**Threat Report**

**Summary**

Cybersecurity threats related to business vulnerabilities with current system administrative policies and current employee activities. Current aggressive cyber-attacks have been noted in media and online news/blogs sites. The business requires an updated and planned to mitigate the current vulnerabilities.

**Intrusion / Attack Timeline**

10.30am - This attack used a phishing email to obtain user login in details. This was initiated with a HR email applying pressure to the users to complete an action related to timesheet submission. The user was requested to activate a link that transferred the user to cloned site and user information was entered and capture by the attacker.

14.00 – The service desk identified a further 62 comprised users within the Risk Department. At this time a compromised program was identified within the cloned site.

15.50 - Lost of access to the file-shares server related to Word documents

**Actions Taken (attack timeline)**

* Isolate the affected file sharing server
* Identify the IP address associated to the bloc
* Configuration to disallow external attachments/programs
* Isolate user devices

**Key watch points**

Outline of Key Cybersecurity Threat Types

**Threat Type**

**Phishing attack** – is a developed malicious file or script allowing aggressive actors in this case via email (**email phishing**), used the HR Timesheet imitation as an attack vector. In this case of social engineering the attack used email phishing which was used to divert the user to a malicious site to gain login information and access and control of files, this attack also delivered a malware file.

**Vulnerability**- are the endpoint user understand of social engineering used to access their system or business platforms.

**Risk** – gain user login details such as password and other platforms within the network having the same password.

**Attack**- used social engineering, the attacker is able to identify the users such as departments to create user error/manipulation. This occurs through human error related to emails

**Mitigation**- Improve users knowledge of cyber security via education and system configurations

* Users education – to look for misspelling in URL’s
* Audit user passwords system prevention systems
* Identify web-based platforms weaknesses

**Malware attack –** is a form of cyber-attack threat that can control the access to the networks and remove system access to users.

**Vulnerability**- the attacker is able to gain further unauthorised access to the system.

**Risk** – the attacker gaining login details leading system access and delivering malicious packages to the system.

**Attack**- After the malicious software / file is downloaded the action of the malware is to limit/stop users from accessing the required files and system platforms, achieved via, distributed denial of service (DDOS) attacks also allow the access to sensitive files.

**Mitigation**-(Ensure the use of Prevention Best Practice)

* Use training to ensure employees are more aware and are proactive. Include endpoint protection software (EDR) Endpoint Detection Response improve system proactive response to the malware.
* Use of Account policies
* Patches are updated