Lifecare
better together

Will cyber security threats bring down your company?

How well do you understand the threats to your business from cyber crime? And how resilient are you to a cyber crime attack?

These are serious questions for business leaders, not just in the Middle East, and not just for large companies but for smaller and medium-sized businesses too. For the third year in a row, the agenda of the January 2017 meeting of the World Economic Forum (WEF) at Davos was dominated by the cyber crime threat; and by the need for businesses to improve their resilience in preventing and combating it.

Cyber crime is big business, *organised business*, and can compromise or bring down any company in any country. Yet in addition to the front-line defences, there is in fact much companies can do to insure against such risks.

A growing threat

In 2015, Lloyd's estimated the annual cost of cyber attacks globally to be as much as USD 400bn per year – more than most countries' GDP. The WEF's leading expert on cyber security, Daniel Dobrygowski, estimates that in 2015 it cost the average US firm USD 15m per year.

The list of high-profile victims now includes names such as TalkTalk, Swift, Yahoo, and the Qatar National Bank, all of which suffered embarrassing data breaches in 2016.

Moreover, companies in the Middle East are suffering larger losses than other regions as a result of cyber incidents. A PwC research paper published in March 2016, *Cyber security in the Middle East*, found that more than half of companies in the region had incurred losses of more than USD 500,000 the previous year, compared to one-third of companies globally. Businesses in the Middle East are

more likely than other companies to have suffered an incident – that's 85% of respondents, compared to a global average of 79%. *Gulf News* reported that the cost of cyber crime in the UAE was USD 1.4bn (AED 5.14bn) in 2016.

These are sobering statistics, and reinforce the view that cyber crime is one of the biggest risks that businesses face across all geographies and industries, both in the Middle East and globally. It is no longer the preserve of lone hackers working secretly in suburban bedrooms, but a reflection of our increasingly connected world: the dark side of the digital boom. And it's not just big players facing the risks. Nor are financial institutions necessarily the prime targets for today's cyber criminals. Smaller businesses of all types are attractive to these criminals because they are softer targets and often easier to penetrate.

What does cyber crime actually mean?

Cyber crime is a deliberate, directed attack on a computer or network, with the aim of committing an illegal act such as individual identity theft, wholesale theft of corporate data, or malicious damage to intellectual property. Thanks to the internet – and now the 'internet of things' and mobile technology – we live in a digitally joined-up world where information is highly vulnerable as well as accessible.

Cyber crime has many faces and forms, and is continually evolving. Most people are familiar with hacking, a term long in use to describe 'breaking and entering' in the digital space. Gaining access to your systems and data is a first step for cyber criminals, and it's important to remember that every organisation and every individual can be hacked. The Pentagon or a corner shop, no organisation is safe from a determined and accomplished hacker. And once a business' defences have been breached, identity fraud and theft of confidential records and sensitive data may follow.

Any confidential data is a prize worth stealing. Medical records are a good example, and the healthcare sector has experienced several notable attacks in recent years. According to the *Associated Press*, there were 2,453 incidents in the United States in 2015, resulting in more than USD 24m in damages. This total includes money paid as a result of ransomware, a form of malware ('malicious software') which infiltrates a company's computer network and encrypts its key data files. The encryption key is held by the hacker, who then demands a ransom to unlock it. Last year, a Los Angeles hospital paid USD 17,000 in Bitcoins after a ransomware hack. Meanwhile, a recent study from IBM revealed that 70% of business victims had paid to retrieve stolen data, with 20% paying more than USD 40,000.

Another widespread tactic is DDoS (Distributed Denial of Service) attacks, which bring down an online service and put a business out of action, either to gain attention, or for extortion or blackmail. Phishing is another common cyber crime activity, luring people into revealing information that is then used for criminal activities.

Cyber criminals have more tools and resources at their disposal than ever before, making it easy to exploit weaknesses. There are many points of potential failure in a company's systems, and any

fallout will only be compounded by a lack of insurance. The cost of cyber crime is always financial in the long run, no matter whether the aim is extortion, theft of sensitive data, or has a political or moral motivation.

Reputation has a significant impact on the bottom line. All businesses depend on their reputations, and reputational risk comes with a hefty price tag. Once you lose credibility, you also lose customers and revenue. You may also face business continuity costs if your company has been brought down, and getting back on your feet after an incident takes time and money. Furthermore, losing private data – as with other types of data negligence – could put your company in breach of regulatory requirements, leading to fines and yet more financial loss.

What can be done to improve cyber resilience?

In response to the cyber crime threat, companies must arm themselves properly. This means creating both a strong security barrier and a strong cyber resilience culture. And it means cyber risks and the measures to combat them need to be owned and addressed at board level .

Also, good cyber resilience means having insurance in place, as a second line of defence against damage and loss if security is breached. Counter-measures alone are not enough. There is no such thing as an impregnable security system, and with the pace of digital change and the growing expertise and cunning of many criminals, all companies are at risk and have a responsibility to continually assess their exposure.

With so many threats and so many entry points for hackers, there is no room for complacency. Companies must be scrupulous in assessing risks, raising awareness, and educating employees about the importance of security. They must ensure that all software across their networks, workstations and servers is fully up to date and protected by the latest and most suitable anti-virus software. Websites and web applications should be scanned for malware, all business-critical data must be backed up, and networks should be robust and sophisticated enough to resist a DDoS. If your business is small and a highly secure network is beyond your financial means, alternative cloud-based solutions are increasingly available; although even cloud technology has vulnerabilities that are being exploited by criminals as more of the world's information processing moves into that space. There is no such thing as a 100% secure system; hence the importance of additional means of protection such as insurance.

Education is fundamental. As a region, the Middle East lags behind Europe and the United States when it comes to cyber awareness. The 2016 PwC report mentioned earlier found that Middle East companies suffered a higher concentration of malware than other regions, in turn facilitating attacks that ranged from successful data thefts to phishing attempts and co-ordinated spam campaigns.

Companies must accurately assess, quantify and monitor the risks facing their business, and ensure they have appropriate security. Then they need to reinforce their security with a level of insurance commensurate with those risks. That may mean taking out cover for business interruption loss, privacy breach loss, cyber extortion, and media liability, amongst other hazards. There is evidence

that the message is beginning to be heard, with *The Middle East Insurance Review* reporting last October that the number of cyber insurance policies taken out in the UAE was increasing by 10% per year.

Taking ownership of cyber security

Perhaps the single most important measure for combating cyber crime is a strong culture. What this means in practice is that cyber crime and cyber resilience cannot merely be an issue for the IT department and back office administrators. These are board-level issues which need to involve HR and other decision-makers all the way through the company.

Only then can the risks be properly contained with the right combination of security measures backed by prudent insurance policies. Cyber protection is more than a matter of firewalls, anti-malware software and other security tools, although all those things are important as front-line controls. In this new environment of heightened online risks it also means ensuring the company is indemnified in the event of a successful attack.

In cyber space, insurance is a fundamental part of protection.

About the author:
Tanvir Haque, Chief Commercial Officer at Lifecare International
Tanvir is responsible for developing and implementing Lifecare's commercial strategy. He thrives on developing customer-centric business relationships, and as such he is currently focused on revolutionising Lifecare's customer experience and driving the company's digital transformation plans – all with the aim of unlocking Lifecare's full technology potential. With a career spanning back more than 20 years, Tanvir's experience has been gathered in professional services, banking, and telecommunications, having worked with PwC in Sydney, Andersen in Sydney and London, and Standard Chartered Bank in London. He relocated to Dubai in 2008 and spent a number of years advising and consulting international businesses on how to drive growth before joining Lifecare in 2015. Tanvir graduated with a Bachelor of Commerce degree from the Australian National University in his home town of Canberra and is a qualified Chartered Accountant and a member of Chartered Accountants Australia and New Zealand.