BANDIT COUNTRY

In an IT world without obvious boundaries, **Amar Singh** explains how to avoid cybercrime and bounce back after an attack

The internet has undergone massive changes in size and complexity in the last five years. More appropriately termed 'cyberspace', it is best described as a loose-knit federation of nations and commercial organisations, albeit without a central authority.

A digital landscape with no boundaries, no immigration controls, no enforceable laws and, more importantly, no single governing body, cyberspace is abundant with both significant opportunities and considerable risks. Cyberspace is the lawless wild west, with multiple opportunities offered to cybercriminals.

Where cyberspace offers tremendous commercial opportunities for growth, there also lurks, in its vast and digitally barren landscape, an astonishingly aggressive, dangerous and bold enemy. Where, on one hand, a business can significantly improve customer satisfaction by social media interaction, increase revenues online and expand its business to touch every single cyberspace consumer in the world, it can very easily fall prey to any one or more of the millions of predators roaming the cyber underworld. These predators have the skill, ammunition and, in many instances, the full backing of sovereign nations or organised criminal gangs to wipe entire digital businesses, steal top-secret intellectual property or compromise a customer and corporate sensitive data.

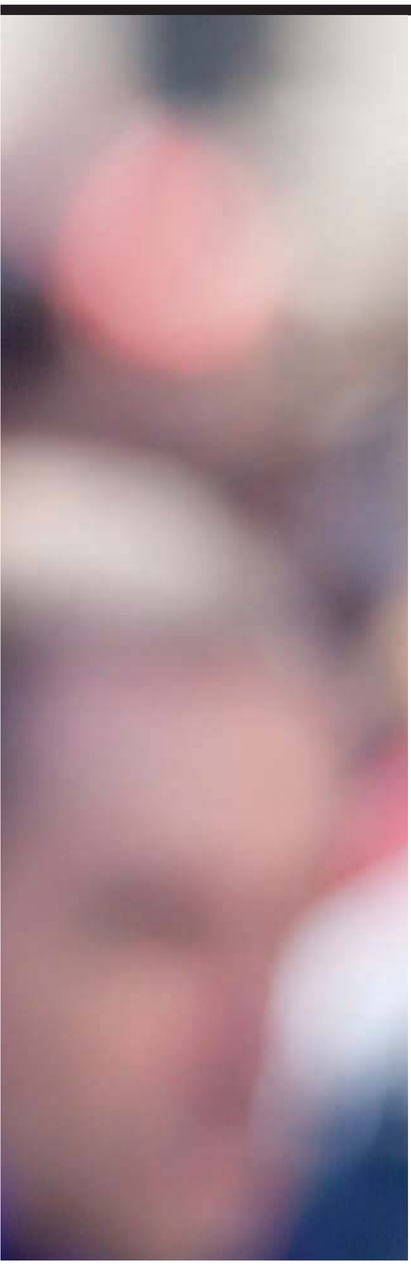
In most cases, the crimes committed in the real world are very similar to the crimes in cyberspace. Consider some examples:

- The theft and consequential online sale of millions of customers' credit card data, including numbers, addresses.
- Illegal online money transfers carried out by sophisticated software installed on an unsuspecting user's computer without their knowledge. This software then intercepts a secure banking transaction and starts moving money to a known account. Imagine this repeated a million times over.
- An anti-capitalist campaigner compromising a tax firm's computers and stealing all its customers' tax returns, their names and their incomes and publishing everything online.

TIME TO FACE THE FACTS

Given the increasing reliance on cyberspace for all types of business transactions, it is vital for organisations to accept the following cyber-truths:

- Your organisation, however small, will - if it hasn't already - fall victim to one or



multiple cyber attacks. ISACA's white paper, *Advanced Persistent Threat Awareness: Study Results*, addressed this in its global cybersecurity survey of more than 1,500 security professionals (bit.ly/VULp4P). The study found that more than one in five respondents said their enterprise has experienced an advanced persistent threat (APT) attack. More than 60% of survey respondents say that it is only a matter of time before their enterprise is targeted. Senior members and executives of the business accepting this fact is the first step towards a working resiliency plan.

- The "baddies", who are often supported by nation states or powerful criminal gangs, are going to be better equipped and trained than the regular IT professional. Consequently, the employees must accept that simply trusting your "techies" and, consequently, laying blame after an incident serves no purpose, and any such actions may have damaging consequences.
- Accept that those who manage your critical systems (the system administrators, the database and spreadsheet managers) may be likely perpetrators of cybercrime. A disgruntled employee with keys to your kingdom's jewels is almost as dangerous as a random cybercriminal opportunist.

TYPES OF CYBERCRIMES AND ATTACKS

Although it's not essential to spend time in the "technical weeds", organisations must be aware of some of the more popular types of attacks carried out by cybercriminals. Attacks can vary from criminal digital trolling or stalking to sophisticated and organised attacks that not only affect the bottom line of a business but have the ability to cripple the economy of whole nations, albeit the latter type of attack has not officially taken place as yet.

Here are the three most common types of attacks that affect commercial and, in some instances, personal users.

Network-based attack

Network attacks are less sophisticated than the other attacks described here. However, a network denial of service attack, where a system or a website becomes unavailable due to continuous attempts to "clog the pipe", can be extremely damaging to a business. Furthermore, a sustained, long term or distributed denial-of-service attack can cripple the most well-equipped online businesses.

Spear phishing attack

The computer, the host, the tablet and the mobile - simply called, "the device" - is an extremely valuable target for a cyber attacker of almost any skill, as it holds personal and corporate data including emails, documents, spreadsheets, passwords, photos, video and audio recordings. It's also "the device" that has access to the intellectual property, the technical plans for the next big thing. Importantly, all devices are now interconnected in some way or the other – think wireless, 3G/4G and Bluetooth connected constantly to the corporate network, to the top-secret assets, to the public internet, the social media networks, the home network, the wireless network in the coffee shop and the airport.

Once an attack is successful and the device compromised, an attacker has access to a treasure trove of data, both corporate and personal.

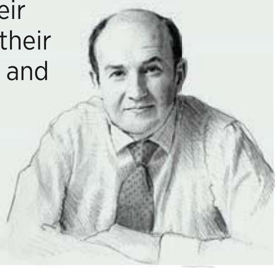
You may ask yourself, "what has spear phishing got to do with my device?" Often, the easiest method to attack and gain control of a device is spear phishing. An attacker will harvest all publicly available information about a target's likes and dislikes, travels and tours, friends and foes and - quite literally - produce a mini biography of the victim's life. All that's required then is a personal email to the victim with a title that reads something like "Thanks for visiting us at the Ski Club last month, here is a special thank you from us". Attached to this email is a nasty, malicious piece of code hidden in a PDF titled "Special thank you for visiting.pdf" that the victim - who has just returned from a skiing holiday at the Ski Club - has no reason whatsoever to doubt the origins or intentions of the contents.

On opening the PDF file, the victim's computer device will be infected with what is commonly called malware (malicious software). This malware will - depending on what the attacker wants it to do - either go on and find another target or start stealing sensitive data and digitally shipping it to the attacker's cyber enclave. The recipient may think that only

Comment from Michael Izza:

"You don't need to be a large organisation to find yourself under attack. A UK-based study from PwC showed that three quarters of UK SMEs, and 93% of large ones, had recently suffered a cybersecurity breach.

Cybersecurity is something that should be at the top of every chief executive's agenda. It's a big issue that will only get bigger as we become more dependent on complex technology. Equally boards need to understand the risks and plan ahead because cyber attacks are a very real threat to their reputation, their bottom line and their share price."



DAN MURRELL

Michael Izza
ICAEW chief executive

a few smart cybercriminals would have access to this type of special malware. There is no need to create the software; on the contrary, this kind of malware can be easily bought in the cyber underworld for as little as a few hundred pounds.

The human attack

Humans will always remain the weakest link, and of great concern today is the privileged user. This user can be anyone who has privileges and rights to access, copy and/or modify customer confidential data; can add or create users on business critical systems; and can make changes to IT systems like apply patches, backup and restore data.

The privileged user is very often an insider who knows the business and has been with the business for many years. Think about your sales executive with access to all your customers, a purchasing manager with relationships with your suppliers, the office techie who just does all the IT stuff. Recovery from this type of attack can sometimes be the trickiest, primarily because these insiders have the benefit of access and the trust of the business. They also have the ability to cause maximum damage, making a quick recovery that more difficult. Beware the scorned employee.

PROTECT AND RECOVER

Cyber resiliency is not just about making sure you have access to a set of new computers, for example if your employees lose their old ones on the train or if you're having an offsite backup of all your data. It's more than just having a remote access virtual private network solution for when the snow causes the usual travel chaos. Some may argue that having a Citrix thin client solution where you allow an employee to use any computer, regardless of manufacturer, to access the company's applications regardless of location and distance is the right course of action. However, to achieve true resiliency, an organisation needs to understand exactly what technology, systems and data underpin the business.

Given the existence of significant risks in cyberspace, how should one go about planning to recover and bounce back from a cybercrime? It's achievable, although not straightforward. Consider a domain name system (DNS) poison attack scenario that causes your e-commerce website that sells tax-saving information to customers to display images of ladies scantily dressed. This attack could cause significant loss of business and reputation. What use would a secondary business site or offsite data backup tapes be during this dynamic DNS cyber attack where every second your site is serving the wrong content may cost millions of pounds of loss?

What is required is being aware of these types of threats and risks and having mitigating plans to swiftly bounce back. DNS is the technology responsible for ensuring your website is reachable when someone types your web address in the internet browser.

CHECK THE PATTERNS

Ask yourself what is normal and abnormal in your organisation. Have you noticed your computer starting to update its software and thought "that never happens on a Monday?" but carry on when the update dialogue window disappears? Alternatively, have you noticed your senior sales executive, who never comes to the office before 10am, coming in and logging on at 8am?

Organisations tend to develop unique and specific work and play culture. An acceptable 3am email from a database admin to one organisation may raise a red alert on the radar of another. Every organisation needs to understand what is normal and acceptable, for its employees, customers and even what is a normal day in the IT lifecycle.

Operation cyber taskforce

Gerry O'Neill, former CEO of the Institute of Information Security Professionals, has a six-point plan for cyber resilience

Firstly a definition ... Nigel Inkster from the International Institute of Strategic Studies defined cyber resilience as: "The ability of a system or a domain to withstand attacks or failures and in such events to re-establish itself quickly."

The key capabilities needed to achieve this are:

1 Organisational readiness

The first step in securing your business against cyber crime is about corporate awareness and ownership at the C-level. Understand the hyper-connected context of your business and the risks, with a key focus on the risk to what's important – your information and reputation.

There is great value in sharing intelligence and experiences with other organisations, learning from professionals elsewhere how they got hit, what damage was done, how the crime was detected and how they are planning to keep similar attacks at bay in the future.

For Employees, consider:

- Does a manager ever log on from home at 1am to copy or email a spreadsheet or Word document?
- Is the laptop the database administrator using corporate-issued? (Depending on your policy you may allow employees to use their own machines, but you should know if that is normal behaviour).
- Does your outsourced service provider normally carry out computer or system patching on a Monday?

> "Humans will always remain the weakest link, and of great concern today is the privileged user"

For an online business you may want to consider:

- Is a customer purchase of £10,000-worth of widgets normal?
- Why have the online sales of widgets suddenly dropped dramatically?
- Why does your website start to show a collection of random images?

DEFINE AND REVIEW YOUR PLANS

Is business continuity (BC) the same as resiliency? Some may argue that having a business continuity plan (BCP) means that you are resilient, but I disagree. To complicate matters, some cross reference IT service continuity with business continuity. The fact is that IT service continuity underpins an organisation's business continuity plans. (The reader is encouraged to explore the BCP and IT service continuity management (SCM) requirements for their organisation, if they currently do not have any contingency planning in place). Cyber resiliency involves bringing together both BC & IT SCM functions - the metaphorical alignment of several planets and moons to ensure a truly resilient plan.

WHERE ARE THE CROWN JEWELS?

Define, secure and protect the most critical assets, including customer, credit card and commercial data. Have your system administrators, the database or spreadsheet administrators, or customer relationship management (CRM) administrators been CRB checked? Have you checked who has access to your salesforce.com or other CRM platform? Do you have a watertight information security, acceptable usage policy?

KNOWLEDGE IS KEY

A business can benefit hugely from having their staff in charge of cyber security properly trained and better informed. In addition to staff retention, training may also offer better career prospects to staff, whilst building a level of loyalty and allegiance to the business.

Consider the knowledge training and certifications from industry leading organisations, including the Certified Information Security Manager (CISM) (bit.ly/hXFD2b) designation and control objective for information and related technology (COBIT) (bit.ly/GTrbQO) from ISACA. A CISM-certified employee could help your business by providing a comprehensive view of the management of information security. A COBIT 5-trained employee could help provide an end-to-end business view of the governance of IT within your business.

Amar Singh, CRISC, CISSP, is a member of the ISACA London Chapter Security Advisory Group and CISO of News International

2 Situational intelligence

You need to have specialist knowledge and monitoring of the latest advanced threats. Today these are a lot more sophisticated and coming from more clearly-defined attack sources.

In the early hacking days attacks came from somebody seeking fame and glory. We had the archetypal image of the spotty-faced teenager with a modem working his way into the Pentagon. Things have moved on significantly.

Cybercrime moved quickly into monetisation, and criminal gangs got involved. We have had a few years of protest 'hacktivism' with groups such as Anonymous and Lulzsec attacking corporate and government infrastructures. Recently - and more seriously - we have had the emergence of significant evidence of corporate espionage, and state-sponsored espionage and disruption.

3 Cyber defence

You need a grip on infrastructure and access security - both physical and technical - as well as staff awareness. You should be strict on access control and remote access control for people who use laptops. Ensure strong visitor procedures for your key buildings and facilities. One of the features of a number of the recent attacks has been staff infiltration, either duping staff to carry out actions or recruiting them with bribes and inducements.

Don't lose sight of basic security here - you should have a routine of changing passwords regularly. If you refresh your infrastructure, modify the way your network is configured and move the shape of the target, you can deter and block a potential long-term attack.

4 Detection

Know when you've had an attack. You should have in place an effective monitoring process, internally and externally. Scan outbound messages for significant volumes of information in order to check for abnormalities in the normal pattern. It helps you to detect whether you have information that's being stolen and, if something is compromised, knowing that it is compromised is the key to early reaction.

5 Mitigation and containment

Part of your role here is to limit the damage to your services and reputation, by limiting the impact or shutting down the source. Having a prepared plan, including PR statements, is key. A number of organisations have really badly mishandled the PR of recent attacks. Ask yourself when it's good to release the news – or if it's a good idea to release it at all.

6 Recovery

The ability to re-establish normal service can be critical to your survival as a business. This includes applying the lessons learnt and feeding back to senior executives. Say, "Here's what happened to us, this is how we reacted, and this is what we've done to prevent or mitigate it, should the threat reoccur."