COVID-19 CYBER RISK MANAGEMENT

As organizations cope with the COVID 19 virus, many have moved to migrate their workforce to being, if not fully remote, at least partially remote, leaving only key employees on-site. While the usual Cyber risks for organizations remain, new risks have been introduced and exacerbated by the fragmentation of the workforce. It is also worth noting that even in normal circumstances, human error is the underlying cause in 80% of Cyber claims at IMA, in a reduced-security environment, an uptick in cyber crime is to be expected.

Below is a brief summary of some of the most common cyber risks and the strategic considerations that should be given to the various areas to help mitigate a business' risk.

ENHANCED RISKS

SOCIAL ENGINEERING

Cyber criminals are opportunistic and recognize that right now many employees are feeling anxious and may potentially be less cautious or may be working in a less secure environment then they are accustomed. Cyber attackers have already been begun to attempt exploit those circumstances, with a significant recent uptick in phishing attempts and credential theft. Often times scams attempt to disguise themselves by posing as legitimate organizations, such as the Center for Disease Control or the World Health Organization.

For cyber attackers, the goal is to monetize security lapses in any way possible. General the targets of these attacks are theft of funds, data exfiltration and ransomware.

TYPES OF DIGITAL ATTACKS

Phishing/Spearphishing – Emails that target everyone or a specific person or role within an organization that include malicious links or entice users to enter their credentials or other personal information on a website designed to mimic a legitimate site.

Social Media Deception – Bad actors create fake profiles to befriend their victims, posing as a current or former co-worker, job recruiter, or even someone with a shared interest on social media. The goal is to trick the victim into providing sensitive information or downloading malware onto their device.

Pre-texting – Attackers focus on creating a false but believable fabricated story, or pre-text, prompting their target to provide certain information in order to confirm their identity.

Water Holing – Attackers compile information about a specific group of individuals within a certain organization or industry, including legitimate websites this group visits. Attackers then look for vulnerabilities in these sites in order to infect them with malware. Once the individuals in the targeted group visit those sites, they become infected with malware.

OPERATIONAL DISRUPTION

Company networks are under stress due to the volume of remote access. Another area of heightened risk is operational disruption due to lack of connectivity. Underlying causes may be security or system failure and may result in prolonged down time.

RISK MANAGEMENT

Employee vigilance is paramount. In addition to standard training, staff should be reminded of basics.

- Do not click on links or open attachments in emails from untrusted senders
- If a request does not seem appropriate, or if there is something non-standard, pick up the phone and contact the sender or review with a trusted colleague before taking action.
- Any suspicious emails should be sent to the company IT department

Mandatory usage of VPN to access company network, including multi-factor authentication when accessing sensitive systems and databases

Do not use "free" WiFi connections to conduct any company business

INCIDENT RESPONSE

In the event of an attack the key is to minimize the potential damage. Through a documented Incident Response Plan (IRP) companies can respond quickly and effectively to any cyber-attacks. A good IRP will help improve both internal and external communication and will help speed time of the response by having clearly defined roles in the event of an incident.

An IRP should include the following:

- Key stakeholders and their roles within the investigation and response.
- Incident taxonomy to help standardize internal communications and more easily share information with any outside agencies that may be helping with the response effort.
- Classification framework for the type of data that has been compromised in the attack. For example, a company might have one processes for confidential customer data and a different processes for a loss of critical intellectual property.
- Some plans include specific procedural guidelines, such as a checklists for containment, eradication, and recovery, as well as guidelines for documenting the response in governance, risk, and compliance applications.
- Any resources or obligations within a Cyber Insurance policy (see below).

In addition, all employees should have a listing of contact information for key personnel at the company (especially IT personnel). This listing should be sent to all employees to download on their local drive in the event of network disruption. The same precaution should extend to members of the IRP team to include local copies of the IRP.

CYBER INSURANCE

If you currently purchase this coverage or considering purchase, there are numerous coverage solutions that could apply.

Cyber Crime: Will reimburse for loss of funds associated with social engineering exploits.

Network Business Interruption: Will indemnify for loss of income due to down time (subject to a waiting period).

Cyber Extortion/Ransomware: Will fund investigative expenses and ransom payments.

Incident Response: Funds to engage first responders (legal counsel, forensic investigators and crisis management firms) in the event of an actual or suspected event.

It is also worth noting that most Cyber policies come with complimentary loss control solutions that can help provide additional resources.

If you are experiencing any issues or would like to discuss in greater detail, please contact your local IMA representative or below:

TIM BURKE
Director Cyber Risk
tim.burke@imacorp.com

We're more than just insurance. IMA goes the extra mile to bring you tools, research and insights to help your business face the many challenges of operating in a rapidly changing environment.