香 港
The BELGIUM - LUXEMBOURG
Chamber of Commerce in Hong Kong

InterSME Breakfast Seminar: Cyber-security

Overall the panellists agreed that the growing use of smart phones, cloud computing technology and the widespread availability of information has not only made our lives easier, it also opened new avenues of attack from cyber-criminals & hackers.

Cyber criminals usually have only 3 goals:

1. obtaining information to subsequently sell (credit card data, identity information);
2. stealing currency (real or crypto) or in another way getting money (ransom deals);
3. embarrassing their victims, showing their skills (usually with big companies claiming to be invulnerable).

When it comes to assessing your cyber security three elements need to be considered and checked: people, processes and technology. Surprisingly many successful cyber attacks happen due to faults in the first 2 (people & processes) opposed to the commonly held belief that successful hackers must use sophisticated technology.

Frequent faults in people are usually related to being unaware of the risks. Clicking on a link in a phishing mail, inserting an infected USB drive in a company computer or using an easy password for a long period of time (especially when your password is ‘password’, bad idea).

Frequent faults in processes usually happen due to a lack of protocol, too complicated protocols or when a person is pressured to circumvent protocol due to imagined or real pressure from a fake person or timing. Examples are the well-known CEO scam, fake invoices, fake urgent payment requests coming in a few minutes before the weekend.

What we can do to secure and defend critical information of our business:

- Promote greater accountability and awareness: share examples of scams with all your employees, invite employees to report possible scams even though they might be false positives. Teach them the common signs of fake communications. Convince them that the best cyber security practices not only benefit the company but also help to protect their own family’s cyber security and vice versa.
- Put proper protocols in place but don’t overcomplicate: verify payment requests before processing payments by double checking account information, contacting the vendor & check with whoever gave the order by phone. Implement payment threshold checks, have another colleague check & sign off for certain amounts. Keep it workable though as colleagues might invent unwanted workarounds to avoid enduring lengthy security processes.
- Be proactive: employ advanced security strategies & tools, pay for a VPN to add an extra layer of security/encryption when using public WiFi. Always install the latest updates for common software. Practice attack situations. Keep some non-digital information available in case of a total blackout attack. Have your risk assessed by an external party or if you are already feeling at risk then outsource addressing your concerns to a specialized agency.

Finally a big thanks to the panellists for their insights, BNP Paribas for having us over today Maison Eric Kayser HK for the tasty breakfast.

Your BLCC often participates in these kinds of events and our members are always invited to join. Keep an eye on our newsletters and website for upcoming events and feel free to join in. See you soon.