Fighting CyberCrime

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions? Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

Cyber-crime is a term that covers many types of illegal activities through the Internet. Global cyber-crime continues to grow and target citizens, businesses and governments. In 2014 it started to focus more on big attacks on financial institutions and companies rather than individual users.

The increase in the use of mobile devices and applications has created opportunity for cyber-crime. About half the world's population owns a smartphone, and an average household now has more than five connected devices. Many users now access online services such as e-government transactions, e-banking and e-shopping on their mobile devices. However, according to Abu Dhabi Police about 80% of phone applications fail security tests. The Android system recorded more than 10 million attacks in 2014 yet 92% of users in the UAE are reported to trust their smartphones. Mobile applications have been highlighted as an area of weakness in terms of security.

Smartphone penetration in the UAE has reached 72% and the Middle East is an area of great interest for cyber-criminals. For example Saudi Aramco, an oil company, experienced a cyber-attack, which deleted the hardware on 85% of its devices. Statistics from Dubai Police show a dramatic 88% increase in cyber-crimes reported in 2013 and the UAE is the second most attacked country in the Middle East. Even Etisalat has fallen victim to cyber-attacks, and the attacks could rise as the World Expo 2020 in Dubai approaches.

Some of the difficulties are in defining, proving and sentencing cyber-crime. There are many types of cyber-crime over the Internet. Cyber-crime can range from identity theft, to fraud, to terrorism, to the recent Stuxnet worm which was designed to attack industrial facilities and was used in a nuclear plant in Iran. Another challenge is finding the cyber-criminals and keeping up with advances in technology. Cyber-crime develops and changes quickly. For example malware has become so common that organisations experience an attack like an email file or web link once every three minutes (FireEye Inc, 2012).

Cybercrimes are international and so agreements are needed between countries to regulate the issues. If the criminals are found, laws dealing with cyber-crime specifically are needed. The ILOVEYOU computer worm, created in the Philippines, attacked files on the local computer and sent itself to all contacts from that computer. It caused an estimated $10 billion in damages worldwide (Brock, 2000). Two young programmers in the Phillipines created the worm and were arrested. However, there were no laws to charge them for this crime at that time so they were not prosecuted.

Despite this, countries of the United Nations failed to make a global cyber-crime treaty in April 2010 and so countries are alone in developing their own local laws against this global danger. Developing countries may find this more challenging than more developed countries. Also many countries do not have cyber-crime specific laws. A further challenge is that technology can change faster than the legislation.

Another difficulty is finding the identity of the criminal and the evidence. The cyber-criminal may be very skillful and the technology can make the person or group's identity impossible to discover. The evidence of cyber-crime is also difficult to discover, and cyber-criminals can cause the evidence to destroy itself on discovery.

The UAE government is trying to tackle cyber-crime. In November 2012 the UAE cyber-crime law created in 2006 was changed to a more detailed law with higher penalties to fight abuse of the internet and protect user privacy. The law outlines many of the ways in which the Internet can be abused and gives penalties for each offense. A lawyer in Dubai says, "The law includes

penalties for insults to religion and inciting conspiracy. It includes everything from privacy and personal protection to human and drug trafficking."

However officials from the Ministry of Justice have called for stronger laws to try to tackle cyber-crime. They said the UAE must use international laws to catch cyber-criminals. The National Electronic Security Authority in the UAE says the challenges are both legal and technological and that systems must be updated and modernised. There are also resource challenges as there is a lack of experts to fight the danger, and there must also be adequate funds for new technologies.

It's clear that the law must continually change to meet the challenges of cyber-crime, and that there must be cyber-crime specific laws. It's also important for countries to work together to develop international strategies against cyber-crime and it is a danger that cannot be fought only by governments as businesses are also in danger.

Sources

Bibliography

Alalwan, N., Alzahrani, A., & Sarrab, M. (2013). Cybercrime Investigation Challenges for Gulf Cooperation Council Governments: A Survey.

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, A. (2010). Dealing with the problem of cybercrime. *Conference Proceedings of 2nd International ICST Conference on Digital Forensics and Cyber Crime.* Abu Dhabi .

Norton. (2010). *Norton Cybercrime Report.* Norton.

Mustafa, A. (2012, November 13). *Cyber-crime law to fight internet abuse and protect privacy in the UAE.* Retrieved from The National : http://www.thenational.ae/news/uae-news/cyber-crime-law-to-fight-internet-abuse-and-protect-privacy-in-the-uae

Mustafa, A. (2013, May 23). Hackers be warned: UAE takes guard against cyber attacks. *The National* .

Malek, C. (2014, April 2). *UAE calls for stronger cybercrimes laws*. Retrieved May 30, 2015, from The National : http://www.thenational.ae/uae/technology/uae-calls-for-stronger-cybercrimes-laws