An intelligence led approach to addressing cyber fraud: proactive fraud auditing

Elizabeth Petrie and Casey Evans

Received (in revised form) 24th December 2016

Elizabeth Petrie, 1101 Pennsylvania Ave, NW, Washington, DC 20004, USA. Tel: +1 202-776-1518; E-mail: elizabeth.petrie@citi.com

Casey D. Evans, American University's Kogod School of Business, 4400 Massachusetts Avenue NW, Washington, DC 20016-8044, USA. Tel: +1 202.885.6675; E-mail: cdevans@american.edu

***Elizabeth Petrie** is the Director of Strategic Intelligence and Planning for Information Security, serving also as the Chief of Staff to Chief Information Security Officer of Citi. Prior to Citi Beth was the head of Cyber Intelligence for the Federal Bureau of Investigation where she oversaw production of threat analysis for senior policymakers. Her career at the FBI also included authoring intelligence assessments on financial crime trends affecting global financial institutions. Beth has over 20 years of experience as an intelligence analyst and holds a Master's in Technology Management from Georgetown University as well as a Master's in Criminal Justice from George Washington University.*

***Casey Evans** is an Executive-In-Residence in the Accounting and Taxation Department at Kogod School of Business in the American University in Washington, D.C. where she teaches undergraduate and graduate accounting courses. Casey also has extensive industry experience handling a range of forensic accounting issues including fraud investigations, Securities and Exchange Commission and Department of Justice enforcement actions, financial reporting and disclosure issues, technical accounting issues and internal control reviews. She also regularly speaks to professional organisations and government entities on various forensic accounting topics. Casey is a Certified Public Accountant and a Certified Fraud Examiner.*

Abstract

It is estimated the global cost of cybercrime will grow to US$2 trillion[1] by 2019. With more than 6 billion[2] devices connected to comprise the Internet of Things the attack surface is growing for cyber fraud, one of the many types of cybercrimes. As more companies digitise the way they conduct business there is more data than ever before available to be stolen and monetised. At the same time, adoption of the internet continues to rapidly increase globally, adding more users for hackers to target. There has also been a sharp increase in the availability and advancement of cyber attack tools online, such as the sale of zero day vulnerabilities, the discovery of which more than doubled in 2015[3]. Such explosive growth in cybercriminal activity demands a new approach to defending against it or companies may be faced with the difficult decision to go out of business if suffering a cyber attack that can cause bankruptcy, either through theft of funds, destruction of data or irreparable damage to reputation. Traditional network defense approaches have been one dimensional, relying on technology as the gate keeper, however the adversary today is not only advanced and persistent but highly adaptable, constantly learning how to overcome defensive measures. As a result organisations must also adapt, using an intelligence led approach to prepare for and defend against such attacks instead of constantly reacting to them.

Keywords: cyber, fraud, intelligence, proactive, auditing

Understanding cybercrime

With the evolution of technology, the industry has also seen a shift from decentralised, individual cyber attackers to highly networked, sophisticated groups. Cyber attackers who started out hacking automated telephone systems were typically individuals who had to develop their own tools to conduct these attacks. As computers began to come online and become mainstream, these hackers went after targets of opportunity and exploited well known vulnerabilities, which users were simply not patching. Their motivation was really about ego and a desire to be recognised for their ability to break the system. But as computer systems became more complex hackers started to band together in loosely knit groups. Financially motivated, these actors became more selective about what they targeted and started to see the value in creating tools and exploits they could then sell to others to conduct attacks. Today these cybercriminal actors operate on the cyber underground, able to purchase and sell every type of attack tool, where fraud-as-a-service has become prolific.

Fraud-as-a-service offerings are one of many shared service models available to enable even the most unsophisticated cyber criminal to commit cyber fraud. These offerings also enable more tech savvy criminals who may only need one or two services they are unable to independently develop to complete their cyber fraud schemes. Here are a few examples of what fraud-as-a-service offerings include:

- *Infrastructure*, such as more computing power if a Distributed Denial of Service (DDoS) attack will be carried out as a diversion tactic while the criminal attempts to issue fraudulent wire transfers from their victims.
- *Delivery* mechanisms, such as malware, to infect the victim.
    - *Ransomware*, malware used to encrypt files until the victim pays, is one of the most popular forms of cyber fraud with 100 new ransomware families discovered in 2015; this was reportedly a record high[4] with losses reported by the FBI from April 2014 to June 2015 totaling over US$18 million[5].
- *Communication services* are also offered to enable cyber criminals to go undetected by law enforcement as well as cashout services that monetise data stolen or provide the capability to place, layer and integrate money to effectively launder it through the financial system.

Organisations must therefore adopt an intelligence led approach to counter every evolving cybercrime activity, which begins by understanding the cyber attacker.

Understanding cyber attackers

An intelligence led plan begins by developing a deep understanding of who is trying to attack the organisation as well as their motives, intentions and capabilities. Contracting with vendors or developing in-house intelligence collection capabilities allows the the threat environment to be deconstructed and defensive programs to be customised to prevent against infiltration.

The cyber security industry generally classifies the types of cyber attackers into five categories: nation state, cyber criminal, cyber terrorist, hacktivist and insider. Alhough it is important to understand the distinction between the actor types in order to best understand which types of cyber attackers could be targeting a specific organisation, it is also essential to recognise the techniques used to perpetrate cyber fraud that could be used to facilitate attacks other than fraud. Nation state actors are focused on the theft of intellectual property and engage in intelligence collection through cyber espionage in order to advance national interests however the methods they use to conduct a network intrusion often involve spear phishing, which cyber criminals commonly use to lure victims into clicking on a malicious attachment in an email in order to capture user names and passwords. Nation state actors are arguably the most difficult to defend against as they have unlimited funding, manpower and the use of the infrastructure of their country to conduct their attacks, but the volume of cyber criminal activity is reaching an almost insurmountable level as victims are many times selected simply because they are targets of opportunity. The commonality of certain tactics and techniques used by these types of actors can make it difficult to assign attribution in some cyber attacks unless it is clear what the attack objective was coupled with the other indicators of compromise.

Although cyber fraud is not the objective of cyber terrorists, who are motivated by ideology and use fear tactics to coerce their victims, fraud schemes do result in funding to support terrorist acts; research however shows there is a limited number of terrorist groups who have demonstrated their capability to carry out cyber attacks. In contrast there are many cyber actors who have aligned themselves to terrorist organisations and carry out attacks without direction but in support of terrorist objectives. Cyber actors able to conduct disruptive attacks for these purposes have the sophistication to carry out cyber fraud for terrorist financing: therefore any measures that can be applied in advance to cyber fraud activity may also have the unintended effect of mitigating terrorist financing.

Hacktivists are similar to cyber terrorists in that their tactics have been limited in overall effect. Motivated by social or political agendas, these actors typically conduct low level attacks such as defacement of websites or Distributed Denial of Service (DDoS) attacks to make websites unavailable. The most harmful activity attributed to these actors has been doxing, a practice of posting highly sensitive information about individuals online including social security number, date of birth, address, information on children and bank account numbers: cyber fraud tactics are not typical of this actor type. Cyber fraud is also atypical of the last cyber threat actor type known as 'insider' where malicious insiders intentionally misuse their trusted access rights to the network of their employer for the purpose of affecting the confidentiality, integrity or availability of the network or its data. Although the most publicised insider cases have typically involved destruction of network operations or theft of information some insiders have committed cyber fraud by abusing their entitlements to fraudulently transfer funds. Typically these actions fall under the category of embezzlement.

The progression in hacking means the gap is widening in the ability of an organisation to defend as quickly as it is attacked. Recent research shows the median number of days in 2015 for some of the most sophisticated attackers to be discovered on the network of a victim was 146[6]. A primary factor supporting this gap in time to detect is the ability of an adversary to seamlessly communicate as cyber criminals do not have to abide by country laws, regulations, company policies or the ability to provide customer service. All of these conditions present constraints to defenders which has resulted in a number of executive orders over the last two years mandating the sharing of threat information. Cybersecurity is now embedded in government policy priorities, such as the Cybersecurity National Action Plan of the US Government[7]. A primary component of this plan is for federal agencies to increase the availability of government-wide shared services for cybersecurity, building upon the 2015 Executive Order Promoting Private Sector Cybersecurity Information Sharing[8], which promotes the sharing of cyber threat information through Information Sharing and Analysis Organisations established by several of the crucial infrastructure sectors. The 2016 Executive Order[9] has further expanded this information sharing capability by enhancing the ability of private companies, nonprofit organisations and government agencies to exchange information on cyber incidents and risks.

Proactive fraud auditing

As cyber criminals diversify in their techniques to conduct cyber fraud it is imperative organisations examine their current approach to cyber security and consider implementing an intelligence led plans to preempt being exploited and exposed by cyber criminals. Proactive fraud auditing is one such proactive investigation technique: developed by W.S. Albrecht, it traditionally has been used by forensic accountants to help clients minimise their risk of falling victim to corporate fraud.

A fraud investigation generally arises from an internal tip that fraud is being perpetrated at a company. This process is reactive in nature and likely occurs long after the fraud initially began: recent research shows that, on average, it takes approximately 18 months to detect a fraud scheme and the longer the fraud goes undetected the higher the financial harm to the company.[10] A more effective approach is to use a proactive plan which limits the duration and cost of the scheme. Per Albrecht, the steps to proactively audit for fraud are: (1) identifying fraud risk exposures, (2) identifying the fraud symptoms of each exposure, (3) building audit programs to proactively look for symptoms and exposures, and (4) investigating symptoms identified.[11] While this technique is most commonly used to fight financial fraud it provides a framework that is a useful model for developing an intelligence led approach to proactively detect cyber fraud.

1. Identifying risk exposures

In addition to knowing the profile of a cyber criminal, building this plan starts with an assessment of the operating environment of an organisation. As criminals have moved to a shared services model to cut costs, so are organisations increasingly moving towards centralisation of services such as the consolidation and offshoring of treasury functions. As a result, many organisations do not have the level of direct oversight on security controls applied to these environments as they once did when the functions were managed from the physically owned and controlled facilities of the parent organisation. A baseline assessment of the operating environment should, at a minimum, include:

- Identification of essential systems and sensitive data that could be the target for an attack: a list of essential systems is often documented by the entity within an organisation responsible for business continuity planning. It is also important to understand if sensitive data being handled within any given department could have a severe effect on the organisation if it were made unavailable, such as patient records at a hospital. Many organisations have a method for classifying information as to its level of confidentiality, classification which can give insights into the data sets that should be prioritised for information security controls.

- An assessment of the vulnerabilities: every department in an organisation has unique procedures in place to define how business must be conducted, such as human resource departments typically able to access social networking sites for the purpose of recruitment. If other personnel in an organisation outside the human resources department are allowed the same level of access to social networking sites, such as security guards with access to the system of the organisation to check the global directory for employee contact information, the firm has introduced a vulnerability into its operating procedures because social networking sites can be used to introduce malware onto a network by an employee clicking on an advertisement infected on a social networking site.

- An inventory of controls: an inventory of the controls in place to close the identified vulnerabilities and protect the essential systems and sensitive data must be undertaken once there is a listing of essential systems, sensitive data and vulnerabilities; for example, organisations have implemented maker and checker procedures to ensure employee entitlements are restricted so one employee cannot initiate and approve a payment transfer. Understanding how essential the controls within a department are in protecting the essential systems of the firm and data can help in prioritising the full implementation of these controls. Sometimes firms overlook doing quarterly or bi-annual assessments on employee entitlements which means that employees who move between departments in an organisation my never have their entitlements granted from their previous positions turned off, creating what the industry calls toxic entitlements.

- Documentation of gaps in defensive: understanding where the cyber threat actor might interact within the environment enables a more accurate assessment as to whether controls in place are sufficient and appropriate policies are in place to govern the application of protocols and procedures to heighten security. Where policies are lacking a crucial gap can be addressed through the development of new policies that dictate the application of controls, such as restricting access to social networking sites by employees who do not need these sites to perform their job duties.

2. Identify the fraud symptoms of each exposure

Once the fraud risks have been identified then symptoms of each risk must be determined. In a corporate financial fraud the symptoms may include unusual journal entries, accounting irregularities, financial statement anomalies, unusual behavior by an employee, a reported tip or complaint. Symptoms for cyber fraud are similar as they most often include a break in protocol for how an organisation typically does business. The Business Email Compromise (BEC) scheme[12] is a prime example for how cyber criminals are adapting their social engineering techniques, resulting in US$3.1 billion in losses as of June 2016. There are multiple tactics used as part of the BEC scheme however all m are predicated on social engineering techniques used to deceive the victim into directing a wire payment to a new beneficiary account outside the normal business procedures of the victim. Social engineering techniques used in this scheme include phishing the victim, spoofing email addresses and calling the victim under the pretext of being a law firm offering services to the firm.

3. Building programs to adequately search for symptoms and exposures

Catching cyber fraud at its earliest stage is necessary to develop a system that will continually target the exposures and symptoms identified in Step 1 and Step 2. The system must be monitored and regularly audited to identify changes or irregularities in fraud symptoms.[13] Programs to identify if an employee has become a victim of a BEC scheme include implementation of verification procedures internal to the organisation when there is a change in beneficiary accounts as well as filters to assess incoming email from external parties. Consider the following scenarios:

- ‘**Urgent’ Request from a Senior Executive**

  One of the BEC scenarios involves an email being sent from the hacked or spoofed account of a senior executive, such as the CEO or CFO, to an employee responsible for wire transfers[14]. The email includes directions to initiate a wire transfer to an account not normally used and includes a sense of urgency, such as a deal which cannot close until payment is made. The email may also come at a time when the senior executive is on travel and cannot be easily contacted to verify the instruction. This scenario is typically successful because requests for new beneficiary accounts by internal employees come with a level of trust: some firms have therefore created an internal verification process wherein a verification code must be sent as a follow up to these types of irregular requests.

- **Request to Change Beneficiary Designations**

  Another BEC scenario involves the request by an external supplier who has a long standing relationship with the company and a level of trust to change beneficiary accounts[15]. Sometimes the cyber fraudster will initiate this change by calling the treasurer and letting them know the request will be coming so the treasurer does not think it is unusual when they receive the email. The request is then made from an email address that appears as the legitimate contact detail of the supplier but is slightly off with the addition of a period or dash, or missing letter in the name. A program to catch this type of cyber fraud is the addition of a filter for incoming email from an external party, such as color coding the email so the recipient knows the email is from an external provider and should be carefully checked. Another program that has been used is disabling the email functionality of the treasurer so the ‘Reply to Sender’ button cannot be used. This prevents the treasurer from replying to a false email address by requiring he or she to pick an address from their legitimate contact list. Most importantly, programs should include the reinforcement of existing procedures by the department head to ensure employees are not shortcutting verification in the event of new account requests, regardless of how urgent the request to do so.

4. Investigating fraud symptoms identified

If a fraud symptom has been identified it should be treated as a red flag. Further investigation will be needed to determine whether the symptom relates to actual fraud or a true unintentional error or glitch in the program built in Step 3. Similar to traditional fraud investigations, cyber fraud investigations require the preservation of documentation such as email communications received in the BEC scenarios. A culture must be created where employees feel comfortable reporting when they think they have been a victim of a cyber fraud without fear of retribution for not having followed the appropriate protocols for verification. Many times employees, particularly those new, do not know who to report to if they receive a possible phishing email, while first line mangers are often unaware of the information security officer of the organsiation who should receive details on the event to ensure the network has not been further breached. Furthermore, once it is established if a cyber fraud has been attempted or successfully committed it is essential to share details of how the scheme was conducted are shared with employees who may be exposed to similar tactics.

Future work

A preventative approach to fighting cybercrime is crucial for any organisation in its battle to protect its information and assets. Developing procedures to identify cyber fraud risk exposures and its symptoms is crucial. Once the risks and symptoms are identified it is important to build programs to aggressively search for those identified risks and investigate all instances detected. The goal of an intelligence-led approach is to detect and deter cyber fraud before it occurs while also limiting the financial and reputational damage caused by cybercrime.

The diversification of services of cyber actors used in an anatomy of a cyber attack has forced organisations to change the way they are defending their networks by customising defensive measures based on a study of the attack patterns of the cyber actor against the network. These defensive measures are however based on a narrow view of the attack activity of the cyber actor as the configuration of the network of the organisation and may preclude the observation of the full capabilities of the cyber actor. That same cyber actor may be attacking the network of another organisation with similar, but perhaps enhanced, techniques because of the structure of the organisation: as a result, neither organisation understands all of the tactics of the cyber actor. These gaps in understanding are referred to as knowledge gaps: organisations are coming together globally to exchange information in both public and private forums in order to address these gaps.

Despite efforts to increase information sharing among private, non-profit and public organisations there are no standards or uniform methods for structuring the information to be shared. Information sharing happens through conferences, phone calls and emails. The sharing of information is often tied to individuals in an organisation whose job it is to represent the company as external liaisons to both government and private working groups. Trust continues to be a crucial factor in sharing information, knowing neither competitive advantage nor prosecution could result from the sharing of cyber attack activity. In order to overcome these challenges of obtaining information that can fill knowledge gaps in how a cyber actor may commit fraud and share this threat information with the broadest group possible it is essential that a standard for reporting must be adopted and thresholds for reporting established.

As a result, organisations across industries must enhance communication channels to share threat information in order to preempt cyber fraud schemes. This requires both an ability to identify the patterns of behavior that indicate cyber fraud activity and a platform for communicating potential threat information. Research is continuing to develop cyber fraud typologies in order to build programs to adequately search for symptoms and exposures within an organisation along with the testing of a variety of tools to facilitate the sharing of cyber threat information.

This paper reflects the views of the authors and should not be viewed as representing the views of Citi nor the American University.

[1] Morgan, Steve. (2016) 'Cyber Crime Costs Projected To Reach $2 Trillion by 2019', 17th January, *Forbes*, available at: http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#466647753bb0 (accessed 10th October, 2016)

[2] Garter (2015) 'Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015', 10th November, *Gartner, available at:* http://www.gartner.com/newsroom/id/3165317 (accessed 17th October, 2016).

[3] Symantec (2016) 'Internet Security Threat Report 2016: A New Zero-Day Vulnerability Discovered Each Week', April 2016, *Symantec*, available at: https://www.symantec.com/content/dam/symantec/docs/infographics/istr-zero-day-en.pdf (accessed 17th October, 2016)

[4] Symantec (2016) 'An Internet Security Threat Report Special Report: Ransomware and Business 2016', 10th August, available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf (accessed 17th October, 2016)

[5] Internet Crime Complaint Center (2015) 'Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes', 23rd June, *Internet Crime Complaint Center (IC3)*. Federal Bureau of Investigation, available at: https://www.ic3.gov/media/2015/150623.aspx (accessed 25th October, 2016).

[6] FireEye (2016) 'FireEye Releases Mandiant M-Trends Report With Insights From Advanced Attack Investigation', 25th February, available at: http://investors.fireeye.com/releasedetail.cfm?releaseid=957111 (accessed 17th October, 2016).

[7] The White House (2016) 'FACT SHEET: Cybersecurity National Action Plan' Office of the Press Secretary, 9th February, available at: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (accessed 6th November 2016).

[8] The White House (2015) 'Executive Order -- Promoting Private Sector Cybersecurity Information Sharing' Office of the Press Secretary, 13th February, available at: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (accessed 6th November 2016).

[9] The White House (2016) 'Executive Order -- Commission on Enhancing National Cybersecurity', Office of the Press Secretary, 9th February, available at: https://www.whitehouse.gov/the-press-

office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity (accessed 6th November, 2016).

[10] Association of Certified Fraud Examiners (2016), ‘2016 Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse’, available at: http://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf (accessed 27th October, 2016)>

[11] Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., and Zimbelman, M. (2016). ‘Fraud Examination’. Cengage Learning.

[12] Internet Crime Complaint Center (2016) ‘Public Service Announcement Business E-mail Compromise: The 3.1 Billion Dollar Scam’, 14th June, available at: https://www.ic3.gov/media/2016/160614.aspx (accessed 6th November, 2016).

[13] Rojo, C. (2016) ‘Fight Fraud by Auditing Internally’ 5th May, HeinfeldMeech, available: https://www.heinfeldmeech.com/resources/blog/fight-fraud-audit-internally (accessed 27th October, 2016).

[14] Internet Crime Complaint Center (2016) ‘Public Service Announcement Business E-mail Compromise: The 3.1 Billion Dollar Scam’ 14th June, available at: https://www.ic3.gov/media/2016/160614.aspx (accessed 6th November, 2016).

[15] Ibid.