response (IR) and business-continuity (BC)/disaster-recovery (DR) plans to cover scenarios relevant to the current crisis. To find weak points in your plans, conduct a short IR or BC/DR tabletop exercise while maintaining social distancing.
- In the longer run organisations may also consider cyber insurance policy which, in the event of a digital disruption to systems, can provide cover for business interruption losses, as well as the costs of engaging forensic experts to investigate and remediate a breach.

Cyber Security Risks (contd.)

3 - Counter opportunistic threats taking advantage of the pandemic

- The support provided to staff regarding how to work securely from home should be reinforced, at the right time, with targeted communications about relevant emerging threats. This currently includes targeted phishing campaigns using COVID-19 lures, or providing awareness to critical users increased risks of email compromise attacks which attempt to exploit different or new ways of working.
- Provide specific guidance to employees to be extra vigilant when it comes to email requests for personal or financial information, or requests to transfer money.
- Given the increased risk at this time, consider implementing additional technical controls to reduce the threat from phishing emails (e.g. configure advance filtering technology to whitelist the file types and to identify suspicious emails.
- Business users having financial authority should be empowered to be diligent in validating any unusual payment requests from senior individuals or customers e.g. by contacting them for confirmation on a separate, trusted communication channel.
- Develop plans to rapidly restrict on-notice employees' access to systems and data by implementing additional logging and DLP policies in order to reduce the risk of data being stolen or systems being damaged. If organisations are not able to physically collect devices from any employee, plans should focus on disabling logical access to physical devices, accounts, and systems within the network.
- Given the increased short-term reliance on technology and the potential for emerging opportunistic threats, organisations should also seek to enhance threat intelligence capability and deploy quick-win technical controls in order to reduce risk.
- Consider deploying or upgrading anti-virus to provide Anti Malware Scan Interface (AMSI) capabilities to detect the malicious use of PowerShell and VBA, restrict the files that can be executed by users on workstations (e.g. PowerShell, HTA, and CHM files) and limit or prevent untrusted Microsoft Office macros from being run.

2 Work from Home – Best Practices



Work from Home – Best Practices

Background

Unprecedented COVID-19 creates more innovation in technology transcends every domain and industry and affords humankind opportunities unimaginable a few generations ago. Devices we carry give Internet access to vast and incredible knowledge with almost unlimited processing power and information storage. Billions of devices are connected to the Internet, and our personal, work, and digital lives are inextricably converging.

Inevitably, there are pitfalls to be navigated. Global economic cost estimates of cybercrime increased exponentially and are assured to be in the hundreds of billions of dollars. At an individual level the impact is much more tangible and personal. Our individual digital identities are keys to personal banking, online shopping, social networks, home automation, building access, remote connectivity to work and much more. Having that identity stolen can lead to bank accounts being plundered,, privacy invasion, blackmail and extortion, reputation and career damage. Every day we make informed and balanced decisions related to the wellbeing of ourselves and families. We need to take on managing our digital security with equal responsibility.

Security is a top priority for the organisations. Proper care should be taken to secure our wireless home networks for those personnel utilising an organisation's PC's from a remote location. These are also practices that you should implement to protect your personal assets and data as well. As such the following have been established as a set of best practices for steps to take to secure your home wireless connection.

This portion of publication gives awareness of common risks facing your digital life along with best practice guidance to reduce those risks. Recognise some guidance may require technical expertise which may need further help from your IT department and colleagues.

For additional resources, you may refer to any instructions distributed by services providers as well as the manuals for wireless devices.

Be ready for now—and prepared for the future. Stay connected with your people, keep them in the know about exposure and make sure they have the resources and information they need to thrive, ensure cybersecure culture so you can help reduce risk to your business.

General Best Practices - Home Wireless Security

1. **Network Encryption -** Set the strongest network encryption that is compatible with device so that any wireless device seeking connection will require the key

   a. To enable security, open your router setup screen and look for a Wireless Security section.

   b. Select the wireless security method of either WPA or WPA2. **WPA2 is the RECOMMENDED encryption method**. :

      WPA and WPA2 are more secure and offer greater protection against hacking and security breaches. WEP does not protect networks against a determined hacker. **If your router only supports WEP, you should upgrade to a newer device.**

   a. Enter the passphrase to generate the keys. At a minimum, this should comply with Leading Password practices: 8 characters, upper and lower case, numbers and special characters. **You should not use your official Password.** This passphrase will need to be entered into every device you use to connect to your home wireless network.

2. **Change the default router password -** Follow Leading password practices. 8 characters, upper and lower case, numbers and special characters.

   You should not use your Official Password or the Password you have used for to connect to your wireless network (WPA/2 passcode).

3. **Change the default SSID (Service Set Identifier) name -** When naming the router do not use your family or any other identifiable information

   The SSID is the name that identifies your wireless router. By default, many routers will use the name of the router as the default SSID, for example, Linksys routers will often use 'Linksys' as the SSID. This is a security risk since it identifies the brand of the router making it easier for a penetrator to identify exploits to use.

4. **Disable SSID Broadcast -** Note that when disabling the SSID broadcast it will require that you manually enter your unique SSID when wanting to connect any new device to your network

   To help make finding your wireless network easier wireless routers broadcast your SSID, which means anyone looking for a wireless router could see your SSID. Disabling the SSID broadcast feature make it more difficult for someone to find your network when browsing available wireless networks.

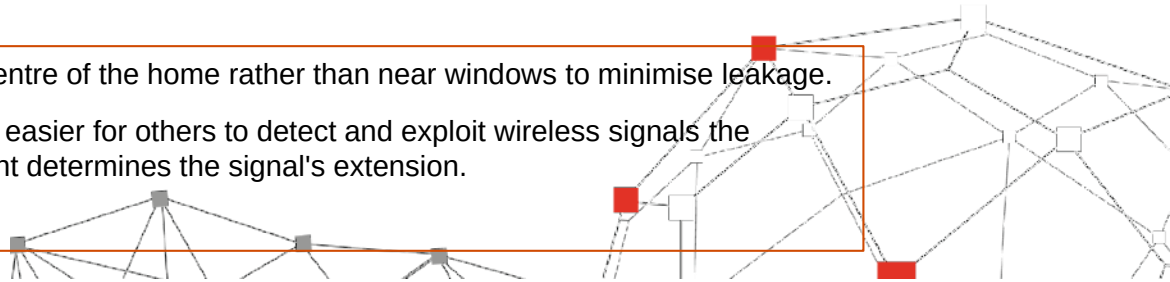
5. **Enable router firewall** – All official laptops should be configured with a firewall software that is deployed via the Endpoint protection for Host Intrusion Prevention.

Recommendations

1. **Position the router / access point safely** - position devices near the centre of the home rather than near windows to minimise leakage.

   Wireless signals typical extend beyond the barriers of a home. It is easier for others to detect and exploit wireless signals the farther out that they reach. The position of the router or access point determines the signal's extension.

2. **Turn off your wireless network during extended periods of non-use**



General Best Practices - Digital Security at Home

This slide summary provides some best practices to help reduce common risks facing your digital life. More and more people are being impacted by cybercrime. This may include identity theft, installation of ransomware (malicious software that encrypts files for criminal to extort money) or attacks that can overwhelm the bandwidth of your network. Take the time to adopt these practices to protect you and your family from cyberthreats.

Recommendations

Passwords

1. Choose multi-factor authentication if available. For example, in addition to a password, include text message verification.
2. Create strong unique passwords unrecognisable by the dictionary: at least 8 characters long made up of upper and lower-case letters, symbols and digits.
3. Change the default password of devices you buy.
4. Never reuse passwords between different devices and accounts.

Install updates, security patches and antivirus / anti-malware.

1. Run the latest version of software (e.g., operating system) and firmware available.
2. Install recommended security patches from legitimate sources as soon as possible.
3. Run and update anti-malware (e.g. anti-virus) software with the newest signatures.
4. Configure your wireless network with the most secure authentication and encryption protocols.

Be careful when clicking links or attachments, running software or giving away information

1. Never enter username and password into a web page unless encrypted.
2. Ensure the domain is as expected, not a close variant.
3. Only click on email links and attachments after determining they go where expected. Even if an email is from someone you know, their system may be compromised. Hover your mouse cursor over the link and read the URL address in the bottom left corner of your web browser.
4. Never ignore warnings provided by your browser about insecure sites and certificates which are invalid.
5. Do not share usernames, passwords or PINs.
6. Think carefully before posting pictures and personal information on social media.
7. Only install software from a legitimate source. Be wary of free software.
8. Be wary visiting websites with adult themed content or torrents; many are known to have embedded malware.

Spot security issues and know how to respond and recover.

1. Your system may be compromised if:
   - Your system is slower than normal
   - Additional pop-up windows or dialog boxes show up (which may appear and disappear quickly)
   - Your web browser has new toolbars, the search engine has changed or the home page is different
   - There are new icons on the desktop
   - Your camera light is on when you are not specifically using it
   - Files are missing
   - Your mouse cursor moves by itself
2. If you suspect your system is compromised, isolate the system from your network and other devices and seek professional advice and help.
3. Ensure you backup your data on a regular basis. Beware; backups can be compromised too. Consider authorised cloud services for off-site backup as well.

General Best Practices – Work from Home

Browsing the Internet Securely @ Home

1. **Check the URLs of the websites you visit.** The URL "https://www.abccompany.com" is legitimate, but a spoofed site may have a domain that looks like "https://www.abccompany.com" or "https://www.abccompany-pk.co.net."

2. **Look for "https" or a lock icon in the address bar of your browser.** These websites have valid security certificates, which means your activity on this website is encrypted and private.

3. **Be wary of anything that seems too good to be true.** Popup ads claiming you won free prizes or online stores with absurd deals may be ploys to steal your information or money.

4. **Use ad blocker or script blocker browser plugins.** These plugins can prevent malicious popups or code automatically running in the background from stealing your information or downloading malware.

5. **Avoid visiting potentially dangerous websites.** Explicit content or torrent based websites or websites that provide downloadable proprietary content for free are examples of websites that may try to download malware onto your device.

6. **Never ignore warning messages from your browser.** Your browser may know if a website is flagged as unsafe, or uses a potentially fraudulent certificate.

Preventing Malware Attacks @ Home

1. **Be wary of clicking links in emails, social media messages, or text messages.** Any message from unknown senders can potentially have links that, when clicked, can download malware onto your laptop or mobile phone.

2. **Be cautious when downloading files from the internet.** Malware can be disguised as legitimate files to infect unsuspecting victims. Whether you're downloading file attachments from an email or free music from a website, always make sure your downloads are from a trusted source.

3. **Make sure to always download and install the latest updates to your software applications, operating systems, and firmware.** Since malware often exploits known vulnerabilities, keeping up-to-date with the latest security patches can prevent malware from infecting your devices. Everything from your computers and phones to WIFI network and smart devices should be regularly updated.

4. **Use antivirus software and set up automatic scans and updates.** Antivirus software can detect and eliminate malware found on your computer, as long as you make sure it's running automatically. Make sure that your antivirus software is also automatically updating its virus definitions to protect yourself from new viruses.

Remember to only use officially managed laptops and devices for business. Personal laptops and devices – such as personally owned phones that are not configured with officially managed security software, are not to be used for work.

General Best Practices – Work from Home (Contd..)

Locking down your technology @ Home

1. **Be mindful about password security.** Using a password manager that generates unique, complex passwords for every website is the best way to keep your passwords safe. At the very minimum, don't use passwords that are easy to guess, and don't reuse the same password for multiple websites or devices.
2. **Utilise firewall software on your computers.** Firewalls prevent unwanted access or unintended output from your computer. Both Mac and Windows have built-in application firewalls. Make sure they are enabled and working properly as per your Organisations' policy.
3. **Use your admin account on your computer for administrative purposes only.** Your day-to-day user account should have restricted rights so if it's compromised, the hacker would not have admin access to the entire system.
4. **Set a password for your wireless network and use WPA/WPA2 if possible.** Keep out unwanted users of your home wifi with a password, and use the WPA/WPA2 security standard to help make it more difficult for hackers to hijack your network.
5. **Change the default credentials for any devices out of the box.** Whether you've installed a network router or smart home devices, the default credentials to access their web-based administrative controls are probably "admin" and "password." Changing these defaults is the first step to protecting these devices.

Protecting your data on the go

1. **Be cautious when using public networks.** Use a mobile hotspot or VPN when accessing the internet to help ensure nobody can spy on your internet activity.
2. **Turn off Bluetooth when you're not using it.** Bluetooth signal is a potential doorway for hackers to take control of your devices. If you're not using your Bluetooth headset at the moment, turn off Bluetooth on your phone.
3. **Require a password after opening your personal laptop.** If your laptop gets lost or stolen, setting up a password upon opening can help prevent people from accessing your data.
4. **Use a complex passcode on your mobile device.** Many mobile devices just require a four-digit PIN to unlock your device. If your phone allows you to set up a longer PIN, it'll be harder for criminals to break into your phone.
5. **Never write passwords on sticky notes and put them on your devices.** Using passwords and encryption are great ways to protect your data, but it's useless if a criminal steals your laptop and your password along with it.
6. **Keep your work devices close to you at all times.** Don't leave your laptop in your car -- bring it with you to help ensure it doesn't get stolen. Do not share work computers and other devices with or used by anyone else in the home.

Cyber Criminals love crisis. Be prepared to secure your technology infrastructure in the face of new threats.
HOPE FOR THE BEST, PREPARE FOR THE WORST

A·F·FERGUSON&Co.

Chartered Accountants

Karachi Office:
State Life Building 1-C
I.I. Chundrigar Road
Karachi – 74000
Pakistan

Lahore Office:
23-C, Aziz Avenue
Canal Bank, Gulberg 5
Lahore – 54000
Pakistan

Islamabad Office
PIA Building
49 Blue Area
Fazl-ul-Haq Road
Islamabad – 44000
Pakistan

pwc

For further information and feedback, please feel free to email us at pk_tech_consulting@pwc.com