## Cyber security Summary report

Cyber risk needs to be addressed in a cross-functional manner that goes beyond just the IT department. Otherwise, organizations can potentially put themselves in dangerous situations. For example, if one department unilaterally signs an agreement with a third party – like a cloud provider – without input from both the IT and legal teams, they are willingly accepting the risks and vulnerabilities that the third party possesses. Neglecting to collaborate with other departments and review the cyber security practices of a vendor or the legal language of the contract can be the difference between being a headline tomorrow and avoiding threats/risks entirely.

Executive Summary

1. Our Instructions and Background
   * We were engaged by the client for the purpose of assisting with dealing with a cyber security incident that arose due to a phishing email received by a staff member of the company
   * Require specific log details for dates
2. 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.
3. Incident response improvements

Waiting until after a breach has occurred to determine a course of action is a waste of time and money. Bouncing back as quickly as possible is crucial to both preventing business interruption, as well as maintaining customer loyalty, hence the need to prepare in advance. At a minimum, here are four things that an incident response (IR) plan should include:

* **Define the organizational structure of your IR team.** You need to figure out which members are parts of the team and what exactly is expected of them. Also decide which parties will need to be alerted during an incident, and specifically under what circumstances they need to be contacted.
* **Determine what is considered an incident – and what isn’t.**In other words, figure out what standards must be met to advance something from an event (which can be routinely handled) to an incident. Also consider the type of attack when determining next steps – is your response altered for a DDoS attack versus an insider leaking information or a connected third party who has been breached? Definitions vary from organization to organization, so prepare in advance and decide what works for you specifically.
* **Follow an IR framework.** Clarify what organizational steps need to take place during every stage of your response to the incident. For example, step one is to log events into a ticketing system, which is followed by a specific member of the team evaluating each one. If it is determined that the event be deemed an incident, the IR team is then activated and predetermined business officers are notified, etc.
* **Create a documentation methodology and repository for every incident.** This will help you learn what worked successfully and what did not. The repository should include after-action reports (AAR) and root cause analyses that occur once an incident is closed.

1. Safety and employee awareness

In an ideal world, employees would report all anomalies, like social engineering attempts or insider threat red flags, but we shouldn’t assume that everything will be reported. Notification from employees shouldn’t be expected to replace systems that detect, monitor, and mitigate threats, like firewalls, intrusion detection systems, well-designed networks, secure ports, logs of device access to the network, and rule based log analysis.

Effective cyber security requires a team effort, so ensure that you are doing your part to keep your organization safe.

1. Cyber hygiene

**Frequently test your systems**

It’s not enough to put processes in place and think that you are protected. You need to test your systems to ensure they are doing what they should be. When you do test, make sure to include stakeholders from multiple departments like security, IT, and human resources at a minimum. Consider also including social engineering in the test, both the classic type (i.e. asking someone to hold the door and following them inside a secure space) and the digital version (i.e. phishing emails).

While testing is important, it’s not sufficient to simply perform a test and read a report. Instead, conduct an AAR in which you discuss what went right and went wrong during testing, as well as how to correct any mistakes moving forward.

1. Monitoring and information management

In performing post incident review services, we align our activities to industry leading and freely available cyber security 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) cyber security resilience framework

1. **Identify** – Identification is the concept of developing a broad understanding of cyber security 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 cyber security strategies or implementations. Moving forward, the establishment of dedicated third party cyber security risk quantification, assessment and on-going management processes would be critical to ensure third party risk is considered as important as internal risks.
2. **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 cyber security safety and awareness program is an important part of an effective cyber security 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 cyber security risk management.
3. **Detect** – Thirdly, the detect phase relates to the development and implementation of the appropriate activities to identify the occurrence of acyber-securityy 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.
4. **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.