CHALLENGES FACED IN THE E-CRIME DOMAIN

As a society, we tend to focus on the positive uses of technology. Yet, with its abundance, we can no longer overlook that its increased usage and advancement has also resulted in its misuse.

Dr Ibrahim Baggili reports

We cannot ignore the continuous advancement of technology. Twenty years ago, a computer was in no way more powerful than today's mobile phone. Today, computers have become compact, powerful, networked, and mobile. As a society, we tend to focus on the positive uses of technology. Yet, with its abundance, we can no longer overlook that its increased usage and advancement has also resulted in its misuse.

E-crime has become a priority around the world for many governmental agencies, private sector, and public sector organisations. The amount of e-crime is constantly increasing as humans continue to become technology-dependent. The next time you are in public, cautiously observe the number of mobile phones that people carry, and you will notice that technology has become so intertwined with our lives that we no longer consider it a luxury, but a necessity. In the United Arab Emirates (UAE) for example, according to the latest statistics on NationMaster.com there are 7,595,000 cellular phones in the UAE when the reported population is 4,621,399. This illustrates that the number of used cellular phones in the UAE exceeds the number of people by 39%.

Key challenges

Over the last couple of years, while I researched e-crime and cyber forensics, I have observed several key challenges, the first being our extensive reliance on the technological aspects of e-crime in both research and industry. I will not be the first to remind readers that all crime, be it an e-crime or not, cannot and will not exist in a vacuum. A computer alone does not commit an e-crime without human interaction. Therefore, it becomes imperative to take a strong step towards understanding the psychological and societal impact of technology on humans, especially in the e-crime domain.

The next challenge I have seen is the lack of a common body of knowledge in the area. Based on my experience, we see dispersed conferences, magazines, academic journals and other sources of knowledge in this realm, and

> Encryption, with its many advantages in the corporate world and in the public sector, poses challenges in investigating e-crime, especially now that encryption is moving towards being implemented at the hardware level.

because of that, we continue to witness a rise in the lack of a collectively-accepted body of knowledge.

Think of the word e-crime for instance. Ask yourself, how many synonyms exist for this term? Cyber crime? Cybercrime? e-Crime? Digital crime? Internet crime? Computer crime? Information crime? Technology crime? High-tech crime?... and perhaps many more.

Other than e-crime synonyms, what does e-crime mean? Is it a word used to denote crimes enabled by technology? If so, are they networked technologies? What if a crime took place on a system that is not networked? Furthermore, what if corroborating evidence was found on a digital device – but that device was not used to commit a crime? Is that part of e-crime?

The points I have attempted to demonstrate in the abovementioned examples portray the lack of a collectively-accepted body of knowledge and agreed upon definitions in the e-crime domain.

The third inevitable challenge is the continuous change and advancement of technology. This poses a challenge for e-crime investigators, especially in cyber forensics. Today we find a solution to forensically acquire and analyse a certain device, the next day a new device is released. This is escalated by the proprietary nature of many of the devices.

The fourth challenge is encryption. Encryption, with its many advantages in the corporate world and in the public sector, poses challenges in investigating e-crime, especially now that encryption is moving towards being implemented at the hardware level. This is a future challenge, and in my opinion, an issue which will always exist. At the end of the day, encryption is strongly tied to the notion of personal privacy, which is another challenge in the information assurance area.

The fifth challenge, which could mainly affect non-English speaking countries, is the lack of education and knowledge base in information security, and e-crime in languages other than English. That, accompanied with the lack of an agreed upon body of knowledge, creates a core dilemma when one attempts to disseminate that knowledge in non-English speaking countries.

The sixth inevitable challenge is the law. Only the law delineates what a crime is, and from various international research efforts, one can conclude that law systems are generally behind when it comes to covering and defining e-crimes. This challenge commonly stems from the fact that law systems are not easily revised. Additionally, the advancement in technology may cause criminals to pursue e-crimes that are not covered under the law.

Consider the well known ILOVEYOU worm for instance, which caused estimated billions of dollars in losses in 2000. When the worm was traced, it was found to have originated from the Philippines where the creators were found. After the criminals were discovered, all charges against them were dropped because there were no e-crime legislations in the Philippines at the time of the incident.

Summary

To discuss the challenges in the area of e-crime is beyond what I am trying to portray to the reader. What I would like to stress on however, is the inevitable need for all professionals, private sector, public sector, and academics to take a positive move towards collaborating and working together as a team in order to understand what this e-crime phenomenon means, how it truly affects our lives, and most importantly how we can combat it.

It is only through organised conferences, meetings, workshops and the establishment of credible international collaborating bodies that we can come together as a community in order to fight e-crime. With meetings like e-Crime Middle East, we take a positive step closer towards mitigating some of the aforementioned challenges. It is our duty as professionals to improve the e-crime discipline by carrying the burden of advancement on our shoulders. I urge the entire community to stand up, and join forces to combat this grand challenge. We should no longer remain in our own silos; all e-crime stakeholders should come together and work towards the future constructive progression of the e-crime domain. ■

Dr Ibrahim Baggili is Assistant Professor and Director of the Advanced Cyber Forensics Research Laboratory at Zayed University, Abu Dhabi, UAE.