Chapter 5

Developing the Social, Political, Economic, and Criminological Awareness of Cybersecurity Experts:

A Proposal and Discussion of Non-Technical Topics for Inclusion in Cybersecurity Education

Marcus Leaning
University of Winchester, UK

Udo Richard Averweg
eThekwini Municipality, South Africa

ABSTRACT

The global shortage in skilled labor for cybersecurity and the risk it presents to international business can only be solved by a significant increase in the number of skilled personnel. However, as the nature of risks proliferate and bifurcate the training of such, personnel must incorporate a broader understanding of contemporary and future risks. That is, while technical training is highly important, it is contended that future cybersecurity experts need to be aware of social, political, economic, and criminological issues. Towards this end, this chapter considers a number of exemplary issues that are considered worthy of inclusion in the development of future cybersecurity workers. Accordingly, an overview is given of the issues of the "dark side of the net" that cause problems for global cybersecurity and international business risk. The issues are discussed so that from these a skill set can be articulated which will attend to (and mitigate against) potential threats.

DOI: 10.4018/978-1-5225-5927-6.ch005

INTRODUCTION

The global shortage of skilled Information technology (IT) security staff presents a significant problem to business. Without qualified and skilled staff, ever increasing cybersecurity threats will make businesses untenable (Evans & Reeder, 2010). However, as explored in this collection there is currently a significant shortage of such qualified and skilled staff. This chapter is concerned with the education and training of such staff. However, despite a number of attempts (Hansche, 2006; Paulsen, McDuffie, Newhouse & Toth, 2012; Vinnakota, 2013; Kim, 2014; Beuran, Chinen, Tan, & Shinoda, 2016) definitions of what constitutes a trained IT security specialist are fairly fluid.

As Martin (2015) notes, there is not as yet a widely accepted structure or framework of skills. Indeed, there is a discrepancy between what different national governments and providers of education see as key areas of such an education (Henry, 2017). For the most part, staff and students willing to gain entry to the lucrative IT security workforce can choose from a very wide and heterogeneous educational market. Courses on offer tend to center upon two main approaches: first are courses that offer training at various levels in specific technological practices to detect and protect organizations from cyber-attacks.

Such training programs range from short upskilling in specific technologies through to full bachelors and masters level degrees in universities. Many of these courses, particularly at the sub-degree level, are accredited by brand leaders in the cybersecurity industry. Second are business and management courses which incorporate a component of cybersecurity. Such programs tend to seek to accord cybersecurity a significant role in management practices and advance the idea that individuals at all levels of an organization have a vital role to play in ensuring there is a robust defense to those wishing to attack it.

In this chapter, the authors contend that cybersecurity training has to-date neglected a significant aspect in its scope. Drawing upon ideas from cultural criminology it is asserted that those charged with defending against cyber threats should be cognoscente of a range of non-technical issues which relate to the reasons for attack. Also included are the wider social and cultural aspects of attacks such as the culture of those attacking understanding the political, economic and psychological motivations of attackers, the economics of the attacker's culture and the cultural norms of the attackers. Cultural criminologists have asserted that through such awareness those involved in defending an organization from external threats can better predict and mitigate future threats (Ferrell & Sanders, 1995; Jaishankar, 2011).

To address such issues, the authors assert that cybersecurity should incorporate a range of topics and issues currently outside of the accepted scope of training. Determining the scope of such topics and issues is problematic and the list of such areas will need to be continually revised as new aspects emerge and new social issues arise. Indeed, ensuring that cybersecurity personnel are as aware of contemporary social issues in security is as difficult as ensuring the technical skills are up-to-date. Mindful of this, the authors here identify four key areas in this chapter that will serve the contemporary and immediate future needs of cybersecurity personnel.

The objective of this chapter is to advance an outline of four areas the authors feel cybersecurity personnel need to consider: (1) the rationale for spam emails; (2) the reasons people hack; (3) the new economy of crypto currencies; and (4) the places of communication used by cyber criminals.

BACKGROUND

The first part of this chapter commences with a discussion of the activity of spam as this often serves as a gateway to and facilitator of many other forms of illicit behavior (Krebs, 2014). Spam refers to the mass sending of unsolicited messages - most typically emails. It is recognised by the authors that the term *spam* is also used to refer to other types of unsolicited communication, such as personal messaging, texting and communication on virtual forums. Spam accounts for a significant proportion of all email traffic and though the prosecution of key spam senders often has an impact upon the total volume, such actions tend to be short-lived and new spammers soon take their place. Spam email currently amounts to 86% of all email traffic (Robertson, 2016) though much spam is caught in the various filters on servers and email clients in organisations. Indeed, only approximately 30% of spam sent gets through the various filters (Stone-Gross, Stringhini, & Vigna, 2011).

Spam is sent so as to make some form of financial gain for the sender. As will be discussed below, the ways in which the financial benefit is achieved is varied but the main purpose is to induce some action on the part of the recipient that will facilitate the sender of the spam email obtaining benefit. Though much spam is sent from legitimate organisations as part of their marketing campaigns, a significant proportion of unsolicited email traffic is sent by or criminal or semi-legal activity and it is this aspect that is focused upon in this chapter. Krebs (2014) sees a strong link between criminally orientated, spam email and organised crime.

The second part of the chapter provides a discussion of hacking which is a topic that has attracted much attention in the popular press and media in general. Rarely a week goes by without a story appearing of how hackers have attacked a bank or financial institution (Collinson, 2017), stolen money from individuals (Jones, 2017), or even interfered with elections (Gilsinian & Calamuir, 2017). This section considers hacking and looks at some of the reasons people hack. Though hacking is a term of some longevity it has multiple common meanings. The word retains its original Anglo Saxon meaning for chopping wood but in more recent years it has been used to refer to the skilled but unorthodox use of a technology. For example, computer scientists often refer to a hack as a way of circumventing a problem or making a computer system do something that it was not originally designed to do.

The term has also been expanded to refer to small techniques used in everyday life to achieve goals (the term ‘life hacking’ is often used in this regard). Here the discussion is limited to the illicit use of or breaking into computers. Such activity is virtually as old as computers themselves. There is a rich history of examples of attacks upon and through computer systems and one may draw upon an early account to define what one is concerned with. Parker (1976) refers to ‘system hackers’ and defines the activity they engage in as computer abuse which refers to “any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain”. Accordingly here the concern is with the ways in which computers and computer networks are attacked, penetrated without the sanctioned user’s permission or against their interests.

The focus of the third part of the chapter is on bitcoin and crypto currencies. Such phenomena are currently very prominent in the news (see the use of bitcoin to facilitate payment for the 2017 international extortion ‘wannacry’ attack launched against the British National Health Service, FedEx, the German railway company Deutsche Bahn AG, the Spanish mobile phone and broadband provider. Telefonica and many other companies and organisations in 150 countries were involved in the unrelated vast increases in Bitcoin’s value in the latter part of 2017). In this section, the focus is not upon the actual means of attack, but rather upon the means of payment, bitcoin as an example of cryptocurrencies. Here some of the key features of bitcoin and how it functions are discussed.

The fourth part of the chapter focuses on the online social environments of the dark use of the Internet. The dark net can be understood as a subset or category of the deep net. As such, one can demarcate the dark net from other forms of communication and data. For the purposes of this chapter, the dark net is identified as a specific section of the deep net that cannot be readily access through search engines. It is not a hidden part of the normal web, such as a secret Facebook group, but a specific approach to hiding information and making the identity of the users of that data difficult to identify. The methods by which the dark net can be reached and some of the available services that exist there, are described.

MAIN FOCUS OF THE CHAPTER

The Activity of Spam: Understanding It as A Social, Criminal, and Economic Action

The Spam Eco System

Spammers make use of a number of different campaign techniques to increase the success rate of spam emails. Spam email campaigns tend to be differentiated by the level of particularity of the email. At one end of the spectrum is the ‘spear phishing’ technique in which emails are crafted for particular people (information about the target is gained through web searching and ‘social engineering’ – contacting the organisation and using charm and simple lies obtaining information about the people and organisation). The information is then used to craft emails that are likely to get through spam filters and be opened and actioned by the intended targets. At the other end of the spectrum is the mass emails distributed to millions of people simultaneously. Such emails require the assistance and collaborative activity of computer system penetration experts and other types of hackers.

Central to the sending of mass spam emails are email lists which are the large lists of email addresses of potential recipients. Email lists can be composed in numerous ways, including the manual and automated gathering of emails from various sites and services. Email lists can also be purchased or rented through various legitimate services. Such lists can be specific and relate to key demographics and psychographics. Email lists are also sold by hackers who purposefully break into an organisation’s central records (such as billing systems or customer databases) to steal email addresses (Spammer-X, 2004).

In some cases, such lists are highly valuable as the proportion of genuine, active email addresses to inactive or false ones tends to be very high. The sale of such lists and the contracting for the commission of thefts of specific lists of email addresses is conducted through various ‘dark markets’ – venues for the trading of illegal merchandise on the internet or through personal contacts.

Botnets

The sending of spam emails for illicit purposes cannot be done through usual email practices which would reveal the spammers identity and make them liable to prosecution and other forms of sanction. Accordingly, spammers often make use of what is termed botnets (robot network) or zombie armies: networks of private computers that have been infected with viruses (which were typically delivered by a spam email). The viruses on such computers operate often undetected and while allowing the legitimate user of the computer to carry on working causing the computer to carry out other tasks simultaneously (hence, the label *zombie*).

For spammers, the most common task is to transform the computers in the botnet into a device that can send and relay emails in a complex network (Stone-Gross et al., 2011). Such compromised computers are used to send and pass on spam emails and to replace details of the originating sender with a fake name. The growth, use and maintenance of botnet armies is a practice often conducted by acolyte hackers as it can be achieved through the use of 'off-the-shelf' hacking software packages. Such packages involve the hacker infecting private computers with a virus and then using a control application to launch email campaigns (or other activities such as a deliberate denial of service attacks on particular web sites or services) from the infected machines.

Types of Criminal Spam

One can broadly identify four main types of criminally-orientated, mass spam emails:

- The first type is emails that serve a marketing purpose for a product. In these emails the product is often 'real' – that is there is a definite product or service for sale though its effectiveness, fidelity or genuineness may vary. Examples of such emails include sales emails for various personal or sexual issues such as the 'enlargement' of various organs, adverts for pornography sites, adverts for illegal articles such narcotics, software or pirated media texts or adverts for cheap replica medicines and drugs (such emails are primarily targeted at citizens of countries with expensive private medical systems in which medicines would be out of the reach of most people. The emails do often offer medicines that are similar to those available in pharmacies but are produced outside of the legitimate supply chain and thus may not be as effective as the genuine drugs);
- A second common form of spam email are those emails termed advanced fee fraud and classified under the Nigerian Penal code as 419 violations. Such emails are varied and function by alerting the recipient to a possible large financial reward for their willingness to engage in a smaller transaction such as sending an 'advance fee'. Of course the larger financial reward will never materialise and the recipient may need to send more money. A variant of this approach is to send a spear fishing attack claiming to be from a friend of the recipient and that they have been robbed or lost a bag while abroad and need emergency cash sent to them;
- A third approach involves attacking the recipient's computer. This form of spam will often contain a link or a file which will install a virus upon the recipient's computer. The viruses can serve a number of functions. The least serious involves using the computer as part of a botnet army to send out further emails to others. A similar use is for the recipient's computer to be used in a distributed denial of service attack against a web host or other computer. Both such activities will involve slowing the host computer down but not damaging it so much that the recipient will want to have the decline in function investigated and remedied as to do so would involve the virus being removed. More severe are viruses that disable the host's computer and demand a ransom fee payable to the sender in exchange for a code that will unlock the computer. Failure to provide the fee within a short period of time will result in an increase in the fee and eventually encrypting of all the information on the computer. Viruses are also used to secure personal details from host computers that can be used in identity theft; and

- A fourth approach involves the recipient being sent what appears to be an email from their bank or other service (such as PayPal) requesting they log in to their account using the link provided – in some instances the email will seek to cause alarm in the recipient so as to encourage rapid action. The linked bank login page is a fake and the user will provide their login details to the fraudster. The details can then be used to steal money and other identity fraud activities.

Many organisations have software filters and rigorous user guidelines to prevent spam emails and hacking incursions. However, skilled spammers and hackers can circumvent such systems with original and cunning tricks. One of the authors of this chapter fell victim to an attack; this involved the use of a spam email that contained the header 'printer malfunction' and was spoofed so as to appear to emanating from the 'ITHelpDesk'. Unfortunately the spam email arrived moments after a document had been sent to print. The author concluded that something had gone wrong with the printing (the printer was in a room on another floor and so could not be checked) and it was an automated response from the networked printer.

The email contained a link which was said to lead to the printer queue – however, upon clicking the link it installed a virus. Remedying the situation involve having the computer reformatted and the user account frozen (and passwords on all internal accounts changed) until it could be determined that no further damage could occur. This resulted in significant inconvenience to the user and a delay of nearly two days. This then had an impact on other parts of the organisation for which time dependent tasks were pending. Even though the user was mindful of the many ways spammers and hackers work, the serendipitous timing plus a brief lack of thoroughness resulted in significant time wastage, inconvenience and a cost to the organisation.

While spam emails are relatively inexpensive to the sender, they can prove to be a costly business risk to an organisation. Spam emails invariably 'rob' organisations of valuable lost productive time when employees attempt to determine the legitimacy (and resultant deletion) of such emails. Furthermore there is also the cost of extra storage space which has been purchased for spam emails that have been quarantined until they are automatically purged. Accordingly, for organisations, a continuous promotion of anti-spam awareness raising activities (such as an organisation's intranet) alongside rigorous technical means of spam defence is advocated. Such technical defence mechanisms for mitigating the resultant damage of spam in an organisation, should include plans and implementation schedules drawn up by reputable anti-spam consultants.

The Activities of Hacking: Identifying the Economic, Political, and Mischievous Rationales for Hacking

The Identity of Hackers

Despite the media stereotype of all hackers being disgruntled youth, there is little that unites hackers beyond their interest in computing. The perpetrators of hacking do not constitute any form of traditional community apart from their interest in the activity itself. Contemporary hackers come from different societies and countries; have different political persuasions; are of different ages, social classes and educational levels. There is no common value system and notwithstanding the selective cultural construction of the ethical hacker, the understanding of and adherence to appropriate behaviour by hackers is varied to say the least.

The Reasons for Hacking

Given the heterogeneity of hackers it is not surprising that the reasons people engage in hacking are very varied. It is asserted that the reason people hack can be understood in three broad categories. These categories have been derived from reports and accounts of hacking within academic and popular literature (for example, see Décary-Hétu & Dupont (2013); Turgeman-Goldschmidt (2005; 2008) and Mitnick & Simon (2009)). Furthermore, hackers may well conduct different hacks for different reasons; that is they may hack two organisations for completely different reasons. The three broad categories that people hack are:

- **Economic Reasons for Hacking:** Hacking for economic reasons can be considered to be those activities that are conducted for financial gain and there are two sub-categories to consider here. First are criminal activities. These are hacks perpetrated to financially enrich the hacker or its organisation. Such activities are increasingly conducted by organised crime syndicates in systematic and complex crimes. The execution of these crimes often utilise other nefarious aspects of the dark net such as spamming and in particular the 'spear fishing' techniques discussed in the next sub-section and bitcoin or other digital currencies to be explored in the next main section. The nature of these crimes is varied but typically involves: stealing money from financial systems such as bank accounts and money transfer systems (Singh, 2015); stealing information either to order (Samani & Paget, 2015) or to sell on data markets (for example, credit card and account holder details stolen from retailers are sold on the dark web (McFarland, Paget, & Samani, 2016)), extorting money through the encrypting computers (see the successful attack on Calgary University in 2016, for example (Marotte, 2016)) and threatening to bring down computers using distributed denial of service attacks (for example, Russon (2016) details attacks made on small business in the United Kingdom and South Africa) and data or revealing personal and incriminating information (O'Neil, 2016)). In addition to the hacking of computers for nefarious purposes there are also numerous companies that offer the service of penetration testing; they attempt to break into computer systems to test the security systems in place for a fee;
- **Political Reasons for Hacking:** The second category relates to what may be termed political reasons for hacking. Here there are two further sub-divisions. First are those who hack so as to seek redress for what they perceive to be a political injustice. These groups deploy hacking skills to further the political aims of particular groups or political parties or to challenge and damage other political groups, agencies and governments. Such groups often operate under the portmanteau of 'hacktivist' – an activist who hacks. A contemporary example of such a group would be the hackers collective Anonymous which has attacked various targets it perceives as being oppositional to it political stance. Anonymous emerged out of the Occupy movement and shares many of the political concerns as Occupy (Goode, 2015). Second are those who hack on behalf of a government against either domestic or foreign targets. Examples of this include governments attacking foreign companies such as North Korea attacking Sony in revenge for releasing the film 'The Interview' – a satirical film about a planned assignation of North Korean Supreme Leader Kim Jong-Un (Sherr & Rosenblatt, 2014) and Israel's involvement in developing the StuxNet virus that was used to disabled a nuclear reactor in Iran (Lindsay, 2013); and

- **Personal and Social Reasons for Hacking:** The third main reasons for hacking may be considered social reasons. These relate to an individual's personal circumstances, beliefs and interests. One may sub-divide the category into three sub-divisions: the first relates to personal interests and includes reasons such as mischief, the desire to vandalise websites for pleasure, the thrill of trespass in systems without permission and the fame and reputation amongst peers (Taylor, 1999). The second sub-division relates to individuals seeking redress against others for perceived slights. Here attention turns to inflicting cyber-mediated harm to another. There have been numerous conflicts between hackers and authority within groups is enforced through hackers attacking each other and 'doxing' (obtaining and releasing personal information about someone) (Sammons & Cross, 2016). The third sub-division concerns disgruntled employees who seek redress for a perceived work-based grievance. Such 'inside jobs' pose a serious problem for organisations as the attacks subvert the defences developed to counter normal externally originating attacks. Furthermore in certain instances it is the very people who are responsible for establishing and maintaining the defences who commit the attacks.

The rationale for hacking attacks is varied and complicated but cognisance of it may well afford organisations opportunity to address potential reasons for hacking through skilled use of public relations - that is due to the varied reasons for hacking which may include non-financial and even political and social reasons, some attacks may be dissuaded by addressing the public face of the organisation rather than technological means.

The Economic Systems: Alternative Currencies

Bitcoin and Crypto Currencies: A New Form of Money

Bitcoin is the most successful of a series of alternative currencies that make use of advances in computing and cryptography – the science of codes and codes. Bitcoins exist solely in the digital realm and there is not physical manifestation of them (though there have been several instances where pseudo coins have been produced bearing the bitcoin logo). Bitcoin was launched through an academic-styled paper published on October 31, 2008 (Nakamoto, 2008a) and was announced on a cryptography mailing list (Nakamoto, 2008b). The author of the paper and the post to the mailing list was listed as Satoshi Nakamoto though this has proven to be a pseudonym (the real identity of Satoshi Nakamoto is a hotly debated topic. An Australian, Craig Wright has made claim to the identity though this has yet to be fully proven (O'Hagan, 2016)).

What distinguishes cryptocurrencies and Bitcoin from other forms of currency, as well as its solely virtual nature, is its use of block chain database technology. Currency is ordinarily transferable between individuals and companies. If the money exists in a material form, such as cash, then ownership is transferred by giving the other person(s) our notes and coins. They then possess the value of the money that the notes and coins depict. They can avail themselves of this value by spending the money for other goods and services. Over the past few years the manner in which one transfers ownership of money has gradually changed and now for any large transaction and many small amounts, one uses electronic means and record the transfer of ownership of money on centralised registers. Indeed, according to some estimates upwards of 92% of the money in the world does not exist in a physical form but is recorded on lists and registers which note legal ownership. Many of these central registers are held by banks and similar financial organisations.

Banks keep records of how much money one has with them, credit card and loan companies record how much one owes them. Thus one's relative wealth is held not in our physical hands but in (often) electronic records. One's money is stored in a bank and they lend it out to other users or to other organisations who then loan it to other users themselves. Thus banks serve as a third party, someone who is trusted and who can record one's wealth in their books. To provide this service, banks make money by charging interest on the money loaned to other people. This is the money provided to them by users and they sometimes (but not always) pay users interest on this money. The difference between the two rates of interest is how banks make their money, they lend it for more than they pay for it. Bitcoin offers an alternative in that users can transfer money between themselves without recourse to a trusted third party. This direct form of transfer is conducted using the block chain database technology.

Prior to the application of block chain technology, there were systems by which money could be directly transferred between users through electronic means. However, without recourse to a centralised register, such as a bank, to police the transaction there was always the very real risk that fraud could occur. The block chain technology offers a decentralised register of transactions which is distributed all over the world. There is no single ownership or storage of records by a third party, rather bitcoin operates by having its register widely distributed.

Block Chain Technology

Block chains are a form of database that make use of the principles of cryptography to produce a record that cannot be changed but can be easily verified. The block chain is a distributed database which records a list of actions or changes made. These changes are stored in a list of discrete sequential, records or 'blocks'. Blocks have two particular features that greatly add to the security of block chains. First, blocks are time stamped at their moment of creation – they carry their exact time of their production within them. Second, each new block on the chain is created with an inherent link to the preceding block. Therefore if someone wanted to alter a block they would have to then alter all subsequent blocks in the chain. These two features mean that once a block has been created it cannot be altered though the information can be easily verified.

Virtual Wallets

When a user wishes to make a transaction they send Bitcoins from their 'virtual wallet' to another virtual wallet. The transaction is then recorded onto the block chain. Simply stated, virtual wallets are a means to store Bitcoins. They are pieces of client software that contain a secure folder on a computer (or in cloud storage) in which to store the digital credentials or the private keys used in public key encryption systems of Bitcoin to produce Bitcoin addresses for transactions. The wallets either contain or access a copy of the block chain and consult it to determine how many Bitcoins are in a user's wallet and whether they have enough to complete the proposed transaction. Bitcoins can also be stored with an exchange or custodian or can be stored entirely off line in what is termed a vault – a file storage system that cannot be accessed through the internet (Villasenor, 2014). This is typically accomplished through either having a computer that is not connected to any form of network that is connected to the internet or through a removable device that stores the Bitcoins until their need arises.

To transfer money to someone's wallet they will provide you with an address, this is a list of between 26-35 numbers and letters. The address is created by the bitcoin client and it is advised that each address is used only once with a new one being created for each transaction. As an example of what an address looks like, bitcoinwiki (2017) offers the following example of an address 3J98t1WpEZ73C-NmQviecrnyiWrnqRhWNLy. This address is then entered as the destination of the transaction. From an external viewpoint this address carries no information as to the identity of the recipient. Though it may be possible to see what transactions have been made to that address, it is impossible to deduce to whom the address actually belongs without additional information.

Once a transaction has been initiated, the instruction is broadcast to all computers on the internet running the distributed Bitcoin software. The transaction is recorded on the block chain by being written into a new block. This writing of a new block or recordkeeping activity is referred to by the disingenuous term 'mining'. It is a long and complex process that requires significant computing power and 'know-how'. This is also referred to as a proof of work and serves as a further security measure – the creation of a block takes significant effort. Once a broadcast of the transaction is made on the Bitcoin network, 'miners' can choose to complete the work. The first miner who completes the work is rewarded with new Bitcoins themselves but also transaction fees. These fees are small rewards that those initiating the transaction offer so that their transactions are mined. Users who do not offer such rewards may find their transactions take longer to be written to the block chain and be finalised.

Advantages of Bitcoin for 'Dark Net' Residents

As detailed above, Bitcoin provides a means by which wealth can be sent to someone without any knowledge of who that person actually is. Accordingly, Bitcoin has provided a completely anonymous, untraceable and covert system for passing money. As the identity of the recipients and senders of money cannot be traced, money passed around through the Bitcoin system cannot be monitored by governments or law enforcement agencies. Transactions can take place that involve illegal activity. There have been numerous instances of this occurring on various fora and play a significant part in facilitating economic activity on the dark net.

Ransomware attacks are likely to get worse in the future so companies and organisations will require enhanced security to protect themselves from such cyber-attacks. The recent attacks underscore the fact that any vulnerabilities will be exploited by hackers and criminals. Even as computing advances provide more secure security software, such vulnerabilities will not simply 'go away'. Companies and organisations will need to proactively avoid the bite of bytes.

The Online Social Environments of the Dark Use of the Net: Reaching the Dark Net and Available Services

The dark net can be understood as a subset or category of the deep net. As such the dark net can be demarcated from other forms of communication and data. For the purposes of this chapter, the dark net is identified as a specific section of the deep net that cannot be readily access through search engines. It is not a hidden part of the normal web, such as a secret Facebook group but a specific approach to hiding information and making the identity of the users of that data difficult to identify. The methods are now described by which the dark net can be reached and some of the forums that exist there.

Reaching the Dark Net: TOR

Dark net web sites are typically accessed using TOR (The Onion Router) – a technology that involves covering network traffic with layers of encryption and then routing the data through multiple network pathways which continually shift.

The TOR technology allows users to visit web pages anonymously and to circumvent attempts to restrict access to particular sites. It is used by dissidents, journalists and others who wish to communicate anonymously for fear of having their messages intercepted by state agencies. As well as being used in the United States of America, Europe, South Africa and other democracies, TOR is used by anti-government actors such as human rights activists in countries such as the People's Republic of China, the Syrian Arab Republic and Iran. TOR was developed by the United States (US) Naval Research Laboratory and was released under a free license in 2004 and then received backing from the Electronic Freedom Foundation. Because TOR is used by numerous anti-systemic groups which the US government has an interest in supporting, it continues to be in part funded (about 60%) by the US State Department and US Department of Defense (Greenwald, 2013).

TOR operates by having numerous computers functioning as nodes. These nodes can relay traffic between them. Once information is sent to the TOR network it is relayed across numerous nodes on its way to its destination. Traffic that is intercepted on the network is heavily encrypted multiple times. Moreover, the data has had both its origin and destination information removed and so is very difficult to trace.

From a client perspective, the TOR system is a browser that can be installed upon any Mac, PC or Linux machine – indeed the browser is a version of the *Firefox* browser. Once the TOR Browser Bundle has been downloaded and installed, the user enters addresses as they would any other web page. However, sites on the TOR network are not reachable via a normal browser and the addresses are constituted differently from normal web addresses and make use of a special top level domain – onion. TOR addresses consist of a string of 16 (seemingly) random numbers and letters with the suffix onion/.

For example, http://4u3ptawty2mn53bz.onion/ (this is a fake address). The actual address is the hash produced by public key encryption when the hidden service to which it points is initially established. Due to the various sites and services available on the dark net / TOR system being unindexed and unsearchable using normal web searching technologies, alternative systems have evolved. There are various search engines for the dark web (only reachable using the TOR browser) and a number of hidden wikis.

Available Services

The services available on the dark net can be grouped into a number of different categories, such as markets, sharing media files, and communication and community:

- **Markets:** There are numerous market places offering a vast array of services and goods. Historically one of the most famous dark net systems was the *Silk Road* – a site launched in February 2011 that was most famous for selling illegal narcotics. The site allowed users to buy and sell virtually any item but was best known for selling drugs in exchange for bitcoins. Allied sites such as *Armoury* sold guns and other weapons.

The *Silk Road* was closed down in October, 2013 after the Federal Bureau of Investigation seized control and impounded all the bitcoins in members *Silk Road* wallets (members had to load bitcoins onto a site specific wallet to purchase or sell items) (Clark, 2013). Following its closure and prosecutions of a number of the operators (who all worked under the pseudonym of the *Dread Pirate Roberts* (the name of the figure-head pirate who was role played by different people in the film *The Princess Bride*)) the *Silk Road* re-emerged as the *Silk Road 2* and then once that had also been closed down (in 2014).

A *Silk Road 3* emerged during 2016 but was unconnected to the original and seemed to have been established to defraud users. As with other market places the *Silk Road* allowed users to buy or sell virtually any goods anonymously.

In addition to the selling of illegal drugs there are also market places for stolen credit card numbers, stolen goods, fake passports, guns and weapons, counterfeit money, hacking software, stolen software and other media content. Services such as the laundering of Bitcoins, hacking and even assassination (though there has been considerable scepticism about whether this service was ever real or simply scams) are also proffered for sale on various market places. *AphaBay* and *Hansa* are both examples of such markets.

Markets on the dark web are unregulated and there is little recourse for buyers and sellers who are deceived. One innovation to remedy the problem of untrustworthy traders and vendors is the use of reviews in a similar way to other more legitimate web markets. Thus purchasers of drugs, fake passports and guns are able to offer a review of the service they receive and thus advise other customers of the reliability of the service;

- **Sharing Media Files:** There are numerous sites for the sharing of media files. These include commercial films and television series that have been stolen or illegally copied, large quantities of various forms of pornography and software. Such sites make use of various additional technologies and practices to share files. These include bit torrents and sharing systems such as virtual private networks that use TOR technology to allow users to share files without risk of interception.

The system *OnionShare* was developed after investigative journalist Glenn Greenwald's partner, David Miranda, was detained at Heathrow Airport under suspicion for transporting 58,000 documents (on a USB pen drive) which he had gained from Edward Snowden. Micah Lee, a staff developer with Greenwald's organisation, developed the system so that documents could be transferred without possible interference from third party agents (Crawford, 2014). Similarly Wiki leaks, the site established by Julian Assange to facilitate the release of government documents, can be found on the dark net; and

- **Communication and Community:** In addition to the commercial exchange and sharing of information, the dark net facilitates various forms of communicative spaces such as forums, blogs and secure email services. The secure email services draw heavily upon privacy and encryption software and a number of email systems are available.

SOLUTIONS AND RECOMMENDATIONS

As noted such topics need to be subject to continual revision and renewal as the political economic and social reasons for hacking are far from stable. As fast as technology changes (for example, the three-tier application architecture is obsolete and no longer meets the needs of modern applications in organisations (Thomas & Gupta, 2016)), so do the reasons for its misuse and organisations need to be 'fleet of foot' to attend to such changes. Such changes will include the effective management of user single sign-ons and the proliferation of cookies. However, while the specificity of the training cybersecurity personnel needs to be continually updated, the authors assert that such training should incorporate aspects of social, political and economic awareness. As other areas of technological education such as engineering have indicated (Crawley, Malmqvist, Östlund, & Brodeur, 2007), for training to be effective for the 21st century it needs to accommodate a human and social aspect as well. Accordingly it is advocated that cybersecurity education incorporates a degree of social, political and economic awareness.

FUTURE RESEARCH DIRECTIONS

As has happened in other forms of practice where technology intersects with social action, future provision of the training and development of cybersecurity personnel may do well to include the development of specific non-technical roles. Technology may not be the only knowledge base required for the successful deterrence of cybersecurity attacks and future cybersecurity personnel and management may well need to broaden their understanding of the reasons and means of execution of various cybersecurity threats. Accordingly one future area for research is the development of greater sociological and cultural criminological investigation into hacking, deep net forums, the economics of spam and the use of crypto currencies to facilitate nefarious activity.

CONCLUSION

It is reiterated how the current labour shortage in cybersecurity experts necessitates the development of skilled workers and it is argued, however, that as well as the technical skills needed such workers will also need cognisance of a range of social, political and economic factors. It is contended that the four broad areas of attention covered here provide a sample of some of the social, political, economic and criminological issues of which current and future cybersecurity workers must be aware.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors. Some of this text appeared in a four-part article series in the *Journal of the Southern Africa Institute of Management Services (SAIMAS)*. Permission was granted by the Editor of SAIMAS to reuse this text.

REFERENCES

Beuran, R., Chinen, K.-I., Tan, Y., & Shinoda, Y. (2016). *Towards Effective Cybersecurity Education and Training*. School of Information Science, Japan Advanced Institute of Science and Technology. Retrieved on August 9, 2017, from: https://dspace.jaist.ac.jp/dspace/bitstream/10119/13769/1/IS-RR-2016-003.pdf

bitcoinwiki. (2017). *Address*. Retrieved on December 4, 2017, from: https://en.bitcoin.it/wiki/Address

Clark, L. (2013). *A guide to the Silk Road shutdown*. Wired. Retrieved on June 2, 2017, from: http://www.wired.co.uk/article/silk-road-guide

Collinson, P. (2017). Lloyds bank accounts targeted in huge cybercrime attack. *The Guardian*.

Crawley, E. F., Malmqvist, J. S., Östlund, S., & Brodeur, D. R. (2007). *Introduction. In Rethinking Engineering Education: The CDIO Approach* (pp. 1–5). Boston, MA: Springer US.

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime*, *14*(2-3), 175–196. doi:10.1080/17440572.2013.801015

Evans, K., & Reeder, F. (2010). *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. Center for Strategic & International Studies.

Ferrell, J., & Sanders, C. (1995). *Cultural Criminology*. Boston: Northeastern University Press.

Gilsinian, K., & Calamuir, K. (2017). *Did Putin Direct Russian Hacking? And Other Big Questions. The Atlantic*. Washington, DC: Atlantic Media Company.

Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. *Popular Communication*, *13*(1), 74–86. doi:10.1080/15405702.2014.978000

Greenwald, G. (2013). NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*. Retrieved on May 9, 2017, from: https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

Hansche, S. (2006). Designing a Security Awareness Program: Part 1. *Information Systems Security*, *9*(6), 1–9. doi:10.1201/1086/43298.9.6.20010102/30985.4

Henry, A. P. (2017). *Mastering the Cyber Security Skills Crisis: Realigning Educational outcomes to Industry Requirements.* ACCS Discussion Paper No. 4, Canberra, Australia: UNSW.

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press. doi:10.1201/b10718

Jones, R. (2017). I thought I'd bought my first home, but I lost £67,000 in a conveyancing scam. *The Guardian*.

Kim, E.-B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115–126. doi:10.1108/IMCS-01-2013-0005

Krebs, B. (2014). *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*. Sourcebooks.

Lindsay, J. R. (2013). StuxNet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. doi :10.1080/09636412.2013.816122

Marotte, B. (2016). Digital hostage. *The Globe and Mail*. Retrieved on September 2, 2017, from: http://www.theglobeandmail.com/news/national/how-the-university-of-calgary-hack-wentdown/article30358657/

Martin, K. M. (2015). Cyber Security Education, Qualifications and Training. *Engineering & Technology Reference.* The Institution of Engineering and Technology. Retrieved on February 22, 2016, from: https://pure.royalholloway.ac.uk/portal/files/25218802/IETEducationTraining.pdf

McFarland, C., Paget, R., & Samani, F. (2016). *The hidden data economy. Mcaffee report*. Intel Security.

Mitnick, K. D., & Simon, W. L. (2009). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Wiley.

Nakamoto, S. (2008a). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved on December 1, 2017, from: https://bitcoin.org/bitcoin.pdf

Nakamoto, S. (2008b). *Bitcoin P2P e-cash paper.* Retrieved on December 1, 2017, from: http://article.gmane.org/gmane.comp.encryption.general/12588/

O'Hagan, A. (2016). The Satoshi Affair. *London EReview of Books*, *38*(13), 7–28.

O'Neil, S. (2016). *The Skype sex scam - a fortune built on shame*. Retrieved on December 2, 2017, from: http://www.bbc.co.uk/news/magazine-37735369

Parker, D. B. (1976). *Crime by computer*. London: Scribner.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a Cybersecurity workforce and aware public. *IEEE Security & Privacy*10(3), 76-79.

Robertson, J. (2016). E-Mail Spam Goes Artisanal. *Bloomberg Technology 2016*.

Russon, M. A. (2016). 'Armada Collective' hackers to launch bitcoin-extorting DDoS attacks on unwitting victims. *International Business Times.* Retrieved on December 2, 2017, from: http://www.ibtimes.co.uk/armada-collective-hackers-launch-bitcoin-extorting-ddos-attacks-unwitting-victims-1579789

Samani, R., & Paget, F. (2015). *Cybercrime exposed: Cybercrime-as-a-service.* Corporate white paper. Santa Clara, CA: McAfee Labs.

Sammons, J., & Cross, M. (2016). *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy*. Elsevier Science.

Sherr, I., & Rosenblatt, S. (2014). Sony and the rise of state-sponsored hacking. *CNET*. Retrieved on February 3, 2017, from: https://www.cnet.com/uk/news/sony-and-the-rise-of-state-sponsored-hacking/

Singh, N. (2015). Online frauds in banks with phishing. *Journal of Internet Banking and Commerce*.

Spammer-X, S. X. (2004). *Inside the SPAM Cartel: By Spammer-X*. Elsevier Science.

Stone-Gross, B., Holz, T., Stringhini, G., & Vigna, G. (2011). The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. *LEET*, *11*, 4–4.

Taylor, P. A. (1999). *Hackers: Crime in the Digital Sublime*. Routledge. doi:10.4324/9780203201503

Thomas, A., & Gupta, A. (2016). *Retire the Three-Tier Application Architecture to Move Toward Digital Business.* Gartner, Inc., G00308298.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review*, *23*(1), 8–23. doi:10.1177/0894439304271529

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, *2*(2), 382.

Villasenor, J. (2014). Secure Bitcoin Storage: A Q&A With Three Bitcoin Company CEOs. *Forbes*. Retrieved on December 19, 2017, from: https://www.forbes.com/sites/johnvillasenor/2014/04/26/secure-bitcoin-storage-a-qa-with-three-bitcoin-company-ceos/#1e36c2815cdd

Vinnakota, T. (2013). *A cybernetics paradigms framework for cyberspace: Key lens to cybersecurity*. Yogyakarta, Indonesia: Computational Intelligence and Cybernetics.

ADDITIONAL READING

Bartlett, J. (2014). *The Dark Net*. London: Random House.

Chertoff, M., & Simon, T. (2015). The Impact of the Dark Web on Internet Governance and Cyber Security. *The Global Commission on Internet Governance*. GCIG Paper No. 6. Retrieved on July 3, 2017, from: https://www.cigionline.org/publications/impact-dark-web-internet-governance-and-cyber-security

Crawford, D. (2014). *Onionshare: the 100 percent darknet file sharing app*. Retrieved on July 3, 2017, from: https://www.bestvpn.com/onionshare-the-100-percent-darknet-file-sharing-app/

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness modeling: Detection of cyber attacks with instance-based learning theory. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *55*(3), 605–618. doi:10.1177/0018720812464045 PMID:23829034

Keizer, G. (2010). Is StuxNet the 'best' malware ever? *InfoWorld*. Retrieved on August 1, 2017, from: http://www.infoworld.com/print/137598

Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. (2012). Something Smells Phishy: Exploring Definitions, Consequences, and Reactions to Phishing. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *56*(1), 2108–2112. doi:10.1177/1071181312561447

Langner, R. (2011). StuxNet: Dissecting a Cyberwarfare Weapon. *Security & Privacy, IEEE*, *9*(3), 49–51. doi:10.1109/MSP.2011.67

O'Brien, D., Budish, R., Faris, R., Gasser, U., & Tiffany, L. (2016, 26 September). *Privacy and Cybersecurity Research Briefing*. Berkman Klein Center Research Publication No. 2016-17.

KEY TERMS AND DEFINITIONS

Block Chain: A digitized, decentralized, public ledger of all cryptocurrency transactions.

Cookie: A small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.

Crypto Currency: A digital asset designed to work as a medium of exchange. It uses cryptography to secure its transactions to control the creation of additional units and to verify the transfer of assets.

Distributed Denial of Service Attack: A cyber-attack where the perpetrator seeks to make a machine (or network resource unavailable) to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet.

Hacking: An attempt to exploit a computer system or a private network inside a computer.

Keylogging: The action of recording (sometimes covertly) the keys struck on a keyboard, so that the person using the keyboard is unaware that their actions are being monitored.

Ransomware: A type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Spam: Unsolicited bulk email or junk mail.