Hengtian White Paper

Global Internet Information Security

TABLE OF CONTENTS

GLOBAL INTERNET INFORMATION SECURITY OVERVIEW

Despite an environment in which 60% of employees admit to taking sensitive data before they leave a company[1] and 20% of data breaches are caused by malicious insiders[2], hacking still remains the biggest single threat of data loss to companies[3].

Recent attacks on the International Monetary Fund, Citigroup and Sony prove that many organizations, particularly in the United States and Europe, have been too focused on regulation and not focused enough at taking a top-down look at their information security needs; in some cases, no efforts were made to encrypt any information that was not required by law to be encrypted. Gretchen Hellman, VP of product management for data security vendor Vormetric, described the problem: "Security has been driven by compliance for the past seven years, starting with Sarbanes-Oxley and going to PCI," she said. "So there's been a focus on complying with regulations, and not focusing on a strong, holistic, layered security program--everything from end-user awareness training to encrypting and controlling access to data with a strong separation of duties program, to monitoring activity to ensure that you can capture malicious activity as soon as it starts." [4]

Attacks on information have come from any number of potential sources, including: organized crime groups, competitive corporations, nation-states, military agencies and individual hackers[5]. Further complicating matters, attackers have been quick to adapt to advances in information security[6]; for

[1] Greenberg, Andy. "WikiLeaks' Julian Assange Wants To Spill Your Corporate Secrets." *Forbes*. Forbes Magazine, 29 Nov. 2010. Web. 06 Mar. 2012. <http://www.forbes.com/sites/andygreenberg/2010/11/29/wikileaks-julian-assange-wants-to-spill-your-corporate-secrets/3/>.

[2] "One Fifth of Data Breaches Result of Insider Issues Says Report." *Infosecurity*. Info Security Magazine, 29 Nov. 2010. Web. 06 Mar. 2012. <http://www.infosecurity-magazine.com/view/14262/one-fifth-of-data-breaches-result-of-insider-issues-says-report/>.

[3] Schwartz, Mathew J. "Hack Attacks Now Leading Cause Of Data Breaches." *InformationWeek*. Information Week Magazine, 12 Jan. 2012. Web. 06 Mar. 2012. <http://www.informationweek.com/news/security/attacks/232400252>.

[4] Schwartz, Mathew J. "What Do IMF, Citigroup and Sony Hacks Share?" *InformationWeek*. Information Week Magazine, 13 June 2011. Web. 06 Mar. 2012. <http://www.informationweek.com/news/security/attacks/230600055>.

[5] "Clear and Present Danger: Cyberattacks, Hackers and the Increasing Threat to Information Security." *Managing Technology*. Wharton School of Business, 7 July 2010. Web. 08 Mar. 2012. <http://knowledge.wharton.upenn.edu/article.cfm?articleid=2535>.

[6] Mills, Elinor. "Why the Security Industry Never Actually Makes Us Secure." *CNET News*. CNET, 03 Mar. 2012. Web. 06 Mar. 2012. <http://news.cnet.com/8301-1009_3-57389046-83/why-the-security-industry-never-actually-makes-us-secure/?tag=mncol;txt>.

example, recent security upgrades to prevent large-scale information security breaches have caused hackers to focus on small-scale targeted attacks[7].

The blurred lines between work and private activity is causing new changes in the ways employees need to access information, thus introducing new points of weakness in the information security system. Due to acquisitions, spin-offs and employee turnover, IT professionals need to keep track of not only employees and company devices, but also non-employees and non-company devices[8]. As networks have expanded and continued to become more pervasive, the number of potential targets for attackers has increased[9].

In this sort of environment, the challenges organizations face to secure their data is threefold: the hackers know exactly what they want, they can attack from anywhere, and everyone and every organization is a potential target[10].

Now more than ever, all organizations need to acquaint themselves with the current state of global internet information security. The following guide details the current state of internet information security in three regions that are key to the IT industry and global industry in general: The Americas and Europe; China; and India and the Middle East.

NOTABLE RECENT GLOBAL INTERNET SECURITY ISSUES

THE AMERICAS AND EUROPE

When it comes to internet information security, companies in North America and Europe face many threats, both domestic and foreign. While international hacking incidents have made for big headlines, persistent threats exist on the domestic front after the rise of the information leaking site, Wikileaks, and the well-known hacking group, Anonymous.

[7] "Can Anyone Create a Hacker-proof Cyberspace?" *Law and Public Policy*. Wharton School of Business, 6 July 2011. Web. 12 Mar. 2012. <http://knowledge.wharton.upenn.edu/article.cfm?articleid=2810>.

[8] "Clear and Present Danger: Cyberattacks, Hackers and the Increasing Threat to Information Security." *Managing Technology*. Wharton School of Business, 7 July 2010. Web. 08 Mar. 2012. <http://knowledge.wharton.upenn.edu/article.cfm?articleid=2535>.

[9] Mills, Elinor. "Why the Security Industry Never Actually Makes Us Secure." *CNET News*. CNET, 03 Mar. 2012. Web. 06 Mar. 2012. <http://news.cnet.com/8301-1009_3-57389046-83/why-the-security-industry-never-actually-makes-us-secure/?tag=mncol;txt>.

[10] "Clear and Present Danger: Cyberattacks, Hackers and the Increasing Threat to Information Security." *Managing Technology*. Wharton School of Business, 7 July 2010. Web. 08 Mar. 2012. <http://knowledge.wharton.upenn.edu/article.cfm?articleid=2535>.

WIKILEAKS

Since its launch in 2006, Wikileaks has proved to be an invaluable medium over which information hackers and turncoat insiders could leak potentially sensitive corporate and government data[11]. While the Wikileaks publication of 251,000 US diplomatic cables have made headlines[12], much of the damage caused by Wikileaks has affected corporations, including the Swiss bank Julius Baer and a pharmaceutical industry trade group[13].

Compounding the trouble Wikileaks causes US companies is the fact that Wikileaks is legally shielded in the US. As it only operates as a conduit for documents, Wikileaks has no legal liability for the damages these leaks may cause[14].

The hackers who provide information to Wikileaks tend to be “hactivists”, hackers who target companies in order to promote their moral, social or political message. Companies with low profiles and responsible corporate governance tend to be at a lower risk for an information leak distributed through the site[15].

ANONYMOUS

Anonymous is a loose association of hackers originally organized through 4chan, a popular message board. Over the past several years, Anonymous has made headlines for its attacks on governments and corporations, big and small, throughout the world. While Anonymous is well-known for its success in Distributed Denial of Service (DDOS) attacks, the group has moved to hitting companies where it hurts the most: share prices. In its most recent attacks, the group has focused on attaining and leaking information that could damage the reputation and share prices of targeted companies[16].

While Anonymous has no official affiliation with Wikileaks, the two groups have coordinated in the past: an Anonymous attack targeted credit card giants Visa and Mastercard after they stopped accepting

[11] Klein, Ben. "WikiLeaks Serves as Evidence of Internet Security Issues." *The Daily Orange*. The Daily Orange, 1 Dec. 2010. Web. 06 Mar. 2012. <http://www.dailyorange.com/opinion/wikileaks-serves-as-evidence-of-internet-security-issues-1.1813885>.

[12] "Wikileaks: Swept up and Away." *The Economist*. The Economist Newspaper, 10 Sept. 2011. Web. 07 Mar. 2012. <http://www.economist.com/node/21528600>.

[13] Greenberg, Andy. "WikiLeaks' Julian Assange Wants To Spill Your Corporate Secrets." *Forbes*. Forbes Magazine, 29 Nov. 2010. Web. 06 Mar. 2012. <http://www.forbes.com/sites/andygreenberg/2010/11/29/wikileaks-julian-assange-wants-to-spill-your-corporate-secrets/3/>.

[14] Greenberg, Andy. "WikiLeaks' Julian Assange Wants To Spill Your Corporate Secrets." *Forbes*. Forbes Magazine, 29 Nov. 2010. Web. 06 Mar. 2012. <http://www.forbes.com/sites/andygreenberg/2010/11/29/wikileaks-julian-assange-wants-to-spill-your-corporate-secrets/3/>.

[15] Claburn, Thomas. "Google: Hackers Targeted Chinese And Vietnamese." *InformationWeek*. Information Week Magazine, 31 Mar. 2010. Web. 06 Mar. 2012. <http://www.informationweek.com/news/security/vulnerabilities/224200944>.

[16] Mills, Elinor. "Anonymous Starts Activism via Corporate Securities Research." *CNET News*. CNET, 29 Sept. 2011. Web. 08 Mar. 2012. <http://news.cnet.com/8301-27080_3-20113668-245/anonymous-starts-activism-via-corporate-securities-research/>.

donations for Wikileaks founder Julian Assange[17]; in a more recent operation, data hacked by Anonymous in a late-December 2011 attack on Stratfor, an intelligence company, was posted on Wikileaks[18]. This kind of collaboration between Anonymous and Wikileaks could prove particularly damaging to targeted companies: by using Wikileaks, hackers can share their ill-attained information with the entire world.

In recent months, Anonymous attacks have focused on the supporters of proposed new standards for intellectual property rights enforcement. Victims of these attacks include the office of the Croatian President, whose website was hit with a DDOS attack, and Prophon, a Belgian music industry group, whose domain was seized in an Anonymous attack[19].

In one notable Anonymous attack, Sony’s systems were compromised, resulting in the release of the names and credit card numbers for millions of customers. The resulting cleanup is estimated to have cost Sony $170 million[20]. The attack also targeted Sony executives. Hackers gained access to and posted information about Sony executives and their families. Compromised information includes executives’ home phone numbers, home address, height, weight, date of birth, wedding anniversary, as well as their children’s names, schools, dates of birth and dates of adoption[21]. This sort of targeted and personal attack could lead to great damage to the company, its profits, its customers, and its employees.

"Anonymous is a wake-up call," said Roger Cressey, senior vice president of Booz Allen Hamilton, a defense and intelligence contractor serving the US government that was attacked by the group last summer. "Any company that is patting themselves on the back and saying that they're not a target or not susceptible to attack is in complete and utter denial."[22]

Despite the fact that senior Anonymous hackers have declared a “guerilla cyber-war” against US corporations and government[23], their attacks have not been limited to US soil. Anonymous Analytics, a

[17] Dharmakumar, Rohin. "Hackers' Haven." *Forbes India Magazine*. Forbes Magazine, 19 Sept. 2011. Web. 08 Mar. 2012. <http://forbesindia.com/article/boardroom/hackers-haven/28462/2?id=28462>.

[18] "WikiLeaks Targets Global Risk Company Stratfor." *The Times of India*. The Times of India, 28 Feb. 2012. Web. 07 Mar. 2012. <http://timesofindia.indiatimes.com/world/us/WikiLeaks-targets-global-risk-company-Stratfor/articleshow/12068466.cms>.

[19] "Anonymous Attacks Croatian Presidency Website." *The Sofia Echo*. The Sofia Echo, 10 Feb. 2012. Web. 06 Mar. 2012. <http://www.sofiaecho.com/2012/02/10/1764013_anonymous-attacks-croatian-presidency-website>.

[20] "Hactivism: The Bright Side of Being Hacked." *The Economic Times*. The Times of India, 5 Mar. 2012. Web. 06 Mar. 2012. <http://articles.economictimes.indiatimes.com/2012-03-05/news/31124260_1_hackers-anonymous-social-engineering>.

[21] Anderson, Nate. "Anonymous Goes after Sony, Makes It Personal... Very Personal." *Ars Technica*. Ars Technica, Apr. 2011. Web. 07 Mar. 2012. <http://arstechnica.com/tech-policy/news/2011/04/anonymous-goes-after-sony-makes-it-personal-very-personal.ars>.

[22] "Hactivism: The Bright Side of Being Hacked." *The Economic Times*. The Times of India, 5 Mar. 2012. Web. 06 Mar. 2012. <http://articles.economictimes.indiatimes.com/2012-03-05/news/31124260_1_hackers-anonymous-social-engineering>.

[23] Isikoff, Michael. "Hacker Group Vows 'cyberwar' on US Government, Business." *MSNBC*. MSNBC, 08 Mar. 2011. Web. 07 Mar. 2012. <http://www.msnbc.msn.com/id/41972190/ns/technology_and_science-security/t/hacker-group-vows-cyberwar-us-government-business/>.

splinter group of Anonymous dedicated to exposing companies with poor corporate governance, has targeted Chaoda Modern Agriculture of China, a produce firm listed on the Hong Kong exchange[24].

Notwithstanding recent high-profile arrests of Anonymous hackers in the US, South America and Europe, the group remains a prominent threat to internet information security for companies and government organizations in the US and around the world[25].

CHINA

In China, as is the case in most countries, one of the greatest risks for breaches in internet information security comes from overseas hackers. 65% of attacks on Chinese sites came from overseas internet protocol (IP) addresses, with the United States, South Korea and Japan being major sources. In attacks on high security facilities, including data centers, terminal controls and automatic industrial control systems, 22% of attacks came from the United States[26].

In one attack, Chinese search engine Baidu was taken down temporarily in 2010 by an Iranian hacker as a result of the incompetency and irresponsible lack of security at US-based Register.com. The hacker used Register's IM support function to request to change Baidu's on-file email address. The Register employee sent a confirmation code to the on-file Baidu email account, but failed to check to see if the code given by the hacker matched the code sent to Baidu. More troubling was that the employee of Register failed to scrutinize a change of an email address from an @baidu domain to a Gmail account that contained a politically charged message[27].

In another recent attack on a Chinese company, the hacker group Swagg Security stole email addresses and passwords from iPhone and iPad manufacturer Foxconn. The hacker group was motivated to attack Foxconn after reading a BBC story about the company[28].

China's government has also been the victim of attacks from overseas hackers. Since mid-February 2012, China's government and national firewall have been targeted by RevolutionSec, a group affiliated with Anonymous[29].

[24] Mills, Elinor. "Anonymous Starts Activism via Corporate Securities Research." *CNET News*. CNET, 29 Sept. 2011. Web. 08 Mar. 2012. <http://news.cnet.com/8301-27080_3-20113668-245/anonymous-starts-activism-via-corporate-securities-research/>.

[25] "Anonymous Hackers: Police Arrest 25 in Four Countries." *BBC News*. BBC, 28 Feb. 2012. Web. 08 Mar. 2012. <http://www.bbc.co.uk/news/world-latin-america-17195893>.

[26] "Businesses Warned over Internet Security in China." *Information Technology*. Info Tech Spotlight, 5 Mar. 2012. Web. 07 Mar. 2012. <http://it.tmcnet.com/news/2012/03/05/6164512.htm>.

[27] Fletcher, Owen, and Robert McMillan. "Baidu: Registrar 'incredibly' Changed Our E-mail for Hacker." *Computerworld*. Computerworld, 24 Feb. 2010. Web. 06 Mar. 2012. <http://www.computerworld.com/s/article/9162118/Baidu_Registrar_incredibly_changed_our_e_mail_for_hacker>.

[28] Muncaster, Phil. "Hackers Claim to Have Penetrated Foxconn Backdoor." *The Register*. The Register, 9 Feb. 2012. Web. 06 Mar. 2012. <http://www.theregister.co.uk/2012/02/09/foxconn_hack_swagg/>.

[29] Stevenson, Alastair. "OpChina: Anonymous Hackers Target China's Great Firewall." *International Business Times*. International Business Times, 16 Feb. 2012. Web. 06 Mar. 2012. <http://www.ibtimes.co.uk/articles/299622/20120216/opchina-anonymous-hackers-china-great-firewall.htm>.

Within the Chinese IT industry, the link between information security and profits is very clear to executives, leading to profitable and secure companies[30]. The Chinese government has taken great steps in encouraging companies across all industries to keep their information secure. In one government initiative aimed at preventing data leaks through phishing attacks, the government collaborated with top banks and search engines to help ensure the safety of Chinese companies' and peoples' data[31].

INDIA AND THE MIDDLE EAST

In India and the Middle East region, the main threats to internet information security are the ongoing cyber-wars between India and its neighbors, Pakistan and Bangladesh.

In the India-Bangladesh cyberwar, the two sides, along with their allies in the region, have traded attacks with increasing frequency since the January 26th, 2012 flare-up on India's Republic Day[32]. This hacking war is fueled, in part, by the increasing number of youths, typically male, who are technically skilled and are either un- or under-employed[33].

In a particularly active 10-day span in late February and early March of 2012, Bangladeshi hackers managed to hit over 30,000 sites, defacing them with Bangladeshi flags, images of Bangladeshi citizens killed or tortured by Indian boarder forces and lists of demands for the Indian government. In this particular attack, the Bangladeshis were assisted by Saudi, Indonesian and Malaysian hackers[34].

During the February-March cyber-war flare-up, India received assistance from Israeli hackers[35]. Israeli cooperation with India in this cyber-war stems from Israel's own ongoing cyber-war against Palestine and Islam, including a net-based disinformation and psychological warfare campaign against Pakistan[36].

Despite recent developments in the India-Bangladesh cyber-war, a director of a major internet security firm believes it will not be a cyber-war of huge consequence, saying, "All the high-end things that

[30] "Businesses Warned over Internet Security in China." *Information Technology*. Info Tech Spotlight, 5 Mar. 2012. Web. 07 Mar. 2012. <http://it.tmcnet.com/news/2012/03/05/6164512.htm>.

[31] "China Urges Tighter Internet Security after Series of Data Leaks." *Reuters*. Reuters, 30 Dec. 2011. Web. 06 Mar. 2012. <http://www.reuters.com/article/2011/12/30/us-china-internet-idUSTRE7BT07M20111230>.

[32] "India Pakistan Cyber-War." *Mid Day*. Mid Day, 28 Jan. 2012. Web. 06 Mar. 2012. <http://www.mid-day.com/news/2012/jan/280112-Indo-Pak-cyber-war-on-Jan-26.htm>.

[33] Nolen, Stephanie. "The Globe and Mail." *The Globe and Mail*. The Globe and Mail, 1 Mar. 2012. Web. 07 Mar. 2012. <http://www.theglobeandmail.com/news/world/border-killing-spurs-india-bangladesh-civilian-hacker-war/article2356107/>.

[34] Nolen, Stephanie. "The Globe and Mail." *The Globe and Mail*. The Globe and Mail, 1 Mar. 2012. Web. 07 Mar. 2012. <http://www.theglobeandmail.com/news/world/border-killing-spurs-india-bangladesh-civilian-hacker-war/article2356107/>.

[35] Nolen, Stephanie. "The Globe and Mail." *The Globe and Mail*. The Globe and Mail, 1 Mar. 2012. Web. 07 Mar. 2012. <http://www.theglobeandmail.com/news/world/border-killing-spurs-india-bangladesh-civilian-hacker-war/article2356107/>.

[36] Shah, Farzana. "Propaganda & Warfare in Cyber World." *Pakistan Tribune*. Pakistan News Service, 2 Aug. 2011. Web. 07 Mar. 2012. <http://paktribune.com/articles/Propaganda-%5E-Warfare-in-Cyber-World-242277.html>.

actually matter have already been compromised by the Pakistanis […]"[37]. In one attack, a group of hackers who call themselves the "Pakistani Cyber Army" hacked thousands of Indian websites including the site of India's Oil and Natural Gas Corporation[38].

In the midst of this multi-national cyber-war, companies in India continue to face threats from Anonymous and other independent hacking groups. Aiplex, an Indian company specializing in anti-piracy operations, has been repeatedly targeted by Anonymous[39].

India's ongoing multi-front cyber-war, combined with the traditional information security challenges faced by the rest of the world, complicate the environment in which India's companies and government operate.

GLOBAL INTERNET INFORMATION SECURITY OUTLOOK

In any organization, three types of leadership will affect information security risks going forward: political, corporate and technological leadership.

With tensions rising between Israel and Iran[40], it is important to note the lessons of the 2008 Russia-Georgia conflict: modern warfare will increasingly contain a cyber-war component[41]. Organizations located in Israel, Iran and their allies, including the US, should take note of the possible information security threats brought about by the hawkish rhetoric coming from their governments. In the Russia-Georgia conflict, the cyber-war proceeded conventional military action[42]. As Israel and its allies keep up the hawkish rhetoric, the risk of a pre-emptive cyber attack upon them only increases.

Beyond the actions of their governments, organizations must also take note of the relationship between their own corporate governance and the risk of an attack on their information. Increased activity by hacktivist groups, like Anonymous, shows that the information is at an increased risk in ethically-challenged organizations[43].

[37] Nolen, Stephanie. "The Globe and Mail." *The Globe and Mail*. The Globe and Mail, 1 Mar. 2012. Web. 07 Mar. 2012. <http://www.theglobeandmail.com/news/world/border-killing-spurs-india-bangladesh-civilian-hacker-war/article2356107/>.

[38] "India and Pakistan in Cyber War." *Al Jazeera English*. Al Jazeera, 4 Dec. 2010. Web. 07 Mar. 2012. <http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html>.

[39] Dharmakumar, Rohin. "Hackers' Haven." *Forbes India Magazine*. Forbes Magazine, 19 Sept. 2011. Web. 07 Mar. 2012. <http://forbesindia.com/article/boardroom/hackers-haven/28462/2?id=28462>.

[40] Marcus, Jonathan. "Israel Warns Time Short to Stop Iranian Nuclear Plans." *BBC News*. BBC, 03 June 2012. Web. 09 Mar. 2012. <http://www.bbc.co.uk/news/world-middle-east-17268478>.

[41] "6 Big Questions on Russian-Georgian Cyberwar." *Popular Mechanics*. Popular Mechanics, 1 Oct. 2009. Web. 09 Mar. 2012. <http://www.popularmechanics.com/technology/gadgets/4277603>.

[42] "6 Big Questions on Russian-Georgian Cyberwar." *Popular Mechanics*. Popular Mechanics, 1 Oct. 2009. Web. 09 Mar. 2012. <http://www.popularmechanics.com/technology/gadgets/4277603>.

[43] Claburn, Thomas. "Google: Hackers Targeted Chinese And Vietnamese." *InformationWeek*. Information Week Magazine, 31 Mar. 2010. Web. 06 Mar. 2012. <http://www.informationweek.com/news/security/vulnerabilities/224200944>

Attackers are quick to adapt to changes to technology and information security[44], so it should be expected that the next frontier of information security would be cloud security[45]. Technologies, new and old, all have their own unique security benefits and flaws; in this regard, cloud computing is no different. Fortunately for companies, cloud providers have become increasingly responsive to security needs[46].

The threats to internet information security are global threats. Naturally, these threats need to be addressed with borderless solutions[47]. Whether threats to information security come from Pakistan, China, Bangladesh or the United States is irrelevant: all threats must be addressed, regardless of their origin.

[44] Mills, Elinor. "Why the Security Industry Never Actually Makes Us Secure." *CNET News*. CNET, 03 Mar. 2012. Web. 06 Mar. 2012. <http://news.cnet.com/8301-1009_3-57389046-83/why-the-security-industry-never-actually-makes-us-secure/?tag=mncol;txt>.

[45] "Clear and Present Danger: Cyberattacks, Hackers and the Increasing Threat to Information Security." *Managing Technology*. Wharton School of Business, 7 July 2010. Web. 08 Mar. 2012. <http://knowledge.wharton.upenn.edu/article.cfm?articleid=2535>.

[46] "Clear and Present Danger: Cyberattacks, Hackers and the Increasing Threat to Information Security." *Managing Technology*. Wharton School of Business, 7 July 2010. Web. 08 Mar. 2012. <http://knowledge.wharton.upenn.edu/article.cfm?articleid=2535>.

[47] Greenemeier, Larry. "China Weighs In On Its IT Security Challenges." *InformationWeek*. Information Week Magazine, 20 July 2007. Web. 07 Mar. 2012. <http://www.informationweek.com/blog/229215585>.