Fighting cybercrime calls for developing effective strategy

Richard McMahon
University of Houston-Downtown

Darlene Serrato
Houston Baptist University

Linda Bressler
University of Houston-Downtown

Martin Bressler
Southeastern Oklahoma State University - Durant, TX

ABSTRACT

Almost every day one can read of another example of cybercrime activity, whether in the form of fraud, embezzlement, intellectual property theft, or other criminal activity. Corporate investors certainly have a concern over this situation as these cyber-crimes impact the bottom-line, but individuals and even the federal government should be concerned with the increasing number of cyber-attacks (June, 2008). Individuals like you and I have our personal data at risk and can fall victim to mortgage and real-estate scams. Government understands that these financial cyber-attacks can undermine our economy.

In this paper, the authors present a description of cyber-crime activity and provide a variety of examples across various industries. Then, the authors discuss preventive measures that can be leveraged into a prevention-detection strategy.

Keywords: Black Hat Hackers, Corporate spooks, Cybercrime, EMV, Fraud Incident Response Plan, Malware, Phishing, Red Flags of Fraud, Social Engineering, Talent Raids

INTRODUCTION

Newspapers and other media regularly report new cases of fraud or cybercrime. Cybercrime can include theft of financial resources through the use of a hacker, phishing activity, employee talent raiding and an increasing amount of theft activity (Chabrow, 2008; Cybercrime against Businesses, 2005; Eisenberg & Shannon & Baker, et al, 1999). Research shows numerous cases of identity theft, fraud, as well as corporate espionage and social engineering. In addition, there also appears to be a rise in proprietary information theft as well as raiding corporate talent or talent raids (Eisenberg, Shannon & Baker, et al, 1999; Fitzpatrick, DiLullo & Burke, 2004; Gottipati, 2012; Holstein, 1998; Horovitz, 2009; How Real, 2009; Perry, 2001) and corporate spook activity (Chabrow, 2008; Chan, 2003; Grosso, 2000; Klausemen, 2007)

Researchers indicate that although fraud in business can be found in the news on an almost daily basis (espionage also known as corporate spook activity) also continues to grow and can be considered on the rise (Gardner, 2002; Lazzara, 2001; Tarm, 2011).

Espionage

Reports of espionage activity can often be found in the newspapers and other media outlets. In addition, corporate spooks are so prevalent that they started a professional association called the Society for Competitive Intelligence Professionals (SCIP). The number of investigative experts or corporate spooks will continue to increase in demand even though companies may be extremely discrete about hiring such trained employees (Higgins, 2004; Klausman, 2007). But, for every investigative employee a company hires, there could very well be an increase in "black-hat" investigators as well. These trained individuals sometimes come from post-Cold War countries, including China. Tarm (2011) reported that the Chinese can be the most active espionage offenders in the United States and the author spoke of a case regarding Hanjuan Jin, a Chinese-born American, who removed documents from Motorola in 2007 stating she needed to refresh her memory after an extended medical absence. Fortunately, a customs agent stopped her on a random check because she carried $31,000 in cash and the customs agent also found many electronically-stored documents. Apparently, without approval from Motorola, the woman began working for a technology company in China during her medical leave and planned to sell the proprietary information to China.

Intellectual property

Sometimes fraud perpetrators utilize pretexting to get confidential information from a company. A recent case involved an accountant at one of the Big 4 Accounting firms. The accountant gave confidential information to an individual over the phone because the caller indicated he was a British Intelligence agent working on a national security project. In reality, the caller was a lobbyist representing a Russian conglomerate. The Russian gentleman apparently was convincing enough for the accountant to give out the requested information. However, an important internal control in place could have required the accountant to place a

phone call to the British government (before handing over the information) and this simple control could have stopped this fraud immediately (Tarm, 2011).

Another failed corporate theft attempt dealt with an employee at Intel planning to steal the blueprints for the Intel Pentium Processor. The employee tried to download the file to his own home computer, but the theft-deterrent software stopped this from happening. Then the employee simply and quickly videotaped each screenshot file without much effort. However, additional controls in place at the company (including employee activity monitoring) could have halted this fraud activity before the perpetrator attempted to sell the videotaped proprietary secrets (Ruhl, 1999).

Talent raids

Gardner (2002) called the phenomenon of talent raids as "War for Talent." The author mentions that in the past, more consideration should have been given toward competition in the market and market niche. However, now battles can be noted on the market for employees (Eisenberg, et.al., 1999). When businesses think of corporate theft, many times they think mostly about cash or property theft. However, proprietary information theft and corporate or talent raids can also be important. Researchers indicate significance in studies dealing with human capital and financial success (Brotherton, 1996; Gardner, 2002). For example, a family from Taiwan working for a Taiwan company attempted to obtain company secrets from Avery-Dennison (the label company) and would have been willing to hire away a United States research engineer to obtain company secrets which would provide the Taiwan company with scarce [trained] human capital (Gardner, 2002).

There can be many strategies to attract and keep these valuable employees; including monetary retention strategies, increased or unique benefit offerings to employees, promotion or lateral career opportunities while the company plans to deflect and/or diminish the attacks of direct competitors. Gardner's study (2002) noted that the higher perceived threat of losing valued employees in an organization, the more likely the firm will respond with externally-focused strategies. In addition, the study noted that *skill mobility* plays an important role on how a firm will deal with a talent raid. The easier it would be for employees to move from one organization to another (easily-transferrable skills), the greater the effort will be made to thwart the raiding company's efforts.

So, what can companies do about corporate raiding (Sullivan, J. 2000)? It is not enough for companies to concentrate on hiring and training their staff. Gardner further indicates that companies need to work to gain advantage over their rival companies and attempt to predict and prepare for possible raiding. The author noted that companies do make attempts via raises and other creative actions which, unfortunately are usually imitated by competitors (Gardner, 2002).

Research suggests that companies should be sure to conduct thorough exit interviews even though Human Resource professionals many times believe these interviews will not be of any value because employees will not share their true reasons for leaving, being afraid to burn bridges. The authors suggest asking questions in order to gain a good understanding of how the employee was contacted, and who conducted the raiding contact. These types of questions will be particularly helpful in understanding employee turnover issues (Brotherton, 1996; Ruhl, 2004). Along with talent raids comes the opportunity for severe security breaches such as trained employees moving from one competitor to another; whether or not these employees signed a non-compete contract.

Security Breaches

All too often heightened security awareness takes the form of yet another press-conference notification of a security breach as large retailers reluctantly report evidence of hackers gaining access to company databases containing customers' financial information. Some of the past year's retailer-admitted compromises include Target, TJX, and Neiman Marcus. The incursion at Target exposed over 40 million customer accounts, at TJX it exposed about the same number (Poulsen, 2014), and at Neiman Marcus it exposed 1.1 million customer accounts. Adding insult to injury, months after rather large incursions such as these should have resulted in similarly large retailers implementing the resulting fix, hackers employed the same malware exploit and obtained financial information of over 56 million Home Depot customers (Krebs, 2014; Pouleson, 2014). The stolen information from both Target and Home Depot customer credit and debit cards both showed up for sale at the same underground cybercrime shop, conclusive evidence of a connection between the two crimes at a very high level.

Typically, cyber-criminals access a large company's customer accounts by way of a smaller third-party vendor with access to the larger company's website for invoicing purposes but that is not always the case even when there are far-reaching implications from a widespread breach. Security standards require debit or credit card payment processing over a secure connection, encryption of card data, authentication for remote access to and from PoS (Point-of-Sale) cash register machines, and many other security measures that help ensure transactions remain safe from unauthorized access (Crossman, 2014).

Sometimes, as in a recent data breach of a sandwich retailer's chain, the process of certifying that a third-party invoicing process can itself be the weakness and all it takes is an unauthorized person gaining access to what should be secure information. The Jimmy John's sandwich restaurant chain recently confirmed that they came under attack when Signature Systems, their secure transaction firm, failed to remain compliant with industry standards and their failure allowed compromised customer information at Jimmy John's 216 sandwich shop locations when a single individual obtained the remote administration access username and password.

Information-stealing malware was then installed on Jimmy John's cash registers and the data from credit and debit cards being read at the point-of-sale registers were compromised. The Signature Systems transaction process had been certified compliant by the firm Chief Security Officers but was not re-certified after that company became defunct (Krebbs, 2014; Pymnts, 2014). Further, Jimmy John's indicated that their breach may also involve customer debit and credit cards at 100 other independent restaurants nationwide who use its products. This attack was also unusual in that normally cyber criminals not only have to find a way to collect the PoS data (http://www.entrepreneur.com/encyclopedia/point-of-sale-pos-system) during each sale but the criminal also has to then "exfiltrate" the stolen data from the victim company's location to their own location so that it is under the criminal's control (Crossman, 2014). The thief in the Jimmy John's incident solved both problems with the unauthorized access obtained from a single user account.

Large retailers are not the only companies impacted by security breaches. Hotel chains Marriott, Sheraton, and Inter-Continental also suffered data breaches through their restaurant and lounge operations (Chabrow, 2008; Reuters, February 3, 2014). White Lodging Services

Corporation operates 169 hotels under those franchise brands across the country. In the past year alone, the Federal Bureau of Investigation (FBI) had under investigation an estimated 20 such security breach cases involving data gathering malware. In fact, Experian reports that small businesses experienced a 300% increase in cyber-attacks from 2011 to 2012 (Experian 2014 Data Breach Industry Forecast).

Furthermore, the nonprofit Privacy Rights Clearinghouse calculated that businesses (including financial institutions and retail outlets) have reported 1,571 breaches involving 470 million customers' financial records during the past 9 years (Lillard, 2014). In addition to noting the significant numbers of these breaches, it should be emphasized that they are usually not haphazard, amateur-like, or opportunistic in nature. Rather, they reflect deliberate efforts and long-term planning of highly dedicated individuals – sometimes probing for weaknesses months ahead of their actual planned attack.

These security issues highlight the need for better debit and credit card technology, possibly using an embedded data chip instead of the usual magnetic stripe of recording media on the back of these cards (Poulsen, 2014). The magnetic data stripe (or magstripe) still widely in use today is based on technology developed in 1960 by Forrest Parry, an IBM engineer (Poulsen, 2014), and used extensively since the 1970's. Recorded in that magstripe is sufficient information to flawlessly create a counterfeit card – the customer's account number, the card's expiration date, and the 'secret' code (called the CVV). The information on that stripe has become criminals' prized targets. In contrast to that strip's ability to store only a limited amount of information and thus able to provide only a low level of security, the newer chip-embedded cards including more security information and can, therefore, provide much higher data security. Target Chief Financial Officer Mike Mulligan estimates the company will spend about $100 million to update their credit cards to the chip technology and install readers in their 1,800 retail stores (USA Today, 2014). However, until that happens, by even conservative estimates, annual losses from fake IDs and fake cards add up to $11 billion (Poulsen, 2014).

According to Andress, 2004. banks and retailers in many countries use chip-and-personal identification number (PIN) or chip-and-signature, or chip-and-choice, also called EMV (Chasepaymentech, 2014),) to secure their transactions with information embedded in a chip on the card instead of simply recorded on a magnetic strip on back of the card. This provides the additional measure vendors such as Micro Trend and Chase (Paymentech, 2014) suggest as a primary method for increasing transaction security. The use of EMV cards is becoming the global standard for debit and credit card payments since the dynamic authentication capabilities (dynamic values existing within the chip on the cards) ensure a particular card's authenticity. The technology was first used in France in 1992 but their use is worldwide and currently there are over 1 billion chip cards in use around the globe.

Crimes by the numbers

Though difficult to estimate, according to the 2013 Online Fraud Report, U.S. firms lost more than $3.5 billion in commercial sales, or approximately .09% of sales to online fraud activity. This figure represents an increase of more than $100,000,000 since 2011. Many consider that to be just one of the costs associated with cybercrime. The U.S. Chamber of Commerce reports that just in the area of intellectual property, the United States loses more than $52 billion annually in lost tax revenue (U.S. Chamber of Commerce press release, February 3, 2010).

Fraud and embezzlement can sometimes be perpetrated through the internet. In addition, cybercrimes also include money-laundering, fraud, insider-trading, and intellectual property theft. With fraud alone, the FBI reports almost a 40% increase in pending cases during the 2007-2011 period (Financial Crimes Report to the Republic). Some instances of fraud especially those in the areas of real estate and financial investments, may involve Ponzi schemes. Such was the case of a Minnesota construction and property management firm. Principal Michael Mangan has been charged with several counts of wire fraud and mail fraud of funds in excess of a million dollars from investors (FBI Press Release, September 25, 2014).

The FBI continues to expand resources directed toward cyber-crime activities. In addition to the Cyber Division at FBI headquarters, there are specially-trained cyber squads assigned to each of the 56 FBI field offices, Cyber Action teams that can travel around the world at a moments' notice, and 93 Computer Crimes Task Forces that work alongside state and local law enforcement agencies. In addition, the FBI operates in partnership with a number of federal agencies including the Department of Homeland Security and the Department of Defense (http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions).

To give the reader an idea of the scope of criminal activity and the resources necessary to combat cyber-crime on a global level, one only needs to look at the high-tech heist of 2008 when more than 2100 ATM machines in at least 280 cities spread over three continents were hit by cyber criminals simultaneously (FBI News Stories, 2009).

Particular caution should be paid to online mobile payments. CyberSource reports that in 2012, mobile commercial sales would be an estimated $24.7 billion. That figure represented an increase of 82% over the previous year, 2011. Despite this meteoric growth, CyberSource reported that mobile commerce would be the least likely channel to be evaluated for payment fraud. In addition, merchants should closely scrutinize foreign orders as the fraud rate for internet orders from outside the United States is more than double the domestic rate –approximately 7.5% vs. 2.9% (2013 Online Fraud Report).

Building thee defense-four security tactics

As can be noted in Figure 1, CyberSource developed IT fraud security tactics that can be broken down into four categories: Customer History, Purchase Device Tracing, Multi-Merchant Purchase History, and Validation Services. Customer History looks at data such as customer order history and customer website behavior. Purchase Device Tracing tracks and verifies the device used to place the order, sometimes using GPS for verification. Multi-Merchant Purchase History data is based upon shared lists, especially negative lists or hotlists. Finally, Validation Services include credit card verification numbers, two-factor phone verification and postal address verification (2013 Online Fraud Report).

CyberSource knows cyber-security, as they are a VISA company. Their experience shows that 40% of companies track fraud for manually reviewed orders and find 4% to be fraudulent (2013 Online Fraud Report). Note that these tactics focus on preventive techniques, the most financially sound way to fight cyber-crime.

Both academic researchers and practitioners generally agree that businesses should first begin with preventive controls, then, focus on developing detection controls and finally, incorporate corrective controls. The emphasis on preventive measures is because it is much better for the firm to prevent a security breach rather than spending time and money investigating, replacing weak internal controls, etc. Even though incidences of embezzlement are

less common than many other types of crimes, in many instances embezzlement can result in more significant losses for the firm. Table 1 below, shows the number of reported instances of embezzlement compared to other types of crimes. As noted, a typical instance of embezzlement costs the company $1,379,447.

Table 1: Cost of Selected Crimes Committed Against Businesses, 2007

Type of Crime	Number of Incidents	Cost	Cost per Incident
Embezzlement	15,151	$20.9 Billion	$1,379,447
Burglary	700,239	$1.4 Billion	$1,991
Shoplifting	785,228	$1.6 Billion	$205

Nonprofit organizations and government agencies should not consider themselves immune to embezzlement. Judith Oakes, an accountant with the San Bernardino, California School District is being charged with embezzlement of an estimated $3.1 million over the last 14 years from the schools' lunch program. Red flags that should have been obvious would be the couples' lavish lifestyle expenditures including an expensive home and multiple recreational vehicles.

A fairly inexpensive preventive measure could be to conduct employee background checks. Another preventive measure would be to initiate credit checks on new employees and periodic credit checks everyone else because employees home life situations, financial situations, etc. can change (Barron et al, 1985). According to Cressey's Fraud Triangle (Cressy, 1973), employees who commit theft or embezzlement are able to do so, in part, because there is an *opportunity* to do so. Sound preventive measures can reduce or eliminate the opportunity for criminal activity (Antenucci, et al., 2009).

TERMINOLOGY

Black Hat Hackers: computer criminals, not to be confused with a White Hat Hackers who are hired as corporate security experts and are not considered criminals. (http://www.ask.com/wiki/Hacker_(computer_security).

Corporate spooks: spies – sometimes called "competitive intelligence professionals." (http://www.commondreams.org/views01/0306-03.htm).

Cybercrime: criminal activity or a crime that involves the Internet, a computer system, or computer technology: identity theft, phishing, and other kinds of cybercrime. (http://dictionary.reference.com/browse/cybercrime).

EMV: stands for Europay, MasterCard and Visa, a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines(ATMs), authenticating credit and debit card transactions. (http://en.wikipedia.org/wiki/EMV).

Fraud Incident Response Plan: an Incident Response Plan which documents a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization. The Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action (http://www.aicpa.org/_catalogs/masterpage/Search.aspx?S=an+Incident+Response+Plan).

Malware: short for malicious software, malware is software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse (http://www.webopedia.com/TERM/M/malware.html).

Phishing: trying to obtain financial or other confidential information from Internet users, typically by sending an e-mail that looks as if it is from a legitimate organization, usually a financial institution. It also typically contains a link to a fake website that closely resembles the real one (http://www.ask.com/web?qsrc=1&o=0&l=dir&q=phishing).

PoS Data: the set of data available from utilizing a computerized network operated by a main computer and linked to several Point-of-Sale checkout terminals (http://www.entrepreneur.com/encyclopedia/point-of-sale-pos-system).

Pretexting: contacting a competitor under some pretext, such as pretending to be a customer to obtain pricing or other competitor information or, in some cases, pretending to be an employee in order to gather data, steal information or plant listening devices (http://dictionary.reference.com/browse/pretexting).

Red Flags of Fraud: warning signs that may indicate a heightened fraud risk. They are not evidence that fraud is actually occurring. Many employees demonstrate one or more of the flags on the list, and the existence of one or two flags is not likely to cause concern. However, if multiple flags are identified that span the three categories of accounting irregularities and/or weak internal controls are identified, the risk that fraud is occurring or could occur is significantly higher (http://www.osc.state.ny.us/localgov/pubs/red_flags_fraud.pdf).

Social Engineering: a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures (http://searchsecurity.techtarget.com/definition/social-engineering).

Talent Raids: usually a recruiting tactic where a competitor successfully hires several employees from a competitor. Raiding differs from poaching in that instead of hiring one key employee, the rival hires multiple employees (http://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1027&context=cahrswp; Perry, 2001).

DISCUSSION

Security Defense

The best defense in security could actually be a good (and well-rehearsed) offense. In addition to implementing an EMV migration (Chasepaymentech, 2014), organizations intent on keeping their transactions secure will need to do an extensive security evaluation. In fact, according to the Illinois Banker (Lillard, 2014), while converting to EMV will relieve many of the present debit and credit transaction headaches, all organizations currently involved with debit or credit card transactions are up against what they call *fraudsters* who are intelligent, coordinated, strategic, and stealthy. Companies need a Fraud Incident Response Plan and those without one already should consider developing one before more widespread incidents involve their customers. During last year's holiday breaches, much less chaos was evident in organizations with such plans in place, especially when those plans had been exercised in planned rehearsals. The need for a plan will still exist beyond even a global EMV migration since thieves will likely develop still more-advanced techniques to steal from consumers and businesses alike.

T
R

Andress, (2004) recommends implementing the following company data center controls:

- Restrict communication in and out of your environment to only what is required.
- Ensure that you are constantly protected against vulnerabilities in both systems and applications, even in-between patch cycles.
- Identify when a system component has been changed.
- Protect against malware and malicious URLs.
- Encrypt communication between applications and data.
- Continuously scan Web applications for potential vulnerabilities.

Organizations should be conducting a security internal control evaluation and IT staff should be reminded that utilizing one solution will not necessarily protect the company's assets, information, etc. from predators. One example of how easy it would be to attack a company's security systems could be the ease of replacing a cell phone battery with a microphone attached so that conversations can be taped. With PCs, a memorizing keyboard could be switched with an existing keyboard so that staff keystrokes could be monitored. In addition, it is sad to say, but individuals can either record conversations and/or spy on staff members inputting their passwords as the technology exists whereby microphones can be set up to record sound from hundreds of feet away (Higgins, 2004).

The SEC has specified that cyber-attacks can expose companies to the following:

"- Remedial costs associated with a loss of data and information in the loss of business after an attack

- Costs of cybersecurity
- Loss of revenues due to a loss of data or customers
- Regular fines
- Litigation costs
- Reputational damage that can lead to loss of customers and reduces investor confidence" (Grant, 2014)

As a result, the SEC is requesting that the integrated audit of internal controls be expanded to include IT controls, including those not directly related to the financial statements. The SEC has gone as far as to require that management specify in the Management Discussion and Analysis (M, D & A) costs related to cyber security or a lack of security. Risk analysis of cyber security should also be specified in the quarterly and annual reports.

When a company has had a security breach, there is a ripple effect on companies that do business with the affected firm. A study by the American Bankers Association and Kaspersky Lab surveyed more than 3,900 financial and other companies worldwide and found the cost of a data breach ranged from $66,000 to $938,000 per organization. The financial institutions are affected by fraudulent use of debit cards and credit cards, with the average loss from Target's data breach being between $331 and $530 per card (Crosman, 2014). The financial institutions also had costs associated with having to reissue debit and credit cards to their customers; having to handle customer service calls; and having to replace customers that left because of the data breach.

As noted previously, a thorough employee screening process should be employed that includes background checks, credit history reports, prior behaviors, etc. (Barron et al, 1985; Pittori, 1998—cited in Fitzpatrick). Holtfreter (2004) indicates that a background check should be conducted asking why prior employees left their jobs. In addition, part of the background check might find criminal activity that the employee forgot to list on their job application.

Again, not only should these techniques be utilized at the hiring date, but they might also be reaccomplished a year or two into the staff's employment as well.

Researchers note that most company thefts will be initiated by employees; which suggests that strong internal controls should be put in place (Lazzara, 2001). Other researchers warn that increases in employee theft will be higher during times of layoffs and other downsizing efforts; indicating that these thefts deal with rationalization of the employees (Cressy, 1973; How Real, 2009).

Schlotter (2003) suggests increased training efforts for security personnel because as security breaches will be corrected, other new security breaches will continuously be a threat. Still other researchers advocate a company-wide effort by being proactive, communicating the importance of security and that security is every employee's job (Lazzara, 2001).

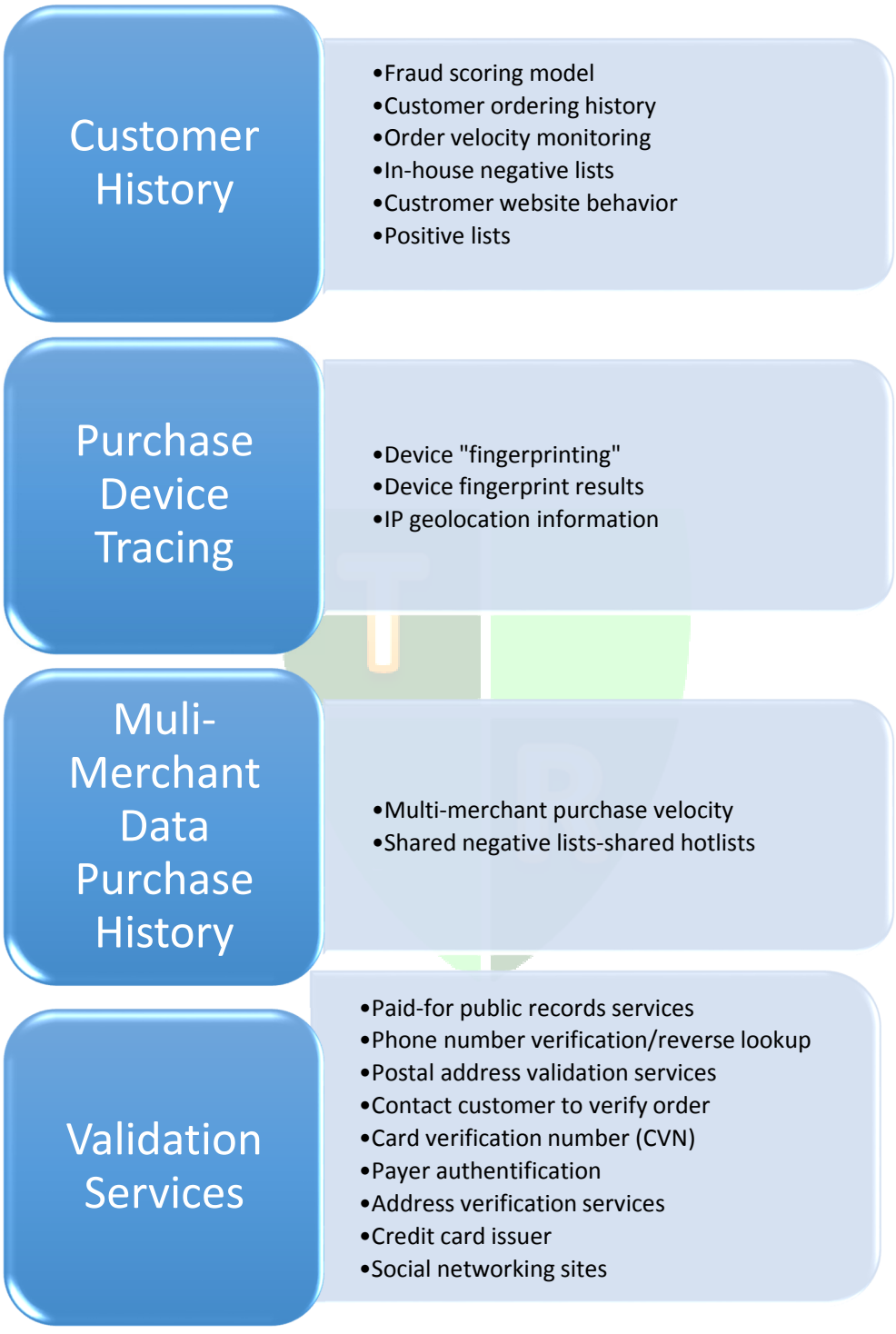
SUMMARY and CONCLUSION

Perhaps a good start in defending against cyber-crimes is legislation that recognizes the seriousness of the crimes and provides for significant punishment to the criminal hackers. New laws addressing cyber-crime activity are being passed which do address various types of criminal activity (Leger, 2014). For example, in 2010 Congress passed H.R. 4061 which addresses various forms of cyber-crime activity, specifically theft of intellectual property. The U.S. Chamber of Commerce lauded this effort, citing the importance of protecting U.S. products and services from global online piracy (U.S. Chamber Hails Passage, 2010).

Legislation however, will simply not be enough to defend against global cyber-crime activity. Companies need to take an aggressive, pro-active stance in protecting their corporate assets. This means funding budgets sufficiently to meet the challenge presented by cyber-criminals. Budgets need to be developed that not only provide personnel and equipment/software, but also training in defending against and uncovering cyber-crimes. Since 1997, when the National Cyber-Forensics & Training Alliance (NCFTA) was formed, private industry, law enforcement and academia have come together to develop best practices in how to deter and detect cyber-crime activity.

Corporations, non-profits and governmental agencies must build a strong defense against cyber-crime beginning with the strategic development of business tools to prevent and detect various forms of cyber-crimes. Should companies fail to do so, they will be putting corporate assets at risk in addition to our economic confidence.

Figure 1 Most Effective Fraud Management Tools



Source: Data compiled from CyberSource, 2013 Online Fraud Report

REFERENCES

2013 Online Fraud Report, Online Payment Fraud Trends, Merchant Practices, and Benchmarks CyberSource, 14th annual edition.

Andress, A. (2004). *Surviving security: how to integrate people, process, and technology*. CRC press.

Antenucci, J., Tackett, J., Wolf, F., & Claypoold, G. A. (2009). The rationalization of academic dishonesty in business students. *Journal of Business and Accounting*, *2*(1), 77-92.

Barron, J., Bishop, J., & Dunkelberg, W. (1985). Employer Search: The interviewing and hiring of new employees. Review of Economics and Statistics, 67(1), 43-52

Brotherton, P. *(*1996*).* Exit interviews can provide a reality check. *HRMagazine, 41 (*August*),* 45–49.

Chabrow, E. (2008, June). A Corporate Spy Story. *CIOINSIGHT*, 13.

Chan, M. (2003). Corporate Espionage and Workplace Trust/Distrust. *Journal of Business Ethics, 42*, 45-58.

Credit card data breach targets Marriott, Sheraton, other hotels. Reuters News Service, February 3, 2014 retrieved at www.reuters.com/assets/USBREA1300120140204.

Cressey, D.R. (1973). *Other People's Money.* Montclair: Patterson Smith.

Crossman, Penny (9/12/2014). How much do data breaches cost? Two studies attempt a tally. *American Banker, 179*, 1.

Cybercrime against Businesses, 2005. Bureau of Justice Statistics Special Report, September, 2008. NCJ 221943.

Eisenberg, D., Shannon, E., Baker, J., Gilbert, M., Maloney, J., Nissenbaum, D. (1999, March 22). Eyeing the competition. *Time, 153, 11*, 26-28.

Experian 2014 Data Breach Industry Forecast.

FBI News Stories, 2009. High-Tech Heist, http://fbi.gov/news/stories/2009/november/atm_111609.

FBI Press Release (September 25, 2014). Federal Bureau of Investigation, Minneapolis Division, Minnesota.

Financial Crimes Report to the Public 2010-2011, Federal Bureau of Investigation, http://www.fbi.gov/stats/publications/financial-crimes-report-2010-2011.

Fitzpatrick, W., DiLullo, S., & Burke, D. (2004). Trade Secret Piracy and Protection: Corporate Espionage, Corporate Security and the Law. *ACR, 12, 1*, 57-71.

Gardner, T. M. (2002). In the trenches at the talent wars: Competitive interactions for scarce human resources. *Human Resource Management, 41, 2,* 225-237.

Gottipati, S. (2012). Survey Finds Widespread Spying by Indian Companies. http://india.blogs.nytimes.com/2012/06/19/survey-finds-widespread-spying-by-indian-companies.

Grant, Gerry H and Grant, C. Terry (May, 2014). SEC cybersecurity disclosure guidance is quickly becoming a requirement. *The CPAJournal, 84,5, 69-71.*

Grosso, A. (August, 2000). The Economic Espionage Act: Touring the Minefields. *Communications of the ACM, 43, 8*, 15-18.

Higgins, J. (2004). Clear and Present Danger, 58(3), 78-83.

Holtfreter, K (2004). Fraud in U.S. Organizations: An examination of Control Mechanisms 88-94. *Journal of Financial Crime, 12, 1* 88-95.

Holstein, W.J. (1998). Corporate spy wars. *U.S. News & World Report, 124(7),* 6-48.Horovitz, S. (2009). If You Ain't Cheating You Ain't Trying: "Spygate" and the Legal Implications of Trying Too Hard. *Texas Intellectual Property Law Journal. 17*, 305-331.
How Real is the Risk of Corporate Espionage Today? Security Director's Report (April, 2009), 09-04, www.ioma.com/secure. http://business.highbeam.com/articles/6079/security-director-report/april-2009.
Retrieved 10/15/2014 from http://www.aicpa.org/_catalogs/masterpage/Search.aspx?S=an+Incident+Response+Plan.
Retrieved 10/04/2014 from http://www.ask.com/wiki/Hacker_(computer_security).
Retrieved 10/07/2014 from http://www.ask.com/web?qsrc=1&o=0&l=dir&q=phishing.
Retrieved 10/15/2014 from http://business.highbeam.com/articles/6079/security-director-report/april-2009.
Retrieved 10/07/2014 from http://www.commondreams.org/views01/0306-03.htmsearchsdigit.
Retrieved 10/07/2014 from http://dictionary.reference.com/browse/pretexting.
Retrieved 10/04/2014 from http://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1027&context=cahrsw..
Retrieved 10/15/2014 from http://en.wikipedia.org/wiki/EMV
Retrieved 09/27/2014 from http://www.entrepreneur.com/encyclopedia/point-of-sale-pos-system
Retrieved 10/04/2014 from http://www.sans.org/security-resources/glossary-of-terms
Retrieved 10/04/2014 from http://searchsecurity.techtarget.com/definition/social-engineering
Retrieved 10/07/2014 from http://www.webopedia.com/TERM/M/malware.html.
June, A.W. (2008). Public colleges fight raids on faculties. *The Chronicle of Higher Education*, August 15, www.fbi.gov http://chronicle.com/weekly/v54/i49/49a00102.htm.
Klausman, William (2007). "Corporate Spooks—Never Heard of'Em." *Journal of Information Ethics 16.1* 99-102.
Krebbs (2014). Home Depot hit by same malware as Target. Krebbs on Security, September 14, retrieved at www.krebsonsecurity.com/2014.
Lazzara, S. (March 1, 2001). Safeguarding the company's jewels. *Machine Design*, 128-134.
Leger, D. (2014). Obama Administration seeks tougher cyber-security law. USA Today, February 4, retrieved at www.usatoday.com/story/news.
Lillard, E. (Jul/Aug 2014). Planning now can limit future data breech losses. *Illinois Banker*, 99(4), 20-21.
Nissenbaum, Dion. Eyeing the Competition. Time. 3/22/1999, 153(11), 58-60.
Paymentech (2014). FAQ: EMV chip card technology. Chase, retrieved at www.chasepaymentech.com/faq_emv_chip_card_technology.html.
Perry, P. M. (2001). Holding your top talent. *Research-Technology Management*, *44*(3), 26-30.
Poulsen, K. (2014). Why the heyday of credit card fraud is almost over.retrieved at www.wired.com/2014/9/emv.
Pymnts (2014). The latest POS breach – Who and how. Pymnts, September 29, retrieved at www.payments.com/news.
Ruhl, C. (Spring, 1999). Corporate and economic espionage: A model penal approach for legal deterrence to theft of corporate trade secrets and proprietary business information. *Valparaiso University Law Review, 33, 2*, 763-811.

Schlotter, C. (2003). Anti-Hacking: The Protection of Computers. SANS Institute Reading Room. http://www.sans.org/reading_room/whitepapers/attacking/anti-hacking-protection-computers_38.

Sullivan, J. 2000. How to block a firm from "raiding"/stealing your employees - (Large scale "anti-raiding" and "blocking" strategies). www.erexchange.com/daily/search.asp?author id=9. Electronic Recruiting Exchange, 21 April. 6/26/2000.

Tarm, M. (2011, November 7). Corporate-China espionage trial begins in U.S. Associated Press, retrieved from Newspaper Source Plus, 09/18/2012.

U.S. Chamber Hails Passage of Cybersecurity Measure Enhancing Efforts to Fight IP Crimes, February 3, 2010, U.S. Chamber of Commerce (https://www.uschamber.com/press-release/us-chamber-hails-passage-cybersecurity-measure-enhancing-efforts-fight-ip-crimes).