“Can’t happen to me, or can it?”

UKWA offers a package of measures to help members manage the risk of a cyber security breach, one of the biggest business management considerations of modern times. Cyber threats are continuously evolving, with 65% of UK firms reporting an attack in the last year. The effects of a cyber attack can be devastating, with most cases resulting in financial loss, customer attrition and damage to corporate reputation.

Teaming up with Perry Appleton Group and Travelers Insurance, UKWA’s brings together a team of experts to help members understand where they may be vulnerable, and to recommend measures to minimise the risk of attack, together with response and recovery support to ensure business as usual should a breach occur.

Cyber criminals have moved away from traditional methods of stealing data to sell on the dark web. There has been a resurgence in more sophisticated tactics, including business email compromise and ransomware, with the goal of a quick financial hit.

According to Advisen, firms are witnessing 504 new cyber threats every minute. Ransomware attacks, by which individuals and organisations are locked out of their systems unless they pay up, have increased this year by an astonishing 500%. And more recently, the UK has been reported as the worst in Europe for ransomware detections.

Ransomware attacks themselves have evolved and become more sophisticated. For example, the high-profile WannaCry attack in 2017 utilised the “spray and pray” method to impact systems across 150 countries, and yet only demanded $300 to $600 in Bitcoin per infection, ultimately receiving a total of $140,000 in Bitcoin transfers. More recently, criminals are infiltrating firm’s email systems – usually through a successful phishing attack against an employee – and studying the firm’s operations, transactions, and system criticalities, in order to strike at the most opportune time. These well-planned attacks, which are further bolstered by the increased sophistication of the malware itself, have led to significantly higher ransom amounts being demanded. It’s no longer uncommon to see ransom demands in the six- or seven-figure range.

Unfortunately, refusing to pay the ransom demand carries its own risk, as witnessed by Norsk Hydro, a Norwegian Aluminium manufacturer. Norsk refused the ransom demand and have spent an estimated £45 million recuperating from the event and are still recovering several months after being locked out of their systems.

As noted by research firm EFT in its recent State of Logistics Technology Report, nearly all logistic service providers recognise the increasing role that technology will play in the industry, with over 70% increasing their technology budget. But increasing technology dependency, coupled with an ever-expanding attack surface exposing new vulnerabilities, requires that these firms increase their cybersecurity proportionally. And there is some evidence that there are some cyber security lags in

the industry. For example, fewer than half of shipping firms and only 30% of logistics firms have a Chief Information Security Officer (CISO). Though improving, only 50% of surveyed firms believe they have adequate employee training on cybersecurity threats.

This is concerning as there are a multitude of ways these logistics firms can be impacted, especially regarding ransomware which almost universally involves employee error at some stage. Critical system failures, which may spiral out of control, preventing order submissions and inventory management, delaying delivery schedules, as well as failure of automatic machinery. In addition to the immediate hit these outages would have to the bottom line, there may be negative implications for a company's reputation.

At a time when ransomware tools are inexpensive and widely available to even the most inexperienced cyber criminals, there is major concern for businesses of all sizes. And the impact of ransomware includes not only direct financial loss (if a ransom is paid), but also significant business disruption and downtime.

Small businesses are typically more exposed than larger firms, which means they can be especially hard-hit following a ransomware event. For small firms without resources, secured backups, employee training, and a cyber security framework, these types of attacks may not only seriously impact their balance sheet, but ultimately their very survival.

It's not all doom and gloom for UKWA members! UKWA's cyber programme not only provides insurance cover for the costs associated with cyber exposure, including public relations costs, data restoration, cyber extortion, business interruption and regulatory proceedings, UKWA offers a free risk assessment and management tools for employee awareness and training.

UKWA offers members an exclusive cyber management programme in partnership with Perry Appleton Group and Travelers Insurance Company. Perry Appleton Group provides expert advice and support to help businesses to assess their cyber risks and to place the right cover for their business. Travelers, as part of their CyberRisk Insurance package, have an exclusive breach coach partnership with the law firm, Pinsent Masons. The team has over 10 years of expert experience handling hundreds cyber breach cases, providing a swift and effective response following a cyber breach.

For more information or to book your FREE risk assessment go to https://www.ukwa.org.uk/contact-us/ or email enquiries@ukwa.org.uk