MODULE 3 – CYBER SECURITY

1 Executive Summary

i. Our Instructions and Background

- We were engaged by the client for the purpose of assisting with dealing with a cybersecurity incident that arose due to a phishing email received by a staff member of the company.
- The client has provided us with a months' worth of Office 365 logs for the purpose of this engagement. The date of the log we were provided is the 01/06/2020 – 30/06/2020. The particular period in which the breach occurred was 25 June – 29 June 2020.

ii. Services Provided

- Forensic collection and analysis of informational assets and network devices provided by the client for the purpose of determining the extent of the compromise
- Provide recommendations and Areas of improvement set out in this report that the client can take away and use as mitigation and remediation processes and procedures.
- During the period of examination, we provided the client with our initial scope as well other supplementary IP and Timeline related information

iii. Observations and Summary of Findings

- Through our analysis of the provided data logging data, between 25 June 2020 and 28 June 2020 we observed logins from the following IP Addresses, both of which are external IPs resolving to Lagos, Nigeria.
    - 168.253.114.9
    - 193.238.28.55
- On 25 June 2020, it was observed that there were 8 failed logon attempts from both external IP addresses on the compromised account.
- On 26 June, 27 June and 28 June 2020 it was observed that there we three successful logins from IP addresses external to that of the organisation.
- On 28 June 2020 from IP Address 193.238.28.55, it was observed that a bulk mail-out occurred from the compromised account. This was evident through the "Activity" within the audit log data, in which it states there was a bulk mail activity, to the ExecCoMailboxes.
- Shortly thereafter on 28 June, it was observed that the sent items that were part of the mail-out were moved to the RSS Feed within the compromised account in an attempt to hide them from the owner of the account.

2 Recommendations / Areas to improve

In performing post incident review services, we align our activities to industry leading and freely available cybersecurity frameworks. Specifically, we have aligned our recommendations and areas to improve on the following frameworks to further assist the client in building sufficient resilience within their organization.

- National Institute of Standards and Technology (NIST) cybersecurity resilience framework

i. **Identify** – Identification is the concept of developing a broad understanding of cybersecurity risk in relation to informational assets within the organization. Opportunities to improve and recommend.

- In the context of this incident, it was advised that there a number of third party service providers that have current supply agreements with the client who have no / little cybersecurity strategies or implementations. Moving forward, the establishment of dedicated third party cybersecurity risk quantification, assessment and ongoing management processes would be critical to ensure third party risk is considered as important as internal risks.

ii. **Protect** – Protect is the second point in the NIST framework and covers the development and implementation of appropriate safeguards to ensure delivery of critical infrastructure and services. Opportunities to improve and recommendations as follows.

- Access Control – The root cause of initial compromise was through the client Office 365 environment which means there are little to no current multi-factor or two factor authentication (2FA) implementations. This means that the only security mechanism blocking unauthorised external, web based access to the client's information is a person's user name and password. The implementation of a second form of authentication would almost completely deter this risk.
- Safety & Awareness - A robust, proactive, regular and engaging cybersecurity safety and awareness program is an important part of an effective cybersecurity strategy and risk management framework. Investment in the human element is as important as an investment in process and technology.
- Information Risk – The transition to cloud based environments with "unlimited" storage introduces information risk. There is the potential for a person's email account and "inbox" to become a primary storage facility, as opposed to being a repository for transient or temporary electronic communications before it is transferred to a dedicated electronic document management system or actioned and deleted. The longer the tenure of an employee, the more data they will store in their inbox and therefore the more information that is potentially available to a malicious actor should they gain access to that persons account. This information risk needs to be factored in to an organisations approach to cybersecurity risk management.

iii. **Detect** – Thirdly, the detect phase relates to the development and implementation of the appropriate activities to identify the occurrence of a cybersecurity event. Opportunities to improve and recommendations as follows.

- Monitoring – The Microsoft Office 365 environment of the client was successfully "logged onto" repeatedly by external threat actors. With this, access resolving to a number of locations including high risk cybercrime global areas like Nigeria. None of this activity was detected at the time of the incident, and it was only after the bulk phishing emails were sent from the compromised account, and the forensic analysis was commenced, that this information was detected. Monitoring tools and alerts within the office 365 environment will allow some visibility over those accessing the account from outside the "Business as Usual" IP range and allow examination of these connections.

iv. **Respond and Recovery** – The fourth and final phase of the framework details that of the response and recovery efforts of organisations in the face of a databreach or exploit.

- Planning - Microsoft Office 365 attacks and compromise are wide spread and highly common globally. As a result, there is an opportunity for the clients IT personnel to match the risk profile of their environment to the security detection and response capabilities that are available from Microsoft, such as increased logging and risk event alerts that will feed a more tailored incident response and recovery plan specific to the Microsoft environment.