Image: iStock/162572497

# COMPUTERS AREN'T EVIL

Surprising at it may seem no computer or robot has yet been charged with a crime, let alone convicted, or punished or brought to justice in any other fashion, says Paul Jagger FBCS CITP, Secretary of the BCS Learning and Development Specialist Group.

Contrary to the plot of many a sci-fi film there is no army of megalomaniac cyborgs, clones or stormtroopers intent on galactic domination, and there is no rebel band of extremist computers using the internet to further their political ends.

Rather it is humans who are responsible for all criminal, extremist, hacktivist or terrorist behaviour in cyberspace. It is humans who conceive, plan and execute cybercrimes, and humans are the targets and victims of those behaviours.

**Cyber education for all**

How do we protect ourselves in cyberspace? The answer can be found in education. The responsibility to increase our awareness and knowledge of cyber security lies with all of us, and not just our governments and employers and certainly not with the police or criminal justice system.

A whole society response is needed in order to tackle the fast moving and pervasive threats. As individuals we should beware of the dangers we face in cyberspace and understand the responsibilities that we have to protect our own information and that which is entrusted to us.

The best estimates available from the IT industry and government agencies engaged in defence against cyber threats show that the majority of the risks cannot be tackled by the application of technology alone, nor by the skills of IT professionals specialising in security. Clearly technology and specialist skills have a role to play, but we cannot rely on them to provide anything approaching an adequate defence, especially when so many of the risks are borne out of human behaviour beyond the control of technology.

Only by changing behaviour can society manage the risks and threats in cyberspace and the way humans change their behaviour is through an unending journey we call learning. The IT profession must be at the vanguard of that learning journey, raising cyber security awareness, knowledge and skill throughout society in general, and within the IT profession in particular.

Significant challenges to changing behaviour in cyberspace exist. Perhaps the greatest is the false perception that cyber security is a deeply technical subject, it is all too easy and common for cyber security to be seen as a complex subject that is someone else's problem to deal with. We also labour under the misconception that if our own actions in cyberspace are entirely legitimate and honest that we are not likely to be a target of cyber criminals, so even taking the simplest of actions seems boring and pointless.

## Clearly cyberspace has become a hot warzone in which nations attack the economic interests and governments.

Lastly the vast array of fast evolving cyber threats seems to present a problem so enormous that we cannot possibly grapple with it. We have to dramatically lower these barriers and demystify cyber security so that we all take the simple and effective measures we know we should, such as using difficult to guess passwords and encrypting data that we don't want prying eyes to see.

The UK government Centre for Protection of Critical National Infrastructure (CPNI) provides advice and examples of good practice that we should all be able to understand and act upon to increase our cyber security skills:

www.cpni.gov.uk/advice/cyber/

**How serious are the threats in cyberspace?**

Cyber security stories are much in evidence in the press and media. It seems that not a week goes by without a multitude of cyber-attacks receiving coverage in the news. The financial press and IT industry journals continue to be awash with articles on cyber security reflecting a growing awareness and interest among businesses, government agencies and the IT profession.

The spectrum of cyber threats now varies from the familiar but rather unsophisticated email phishing scam that targets the gullible and the greedy to highly sophisticated and coordinated attacks on vital national infrastructure sponsored by governments and extremist groups.

Between those two ends of the spectrum are a myriad of intermediate threats from identity theft, to large-scale online fraud, and industrial espionage to highlight but a few. In December 2013 Dell Secureworks reported that over 250,000 PCs had been infected by Cryptolocker ransomware, with the US and the UK being the most infected countries. The ransomware encrypts data on the users' PC and attempts to extort payment in order to unlock the data.

However, not all threats are motivated by malice, many an inadvertent information security breach has been the result of simple human error or motivated by a trusted individual with legitimate access to sensitive information leaking it to the press for their own idealist motivations. The examples of Bradley Manning and Edward Snowden show that technology alone will never be an effective countermeasure to the motivated individual intent on sharing confidential information.

**Cyberspace - now a virtual war zone**

Nation states see cyberspace as a legitimate theatre for the projection of political and military power.

By way of example, in March 2013 the South Korean banking system and several TV stations were severely impacted by a cyber terrorism attack that infected an estimated 32,000 computers and was believed to have been launched from North Korea. Later in the year there was a similar coordinated attack against the website of the South Korean Presidential office and other official government and media related sites. These followed similar attacks in 2009 and 2011 that are believed to come from sources in North Korea.

In February 2013 cyber security firm Mandiant identified a secretive unit of the Chinese Army as possibly the most active and prolific state body engaged in cyber espionage, having at that time attacked 141 companies in 20 industries, with 87 per cent of the targets in the English speaking world.

Clearly cyberspace has become a hot warzone in which nations attack the economic interests and governments of their enemies.

The seriousness of the cyber threats to

doi:10.1093/itnow/bwu019 ©2014 The British Computer Society

the UK national interests was underscored in September 2013 when the UK's Secretary of State for Defence announced the formation of a Cyber Defence reserve forces unit to support their regular counterparts, part of the £1.2bn being invested in transforming the UK reserve forces between now and 2020. Clearly both the diversity of threats and the awareness of them have increased, and will very likely continue to increase as the internet of things becomes a reality and access to mobile computing becomes pervasive. Our ability to counter such threats needs to be as diverse, dynamic and sophisticated as the challenges cyber security presents.

**Cyber security - not just for the IT guys**

Headlines that employ phrases such as cyber-attack, cyber security, cyber defence, cyber terrorism and the latest incarnation cyber streetsmart all add an aura of technologically advanced black arts to any article.

Whilst the word cyber may be attractive to editors in the press and media, it is misleading and counterproductive to label cyber security as an issue just for deeply technical specialist IT practitioners that is beyond the understanding, interest or responsibility of mere mortals.

This perception exists as much in the boardroom as it goes government corridors and society in general. Cyber security has become synonymous with a problem for the IT guys to fix, and within the IT profession it's a problem for the IT security specialists to fix. This perception is akin to believing that all threats of security to property are a problem for the police to fix.

The cyber label is one that gives the impression that the cause of cyber security threats and the associated counter measures are deeply rooted in technology. The reality is that no technology will ever provide a complete defence against a motivated and knowledgeable human intent on doing harm. All threats in cyberspace stem from the motivations of humans – a crime committed using the internet is still perpetrated by a human criminal.

As access to technology increases, so the opportunities for crime, hacktivism, extremism and terrorism being conducted in cyberspace increase.

For right or wrong cyber is the catchy short-hand that has stuck, and one we have to live with, but the cyber security is not a matter just for a sub-group of IT specialists (although they have an important role to play), rather it is a matter for all of us since we are all, individually and collectively, the target of cyber security threats. Acceptance of this reality is the first step on our shared learning journey.

Image: iStock/163881431

**Cyber security - it starts with us**

Most low-level and common information security risks are related to the behaviour of the users that access the system, whether they are internal or external to the organisation concerned. For example, I once sat, unsupervised, in an office at a police station in the UK where there was a hand written sign on a wall that read 'The password to the neighbourhood watch computer is...' With this sort of behaviour evident in a police station, cyber criminals don't need to be particularly sophisticated.

We are all responsible for the confidentiality, integrity and availability of information we are entrusted with.

We are all responsible for the confidentiality, integrity and availability of information we are entrusted with, whether it be a posting on a social media site, our own banking details, passwords for systems we use at work or the commercially confidential data of our clients. The advent of mobile computing and work environments that support bring your own device access to IT systems places greater responsibility on the individual to take appropriate measures to secure access to information at home, on the move and in the workplace.

Just as we are all responsible for the security of our homes and our families – we are responsible for our cyber security and those we hold a duty of trust to. Most large employers and government departments now have policies, procedures, education and IT solutions in place to help employees reduce the risks of a cyber-attack upon corporate assets. They will also likely have specialist IT professionals tasked with the technical aspects of cyber security and a governance framework in place with senior leadership accountable for security. Small and medium businesses are perhaps more exposed, with limited resources, a lack of senior level leadership, absence of governance and little education available for employees.

**Time for a global skills framework**

The need for better awareness, education and skills in cyber security is not aided by the proliferation of competing standards, professional bodies, industry and government standards for cyber security skills in the IT profession. It's time for the IT profession to get its own house in order where cyber security skills are concerned.

There is currently no common view within the IT profession, or among government agencies, of the skills required of a security specialist, with different governments (and even departments in governments), professional bodies and certification providers emphasizing different aspects of cyber security – some broad, some narrow, some deep, some shallow. To employ a navigational analogy there is no map and no agreed scale or legend of commonly accepted landmarks for cyber security skills, making it extremely difficult to plan a learning journey or track progress.

The UK government and intelligence community have, for example, adopted an approach that emphasises information assurance as focus of cyber security, with the CESG Information Assurance Certification being a license to practice in the public sector.

The Institute of Information Security Professionals (IISP) in the UK has developed its own skills framework linked to various certificates. ISACA has its Certified Information Security Manager (CISM) qualification, and ISC$^2$ has its Certified Information Systems Security Professional (CISSP) qualification. These are but a few of the many different organisations and qualifications available to the IT professional choosing to specialise in cyber security.

What the IT profession needs now is a single, unifying global skills framework that recognises cyber security as an integral aspect of the wider IT profession, one that touches all aspects of IT practice from strategy and governance to user interface design and maps out the different paths on the skills journey.

Since cyber security is not a specialism clean and apart from the rest of IT, and certainly not apart from the wider needs of the information society the tried, tested and globally adopted Skills Framework for the Information Age (SFIA) model would seem to be the ideal model to bring together the existing standards, skills definitions and qualifications.

With consultation on SFIA version 6 about to commence, now is the time to bring a little order to the skills and qualification framework for cyber security professionals.

**www.bcs.org**