Impact of Cybercrime on Organizations

Kanav Singla

Professional Communications (PRS 603 I01)

University of North Alabama

Author Note

Kanav Singla, Department of Interdisciplinary and Professional Studies, University of North Alabama

Correspondence concerning this article should be addressed to Kanav Singla, provide a mailing address

Contact: [ksingla@una.edu](mailto:ksingla@una.edu)

Table of Contents

[Abstract 3](#_Toc7260231)

[Introduction and Statement of Problem 4](#_Toc7260232)

[Justifications of the Study 5](#_Toc7260233)

[Financial loss due to Cybercrime 6](#_Toc7260234)

[Steps taken by Organizations 6](#_Toc7260235)

[Data lost due to Cyber Crime 7](#_Toc7260236)

[Literature Review 8](#_Toc7260237)

[Categories of Cyber Crime 8](#_Toc7260238)

[Data Crime 8](#_Toc7260239)

[Network Crime 10](#_Toc7260240)

[Access Crime 10](#_Toc7260241)

[Types of Cyber Crime 11](#_Toc7260242)

[Theft of Telecommunications Services 11](#_Toc7260243)

[Communications in furtherance of criminal 11](#_Toc7260244)

[Sales and Investment Fraud 12](#_Toc7260245)

[Electronic Funds Transfer 13](#_Toc7260246)

[Impact of Cyber Crime 13](#_Toc7260247)

[Impact of Cyber Crime over Private Industry 13](#_Toc7260248)

[Impact of Cyber Crime over Business 14](#_Toc7260249)

[Future Trends in Cyber Crime 14](#_Toc7260250)

[Summation of Literature Review 15](#_Toc7260251)

[Recommendations 15](#_Toc7260252)

[Awareness Building 15](#_Toc7260253)

[Technological Backup 16](#_Toc7260254)

[Working with invested partners 17](#_Toc7260255)

[Implementation of Recommendations 17](#_Toc7260256)

[Raising Awareness 17](#_Toc7260257)

[Leveraging trusted resources 18](#_Toc7260258)

[Hire Professionals 18](#_Toc7260259)

[Evaluation and Follow-Up 19](#_Toc7260260)

[Conclusion 20](#_Toc7260261)

[References 21](#_Toc7260262)

# Abstract

As cyber-attacks increase in severity and complexity, the private sector must seek to reduce as much vulnerability as possible. Based on recent studies, the attackers are rarely lone wolves but organized groups of criminals with vast networks and resources. Many of the organizations are state-affiliated, presenting an increasingly complex political frontier for the private and public sectors. As organizations deal with current issues they also face the task of preparing for future ones. Cybercrime has impacted organizations and big giants like Amazon, Google, Microsoft have also taken steps to enhance their security because the privacy of data is the biggest challenge to companies. This research shows that cybersecurity is now one of the top security priorities for nine of ten companies worldwide. The saying among security professionals is that there are two types of organizations: those who have been infiltrated and those who have and do not know it yet. Though it is largely impossible to completely prevent attacks implementing formal policies and security tools can protect networks and mitigate the damage of a breach.

*Keywords:* Organizations, Employee, Cyber-attacks, Privacy, Cybersecurity.

# Introduction and Statement of Problem

In our modern technology-driven age, keeping our personal information private is becoming more difficult. The truth is, highly classified details are increasingly being stored in public databases, and our personal data with organizations are more interconnected than ever. Further, these data are available for almost anyone to sift through due to this interconnectivity. This creates a negative stigma that the use of technology is dangerous because practically anyone can access one's private information for a price (Williams,2002). Technology continues to promise to ease our daily lives; however, there are dangers of using technology. One of the main dangers of using technology is the threat of cybercrimes.

Common internet users may be unaware of cybercrimes, let alone what to do if they fall victim of cyber-attacks. Many innocent individuals fall victim to cybercrimes around the world, especially since technology is evolving at a rapid pace. Cybercrimes are any crimes that cause harm to another individual using a computer and a network. Cybercrimes can occur from issues surrounding the penetration of privacy and confidentiality(David,2008). When privacy and confidential information is lost or intercepted by unlawful individuals, high profile crimes such as hacking, cyber terrorism, espionage, financial theft, copyright infringement, spamming, cyber warfare and many more crimes may occur. Further, these crimes can be initiated anywhere in the world. Cybercrimes know no geographic borders and can happen to anyone once their information is breached by an unlawful user.

The purpose of this paper is to educate business organizations who do not know what cybercrimes are and to explain to them the importance of becoming more technologically aware. Understanding the threat of cybercrimes is a very pertinent issue because the use of technology to conduct business and personal affairs is widespread across many societies. Cybercrime is growing every day because technological advancements in computers make it very easy for anyone to steal without physically harming anyone because of the lack of knowledge to the employees of the organization regarding how cybercrimes are committed and how they can protect themselves against such threats that cybercrimes pose. This paper will discuss several aspects of Cybercrimes including defining the term, explaining why cybercrimes occur, laws governing them, methods of committing cybercrimes, who is affected, and prevention procedures. This research will also advance practical recommendations and implementable strategies to better protect business organizations from cybercrime.

# Justifications of the Study

## Financial loss due to Cybercrime

In February 2000, Amazon.com, Ebay.com, and Yahoo.com were among many Internet sites affected by a group of cyber-terrorists who hacked into the companies’ websites and made alterations to program coding. The problem was so severe that the companies were forced to shut down in order to repair the damage and stop the unauthorized activity. As a result of the site closing, program changes were made to help prevent future break-ins (Kathryn,2000). The Western Union branch of First Data Corp also came under attack by a private hacker. In September 2000, the perpetrator hacked into the company site and stole credit-card information for 15,700 customers. Apparently, the theft was made possible during a routine maintenance process when an employee left the files unprotected and vulnerable to attack. First Data Corp immediately notified authorities and both the FBI and CIA became involved with the investigation (Colden & Anne,2000).

Globally, the private sector controls a significant portion of critical infrastructure and government services, and as a result, cyber-attacks are an enormous danger to both private and public security. As organizations work towards developing best practices they are also tasked with balancing governmental laws and regulations. Governments, on the other hand, must form partnerships with other nations and incentivize the private sector to share information and allocate greater resources for security. As the cyber landscape changes and threats evolve attacks on the private sector will continue to pose an enormous risk to innovation, economic growth, and national security. The ability of the private sector to effectively manage threats from malicious actors and protect critical assets from breaches will prove pivotal in determining the future of cybersecurity in an increasingly technology-dependent world.

## Steps taken by Organizations

According to a Dell survey of IT decision-makers at global organizations, in the next 2-3 years, 74% of business respondents intend to increase their spending on cybersecurity and employee education and half of respondents believe a loss of critical business data to be the top security concern for their company (Dell & Bourne, 2014). Nearly half of executives at large and midsize businesses believe they are more vulnerable than ever to an insider threat. Use of personal devices on computer networks (so-called Bring Your Own Device or BYOD threats), phishing, and email viruses pose enormous risks to private networks. Across all sectors, access management tools and regular vulnerability assessments are vital tools to combating potential privilege abuse (Oltsik & Jon,2013). A Cisco study found that 11% of employees reported they or their colleagues had stolen computers or accessed unauthorized data and sold it for profit (Cisco, 2014). A formally defined policy for employees that includes education on security is vital for preventing unintended breaches, but it can also be useful for providing a channel for employees to report suspicious or alarming behavior in the workplace.

## 

## Data lost due to Cyber Crime

In February 2014 a cache of personal data containing credentials for 360 million accounts and 1.25 billion email addresses went up for sale on an online black market in what is widely considered the largest data breach in history (Holdsecurity,2014). The massive data collection was acquired through attacks on Google, Yahoo, and Microsoft among others over three weeks including one haul of nearly 105 million records. The February breach is indicative of an increasingly menacing trend of actors utilizing cyber-attacks as a means to cause significant damage to the private sector and threaten national and economic security. An October 2013 Ponemon Institute report found that across six countries and 234 multinational companies nearly all had been a victim of a malware attack and 57% experienced Distributed Denial of Service (DDoS) attacks. According to the report, companies were breached 1.3 times a week at an annual cost of approximately $7.2 million (Ponemon Institute, 2013).

The rise in malicious activity indicates that organizations can no longer avoid the inevitable cyber threat and must adequately prepare or risk significant loss. Cyber-attacks have proven to be a force for hacking groups and state-sponsored organizations seeking to level the playing field with competitors. The hacker threat paired with the enormously dangerous and costly threat of fraud or intellectual property theft by insiders has created a volatile situation in the private sector. While a majority of internal breaches are due to employee negligence or human error, attacks by malicious insiders with access to sensitive company information have increased dramatically in recent years. The threat of financial loss, theft of sensitive information, and destruction to critical sectors have made cybersecurity a top security priority around the globe (MacAfee, 2014). Whereas the increase in frequency and complexity of attacks on the industry has increased the danger of being unprepared, it also has influenced the cost of preventing and recovering from cyber-attack.

# Literature Review

Literature review of Cyber Crime has been divided into four parts.

## Categories of Cyber Crime

There are three categories.

### **Data Crime**

*Data Interception*. An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however, in some variants, the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream (CAPEC,2010).

*Data Modification*. Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites (Oracle,2003). In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a banking transaction from $100 to $10,000. In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid $100 bank account transfer transaction.

*Data Theft.* Data Theft term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.

### **Network Crime**

Computer and network surveillance is the monitoring of computer activity and data stored on a [hard drive](https://en.wikipedia.org/wiki/Hard_drive), or data being transferred over computer networks such as the [Internet](https://en.wikipedia.org/wiki/Internet). The monitoring is often carried out covertly and may be completed by governments, corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent government agencies.

Computer and network surveillance programs are widespread today and almost all [Internet traffic](https://en.wikipedia.org/wiki/Internet_traffic) can be monitored. Surveillance allows governments and other agencies to maintain [social control](https://en.wikipedia.org/wiki/Social_control), recognize and monitor threats, and prevent and investigate [criminal](https://en.wikipedia.org/wiki/Criminal) activity. With the advent of programs such as the Awareness program, technologies such as [high-speed surveillance computers](https://en.wikipedia.org/wiki/NarusInsight) and [biometrics](https://en.wikipedia.org/wiki/Surveillance#Biometric) software, and laws such as the [Communications Assistance For Law Enforcement Act](https://en.wikipedia.org/wiki/Communications_Assistance_For_Law_Enforcement_Act), governments now possess an unprecedented ability to monitor the activities of citizens

### **Access Crime**

*Unauthorized Access.* Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a [password](https://www.computerhope.com/jargon/p/password.htm) or [username](https://www.computerhope.com/jargon/u/username.htm) for an account that was not theirs until they gained access it is considered unauthorized access. Unauthorized access could also occur if a user attempts to access an area of a system they should not be accessing. When attempting to access that area, they would be denied access and possibly see an unauthorized access message.

Unauthorized access can create dangerous situations for any business or organization, so it’s important to choose access control technologies that will combat this risk. If organization is susceptible to any or all of these risks, it’s important to seek an access solution that will address those specific risks to reduce or even eliminate the possibility of unauthorized access and ensure the highest level of security for your facility.

*Virus Dissemination. Malicious* software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit, and Bacterium are examples of malicious software that destroys the system of the victim (Virus Glossary,2006).

## Types of Cyber Crime

### **Theft of Telecommunications Services**

The "phone phreakers" of three decades ago set a precedent for what has become a major criminal industry. By gaining access to an organization’s telephone switchboard private branch exchange (PBX) individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties. Offenders may gain access to the switchboard by impersonating a technician, by fraudulently obtaining an employee's access code, or by using software available on the internet. Some sophisticated offenders loop between PBX systems to evade detection.

### **Communications in furtherance of criminal**

*On conspiracies.* Just as legitimate organizations in the private and public sectors rely upon information systems for communications and record keeping, similar activities of criminal organizations are enhanced by technology. There is evidence of telecommunications equipment being used to facilitate organized drug trafficking, gambling, prostitution, money laundering, child pornography and trade in weapons (in those jurisdictions where such activities are illegal). The use of encryption technology may place criminal communications beyond the reach of law enforcement. The use of computer networks to produce and distribute child pornography has become the subject of increasing attention. Today, these materials can be imported across national borders at the speed of light (Grant, David and Grabosky 1998). The more overt manifestations of internet child pornography entail a modest degree of organization, as required by the infrastructure of IRC and WWW, but the activity appears largely confined to individuals.

*Telecommunications Piracy.* Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many. This has caused considerable concern to owners of copyrighted material. Each year, it has been estimated that losses of between US$15 and US$17 billion are sustained by industry by reason of copyright infringement (Information Infrastructure Task Force, 1995, p.131). When creators of a work, in whatever medium, are unable to profit from their creations, there can be a chilling effect on creative effort generally, in addition to financial loss.

### **Sales and Investment Fraud**

As electronic commerce becomes more prevalent, the application of digital technology to fraudulent endeavors will be that much greater. The use of the telephone for fraudulent sales pitches, deceptive charitable solicitations, or bogus investment overtures is increasingly common. Cyberspace now abounds with a wide variety of investment opportunities, from traditional securities such as stocks and bonds to more exotic opportunities such as coconut farming, the sale, and leaseback of automatic teller machines, and worldwide telephone lotteries (Cella and Stark, 1997). Indeed, the digital age has been accompanied by unprecedented opportunities for misinformation. Fraudsters now enjoy direct access to millions of prospective victims around the world, instantaneously and at minimal cost.

### **Electronic Funds Transfer**

Electronic funds transfer systems have begun to proliferate and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited. Just as an armed robber might steal an automobile to facilitate a quick getaway, so too can one steal telecommunications services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy(Ghosh,2011). Computer-related crime may be compound in nature, combining two or more of the generic forms outlined above.

## Impact of Cyber Crime

### **Impact of Cyber Crime over Private Industry**

According to the report "Second Annual Cost of Cyber Crime Study – Benchmark Study of U.S. Companies" published by the Ponemon Institute, a study based on a representative sample of 50 larger-sized organizations in various industry sectors, despite the high level of awareness of the cyber threat the impact of cybercrime has serious financial consequences for businesses and government institutions. The report shows that the median annualized cost of cybercrime for 50 organizations is $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company. The total cost is increased if compared to the first study of the previous year. Report demonstrates that virtually all companies experienced attacks moved using malware, very interesting also the data related to the action made by the insider and the damages caused by social engineering attacks. The conclusion is that industries fall victim to cybercrime, but to different degrees and with different economic impact. Defense, utilities and energy, and financial service companies experience higher costs than organizations in retail, hospitality and consumer products(Hunton,2011).

### **Impact of Cyber Crime over Business**

According to the FBI and the Department of Justice, cyber-crime is on the rise among American businesses, and it is costing them dearly. Cyber-crime includes a myriad of devious criminal practices designed to breach a company's computer security. The purpose of the electronic break and enter can be to steal the financial information of the business or its customers, to deny service to the company website or to install a virus that monitors a company's online activity in the future (Denning,2000).

## Future Trends in Cyber Crime

The pace at which cybercrime is growing is one of the most disturbing trends. Valerie McNiven, a U.S. Treasury Advisor, proclaimed “Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion." She further added that "cybercrime is moving at such a high speed that law enforcement cannot catch up with it”. It seems clear that the issue will only become worse in the next few years, now that professionals have realized the potential windfalls if exploited properly. Recently, there has been significant discussion over the amalgamation of organized criminals and cybercrime. Such a pairing indeed forebodes an ill omen for the near term future.

With most of the criminal groups operating out of Eastern Europe, Russia, and Asia, where laws and enforcement are scanty, there seems little hope in containing and neutralizing the threat through traditional means. Phil Williams, a visiting scientist at CERT, summarized the issue succinctly. As cyber-attacks increase in severity and complexity, the private sector must seek to reduce as much vulnerability as possible. Based on recent studies, the attackers are rarely lone wolves but organized groups of criminals with vast networks and resources. Many of these organizations are state-affiliated, presenting an increasingly complex political frontier for the private and public sectors. As organizations deal with current issues they also face the task of preparing for future ones.

# Summation of Literature Review

Cybersecurity is a shared responsibility and requires the attention of a broad range of stakeholders. It requires an effective public/private partnership that incorporates businesses and institutions of all sizes along with national, state, local, tribal and territorial agencies to produce successful outcomes in identifying and addressing threats, vulnerabilities and overall risk in cyberspace. Individual consumers also have a role, and adding cybersecurity to K-12 as well as higher education curriculums will help raise awareness for all users. Teaching users how to better protect themselves is a necessary component of any strategy.

# Recommendations

## Awareness Building

Most businesses have some form of firewall to prevent unauthorized access to their network. However, basic firewall can’t withstand sustained and sophisticated attacks, this is where Security Appliance comes in. Security Appliances or Unified Threat Management (UTM) appliances provide a consolidated and manageable interface for software security bundles. UTM combines the functions of firewalls, IDS, and network vulnerability scanners into one package thus making it more effective than single software solutions. Portable devices are popular and convenient to use but they come with the risk of getting lost and falling into the wrong hands. A smart security policy is to do full device encryption to protect your business data in case of data loss or theft. Many encryption software and hardware are available from which you can choose based on your business needs. Businesses use passwords to restrict access to confidential data and resources but the purpose of a password can be defeated if there is no consistent powerful password policy across business operations. You can improve your business security by improving the password creation and resetting process. Your business should create policies that ensure periodic password change and enforces the creation of difficult to hack passwords. If attackers crack any of your business’ network passwords, they can inflict maximum damage, you can prevent such from happening by disallowing the creation of weak passwords.

## Technological Backup

All the security methods discussed above cannot guarantee a perfect protection against all attacks. There is the possibility that some slip-ups may aid attackers in gaining access to your business networks. Should that happen, a cyber-insurance can help mitigate the impact of such a breach by helping to offset the costs associated with the hack and also shortening business recovery period. You definitely need cyber insurance for a complete system protection. It is unusual to be able to use the tool of cybercriminals against them. But researching on the Dark Web can help your business stay secure. Monitoring the dark web can help you spot the latest attack methods and also discover if your business is on the radar of attackers or has been compromised.

Due to the safety of the dark web, cybercriminals have set up their illegal business trading in stolen data and malicious software, your business can benefit from getting timely information to help you prevent attacks or manage them. Because your systems can crash, get its data corrupted or lost, you should always backup important data on a regular basis. The frequency of backup should be as short as possible, important applications should be backed at shorter interval periods while a system-wide backup should be scheduled during off-peak hours. To be effective, the backup process should not only cover important applications and data but other less used ones and backups should be stored on both on-site and off-site servers whenever possible.

Working with invested partners

Improving our national and global capabilities to detect, prevent, mitigate and respond to cyber events through a joint, integrated, 24x7 public/private operational capability that leverages information sharing, analysis and collaboration should be a priority. To build a mature operational capability for cybersecurity, we should learn from how the National Weather Service and the Centers for Disease Control and Prevention leverage technology and data analytics to identify patterns and trends to issue early alerts and warnings as well as recommendations for potential protective measures. Working through the global community to address gaps and coordinate law enforcement, investigation, and prosecution of cybercriminals will help tackle both the economics and the challenges of anonymity in nefarious cyber activity(Stepehens,2011). A global agreement on cyber deterrence and norms of cyber conduct will benefit national and economic security, public health and safety and everyday life in cyberspace.

# Implementation of Recommendations

## Raising Awareness

One way to know the state of your business’s security is by conducting a regular security assessment of all your business assets. Threats could stay hidden and undetected indefinitely if you do not assess your business’s network’s security. It bolsters the security of your organization and the information you learn from the assessment can be used to develop preventative measures against a future attack thus increasing your awareness and those of your employees. Email is at the heart of many business communications and operations. Unfortunately, a significant amount of emails received turn out to be spam or worse a phishing email used for stealing credentials.

Valuable time is often wasted opening and deleting spam messages and some attackers do package malicious code that can hijack a system as email. Installing an advanced email filtering program can help in cutting down time wasted treating junk mail and prevent your organization’s system from being hacked. Hackers can get a hold of you or your employees’ passwords and operate like legitimate users undetected. Two-Factor Authentication(2FA) was developed to make such attacks less successful by making passwords useless without an additional verification method which is usually harder to get. 2FA makes your business more secure by requiring two separate means of confirming a user’s identity.

## Leveraging trusted resources

Building, maintaining, scaling and updating an online source of information on how users of all levels of sophistication can establish and improve their protection profiles in cyberspace is imperative. Leveraging capabilities, such as those created in the United States by the National Cyber Security Alliance through Stay Safe Online or in the United Kingdom with [getting Safe Online](https://www.getsafeonline.org/), to implement a comprehensive and sustained national education and awareness campaign is a fundamental component of any successful cybersecurity program. Current cybersecurity efforts, such as the Stop-Think- Connect campaign sponsored by the Department of Homeland Security, are a good start (Oltisk,2011). However, existing programs need to scale more broadly to accelerate positive change. Enterprises can reference valuable tools such as the [NIST Cybersecurity Framework](https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf), Center for Internet Security/SANS Top 20 Controls, [ISO 27001](http://www.iso.org/iso/iso27001) and [NIST 800-53](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) for recommendations on improving an overall cybersecurity profile.

## Hire Professionals

Even large organizations with top talent and significant resources devoted to cybersecurity have suffered major cybersecurity compromises, and organizations that do not have such levels of talent or resources face even greater challenges. More highly skilled workers in cybersecurity roles would help the nation respond more robustly to the cybersecurity problems it faces. All organizations need to understand their threat environment and the risks they face, address their cybersecurity problems, and hire the most appropriate people to do that work. The-Cost-Of-Protection Companies that want to protect themselves from online thieves have to pull out their wallets to do it. There are costs in identifying risks, building new and safer operating procedures, and buying protective software and hardware. For businesses with complex or sensitive operations, this often involves hiring a cyber-security consultant to develop a customized solution. Not only are the upfront costs of protection expensive, but the systems must be tested and monitored regularly to ensure that they are still effective against emerging cyber-attacks. These costs are often passed on to the customer through higher prices of goods and services.

# Evaluation and Follow-Up

The barrier to entry to the cybercrime field is so low almost anyone can experiment and join the swelling ranks of cybercriminals. Such a low learning curve should prompt discussion on the need for a new paradigm of thought in how to preempt and deal with criminals in a way that is no longer tied to traditional methods. For example, for someone to break into a house, not only do they need to plan the opportune moment, but they may also have to be aware of lock picking, security system evasion and possess a degree of gumption to overcome moral thresholds. In contrast, the ease of cybercrime seems inversely proportional to the lucrativeness that it bestows and moreover, these trends show signs of accelerating. Paying respect to data security guidelines like those imposed on regulated industries such as finance and healthcare can be a starting point for best practices.

# Conclusion

The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber-apocalypse still abound, while the potential extent of damage that can be caused by wide-scale fraud is nearly unbounded. These anxieties should be rationally tempered with the knowledge that the problems are being addressed, although perhaps not fast enough. The usefulness of the Internet has proved itself in numerous and myriad ways that will hopefully be enough to ensure it does not become a wasteland of criminal activity and a bastion for the malicious. The government still has an important role to play, but most of the prevention needs to be done by commercial entities producing software and those with the ability to stop fraud. Relying on consumer education programs will only affect the percentage of possible victims. The others need to be automatically protected through measures that do not stress and require considerable participation. Security needs to be easy and effective if it is doing work. Whether cybercrime is still a pertinent issue ten years from now is unknowable in a sense, but if the Internet will continue to grow, it must be solved so that the realities of cybercrime will be proportional to real-world crimes, if not better.

# 

# References

Colden, Anne. (2000). Western Union reassures clients No financial fraud found since hacking.

Denver Post (Sep 12): p. C1.

Center, Finjan Malicious Code Research. "Web Security Trends Report." Securing your web (1996-2008): 1-20.

eSecurity Planet. 2011. 16 January 2011 <http://www.esecurityplanet.com/trends/article.php/3871456/Cyber-Crooks-Doubled-Their-Take-in-09-FBI.htm>.

Phil Williams, Cert Coordination Center. "Implications for Business." Organized Crime and Cyber-crime (2002): 1-7.

Wall, David S. "Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime." International Review of Law, Computers & Technology 22.1/2 (2008): 45-63. Academic Search Premier. EBSCO. Web. 18 Jan. 2011.

Stephens, Gene. "CYBERCRIME IN THE YEAR 2005." Futurist July 2008: 32+. Academic Search Premier. EBSCO. Web. 15 Jan. 2011.

Ghosh, Sumit. "The Nature of Cyber-attacks in the Future:A Position Paper." Information Systems Security 13.1 (2004): 18-33. Academic Search Premier. EBSCO. Web. 19 Jan. 2011.

Hunton, Paul. "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model." Computer Law & Security Review 25.6 (2009): 528-535. Academic Search Premier. EBSCO. Web. 22 Jan. 2011.

Denning, D., “Cyberterrorism”, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000. (http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html)

CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at <http://capec.mitre.org/data/definitions/117.html>

Crime in the Digital Age by Peter Grabosky and Russell Smith, Sydney: Federation Press, 1998

“Data Leakage Worldwide White Paper: The High Cost of Insider Threats.” Cisco. Web. 29 Jun 2014. [https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss- prevention/white\_paper\_c11-506224.html](https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-%09prevention/white_paper_c11-506224.html)

DSL Reports (2011), Network Sabotage, Available at <http://www.dslreports.com/forum/r26182468>- Network-Sabotage-or-incompetent-managers.

“Hold Security, LLC announces Credential Integrity Services. “Hold Security. 25 Feb 2014. Web. 1 Jun 2014. <http://www.holdsecurity.com/#!news2013/c13i1>.

IMDb (2012), Unauthorized Attacks, Available at <http://www.imdb.com/title/tt0373414/>

Kranhold, Kathryn. (2000). Handling the Aftermath of Cyber sabotage. Wall Street Journal (February 10): B22.

“Net Losses: Estimating the Global Cost of Cybercrime.” Center for Strategic and International Studies. Jun 2014. Web. 18 Jun 2014, p.6. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>

Oracle (2003), Security Overviews, Available at http://docs.oracle.com/cd/B13789\_01/ network.101/ b10777/overview.html

Oltsik, Jon. “2013 Vormetric/ESG Insider Threats Survey: The Ominous State of Insider Threats. “Enterprise Strategy Group and Vormetric. Sep 2013. Web. 8 Jun 2014. <http://www.vormetric.com/sites/default/files/ap_Vormetric-Insider_Threat_ESG_Research_Brief.pdf>.

“Protecting the Organization against the Unknown: A New Generation of Threats.” Dell and Vanson Bourne. Feb 2014. Web. 18 May 2014. <http://software.dell.com/documents/protecting-the-organization-against-theunknown-whitepaper-27396.pdf>.

Virus Glossary (2006), Virus Dissemination, Available at: <http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml>

“2013 Cost of Cybercrime Study: Global Report. “Ponemon Institute. Oct 2013, p. 10. Web. 9 Jun 2014. DDoS attacks are comprised of a flood of messages to a system which is intended to knock websites offline by overwhelming them with traffic.