PROTECTION GROUP INTERNATIONAL

Unless we normalise the cyber threat we can't manage risk

Education and normalisation are the keys to tackling the cyber threat, says **Matthew Olney**, communications and content executive at PGI

On New Year's Eve 2015, the BBC's website was knocked offline. Immediately social media was abuzz with rumours and it wasn't long before the press got involved. Headlines blamed the so-called Islamic State for the attack. In reality, it turned out to be the handiwork of anti-IS hacktivists who were testing their capabilities. Either way, the question remains whether a simple piece of temporary online vandalism merited the media profile it generated.

People fear what they do not understand

Cyber is a word that can cause the mind to race. A "cyberattack" is as dramatic as whatever an imagination makes it. With the right stimulation, "cyberattacks" make good headlines and great scare stories. The best way to tackle the threat posed by cyber criminals is to educate people so that they understand how such attacks occur and in turn learn how to counter them. If we regard cyber crime in a similar context to, say, burglary, immediately the threat becomes normalised.

Every decision we make in our lives – be it conscious or subconscious – is based upon some kind of risk assessment. Unless an understanding of the "new cyber threat" is thorough and widespread, the associated risk will continue to be seen and treated as extraordinary.

In the 21st century, where technology underpins just about everything we do and use, this is an unsustainable and unaffordable position.

In business and government worlds this lack of understanding continues to be relentlessly exploited by an IT security industry that perpetuates the idea of dramatic and increasingly apocalyptic consequences if its new security technology is not adopted. The industry continues to use the same hi-tech, complicated scare language that it adopted in the run-up to the millennium that burned its credibility and confidence in its integrity.

The real-world consequence of this lack of understanding and consumer scepticism is that the take-up of cyber security risk management is far slower than it should be.

Perhaps, unlike Y2K, there are genuine threats and risks which are, and will continue to be, an inherent and perpetual aspect of adoption of technology. There are always people who will seek to exploit good things for nefarious or criminal means, and technology is no different. But that doesn't undervalue the huge benefits of adopting technology. Nor does it mean – just like with all other security risks – that the threat is anything to fear disproportionately.

For years, law-enforcement agencies have educated the public on how to protect property from would-be thieves, and just like with conventional crime there are measures that people and organisations can take to prevent themselves from becoming victims of a cyber crime.

The risks vary hugely, depending on the environment in which they are considered and, again, just like with other security risks, proportionate treatment of them for the vast majority need not be expensive, complicated or anything other than a normal cost of living and operating in the 21st century. Even for those such as banks, the defence industry, some government departments and other industries where the nature of the threat is more complex and has more impact, effective risk management need not be any more challenging.

Let's tackle crime

Cyber crimes are the most common in, but only one part of, the spectrum of activity referred to as cyberattacks. But such incidents aren't "attacks". They are theft, vandalism, blackmail or ransom – or, indeed, any version of illegal activities that have plagued society for thousands of years. The main differences between "cyber crime" and "conventional" crime is the scale of effect that can be achieved.

Conventional theft is limited by how much swag the perpetrators can physically carry. Cyber crime is not.

Conventional crime, unlike cyber crime, often can be investigated and solved within one national jurisdiction. Cyber criminals can carry out crimes against their victims simultaneously, very cheaply and without necessarily leaving "home".

Does that sound scary? It doesn't have to be. The police and other agencies are very good at thwarting conventional crime. They've had many years to develop new methods of crime-fighting, from taking fingerprints to DNA profiling and other sophisticated techniques.

The same principles apply to cyber terrorism, cyber warfare, online activism, etc – each sits at a different point on the cyberattack spectrum.

Normalising the hacker

The portrayal of hackers in the media conjures up evil masterminds or sophisticated military units based in some secret bunker, and surrounded by racks and racks of highly expensive and sophisticated equipment.

Of course, many do work for nation states, subversive or proscribed organisations or sophisticated international criminal gangs. Yet many hackers are bored teenagers experimenting and operating out of their bedroom or their parents' basement, or they are ordinary, self-taught criminals who find this type of crime somewhat less arduous than others.

Just like any other opportunistic thief, these hackers would rather attempt to steal from an easy target. And just like other types of criminal, they rely on their victims' naivety and carelessness. When looking for a target, a hacker will typically choose something that will not require too much effort to attack.

As with any regular criminal, if they think security is too tight they will move on and seek out easier prey. If every person and organisation puts effective, basic security into place, the number of incidents we see so frequently will fall. By demystifying hackers and their mindset, they won't seem as scary.

Knowledge is strength

To quote one FTSE-100 chief executive: "This debate is controlling us, not vice versa." Effective education, underpinned by informed investment in the right things at the right time, will place control of the debate, as well as the solution, back in the right hands.

PGI aims to be a major contributor in helping to normalise the new cyber security threat.

All of our instructors are established cyber security professional who hold leading industry certificates and have a wealth of real-world experience. They combine their teaching with daily operational activity, keeping their knowledge and training material fully up-to-date and relevant.

Whether you are a small company or a large organisation, we have the skills, experience and expertise to offer businesses and governments tailored solutions that will make the difference in tackling the threats posed by cyber crime.

PGI believes in education and awareness. In addition to training cyber security professionals, cyber security education and training for mainstream IT professionals, users and executives stand at the core of our posture.

To assist with this, PGI opened its Bristol-based Cyber Academy. The Academy is a custom-built, multi-functional learning environment, offering the most sophisticated training on the market in techniques for cyber defence, cyber threat intelligence analysis and organisational leadership roles, with training delivered both on and offsite.

We hope that increasing awareness and education will lead governments, law-enforcement agencies, businesses and the public to adopt the right posture.

Cyber crime is nothing to be complacent about, but neither is it anything to fear. It is simply one of the modern risks of operating in the 21st century.

www.pgicyber.com
Telephone: 0845 600 44 03
Email: enquiries@pgitl.com