University of Essex

Principles of Digital Forensics and Cyber Law January 2022

Unit 12 - End of Module Assignment - Expert Report

Introduction:

The Internet has drastically changed criminal activity, creating new opportunities to support existing crimes and new ways of carrying out these crimes. It also expands the geographic scope of crime in a way that is not achievable without technology. Beyond this, it creates new types of crime as well. For example, one type of cybercriminal activity that often appears in the media is CyberID theft and related fraud.

The Internet gives rise to a form of identification robbery that is not limited to stealing physical identification documents. Instead, online thieves can steal identity tokens - information that may be even more valuable because it is so easy for hackers to acquire and sell. The Internet also provides opportunities for engaging in illegal activities with stolen identity brands. For example, online banking and e-commerce are vulnerable to this type of activity.

There is a new, more sophisticated type of identity theft scam out there. It involves the attacker intercepting personal information such as name, address and bank account details. The attacker can then open up their credit card account and apply for an additional loan on behalf of the victim with all the personal information they have collected from the victims. As a result, victims lose financial security and other parts of themselves- their livelihoods- when this type of identity theft scammer steals them. Hacking has been employed successfully to obtain mass identifying information, including the account information held by Card Systems Solutions for 40 million credit card customers(Haygood & Hensley, 2006)

The internet has opened up new and informative sources for scammers. As a result, many users are relaxed about sharing knowledge with online services and other users. However, even security-sensitive people are at risk of malware designed to steal personal information from their PC, mobiles or phishing emails that trick people into revealing their personal information. In addition, major hacking retailers can expose millions of records to potential misuses, such as the recent Ashley Madison breach in July 2015, where more than 36 million accounts were revealed through hacking.

How cyber identity theft has manifested in the EU:

Recently, theft of personal data has become an issue at the desks in sites and community agencies. This phenomenon did not seem to justify political concerns within the EU until the early 2000s. On the one hand, the use of new technologies increases. However, especially the 9/11 terrorist attacks address this new criminal activity described as one fastest growing crimes in the United States. Brussels aroused interest with large scale economic loss from financial institutions and collateral damage for citizens who need to restore their identities.

From the Federal Trade Commission to dramatic stories in North America, no one does not know about this criminal activity that is causing enormous damage.(Hoonfnagle, 2016) What makes it worse? The fact that EC (European Commission) has also made this threat more severe by taking note of its effects on personal information theft. In 2003 and 2004, it has been observed how criminals using personal information were related to other crimes which required no special attention. At that time, a document was released stating thieves had taken notice of their concern for privacy theft as a specific crime problem. The main policy change in the EU has been to shift from the peace model to a war/readiness model.(Levi & Wall, 2004).

Cyber ID theft involves the misappropriation of ID tokens online. A standard online ID token is a combination of username and password used to access systems like email addresses, web pages, and internet banking. Traditional IDs can also be collected this way- contact details such as name, address, social security number or tax number can all make up one's identification within an organization. These identifiers are sufficient for one person to receive credit cards in their victim's name if they had this information available.

Many cybercriminals steal personal information by using the power of new technology like hacking, phishing, and pharming. They also use traffic diversion, prepayment fraud or even forged tax statements to trick victims into revealing online identifying information. However, the ease at which a person can obtain personal information tokens or identify information online has changed the range in which it is stolen and its potential victims.

The most commonly used way to steal personal information online is phishing. Social engineering techniques are most commonly used when perpetrators pretend to be legitimate companies requesting sensitive data. Also, there are more advanced attacks, such as targeting profiled groups based on their desire for products and services to increase the success rate of theft. People should avoid social engineering instead of targeting software that causes automated redirects to fraudulently imitated websites because mobile internet users are vulnerable through SMS text messages. Online banking credentials can also be obtained via malware. The malware installs on the personal computer without the user's knowledge and is designed to record keystrokes, insert fake web pages, perform malicious actions, and collect passwords and financial information.

Considerations of rights and ethics in cyber identity theft:

The Budapest Convention recognizes that a proper balance between the fight against cybercrime and the protection of individual rights is an essential factor. It also recognizes that care must balance law enforcement agencies' interests and respect for human rights. That includes freedom of expression, privacy, and data protection. Hence, these basic principles are not negligible in any place or time. Article 15 requires Parties to establish conditions and safeguards to limit and prevent abuse of law enforcement powers and to protect human rights.(Seger, 2011)

The European Court of Justice's abolition of the Data Retention Directive (DRD) is not afraid of the EU's balance, even if it knows that law enforcement and prosecutors will have difficulty accessing individuals. Clearly shown data to get companies. Furthermore, GDPR (General Data Protection Regulation) provides the necessary protection for personal data. The EFF(Electronic Frontier Foundation) has released a statement affirming this decision as an "urgent call" for surveillance reform in Europe. This ruling may lead to changing attitudes about privacy across our continent. The opinion states: "Digital communications cannot be stored indefinitely without being processed".

The data be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.(Chassang, 2017)

Full compliance with data protection regulations and principles is an asset to preventing and fighting cybercrime. The European Union has taken this responsibility seriously, whereas they have also gone beyond the safeguards provisions of the Convention to operational activities. An example of their work is EC3's endeavours, which are working on independent data protection monitoring capabilities in cooperation with Europol and secure information exchange protocols. They also mandate to reach out to private sector companies that share sensitive personal information or process it within datasets – all while keeping up full compliance.

The Economic Crime Centre in the European Union allows for a more cooperative approach to fighting cybercrime. This is because an individual's rights are being protected simultaneously as working with EU member states to enact this cooperation. The success of this approach can be seen through its implementation in the Europol Expert Platform, which was created to facilitate sharing of best practices and tools between various countries within the EU that were combating cybercrimes.

Europol has a comprehensive, robust and tested regime in place which is widely recognised as safeguarding and ensuring the highest standards of data protection in the law enforcement world.(Drewer & Ellermann, 2012).

The law and the offence of cyber identity theft:

The focus of law enforcement is usually on the use of identity information in crimes like fraud. However, this leaves a potential loophole in the law dealing with identification information collection, retention and transaction preparation stages. This behaviour can be easily explained by personal information theft when someone takes people's names without permission to get something they should not have or commit crimes under people's identity.

The access without right, to the whole or to any part of an information system, is punishable as a criminal offence.(EUR-Lex, 2013). The offence could be seen as a first step toward understanding the legal aspect of hackers' activity.

The first definition of illegal access is related to the consent or absence of the person who owns data. So, for example, somebody testing a company's defences cannot be prosecuted for accessing records without permission if that company has approved them.

Criminal offences of illegal interception of private communications are different from other types, as their nature is closely related to privacy protection. However, because crime does not depend on the nature of data collected or processed (illegally), it is a mistake to equate this crime with a simple criminalization when processing personal information. It also does not matter whether there was actual interception; if illegally obtained data has been saved and archived, that would be considered illegal.

Member states shall ensure that intercepting, by technical means, a non-public computer transmission of data to or from an information system is punishable as a criminal offence.(EUR-Lex, 2013)

Data intrusion is a crime where someone tries to bring a legal dimension to the computer malware phenomenon. Data intrusion is just the means needed for another crime in other cases.

Member states should ensure that deleting, damaging, deteriorating or alerting data on an information system is punishable as a criminal offence.(EUR-Lex, 2013)

Challenges of cyber identity theft tools:

Cybercrime is challenging to investigate due to the wide range of cyber-related technologies. Digital evidence cannot be restored and investigated quickly without the use of appropriate skills, tools, and equipment. For digital research related to criminal investigations involving technology, technical investigators will select what tool they need depending on various factors such as their proficiency with certain types or all types of tech devices being examined for potential evidence. Additionally, the nature and availability of both law enforcement response time after receiving notification about a cyber-related crime scene investigation requiring an expert investigator and any other relevant temporary or permanent investigative resources available depend on many factors like product type/nature.

For example, The increased misuse of cryptographic and anonymization tools to protect communications, obfuscate financial transactions, and evade detection by criminals is also a critical issue identified in IOCTA (Internet Organised Crime Threat Assessment). Important information gets lost when we use virtual private networks (VPNs), Tor, and encryption, among many other things. The encryption of electronic data is a growing problem for police agencies. Encryption makes data unreadable by means of an algorithm and the data can only be made readable again with a so-called decryption key.(Pool & Custers, 2017)

Law enforcement agencies observe increasing abuse by cybercriminals for secure communication applications with end-to-end encryption. Ransomware shows the "aggressive" abuse of cryptography by criminals; it is becoming an established trend in all areas of cybercrime.

Another example is the Cryptocurrencies. Cybercriminals exploit many cryptocurrencies, including Bitcoin, which has been a favourite for digital extortion in ransomware and DDoS attacks. The truth about these cybercriminals is that they have found their preferred currency of choice-bitcoin-to use as payment on the crime market. These show that law enforcement agencies need to ensure they have skills, tools, and regulatory measures to keep up with challenges presented by cryptocurrency users such as Bitcoin enthusiasts or hackers who abuse virtual currencies like Ethereum or Monero (Ransomware). Law enforcement also knows about bitcoin but has had a hard time following other types of cryptocurrencies used on the criminal network.

Dash and Zcash enable users to keep their activity history and balances private, which ultimately restricts law enforcement investigators from identifying and tracing suspicious transactions. (Tziakouris, 2018)

Furthermore, more challenges come from implementing the NAT (Network address translation) technologies from the internet service providers' side. ISPs use NAT technology to share a single public IPv4 address with multiple end-users simultaneously. As a result, cyber investigators face a list of hundreds or thousands of end-users who may be connecting to such an IP address. These require many resources, have long delays and cause privacy issues for innocent customers. In addition, they are often pulled into investigations because they have been assigned the same IP address as someone else who committed cybercrime in that particular geographic region. (Gozukara, 2021) Tracking crime suspects from IP addresses is an internationally used methodology. However, when the subscriber is behind a NAT, it becomes challenging to determine the true owner of the IP address.

Victims and social perception of cyber identity theft:

Cyberspace has had an incredible impact on all aspects of civilization. The daily lives, fundamental rights, social interactions and economy depend on information and communication technology that works smoothly. Open cyberspace has promoted inclusion in politics and society worldwide: it breaks barriers between countries, communities and citizens by enabling interaction through sharing information or ideas. Moreover, technology is an integral part of almost every sector in the world economy, including banks, telecommunications, and utility grids.

People weigh four aspects of online risk: the ability to control or avoid it, their fear of consequences, the unknown risks associated with a situation and how soon they will be impacted. Cyberattacks are not just something that people know about, and actions taken in response vary among individuals. Some respond logically, while others instinctively react based on their feelings about technology-related risks. Emotions can act as a spotlight for focusing attention and motivate people to take action by directing them towards particular outcomes like protecting themselves from cybercrime due to an emotional attachment to avoiding certain losses associated with this type of crime. people can decide on acting on risks related to technologies based on their feelings toward specific outcomes(Nurse, 2018)

In addition, customer records may be at risk of cybercrime-related security breaches. Customers whose credit cards and other financial information have been hacked or stolen by intruders lose trust in the organisation and go elsewhere. Finally, many organisations rely on increased security measures to neutralise cybercrime that can negatively impact employee efficiency due to time wasted on entering more passwords or performing other tasks.

Consequently, people must be aware of the potential threats when digitising life. Also, cyberspace needs to be protected from incidents, malicious activity and misuse in order for cyberspace to remain free and secure.

Conclusion:

It seems the number of cybercriminals is on the rise. This increase in numbers is primarily due to more accessible technologies for non-technical people and much more accessible than before. In particular, criminals feel emboldened because of increased anonymity services that allow them to operate behind a screen without revealing their identity.

The EU's goal to introduce a unified system of legal conduct is admirable. The 2013 EU Cybercrime Directive introduced standard minimum rules defining crime and sanctions in cybercrime. In addition, Europol / EC3 was also launched in January 2013 and kept it up-to-date as a visible signal of their motivation. It will be easier for them to address and combat cybercrimes more effectively now that they have begun cooperating better with each other.

Finally, Fighting cybercrime does not mean "winning" or defeating criminals entirely; instead, reducing risks associated with using computers online should be everyone's goal because cybercrime cannot be eliminated.

References:

- Haygood, R. and Hensley, R. (2006) Preventing identity theft: New legal obligations for businesses. Employment Relations Today, 33(3): 71–83. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1002/ert.20120. [Accessed 01 April 2022].
- Hoofnagle, C.J. (2016) Federal Trade Commission privacy law and policy. Cambridge University Press. Available from: https://books.google.com/books?hl=en&lr=&id=sSR0CwAAQBAJ&oi=fnd&pg=PT15&dq=cybercrime+%22Federal+Trade+Commission%22+to+dramatic+stories+in+North+America,+no+one+does+not+know+about+this+criminal+activity+that+is+causing+enormous+damage&ots=5wFbvrJh9M&sig=DznaCamdneLIkUl2YO4sPxBYewM. [Accessed 01 April 2022].
- Levi, M. and Wall, D.S. (2004) Technologies, security, and privacy in the post-9/11 European information society. Journal of law and society, 31(2), pp.194-220. Available from:

https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-6478.2004.00287. [Accessed 03 April 2022].

- Seger, A., 2011. The Budapest Convention 10 years on: lessons learnt. ISP C, 167. Available from: https://youracademy.fr/wp-content/uploads/2019/08/Cybercriminality-Finding-a-balance-between-freedom-and-security.pdf#page=152 [Accessed 04 April 2022].
- Chassang, G. (2017) The impact of the EU general data protection regulation on scientific research. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5243137/. [Accessed 02 April 2022].
- Drewer, D. and Ellermann, J., 2012, November. Europol's data protection framework as an asset in the fight against cybercrime. In ERA Forum (Vol. 13, No. 3, pp. 381-395). Springer-Verlag. Available from: https://link.springer.com/article/10.1007/s12027-012-0268-6. [Accessed 08 April 2022].
- EUR-Lex (2013) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Article 3. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040. [Accessed 08 March 2022].
- EUR-Lex (2013) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Article 6. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040. [Accessed 09 March 2022].
- EUR-Lex (2013) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Article 5. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040. [Accessed 09 March 2022].
- Pool, R.L.D. and Custers, B.H.M. (2017) The police hack back: Legitimacy, necessity and privacy implications of the next step in fighting cybercrime. European journal of crime, criminal law and criminal justice, 25(2), pp.123-144. Available from: https://brill.com/view/journals/eccl/25/2/article-p123_3.xml. [Accessed 07 March 2022].
- Tziakouris, G., 2018. Cryptocurrencies—a forensic challenge or opportunity for law enforcement? an interpol perspective. IEEE Security & Privacy, 16(4), pp.92-94. Available from: https://ieeexplore.ieee.org/abstract/document/8425619/. [Accessed 09 March 2022].
- Gözükara, F. (2021) Challenges and possible severe legal consequences of application users identification from CNG-Logs. Forensic Science International: Digital Investigation, 39, p.301312. Available from: https://www.sciencedirect.com/science/article/pii/S2666281721002377. [Accessed 10 April 2022].
- Nurse, J.R. (2018) Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624. Available from: https://arxiv.org/abs/1811.06624. [Accessed 10 April 2022].