Innovative Minds • On Point • One Group

THE IMPACT OF CYBER ATTACKS ON THE PRIVATE SECTOR

A White Paper by Bryan Watkins

Presented by:

MindPoint Group, LLC

7800 Rose Garden Lane
Springfield, VA 22153

■ (o) 703.636.2033 ■ (f) 866.761.7457
■ www.mindpointgroup.com

■ SBA 8(a) Certified Small Disadvantage Business ■ Woman-Owned Small Business (WOSB)
■ Economically Disadvantaged Woman-Owned Small Business (EDWOSB) ■ Minority-Owned Small Business

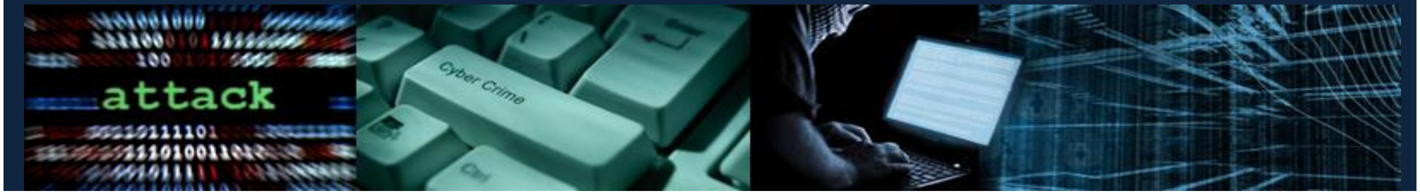

TABLE OF CONTENTS

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. 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.[1] 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 victim of a malware attack and 57% experienced Distributed Denial of Service (DDoS) attacks.[2] According to the report, companies were breached 1.3 times a week at an annual cost of approximately $7.2 million.[3] 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 hazardous and costly danger 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.

Threat of financial loss, theft of sensitive information, and destruction to critical sectors have made cybersecurity a top security priority around the globe. Whereas the increase in frequency and complexity of attacks on industry has increased the danger of being unprepared, it also has influenced the cost of preventing and recovering from cyber attacks.

1. THE PRICE OF CYBER ATTACKS

US National Security Agency (NSA) Director General Keith Alexander referred to cyber espionage as “the greatest transfer of wealth in history.” Globally, the cost of cybercrime is estimated to be upwards of $385 billion.[4] The UK National Audit Office estimates cybercrime costs the UK between £18 billion ($30 billion) and £27 billion ($45 billion) a year.[5] In the US that figure is estimated to be roughly $100 billion.[6]

In 2013, 54% of total cyber attacks targeted the US, the most of any country, followed by Russia and India, respectively.[7] Nearly half of all attacks originated in China followed by the US at 19% and Canada at 10%.[8]

Cyber attacks can cause significant loss of business intelligence and intellectual property, drive up the cost of security, disrupt workflow, and damage company reputation. Companies reporting major attacks suffer a 1-5% drop in stock value;[9] while some companies recover, others may lose everything. Canadian telecom giant Nortel Networks Ltd. had been infiltrated by Chinese hackers for nearly a decade before filing for bankruptcy in 2009. The intrusions were so well hidden it took investigators several years to discover the extent of the damage to critical data.[10]

Overall, cyber espionage may be the greatest threat facing the private sector. Theft of intellectual property is projected to account for nearly three-quarters of financial loss from cyber attacks for companies.[11] The imagery is compelling when you consider at any given time the equivalent of hundreds of unauthorized people walking through the halls of The Pentagon, BAE Systems, or Google undetected with the ability to view and take whatever they please. That is essentially what occurs in the computer networks of many companies each day.

Companies are turning to insurance as financial protection against the inevitable threat of attacks. While cyber insurance often covers the cost to repair systems after security breaches as well as regulatory fees, most policies have exceptions limiting the scope of coverage to excludes loss of stolen intellectual property or business intelligence. Still, cyber insurance is a booming business. In the US insurance grew from less than $100 million in annual premiums in 2002 to $800 million in 2011 and now similar growth is occurring in Asian and European markets as the loss due to attacks continues to rise.[12]

2. THE THREAT LANDSCAPE

Cybercrime is often associated with small organizations or rogue actors, however a UN study found that 80% of the 500 incidents reviewed entailed some form of organized activity, most of which was state affiliated.[13] A Lieberman Software survey indicated that 62% of respondents believe their organization will be targeted in a state-sponsored attack within the next six months and less than half believe the organization will be able to detect such an attack. [14]

According to the Ponemon study, defense ($16.10 million per year), financial services ($11.50 million per year), and energy and utility companies ($10.60 million per year) faced significantly higher annual cybercrime related costs than other industries largely due to the volume and complexity of attacks.[15]

Attacks against defense giants BAE Systems, Lockheed Martin, the Japanese Aerospace Exploration Agency, and L-3 Communications, among others have exposed the vulnerability of government contractors to breaches of valuable intelligence and demonstrate the extent of financial and military risk present in the private sector.[16] Iranian hacking organization Ajax Security Team utilizes custom malicious software to spy on military contractors. In one campaign, Ajax established a fake website nearly identical to the 2014 IEEE Aerospace conference and tricked recipients into downloading malicious software disguised as conference registration granting the hackers access to defense networks.[17]

In 2012, a massive financial cyber-heist dubbed “Operation High Roller” was launched from servers in Russia, Albania and China. The attack caused significant damage to the global banking system including between $78 million and $2.5 billion in losses from bank accounts across Europe, the US, and Latin America.[18] Recent breaches at global retailers Target and Neiman Marcus resulted in the theft of credit card information from 40 million and 1.1 million customers, respectively.[19] Cyber criminals are turning an enormous profit at the expense of banking institutions; the three most sophisticated organized crime groups in the world steal more than $100 million from financial institutions annually.[20]

Successful breaches on the energy sector have skyrocketed causing insurance companies to deem many energy firms uninsurable. The 2009 Stuxnet worm sabotaged centrifuges at an Iranian uranium-enrichment plant;[21] then in 2012 the Shamoon virus destroyed hard drives and shut down more than 30,000 computers at major energy companies in the Middle East.[22] The attacks demonstrate both the potential for cyber weapons to cause physical damage to critical systems as well as the overall vulnerability of energy sector systems.

Defense of intellectual property and business intelligence is a key security priority in the public and private sectors. A 2012 report leveled extensive hacking accusations against a Chinese group referred to as APT1 that had hacked into 141 entities in the EU, US, and Canada; in one instance APT1 maintained access to a network for nearly five years.[23] Following a number of allegations of state-sponsored hacking, the US recently filed charges including economic espionage against five Chinese military officers for stealing industry secrets on nuclear and solar power. The landmark charges are the first instance of a government formally accusing another nation of cyber espionage and may prove significant for international cybercrime law.

3. APPROACHING THE THREAT

Organizations are generally outmatched by the tools and resources of state-sponsored organizations. In response to this growing challenge businesses are allocating more resources towards security and looking to government for guidance. In addition to increasing their security budget, companies have utilized intelligence sharing channels with other businesses and governments to identify cybersecurity threats and vulnerabilities.

The financial sector is a model of how intelligence sharing on cyber attacks can be a valuable tool. Barclays has reported that exchanging cyber attack information with other banks has led to a reduction in cyber fraud related losses in the British financial sector from £59.7 million ($100 million) in 2009 to £35.4 million ($60 million) in 2011.[24] Companies across different sectors are taking advantage of information-sharing and analysis centers (ISACs) to spread attack information and best practices. The approach allows organizations to see attacks from different angles to deal with current threats and anticipate future ones.

In response to the prospect of infiltration by malicious actors many organizations have implemented proactive methods for loss prevention including a formal incident response plan; a compliance plan comprised of policies, audits, training, and education; detection systems; and procedures for maintaining evidence of an incident.

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 that loss of critical business data to be the top security concern for their company.[25] Nearly half of executives at large and midsize businesses believe they are more vulnerable than ever to an insider threat.[26] 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. 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.[27] 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.

4. STATE INVOLVEMENT

Private business has a significant impact on economic and national security and governments want to have a stake in protecting critical private infrastructure as it does with other government assets. As nations push to boost their cyber capabilities the ability of government to incentivize the private sector to share information in a timely manner will greatly impact the effectiveness of cybersecurity management. In 2013, NSA Director General Keith Alexander stated that cyber attacks on private industry were rising such that without a change in security posture governments would need to step in to defend the private sector.

While some organizations believe the private sector is best suited to protect itself, others believe that a public-private partnership (PPP) and increased regulation is essential. According to 84% of respondents in the Dell survey of IT decision makers, the government plays a role in determining the organization’s security strategy and most believe that the government’s role in security is helping their organization’s operational effectiveness.[28] To further this partnership governments are seeking to incentivize companies to increase resources for security and disclose threats and breaches.

In early 2014, the US and EU unveiled cybersecurity standards resulting from a joint public-private effort to formulate best practices for critical infrastructure providers. Both frameworks stress the need to address the growing cyber threat to the private and public sectors. For the US, privacy and liability disputes stalled several bills before the executive office and National Institute of Standards and Technology (NIST) released the cybersecurity framework. However, the framework provides a substantial baseline for organizations to develop a security strategy. The EU proposal, if adopted, would replace the voluntary approach with a regulatory cybersecurity standard. Member states would be required to harmonize their national laws with the legislation.

The European Commission's cybersecurity strategy focuses on reducing cybercrime; incorporating cyber defense into the EU Common Security Defense Policy; and developing industrial resources for cybersecurity. Both hope that their policy will be used as a global standard in the future. The US framework increases information sharing channels for the public sector with critical infrastructure and seeks to incentivize the private sector to adhere to comply with the standards established by NIST.

The EU and US have engaged in cybersecurity dialogue dating back to 2010 but recently committed to strengthening their level of cooperation at the Brussels Summit in March 2014. The goal of the increased collaboration being to create a platform to improve information exchanges on threats, apply international legal standards, and enhance partnerships between the public and private sectors.

Other countries have laid the foundation for national standards as well. In 2012, India released its Recommendations of the Joint Working Group on Cybersecurity. The Recommendations come as protection on the heels of the Edward Snowden leaks alleging US spying on India and is seen as an important step to getting ahead of cybersecurity challenges and protecting critical infrastructure. In Japan, the National Information Security Centre (NISC) released its strategy last year to outline the roles of critical infrastructure providers and government, among others. The Japanese strategy stresses increased cooperation with other countries and the private sector as the key component to combatting cybercrime on a global scale.

5. INTERNATIONAL COOPERATION

As technology has evolved so to have international efforts to govern cyberspace. Cyber attacks present a multitude of border issues; establishing jurisdiction is complicated and is made even more challenging by the difficult task of attributing the attack to an organization or nation. Despite the challenges, nations and organizations have implemented a number of mechanisms to defend and combat cyber attacks.

In 2004, the Convention on Cybercrime, or Budapest Convention, became the first international treaty to address internet crime through the harmonization of national laws. On the belief that cybercrime is best approached on a global scale, the European Council underwent four years of negotiations to create the Convention which promotes inter-industry cooperation between nations and private industry; stresses the security of public assets; and sets out to pursue a criminal policy to protect against cyber attacks. The convention has been ratified by 31 nations primarily from the Council of Europe (Canada, Japan, The US and Republic of South Africa are the non-Council ratifying nations) and is widely considered one of the best mechanisms for international cooperation on hacking.

The UN has passed two resolutions criminalizing the misuse of information technology and declaring that international law applies to cyberspace. The North Atlantic Treaty Organization (NATO) has propelled cybersecurity harmonization among its members including a 2011 policy and Action Plan which sets out a vision for the alliance to strengthen defense efforts and Interpol is in the process of establishing a Global Complex for Innovation (IGCI) in Singapore to facilitate cross-border cooperation on cybercrime.

According to the UN Study on Cybercrime, a vast majority of cyber incidents encountered by police were transnational. Still, there are significant political and economic roadblocks to a comprehensive international agreement.[29] Some of the governments with the most advanced technological capabilities (and therefore, the most to lose) have contrasting views on cybersecurity policy creating a significant barrier to an effective international treaty. As a result many nations rely on bilateral agreements or informal cooperation as opposed to international treaties. Almost 60% of countries in the UN study reported that they rely on bilateral instruments as the legal basis for extradition in cybercrime cases.[30]

A recent two-year global sting led to the arrest of 97 people in 19 countries for infecting computers with 'BlackShades,' malware which allowed perpetrators the ability to gain complete control of more than 500,000 computers worldwide. The sting demonstrated an unprecedented level of cooperation between law enforcement agencies in Europe and the Americas. It also provides a model for how mutual agreements and reciprocity can be paired with domestic law enforcement in future prosecution.

6. A LOOK TO THE FUTURE

As cyber attacks increase in severity and complexity, the private sector must seek to reduce as many vulnerabilities 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. While organizations deal with current issues they also face the task of preparing for future ones.

Attacks against the healthcare and pharmaceutical industries are expected to continue to rise. Medical records contain valuable personal information allowing hackers to steal identities and commit fraud in a way that is difficult for agencies to detect. Criminal attacks on healthcare companies increased 100% between 2010 and 2013 and will continue to escalate.

The shift by many companies to cloud computing poses an enormous security threat as nearly three-quarters of respondents are utilizing cloud computing however less than half employ cloud security.[31] As the extent of information stored in cloud increases, so does the risk of cyber attacks and necessity for tools to protect cloud data.

Rapid increase in personal device use on company networks has created a growing security threat. For instance, an employee's personal device gets infected with malware on a home or public network, the employee brings the device to work and connects to the network, unknowingly providing a hacker access to vital company information. To manage the threat, companies will need to counteract the surge in personal device use with policies and education to mitigate potential loss paired with controls such as device scanning, data encryption and wiping company data from personal devices.[32]

Cybersecurity is now one of the top security priorities for nine of ten companies worldwide.[33] 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.

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 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.

Notes

[1] "Hold Security, LLC announces Credential Integrity Services." *Hold Security*. 25 Feb. 2014. Web. 1 June 2014. <http://www.holdsecurity.com/#!news2013/c13i1>.

[2] "2013 Cost of Cybercrime Study: Global Report." *Ponemon Institute.* Oct. 2013. p. 10. Web. 9 June 2014. DDoS attacks are comprised of a flood of messages to a system which are intended to knock websites offline by overwhelming them with traffic.

[3] Ibid. pp. 1, 10.

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

[5] Baud, Emmanuel G, et al. "Europe Proposes New Laws and Regulations on Cybersecurity." *Jones Day*. 1 Jan. 2014. Web. 10 June 2014. <http://www.jonesday.com/europe-proposes-new-laws-and-regulations-on-cybersecurity-01-02-2014/>.

[6] "The Economic Impact of Cybercrime and Cyber Espionage." *McAfee*. 2013. p.5.

[7] "2014 Data Breach Investigations Report." *Verizon.* 2014. Web. 28 May 2014.

[8] "Fourth Quarter 2014: State of the Internet." Akamai. Vol. 6, No. 4. 2014. Web. 23 May 2014. <http://www.akamai.com/dl/akamai/akamai-soti-q413.pdf?WT.mc_id=soti_Q413>.

[9] *See Supra 6* at p. 12.

[10] Gorman, Siobhan. "China Hackers Suspected in Long-Term Nortel Breach." *Wall Street Journal Online.*14 Feb. 2012. Web. 1 June 2014. <http://online.wsj.com/news/articles/SB10001424052970203363504577187502201577054?

[11] *See Supra 6* at p.12.

[12] Beck, David, L and Siemends, Rene L. "Cyber Insurance—Mitigating Loss from Cyber Attacks." *Pillsbury Law*. 2012. Web. 29 May 2014. <http://www.pillsburylaw.com/publications/cyber-insurancemitigating-loss-from-cyber-attacks>.

[13] Comprehensive Study on Cybercrime: *UNODC.* Feb 2013. p. xvii. Web. 25 May 2014. <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf >.

[14] "2013 Survey of Information Security Professionals: Defending Against State-Sponsored Attacks and Other Advanced Persistent Threats." *Lieberman Software*. 4 Sept. 2013. Web. 2 June 2014. <http://www.liebsoft.com/uploadedFiles/wwwliebsoftcom/MARCOM/Press/Content/2013-IT-Security-Survey.pdf>.

[15] *See Supra 2* at p.9.

[16] Cenciotti, David. "Exclusive Infographic: all Cyber Attacks on Military Aviation and Aerospace Industry" *The Aviationist***.** 21 Feb. 2012**.** Web. 6 June 2014. <http://theaviationist.com/2012/02/21/cyberwar-infographic/>

[17] Dune, Lawrence. "Iranian Hackers, Getting More Sophisticated, Target U.S. Defense Companies." *Bloomberg Businessweek.* 14 May 2014. Web 4 June 2014. <http://www.businessweek.com/articles/2014-05-14/iranian-hackers-getting-more-sophisticated-target-u-dot-s-dot-defense-companies?

[18] Messmer, Ellen. "Bank hack: 'Operation High Roller' has netted $78M – so far." *Network World*. 26 Jun. 2012. Web. 7 June 2014. http://www.networkworld.com/article/2189619/malware-cybercrime/bank-hack---operation-high-roller--has-netted--78m---so-far.html; Kelley, Michael, B. "Operation High Roller: This Massive Cyberattack Has Siphoned as Much as $2.5 Billion from World Banks.: *Business Insider*. 28 Jun. 2012. Web. 4 June 2014. < http://www.businessinsider.com/operation-high-roller-2012-6>. As a result of the complexity and depth of the attacks security officials were unable to precisely determine the loss and damage caused by the attacks.

[19] Harris, Elizabeth A, et al. "Neiman Marcus Data Breach Worse Than First Said." *The New York Times*. 23 Jan. 2014. Web. 2 June 2014. <http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html?_r=0>.

[20] Farrell, Greg and Michael A. Riley. "Hackers Take $1 Billion a Year as Banks Blame Their Clients." *Bloomberg.* 4 Aug. 2011. Web. 23 June 2014. <http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html>.

[21] Kelley, Michael, B. "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." *Business Insider*. 20 Nov. 2013. Web. 7 June 2014. <http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>.

[22] Nakashima, Ellen. "Cyberattack on Mideast energy firms was biggest yet, Panetta says" *The Washington Post*. 11 Oct. 2012. Web. 21 May 2014. http://www.washingtonpost.com/world/national-security/cyberattack-on-mideast-energy-firms-was-biggest-yet-panetta-says/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html

[23] "APT1: Exposing One of China's Cyber Espionage Unites." Mandiant. 19 Feb. 2013. Web. 21 May 2014. <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.

[24] Blitz, James. "Maude Warns on EU cyber security plans." *The Financial* Times. 27 Mar. 2013. Web. 2 June 2014. <http://www.ft.com/cms/s/0/446e4702-96f7-11e2-a77c-00144feabdc0.html#axzz319C55zx3>.

[25] "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-the-unknown-whitepaper-27396.pdf>.

[26] Oltsik, Jon. "2013 Vormetric/ESG Insider Threats Survey: The Ominous State of Insider Threats." *Enterprise Strategy Group and Vormetric.* Sept. 2013. Web. 8 June 2014. <http://www.vormetric.com/sites/default/files/ap_Vormetric-Insider_Threat_ESG_Research_Brief.pdf>.

[27] "Data Leakage Worldwide White Paper: The High Cost of Insider Threats." *Cisco.* Web. 29 June 2014. <http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.html>.

[28] *See Supra 25* at p.8.

[29] Comprehensive Study on Cybercrime: *UNODC*. Feb 2013. Q. 83. Web. 25 May 2014. <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf >.

[30] *Ibid* at p. xxv.

[31] *See Supra 25* at p.4.

[32] Mello, John P., Jr. "Spotlight on Security: BYOD Security Is All About Juggling Risks." BYOD Security Is All About Juggling Risks. 23 Sept. 2013. Web. 4 June 2014. <http://www.technewsworld.com/rsstory/79018.html>.

[33] *See Supra 25* at p.13.