Spring 2017 Vol: 2 No: 1

Resilience Matters

Here to help SMEs and sole practitioners

Contents

Resilience Matters is published quarterly by Camtek CSI, London.

Latest news may be found at www.cybersecuritylondon.com

Cyber security and hacking incidents are on the increase

The media has been highlighting for some time that cyber security and hacking incidents cause major disruptions to large corporates, banks and internet service providers.

Yet you cannot overlook the damage done by chance attacks to SMEs and sole practitioners.

Cyber-attacks may directly target your business, or you may just fall foul of a chance attack by doing something as simple as clicking on a malicious web link or downloading a fraudulent email attachment.

Many businesses just do not believe it will happen to them. (contd. page 2)

Are you ready to meet the requirements of the new EU General Data Protection Regulation?

Regardless of Brexit the new European Union General Data Protection Regulation (GDPR) becomes law in all member states, including the UK on 25 May 2018.

This invokes more harsher penalties for breaching data protection with fines of up to 4% of annual worldwide turnover and €20 million whichever is greater.

Article 50 to withdraw from the EU has now been agreed and the Government means to trigger it on 29 March 2017.

It is not yet clear what EU laws will remain and what laws will revert to old UK law or what will be modified. However, existing EU law is likely to remain until the UK has completed its exit process.

Cyber issues remain one of the main causes of data breaches and non-compliance. With these new higher fines coming, now is the time to review your security.

But training should be the key issue to keep front-end customer-facing staff aware and also brief senior executives and director/owners with what is waiting out there in cyber space.

According to the 2016 Cyber Resilience Report by the Business Continuity Institute, the top five causes of cyber disruption are;

- phishing and social engineering (61%)
- malware (45%)
- denial-of-service (24%) and,
- out of date software (21%)

It is important to realise that cyber security needs to be addressed at board room level and not left to an often out stretched IT department whose main job is to keep networks running.

Camtek CSI has two specific training courses dealing with these security matters. One is specifically designed for front-line customer-facing staff and the other is designed for owner directors and senior managers.

It can helps SMEs and sole practitioners with cyber security, business continuity and digital forensics issues by offering threat evaluations, consultancy and training.

We welcome enquiries and informal discussions without any obligation.

Cyber security threats lurking within every company

Your IT department works hard to ensure that your computer systems are working efficiently, data is backed up and software programmes and patches are up-to-date.

But there are other threats that can affect a business with more than one employee and they come from the inside.

- Employees – these are members of staff who unwittingly cause an incident purely through bad judgement.
- Ex-employees –who may hold a grudge against the company.
- External contractors – Many companies outsource parts of their business operation.
- Adding external devices – such as USB flash drives and BYOD devices.

Employees can cause incidents merely by downloading an email attachment, notably invoices or surfing malicious websites. Former employees may attempt to introduce malware or even copy sales databases either for themselves or to sell. External contractors often gain access to sensitive information due to bad management of password control or hardware security tokens.

Internal threats are possibly the most prevalent but they are also probably the easiest to foil. This can be by a strong audit trail, behavioral analytics and by using stronger passwords and two-factor authentication. Many businesses do not even change the default password on hardware items such as broadband routers and security cameras. (contd. p3)

There has been several recent reports showing that innocent devices, such as networked security cameras, have been infected to form part of a 'web-bot' network to launch a distributed denial-of-service attack on a major high street bank. Any device that has internet access, contains a processor and some sort of embedded operating system can be a risk.

Some companies are encouraging their employees to bring their own devices to work to hook up to the company network. Care must be taken as items such as USB keyboards and flash drives can hide nasty surprises.

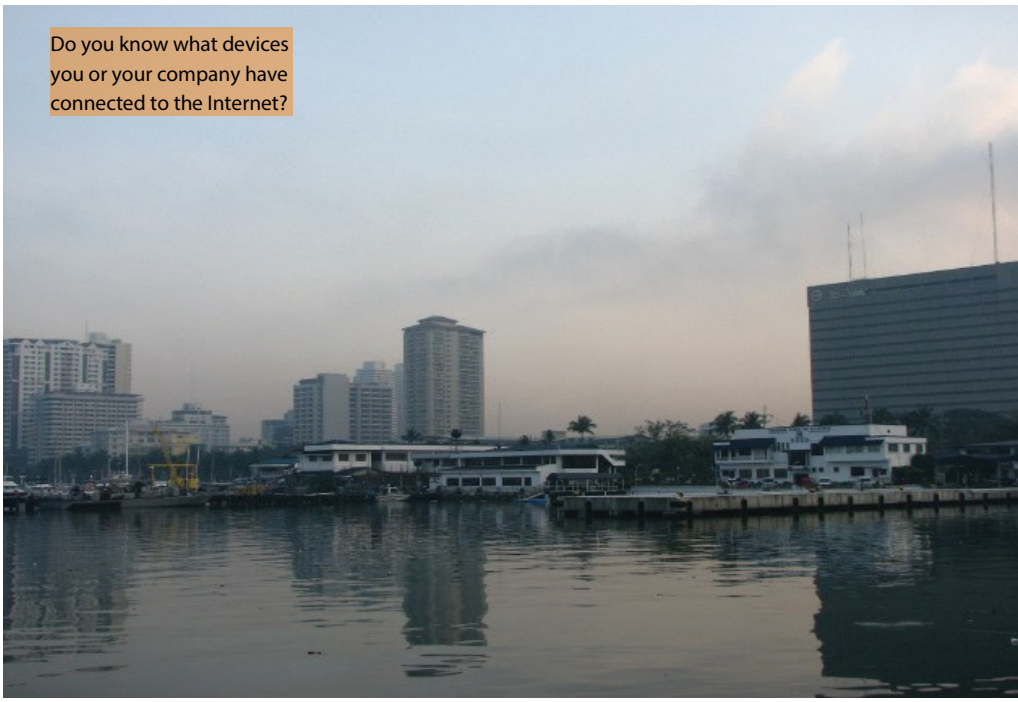
It is the human link that is always the weakest and the one that is likely to have the company's data encrypted by ransomware simply by clicking on the wrong link.

Businesses large and small need to be aware of what can happen and should have some sort of forensic readiness plan in place even in its most simplistic form.

Internet of things (IoT) – best advice.

Any device that has a built in processor, rudimentary operating system and a network connection can be compromised. Examples included smart fridges, smart meters, smart home interfaces and remote TV set top boxes.

Ensure all default passwords are changed to STRONG passwords and that services not required are DISABLED.



Last year the Internet was ambushed by domestic equipment

Last October cyber criminals used 'botnet' technology to connect home devices such as IP-cameras, DVR's, printers and baby monitors to launch a distributed denial of service (DDoS) attack against a company called Dyn in the United States. Dyn provides Domain Named Server (DNS) services to Twitter, Amazon, PayPal, Netflix and others.

DNS services provide the 'telephone directory' for the internet that link actual written web addresses to the IP addresses which computers and networks actually use. Without the 'telephone directory' being found these websites and services went down or worked intermittently. The home devices were infected with Mirai malware which uses around 550,000 'bots' and is designed to flood their designated target with so many information requests at the same time that their systems flood. The attackers used default passwords to gain access to online devices.

This attack, like so many others, compromised Internet of Things (IoT) devices and exploited the fact that most people just do not change the default passwords that manufacturers use to initially set their devices up. Such devices also very rarely have firmware upgrades to protect them unlike personal computers.

The best advice for anyone using these devices is to ensure that all default passwords are changed to prevent them from being remotely accessed. And this includes home routers which are the gateway devices to the home network.

DATA BREACHES – LinkedIn was hacked last May and over a million accounts had the password '123456'

Last year Yahoo admitted that in late 2014, 500 customers' data was hacked which included names, email addresses, encrypted passwords and more. In October 2016, TalkTalk was hacked 'with ease' due to technical weaknesses exposed in their systems. Six people under the age of 21 were arrested – basically 'bedroom hackers' eager to impress their friends. The list is endless.

Despite repeated pleas from the security industry and the media, people often just use easy-to-guess passwords, such as the name of their pet – and reuse them on several accounts. If one account has been compromised then all of the others have been compromised as well. In May 2016 a hacker known as 'Peace' attempted to sell 117 million LinkedIn email addresses and passwords that had previously been stolen. It was later found that more than a million of the stolen passwords were **'123456'.**

The issue of password security comes up time and time again. This is why many providers, including Google, Apple and Microsoft now offer two-factor authentication. This requires the user to input a code sent to a hardware device (banks do this) or a code sent to a pre-designated mobile phone. Two-factor authentication enhances security but only if it is required and not if it is just an option. The fact that TalkTalk was fined £400,000 by the UK's Information Commissioners Office highlights the need for cyber security to be a boardroom issue.

If you have any comments or would like to know more – we are here to help. Why not call us?

Camtek CSI – London W1B 3HH
t: 020 3642 9373 tw: @camtekcsi
enquiries@camtekcsi.com
www.cybersecuritylondon.com