BERMUDA MONETARY AUTHORITY

INFORMATION BULLETIN

CYBER RESILIENCE AND REMOTE WORKING

29 June 2020

TABLE OF CONTENTS

I. SCOPE

1. This Information Bulletin (bulletin) is addressed to all Bermuda registrants regulated by the Bermuda Monetary Authority (BMA). The bulletin covers and provides best practise guidance on two topics: cyber resilience (section A), and the risks and related risk response relevant to remote working (section B). Established under the Bermuda Monetary Authority Act 1969, the BMA supervises, regulates and inspects financial institutions operating in or from within the jurisdiction.

II. INTRODUCTION

2. The recent shift of business operations to a remote working model may present a number of changes to an organisation's cyber risk profile.
3. *Cyber resilience* is the ability to prepare for and recover rapidly from disruption resulting from deliberate attacks, accidents or naturally occurring threats or incidents. Cyber resilience should be managed as part of the overall operational risk process of an organisation. Ultimately, the senior management team should have oversight of and overall accountability for cyber risk and the related risk response.

III. SECTION A - A CYBER RESILIENCE POSTURE REVIEW SHOULD INCLUDE THE FOLLOWING:

a. **Business Continuity Planning (BCP) and Disaster Recovery (DR) capabilities** – organisations should have documented BCP and DR plans in place that have been tested to provide assurance on their effectiveness. It is important that the senior management team is given full visibility of the BCP plan, detailing which services are scoped to be restored in the event of a disruptive event. Additionally, IT service providers should conduct regular recovery tests
b. **Crisis management team review** – review roles and responsibilities, including interaction with the business operational risk incident process and the cyber incident process
c. **IT strategy and architecture** – identify single points of failure and ensure systems redundancy is in place. Cloud and virtual services offer a number of capabilities in the flexible provision of IT services. Virtual desktop infrastructure and desktop as a service enable IT teams to centrally manage user desktops
d. **Critical third-party suppliers** – analyse the organisation's key dependencies and how the impact will be mitigated should third-party services be subject to disruption. Confirm that outsourced providers are applying the appropriate controls
e. **Utilising the three lines of defence** – operational controls, risk oversight and audit can all be used to reduce potential impacts on an organisation

f. **Cyber ecosystem controls** – asset management to identify assets, controls management to formalise controls and control effectiveness, configuration and change management to maintain operating stability
g. **Incident and Vulnerability Management** – to ensure that new vulnerabilities are identified and managed and that incidents are formally managed to minimise potential disruption
h. **Training and awareness** – staff training to ensure that staff identify risk and respond accordingly to the desired risk response

4. A cyber resilience review may also scope in the role of digitalisation. *Digitisation* involves keeping the business process essentially the same but converting analogue to digital. *Digitalisation* involves doing completely different things facilitated by technology. Digitalisation is more than just technology; it can facilitate rapid responses to changing situations.

IV. SECTION B - IT RISKS ASSOCIATED WITH THE RECENT SHIFT TO REMOTE WORKING

5. Where new remote working services have been configured, this has changed the company's "attack surface". New services that have not been subject to standard security hardening and testing will introduce new vulnerabilities. Remote services by nature are internet-facing and are at high risk of exploitation by malicious actors. Examples of risks presented include:

a. **New conferencing and collaboration tools –** these tools may operate with default insecure configurations. Examples of this include: conferences set up without passwords, option to run without end-to-end encryption, data may be shared with unknown third parties
b. **Increased use of "shadow IT**" – remote working is likely to result in greater use of services that circumvent traditional IT controls. One example is internet file-sharing services
c. **Increased use of personal devices** – personal devices are likely to be less secure than corporate devices. For example, they might not have all the latest security updates installed or run anti-malware software.
d. **Network capacity and performance** – new remote services may subject IT infrastructure to increased volumes of traffic which could lead to performance or capacity issues
e. **Insecure home working environments** – key risks are data storage and exfiltration, unauthorised access and hardware security

6. Threat actors are exploiting interest in COVID-19 to target end users:

    a. **Phishing attacks** – cybercriminals are targeting users with phishing emails to trick them into clicking on malicious links or downloading malicious applications or files that contain malware
    b. **Social engineering** – attack vectors include telephone calls, texting, social media, as well as email

Risk response: Key cyber risk controls

a. **Communicate remote working policies to all employees** – staff should be given clear guidance for working in the home environment. For example, securing Wi-Fi services, shredding confidential papers and preventing unauthorised access to company devices
b. **Conduct a risk assessment on the new remote working operations** – ensure that the business' new risk profile is assessed, communicated to senior management and the appropriate risk response is agreed. This should include the review of any new "ad hoc" business processes that have been put in place
c. **Secure communications on external networks** – use encryption technologies to protect the confidentiality and integrity of communications
d. **Confirm staff identity in business communication processes** – for example, a staff member's identity must be confirmed before an IT helpdesk gives out confidential network access credentials
e. **Secure remote access servers** – ensure that remote access servers are kept fully patched and that they can only be managed from trusted hosts by authorised administrators
f. **Secure remote access connectivity** – utilise two-factor authentication. Consider endpoint validation controls that check a remote device's patching and anti-malware status before allowing connectivity to the network
g. **Updating remote devices** – ensure endpoints are still subject to patching and anti-malware updates
h. **Mobile device management** – publish bring your own device policies and consider deploying mobile device management software
i. **Review data loss prevention controls** – this can help prevent unauthorised exfiltration of data from the network
j. **Secure the remote desktop** – review access to home printers and removable media devices. Consider restricting copying data from virtual desktops. Ensure endpoint client traffic is routed through proxy filter services to filter malicious code and manage content access

k. **Review denial-of-service threats and defences** – a successful distributed denial-of-service attack may prevent remote users from connecting to corporate remote access servers
l. **Cyber insurance policies** – remote working places a dependency on internet service providers and network links. Some policies may cover business interruption losses resulting from third-party service failures
m. **Security testing** – any new internet-facing services should be penetration tested

References

https://www.thebci.org/knowledge/coronavirus.html

https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit

https://csrc.nist.gov/publications/detail/itl-bulletin/2020/03/security-for-enterprise-telework-remote-access-and-byod/final

https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus

https://www.ncsc.gov.uk/guidance/home-working

https://www.us-cert.gov/ncas/alerts/aa20-099a