Don't be a **victim**

According to the police, the typical transport and logistics business presents the ideal target profile for the cyber-criminal. Peter Shakespeare reports

The global cyber-attack of 12 May 2017 highlighted the vulnerability of our internet society and fragility of the business world dependent on computers. Its high-profile damage to large parts of the NHS network took public awareness to a new level.

But the scale of that single event was the exception, not the rule, according to the digital intelligence community; in fact, cyber-crime is a daily occurrence. Alarmingly, police in the UK say that 50% of attacks go unreported.

Most – 80% – of the UK road transport and logistics industry falls into the SME category. It is almost totally reliant on IT systems to manage operations: fleet, warehouses, compliance and business administration. Hauliers are right in the firing line.

According to Transport for Greater Manchester, those who hope to steal tractors, trailers or cargo may try to use cyber-attacks to break into transport managers' databases to determine loads, registration numbers, drivers' names, routes, destinations and cargo.

Combatting cyber-criminals is taking policing down new avenues. Unlike an old-fashioned break-in, where the culprit is likely to live in the area and most importantly is within the jurisdiction of the UK authorities, cyber-criminals are often based abroad. Even if police know where they are – and often who they are – they remain comparatively impotent when it comes to apprehending them and terminating their activities.

As a result, Hampshire Constabulary, like some others, has moved cyber-crime policing toward protection strategy, and now performs community outreach.

Hampshire's cyber-protection officer is Lucy Dibdin. She says: "Cyber-enabled fraud is the biggest threat when it comes to cyber-crime. It is estimated to cost the UK £193 billion per annum. Of this, £37.5 billion is attributed to public sector losses and £10 billion to individuals. The remainder is private sector business losses, with 80% of attacks targeted at SMEs."

She offers two examples of specific types. In **CEO fraud**, criminals impersonate senior company officials and coerce employees to transfer company money under the auspices of a legitimate business purpose. In **mandate fraud**, an impostor gets a customer to change a direct debit, standing order or bank transfer mandate, by pretending to be an organisation to which regular payments are made.

Criminals use a variety of means to gather information. This ranges from the theft of computer hardware such as laptops and USB sticks to blackmail

"In the case of the logistics industry around Southampton docks, for example, loads have been targeted by criminals, because they have gained information through social engineering"
Lucy Dibdin

and so-called '**sextortion**' – coercion involving sexual favours. Cyber-stalking and romance fraud are other ploys and the threat often involves someone from within a business.

Dibdin continues: "Cyber-crime terminology is alien to many of us. Most cyber-crimes involve a degree of '**social engineering**', or human hacking. This tactic exploits people's natural inclination to trust and is the easiest way to manipulate people so they give up confidential information." Common types of information sought are passwords or financial information.

"In the case of the logistics industry around Southampton docks, for example, loads have been targeted by criminals, because they have gained information through social engineering," she explains. "The information comes from individuals posting personal or work-related information on social media, disposing of confidential information irresponsibly, or simply being taken in by a seemingly innocent conversation."

She lists other common types of attacks. '**Phishing**' is where fraudulent emails are sent purporting to be from reputable companies. They often ask the recipient to disclose passwords or financial details. '**Vishing**' is the same practice, but over the phone. '**SMishing**' is via SMS messages, where the recipient can also risk downloading malicious software on to their phone or tablet. '**Pharming**' is the fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, to obtain sensitive data.

The list of cyber-threats also includes: **malware** (hostile software), **computer viruses** (software that primarily damages a computer), **worms** (self-replicating malware that more often affects a network), **Trojans** (malware that breaks into computers through deception), **ransomware** (malware that holds computer data to hostage), **spyware** (software that enables remote monitoring of a user's activities), URL hacking and Wifi router hacking.

The cyber-protection officer continues: "A golden rule is never share confidential information across a public Wifi connection. Another little-known vulnerability is **the open port**. Not all the ports on company servers are used. Business telephone systems are often also configured through their computer networks. Many firms leave computers turned on at weekends and at night. The criminals can use this time to access networks through these open ports."

When it comes to **phishing** emails, an eye for detail, common sense and a dash of scepticism will help safeguard potential victims. Dibden points out that bogus emails are rarely addressed to the individual, contain poor grammar and use informal language. Hovering the mouse over the sender's email address often reveals another email address behind it. As for **vishing**, she states: "No legitimate service or business will call and ask for personal details. They will never ask you to login to an account or ask for remote access to your computer.

"If you are even slightly suspicious, disclose nothing and hang up. Then contact the organisation the caller claims to represent by another means of communication. You might have thought you had hung up, but there are ways the criminals can keep you on the line. You end up talking to them again, but this time you say what they want to know."

SME businesses are targeted because they lack the understanding, resources and often time to implement protection measures. A busy haulage operation is a typical example and much lorry load theft results from the activities of cyber-criminals.

Concludes Dibdin: "Large corporates can survive cyber-attacks financially, but many SMEs are quickly wiped out thanks to fraud or data loss. None of what we recommend will guarantee you will not be affected by cyber-crime. But understanding the threat and protecting against it is the very best you can do to prevent it happening in the first place." TE

WHAT TO DO

Advice from cyber-protection officer Lucy Dibdin

1. Businesses must carry out risk assessments and clearly document procedures to deal with 'approaches' (potential cyber-attacks).
2. Staff must receive training and must report any approaches to managers; all attempts should be reported to ActionFraud, the UK's national fraud and cyber-crime reporting centre (*https://is.gd/golefo*).
3. There must be at least a daily system back-up, with data held on a standalone device, such as an external hard drive.
4. Most importantly, operating systems must be up to date, be protected by firewalls, anti-virus and malware software, and all system updates must be installed. Obsolete computers must have their hard drives physically destroyed.
5. Businesses should control access to computer networks. Each employee should have a personal login that is changed regularly. Passwords should be 10 characters containing upper and lower case letters, numbers and at least one symbol. The threat can be internal, so staff should also be aware of **shoulder surfing** and close screens down if they feel overlooked.
6. Computers and digital telephone systems should be shut down at night.
7. Businesses must have a continuity plan in the event of a cyber-attack.

FURTHER INFORMATION

https://www.cyberaware.gov.uk

https://www.getsafeonline.org/business

Cyber-security and the trucking industry, by GTG (2016) – https://is.gd/ajareh

Cyber-security for the automotive industry, by Vector (2016) – https://is.gd/yovoxe