Cyber Security – Good News and Bad News

Cybersecurity threats to cost organizations in Asia Pacific US$1.75 trillion in economic losses -Microsoft Asia News Center, May 18, 2018

Iranian hackers attacked college professors, US agencies and companies: Justice Department - CNBC, March 23, 2018

So far in 2018 there has not been as many data leaks, system crashes, or malware attacks as the same period last year. That's the good news and it ends there.

The bad news is that corporate security improvements are lagging and critical infrastructure security hangs in the balance. On top of that, state-backed hackers are also getting bolder and bolder – Russia, North Korea are commonly known; in March the US DOJ indicted 9 Iranian hackers bent on infiltrating 144 US Universities and 176 Universities elsewhere in 21 countries. Other targets are wide and varied, such as national infrastructure such as power grids and of course Financial Institutions including Banks and Exchanges.

The hackers employed 'Spearphishing emails' to trick university staff into clicking on malicious links which gave them entry into the systems and they stole 31 trillion terabytes of data worth $3 billion. Of 100,000 accounts targeted they were able to gain 8000 credentials data. It doesn't matter though how big you are or what data you have, if you are hacked it could ruin your reputation and business future as well as being extremely expensive.

The first line of defence of any organization is your workforce. Knowing what to do or more importantly what NOT to do and how to behave in day to day activity is simply crucial. If your employees let the guard down it undermines any IT security you have in place.

But luckily there are good ways to train your staff, and then follow up that training with updates throughout the year. Add in fake attacks and an ever-learning database that feeds back key information to the clients, ways to measure your readiness and the risks inherent in your supply chain, and you have more comfort of mind that you are doing your utmost to protect your business.

The Intuition-CybSafe Cyber Security Awareness eLearning related to this article consists of these **Core Modules**:

- What is CybSafe?
- Am I Really a Target?
- Passphrases
- Preventing Identity Theft
- Public Wi-Fi
- Browsing Securely
- Device Security
- Malware & Breach Recovery
- Social Engineering
- GDPR & Your Rights

The topics covered in Intuition Asia Perspectives are current developments or topics currently in the market. Intuition Asia provides bespoke learning solutions, both eLearning and Instructor-led courses. These can also be blended in a program to provide the most effective form of learning. These workshops can be structured as lunch & learns, webinars or full day deliveries. Clients can use these to keep their workforce updated with the latest developments in the market and complete their mandatory CPD learning hours.

Get in touch with your Intuition account manager at asiainfo@intuition.com for more details.