Cyber security for your business.

Basic rules and essentials to prevent, detect and respond to cyber attacks to safeguard your valuable data and information.

The impact of a cyber attack can go beyond the obvious financial consequences. They will also hurt or even destroy your brand reputation or affect your competitive edge in case your intellectual property is stolen. So what about small to medium sized organisations who can't afford to lose even the smallest per cent of your vital customer base?

Implementing effective cyber security measures that are cost-efficient can be a challenge and getting cyber security right from the start becomes something that cannot be overlooked. One of the most common mistakes businesses make when asserting if they have an adequate level of cyber security controls in place is the misconception that safeguarding of data and information is as a technology issue, and that compliance is enough. Also, the idea that even a small business or individual is statistically unlikely to experience a security breach is not true. According to a multitude of research, the chance that you will suffer a breach at some stage is high. So it's important to have a plan in place and that your employees understand their roles and duties in case such an event happens.

Securing your valuable data and information is an ongoing process and its importance will only become more vital for your business with the fast growth of innovations and technological developments which will introduce more risks to account for. In addition, good cyber security can enhance the reputation of your business and open up new commercial opportunities.

Where to start

A good way to start is to benchmark your organization's cyber security maturity to that of comparable companies within your industry. Secure organisations regard cyber security as part of their company's risk management strategy and profile. Like other business risks, it takes four layers of protection.

- Governance

Make cyber security a priority in your organisation to protect valuable data and information. Leading by example, top-down, board members must recognize the importance of cyber risks as part of their overall strategy. Your board should build a governance structure and determine their risk appetite from a business perspective.

- People

Invest in educating and training of your people on cyber security. Research argue that most security breaches can be traced back to human error. Your employees are the weakest link in the cyber risk chain for bad actors. Moreover, IT staff within your organisation should certify to ensure that they are up-to-date with the latest technology trends.

- Processes

Build processes and procedures around your cyber security strategy to mitigate cyber risks. These procedures are key to ensure the maintenance of an appropriate level of security during changes and an up-to-date environment.

- Technology

Implement and maintain the right technology. Technologies that protect against cyber attacks, range from offline defensive mechanisms to offensive weapons for uncovering hackers or taking down their arsenal. There are already technologies in the market that provide access controls with biometrics, monitor user behavior and analyze network traffic, mitigate third party cloud vendor security risks, and deceptive technologies designed to disrupt an attacker's activity or to fool hackers with fake vulnerabilities.

Best practices to follow:

Identify

- Appoint roles in the organisation that are responsible for implementing and assessing cyber security.
- Identify which financial and information assets are most valuable for your business and make it a priority to secure these assets.

- Have a complete understanding of the devices and machine equipments that are being used in your business, such as mobile and personal IT devices. Know how these are being managed, where they store your data, and who has access.
- Perform a cyber risk assessment, penetration test or IT audit periodically.

Protect

- Be vigilant, trust and verify the sources of digital information at all times.
- Introduce frequent meetings and/or organize company workshops to create awareness on cyber risks, such as phishing, ransom ware and social engineering tactics.
- Beware of social-media risks on the work floor. This is where people usually let their guard down. Cyber criminals are targeting small to medium sized businesses through these channels. Criminals use detailed information to attack employees based on daily user routine behavior.
- Enforce good password management policies. Use a strong mix of characters and don't use the same password for other accounts, don't allow sharing passwords with others, writing it down or sticking it on a post-it note attached to a desk. Password management software applications can protect and collect all passwords for you. At the same time, using these applications make passwords more convenient to use.
- Introduce two-factor authentication by using a smartphone or token to provide the second phase of user credentials to gain authoritative access.
- Restrict access to data and information to the minimum required by managing user privileges on a need-to-know basis, also for IT staff.
- Be aware that Bring Your Own Devices (BYOD) and mobile device that contain corporate information increase threats by adding complexities of data and information flow.
- Ensure that your IT staff has malware protection and network security in place.
- Change all default passwords of applications and devices, and decide a secure standard configuration for all IT equipment connected to your business.

- Update software on user machines regularly. Updates and patches not only makes your machines more secure, but also increases functionality, user experience and ultimately can increase productivity.
- Protect all pages on your public-facing websites, not just the checkout and sign-up pages.
- Implement measures to encrypt sensitive and critical data and make sure that only authorized users have access. Encrypt data when stored or transmitted. Also critical data in the cloud.
- Backup the critical data on all computers daily and make sure that backups can be restored.
- Third-party and cloud service providers can introduce cyber risks. Assess the security controls of your service providers and review your contracts and service level agreements. Request more information about how your suppliers deal with mitigating cybersecurity risks.

Detect

- Monitor usage of IT equipment and behaviors of users by considering the implementation of behavioral analytic tools. These tools can detect anomalies in user behaviors that might introduce risks to your business.
- Monitor malicious network traffic to identify a breach.
- Put procedures in place for employees to identify and escalate a security incident.

Response

- In the event of a data breach you should know how to respond. This includes isolating and removing residual malware, informing the business and IT, evaluating and understanding what causes the incident to happen and immediate actions to minimize the impact. Those responsible for legal, compliance and corporate communications should know how to internally and externally handle the situation.

Recover

- Have a short-list of reliant cyber security experts to help you recover in the event of a breach. Have a concrete plan in place to ensure business continuity in case of an attack.
- Know who to contact and report to at the local authorities from the Hong Kong Police Force, Cyber Crime unit.
- Consider using some sort of cyber security liability insurance. There are already insurance products in the market to transfer risks.