

Cybersecurity in the Media Industry: The Growing Threat of Cybercrime and the Strategic Options to Defend Against It

By: Eric Fleddermann, University Honors, Spring 2013

Abstract:

Depleting billions of dollars every year from the U.S. economy, cybercrime is a large and growing problem for corporations in the United States. While cybercrime can hurt companies in almost any industry, recent incidents have demonstrated that media companies are particularly vulnerable targets for cybercriminals looking to steal valuable information and undermine the American media sector. This paper analyzes the issue of cybercrime, explains the specific threat to the media sector, discusses the lack of regulation to guide companies, and considers options that media companies can pursue to deal with cybersecurity issues. Using News Corporation as a case study, this paper makes recommendations about what media companies can do to improve their cybersecurity. While Congress has not yet passed legislation mandating media companies to take particular cybersecurity measures, this paper asserts that News Corporation should learn from its past hacking incidents and take initiative to become a model of cybersecurity for the media sector. This paper recommends that News Corporation increase the presence of in-house information security personnel, follow procedures for increasing its network defenses, and engage consultants from cybersecurity firm Mandiant Corporation to improve its cybersecurity. By taking these steps to defend itself against cybercrime, News Corporation can better protect its reputation, intellectual property, proprietary information, and news sources, and it can provide a model of quality and security for other media companies to follow. This paper concludes by asserting that, through its commitment to cybersecurity, News Corporation can become a more secure and successful media company in the 21st Century.

Cybercrime—The Threat:*Overview:*

As the world moves farther into the Information Age, an increasing number of human interactions have gone from the physical world into an electronic realm made up of computers, mobile devices, and the Internet—a world called cyberspace. Social conversations, banking transactions, product purchases, customer feedback, and a host of other activities that used to take place exclusively in the physical world now take place online between users of different devices. While the migration to cyberspace has increased speed and efficiency of long distance commerce and communication, it has also opened the door to a new kind of criminal activity. Instead of robbing a bank, criminals can now hijack electronic transactions and steal money online. Instead of breaking into an office and stealing documents, criminals can steal confidential data remotely from a computer. And instead of vandalizing the headquarters of a business, criminals can deface websites of corporations, allowing the entire world to see their message. As much of the world's business has moved online, so too has the business of crime. As a result, many individuals and businesses around the world are now vulnerable to the threat of cybercrime.

In 2011, Symantec conducted a survey of over 20,000 people in 24 countries to examine common thoughts on cybercrime. According to Norton Lead Cybersecurity Advisor, "Cybercrime is much more prevalent than people realize. Over the past 12 months, three times as many adults surveyed have suffered from online crime versus offline crime, yet less than a third

of respondents think they are more likely to become a victim of cybercrime than physical world crime in the next year."¹

The threat of cybercrime is a serious and growing problem. Cyber criminals from around the world try every day to get inside the systems of U.S. corporations in order to steal money, information, identifications, and secrets. Law enforcement is struggling to keep up with the rate at which new technologies create new opportunities for cybercriminals to commit their crimes. These criminals are rarely caught and even less often prosecuted. There is little to lose and a lot to gain for criminals with the time, the hardware, and the know-how to undertake criminal activity online. In today's world, many decide to engage in cybercrime, and while some of their activities target individuals, cybercriminals are constantly attacking corporations. Congress has not yet passed any legislation mandating companies to take particular cybersecurity measures, leaving companies largely on their own to deal with the pressing issue of cybersecurity.

Cybercriminal Tactics:

Before discussing the implications of cybercrime, it is important to understand how cybercrime works and some of the ways that criminals can hack into a network to steal someone's digital information or money. There are a variety of methods that cybercriminals use to conduct their activities. Described below are a few of the most common attack vectors against corporate targets.

Malware:

One of the most common methods that cybercriminals use to hack into other networks through the use of something called malicious software (known as malware). All software used

¹ Albanesius, Chloe. "Cyber Crime Costs \$114B per Year, Mobile Attacks on the Rise." *PCMag.com*. PC Magazine, 7 Sept. 2011. Web. 4 May 2013. <<http://www.pcmag.com/article2/0,2817,2392570,00.asp>>.

on computers, whether it's operating system software like Windows 8 or application software like Adobe Reader, is made up of many lines of code—the more complex the software, the more code is involved. Within those thousands, sometimes hundreds of thousands, of lines of code, there are always mistakes, known as 'bugs', that criminals can exploit and alter.²

When criminals discover a bug in a particular type of software, they can code lines of malware that, when downloaded, embed themselves into the existing software on the victim's computer. Once the computer is infected with malware, the criminal is then able to do whatever the malware was designed for—potentially hijack the computer for use in a botnet (described below), steal username and password information, or wait until a credit card transaction is made and steal money from the victim.

Typically, not always, there needs to be some kind of human trigger to install malware on a device. One of the most common ways for malware to be installed is through a phishing email—an email with a malicious attachment that tries to appear legitimate in order to trick the user into opening the attachment.³ An example of a spear-phishing message—a phishing email specifically tailored to a particular person—is given in Appendix 1.

DDoS Attacks:

Distributed denial of service (DDoS) attacks occur when a cybercriminals flood a website or a network with traffic with the intention to slow down or possibly crash the system. The criminal is able to send a huge amount of traffic to one site by harnessing a botnet.⁴ The criminal first uses malware to infect computer after computer with a malware that allows the criminal to

² Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco, 2010. 81. Print.

³ Ibid. 81.

⁴ Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: Wiley-Interscience, 2006. 413. Print.

direct the actions of the computer. Oftentimes, a computer can be actively contributing to botnet activities without the owner's knowledge. The owner may notice the computer acting more slowly than normal but often has no idea that his or her computer is being used to attack a website. Criminals can harness botnets of thousands, even hundreds of thousands, of computers to overwhelm websites with traffic.

Wireless and Mobile Attacks:

Today, many technologies communicate wirelessly, allowing anyone within range of the wireless network the opportunity to interfere with activity being conducted over the network. In some situations, a cybercriminal can capture information through wireless networks, and in others, the cybercriminal could potentially use an insecure network as an entry point to embed in a network. According to the 2012 Norton Cybercrime Report, two out of three online adults use free public or unsecured wi-fi and 44% of adults use that unsecured wi-fi to access personal email accounts.⁵ These unsecured networks make connected devices vulnerable to penetration by cybercriminals.

Digital Insiders:

Of course, one of the simplest ways for cybercrime to occur is when a trusted individual takes advantage of account access and steals information from within a company. As incentives increase for corporate espionage and more information can be accessed by individual employees on company networks, the digital insider threat becomes increasingly more problematic for corporations.⁶ The digital insider can be individuals acting on their own volition or they can be

⁵ Norton. *2012 Norton Cybercrime Report*. 7 Sept. 2012. Web. 5 May 2013. <<http://www.slideshare.net/NortonOnline/2012-norton-cybercrime-report-14207489>>.

⁶ Kellermann, Tom. *How to Thwart the Digital Insider: An Advanced Persistent Response to Targeted Attacks*. TrendMicro.com. TrendMicro Security. August 2012. Web. 30 April 2013. 1.

associated with organized criminal groups who often “recruit, or even place, insiders in a position to embezzle or skim monetary assets” from a company.⁷

Cybercrime Statistics:

- A new piece of malware (malicious software) is created every second.⁸
- Over 90% of enterprise networks contain active, malicious malware.⁹
- In 2011, 52% of companies failed to report or remediate a cyberbreach.¹⁰
- Under U.S. law, only 7% of all cybercrimes, from fraud to money laundering to data theft, are successfully prosecuted.¹¹
- 556 million victims of cybercrime per year, over 1.5 million per day, nearly 18 per second¹²
- Total annual losses globally from cybercrime are in excess of \$1 trillion, much of that is borne by the U.S. economy.¹³

As demonstrated by these statistics, cybercrime has become a major problem for both individuals and corporations. As Dmitri Alperovitch, Vice President of Threat Research at McAfee, said of cybercrime, “Today we see pretty much any company that has valuable intellectual property or trade secrets of any kind being pilfered continually, all day long, every

⁷ Verizon Risk Team, and U.S. Secret Service. *2010 Data Breach Investigations Report*: Verizon, 2010. Print. 33.

⁸ Kellerman, Tom. *How to Thwart the Digital Insider*. 1.

⁹ Ibid. 1.

¹⁰ McAfee & SAIC. *The Underground Economies*. Page 15.

¹¹ Jorgenson, John. *The Statistics of Cybercrime*. The Sylint Group. 2008. <<http://infragardtampabay.org/CyberSecurity/tabid/57/Default.aspx>>.

¹² Norton. *2012 Norton Cybercrime Report*.

¹³ Jorgenson. *The Statistics of Cybercrime*. Page 5.

day, relentlessly.”¹⁴ While almost every industry is vulnerable to cybercrime, the next section will explore the growing threat to the media sector, in particular.

The Risk to the Media Sector:

Overview:

Since the turn of the millennium, there have been countless headlines of cyber attacks against major corporations. Among some of the most serious were the Slammer worm incident of 2003 and the electronic heist of the Royal Bank of Scotland in 2008. Incidents like these have caused a lot of concern for the vulnerability of the financial and energy sectors to cybercrime. However, recent events have demonstrated that the media industry is also a target and is becoming increasingly more vulnerable to cybercriminal activity.

Most recently, an attack on the media sector made headlines across the country when, on April 23rd, 2013, the official Associated Press Twitter handle tweeted a message saying that there had been explosions at the White House and that President Obama had been injured. As a result of the message, the Dow Jones Industrial Average dropped 128 points in the five minutes following the tweet.¹⁵ The market regained value as soon as word spread about the tweet being false, but the incident had proven how vulnerable trusted news sources like the Associated Press are to cybercrime. While this incident is just one of many cybercrimes to have afflicted the media sector, one media company in particular, News Corporation, has had to deal with a number of cyber incidents over the years.

News Corporation Background:

¹⁴ Kellermann, Tom. "Introductory Lecture." ITEC-596: Information Security Risk in the Digital Economy. Ward Circle Building, American University, Washington, D.C. 21 Jan. 2013. Lecture.

¹⁵ *Timeline of AP Hacking, Reaction*. 23 April 2013. 30 April 2013.

<http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/>

News Corporation is an integrated media conglomerate that controls a variety of subsidiaries in book publishing, newspapers, magazines, and TV stations around the world. As the parent company of media brands like the Wall Street Journal, Fox News, 20th Century Fox, and National Geographic, News Corporation is responsible for managing assets in North America, Europe, and Australia. Last quarter, News Corporation had over \$2.3 billion in net income from its various brands and subsidiaries,¹⁶ and it controls of \$55 billion in assets¹⁷ (News Corporation's FY2012 Income Statement can be found in Appendix 2). As a company with so much valuable corporate data, proprietary information, and intellectual property traveling throughout its networks among its various media brands, News Corporation is a major target for cyber criminals, both domestic and foreign, looking to steal valuable information and to undermine the American media sector.

Previous Cyber Attacks on News Corporation:

Over the past several years, News Corporation has had a number of cyber attacks against it that have proven its vulnerability to cybercrime. A few of the more notable ones include the following:

DDoS Attacks against U.S. corporate sites (2009)—North Korean hackers manipulated a botnet (a massive, global network of infected computers) to wage a Distributed Denial of Service (DDoS) attack against U.S. companies, causing some websites to slow down and others to completely crash. Sites affected by the attack included notable media sites such as

¹⁶ *News Corporation FY2012 Income Statement*. finance.yahoo.com. Web. 29 April 2013. <<http://finance.yahoo.com/q/is?s=nwsa>>.

¹⁷ *News Corporation FY2012 Balance Sheet*. finance.yahoo.com. Web. 29 April 2013. <<http://finance.yahoo.com/q/bs?s=NWSA+Balance+Sheet&annual>>.

voanews.com, washingtonpost.com, and News Corporation's marketwatch.com.¹⁸ The attack persisted for several days, denying both employees and customers access to media websites and harming operations of News Corporation.

Lulz Security Hacks News Corporation Websites (2011)—Hackers from a politically motivated “hacktivist” group posted a fake news article on several News Corporation websites about the death of CEO Rupert Murdoch. Members of the hacktivist group claimed to be acting in response to the News of the World wiretapping scandal.¹⁹ During the attack, the hackers stole login credentials for over fifty News Corporation employees and used them to access employee email accounts and steal both corporate and personal information.

APT1 (Advanced Persistent Threat 1) - U.S. Media hacks (2007-2013)—Hackers associated with a Chinese military cyberespionage group stole information about anonymous news sources from numerous U.S. media outlets, including the New York Times, Washington Post, and Wall Street Journal. The hackers were able to monitor computer activity of employees from these media outlets and access their employee emails. The extent of information that was compromised by APT1 is unknown, but the media outlets lost a number of sources in China as a result of the attacks. Whenever an anonymous source from China would reveal identifying information in an email to media reporters, the media outlets would often not hear from the source again. APT1 demonstrated that corporations are not just up against small-time criminals but state-funded military operations trying to steal secret information. While the media sector was one sector that APT1 attacked, the group also targeted a range of other U.S. industries,

¹⁸ McAfee. *Ten Days of Rain: A White Paper on the 2009 DDoS Attacks*. <http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf>

¹⁹ Bilton, Nick. “Lulz Security Says It Hacked News Corporation Websites.” *The New York Times*. 18 July 2011. 30 April 2013. <http://bits.blogs.nytimes.com/2011/07/18/lulz-security-says-it-hacked-news-corporation-sites/>

ranging from defense contractors to law firms, over a long period of time. In February 2013, a cybersecurity firm called Mandiant Corporation produced a report, detailing specific intelligence its analysts had gathered on APT1, including personal information on people involved in the group, the exact location of the group's headquarters, and the methods the group used to hack various industries.²⁰ The report included a timeline of the industries hacked by APT1 (Appendix 2). In the wake of the news breaking about the attack, several media companies—like the New York Times and the Washington Post—hired Mandiant's cybersecurity consulting services to provide incident response.²¹ News Corporation's Wall Street Journal engaged Mandiant consultants to investigate the incident.²²

Increased Risk to Media Activities:

As consumers purchase more mobile devices and integrate them into their daily lives, media companies have begun abandoning print formats and have been exploring new ways to deliver news, entertainment, and other media to consumers through the Internet to electronic platforms. According to a study by the Pew Research Center, "the majority of Americans now get news through at least one digital, web-based device."²³ In order to take advantage of this

²⁰ Mandiant Corporation. *APT1: Exposing One of China's Cyber Espionage Units*. Mandiant.com. 19 February 2013. 30 April 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. Page 23.

²¹ Sanger, David E., David Barboza, and Nicole Perlroth. "China's Army Unit Is Seen as Tied to Hacking Against the U.S." *Nytimes.com*. The New York Times, 19 Feb. 2013. Web. 07 May 2013. <<http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all>>.

²² Holland, Steve. "Mandiant Goes Viral after China Hacking Report." *Nbcnews.com*. NBC News, 20 Feb. 2013. Web. 07 May 2013. <<http://www.nbcnews.com/technology/technolog/mandiant-goes-viral-after-china-hacking-report-1C8513891>>.

²³ Christian, Leah, Amy Mitchell, and Tom Rosenstiel. "Mobile Devices and News Consumption: Some Good Signs for Journalism." *State of the Media*. Pew Research Center,

shift in consumer habits, media companies, like News Corporation, are taking more of its activities online. For instance, the Wall Street Journal operates several different websites, such as WSJ.com and marketwatch.com, that allow customers to create customized profiles and manage their subscriptions online. Providing these services requires News Corporation to house databases with customer usernames, passwords, email addresses, physical addresses, and other sensitive information. Since these databases inherently have to send and receive signals from the Internet, they can be compromised by cybercriminals. Additionally, as News Corporation seeks to expand its operations around the world, information such as bids for mergers and contracts become targets for cybercriminals looking to undermine corporate dealings. News Corporation has already had to deal with cybersecurity issues in the past, and as more media activities take place in cyberspace, there will be more digital information for cybercriminals to compromise and cybercrime will continue to be a threat to News Corporation and other companies in the media sector.

Lack of Regulation:

Overview:

Despite the serious threat that cybercrime poses to U.S. corporations, there is surprisingly little regulation of cyberspace and guidance on cybersecurity. This lack of legislation creates a problematic environment where criminals have incentive to take the offensive and try to execute cybercrimes and companies do not have regulations to follow to understand what measures they should take to defend themselves. While the White House has issued executive orders on cyber initiatives and Congress has attempted to pass several bills to regulate cyberspace, these attempts at legislation have had little effect on changing the legal environment surrounding cybercrime.

2012. Web. 05 May 2013. <<http://stateofthemedias.org/2012/mobile-devices-and-news-consumption-some-good-signs-for-journalism/>>.

Recent Attempts at Passing Cyber Legislation:

In May of 2009, President Obama declared our digital infrastructure a strategic national asset and made protecting this infrastructure a national priority.²⁴ On February 12, 2013, President Obama issued an executive order in an attempt to improve the cybersecurity of U.S. critical infrastructure. The order expanded public-private information sharing, improving communication between the Department of Homeland Security and corporate managers who need information about new cyber threats. It also directed the National Institute of Standards and Technology (NIST) to create a more stable cyber framework that will lessen risks to critical infrastructure.²⁵ While this order indicates political will in the White House to address cybercrime, these measures fall short of mandating serious action by industry leaders to shore up their cyber defenses. That type of legislation would have to come from Congress, which so far, has failed to pass meaningful cybersecurity legislation.

Most recently, the U.S. House of Representatives passed the Cyber Intelligence Sharing and Protect Act (CISPA). The bill now faces Senate deliberations and could potentially be signed into law. However, as with other cyber regulation, the bill faces skepticism from people who see the bill as an attack on personal privacy. According to Tom Kellermann, Vice President of Cyber Security at Trend Micro, when it comes to cybercrime, it's the lack of regulation, not the regulation itself, that undermines privacy. The current state of cybercrime is such that criminals can breach systems, steal information, and cause damage online without ever being punished. Privacy concerns surrounding cyber regulation largely stem from public worry that

²⁴ Office of the Press Secretary. "Executive Order on Improving Critical Infrastructure Cybersecurity." *Whitehouse.gov*. The White House, 12 Feb. 2013. Web. 04 May 2013. <<http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0>>.

²⁵ Office of the Press Secretary. "Executive Order on Improving Critical Infrastructure Cybersecurity."

government agencies like the FBI will have the ability to monitor web traffic; however, the alternative is for cybercriminals to conduct their activities unchecked across the Internet and steal data from American citizens.

In addition to privacy concerns of cyber legislation, politicians can be hesitant to adopt cyber reform because some congressmen and women have been threatened over the passage of cybersecurity legislation. Representative Dutch Ruppersberger, who sponsored CISPA, has been targeted by hacker group Anonymous for his support of cyber regulation. Anonymous is the same group that took credit for crashing the websites of USTelecom and TechAmerica—two trade unions that publically supported CISPA in its nascent stages.²⁶ Unfortunately, without the political will to pass cyber legislation, cyberspace will continue to go unregulated, there will still be strong incentive for criminals to engage in cybercrime, and corporations will receive no definitive guidance to address their cybersecurity issues. As a result, News Corporation and other media companies are largely on their own to deal with the pressing issue of cybercrime.

Options to Improve Cybersecurity:

Overview:

Without legal guidance or regulatory requirements, many companies fail to recognize the importance of cybersecurity and do not invest enough capital in protecting themselves against cybercrime. While the financial and energy sectors have begun to invest more in defending their networks against cybercrime, the media industry, as demonstrated by the cyber attacks against News Corporation and other companies, still lacks adequate defenses against cybercrime. Media companies should consider various options for improving their cybersecurity and take action to

²⁶ Martinez, Jennifer. "Ruppersberger: Hacker Group Anonymous Made Threats over CISPA." *TheHill.com*. News Communications, Inc., 27 Apr. 2013. Web. 30 Apr. 2013. <<http://thehill.com/blogs/hilicon-valley/technology/296531-ruppersberger-hackers-threatened-lawmakers-over-cispa>>.

protect themselves as they take more of their activities online. In particular, News Corporation should learn from its previous hacking incidents and take initiative to invest in cybersecurity initiatives and become a model for cybersecurity in the media industry in the 21st Century. There are numerous options News Corporation could pursue to increase its cybersecurity, and the following sections discuss a few of these options.

Hire Information Security Personnel:

One major problem with corporate cybersecurity is that employees are often unclear on who is responsible for dealing with security issues. Some companies consider security to be a responsibility that pervades all other functions, so they do not hire personnel for the separate role of handling security.²⁷ One major step that media companies can take is to hire employees with the specific task of keeping their information secure from cybercriminals. Increasingly, companies have begun to incorporate the position of Chief Security Officer (CSO) into their upper management positions. While having a CSO is a step in the right direction, a CSO is inherently responsible for both physical security and information security, both of which are very different functions that require different types of expertise.²⁸ To ensure that cybersecurity issues are addressed by someone with specific expertise in information security, companies should designate a specific Chief Information Security Officer, with the sole task of protecting a company's networks. Currently, News Corporation employs a CSO, but does not have a separate CISO.²⁹

²⁷ Furnell, Steven. *Computer Insecurity: Risking the System*. [New York]: Springer-Verlag London Limited, 2005. 44. Print.

²⁸ Ibid. 45.

²⁹ News Corporation. "Hemanshu Nigam, News Corporation Chief Security Officer, to Transition to Role of Safety Advisor." *Newscorp.com*. News Corporation, 20 Apr. 2011. Web. 06 May 2013. <http://www.newscorp.com/news/news_450.html>.

Employing a CISO with specific responsibility for cybersecurity can provide several advantages. First, it brings puts a face to information security and cyber risk management. Employees across the company who come across security issues always have one person to go to, and all security problems flow directly to one person to assess and manage. Additionally, having a CISO gives cybersecurity issues a representative at the highest level of management in the company, helping to ensure that strategic decisions are made with the best interests of security in mind. Finally, and perhaps most importantly, the institution of the CISO position communicates the importance of information security to the rest of the company, and it creates an attitude across all employees that the company takes cybersecurity seriously.

While News Corporation already employs some information security personnel, it does not yet have a chief level position dedicated to information security. By instituting the position of CISO at the top level of the organization, News Corporation can demonstrate to its employees, its customers, and other companies in the media industry that it is organizing its corporate structure to emphasize the importance of cybersecurity.

Implement SANS 20 Critical Controls:

Media companies who have in-house information security personnel can shore up their defenses by following the detailed procedures of the SANS Institute's 20 Critical Controls. The SANS Institute is one of the leading information security education institutions in the world. In addition to offering classes and products to help cybersecurity professionals, the SANS Institute publishes a guide called the 20 Critical Controls, which highlights twenty essential steps for information security officers to go through when securing a network. Media companies should ensure their information security personnel are completing the steps outlined in this guide to maintain and improve their defenses against cybercrime.

The 20 Critical Controls begin by discussing inventory functions for information security personnel to undertake. They mandate that security personnel should take inventory of every device—desktop computer, laptop, mobile device, printer, etc.—that is allowed to access the company's network. This inventory collection allows information security personnel to keep track of all the endpoints of a network and ensure that they are all fully patched and have the most up-to-date software. Additionally, by allowing administrators to monitor traffic across inventoried endpoints, this control helps prevent against digital insiders who may be introducing new devices onto the network.³⁰ In addition to taking inventory of all hardware that accesses the company network, security personnel should also take inventory of all software running on devices that have access to the network. By controlling which software can be installed on devices, security personnel can ensure that all software is up-to-date and minimize vulnerabilities in the network.

In addition to inventory controls, the 20 Critical Controls include instructions for security personnel to set up defenses against malware and wireless attacks by installing and maintaining effective antivirus software and securing the company's wireless networks. Additionally, the 20 Critical Controls stresses backing up all electronic data. While data theft can be very harmful to a company in terms of finances and reputation, data destruction can be crippling to a company's operations. In order to ensure that media company's keep their data safe, security personnel need to have backup systems in place to ensure that company data is secured in more than one place.

³⁰ "20 Critical Security Controls Version 4.1." *SANS.org*. Center for Strategic and International Studies, 2013. Web. 05 May 2013. <<http://www.sans.org/critical-security-controls/>>.

Finally, the 20 Critical Controls advises companies to conduct vulnerability assessments and red team testing. These controls involve a company's own information security personnel taking the role of cybercriminals and seeing if they can penetrate the company's network from the outside. This control gives information security personnel the ability to test for bugs in the system and figure out the harm those bugs could cause if exploited. Red team testing also helps other company personnel practice emergency preparedness in the event of a data breach and allows for company-wide incident response exercises. These 20 Critical Controls are not easy to implement and require information security expertise to handle effectively. However, if a media company has the information technology or security personnel on staff who can implement them, the 20 Critical Controls provides companies with a good "do-it-yourself" guide to information security.

Engage Cybersecurity Consulting Services:

While the previous options involve in-house restructuring and procedures to address the issue of cybersecurity, there is also the option to bring in outside help from cybersecurity consultants. Several companies, such as McAfee, SAIC, Kroll, and many others offer cybersecurity services; however, few companies match the impressive credentials of Mandiant Corporation, a company that media companies, including News Corporation, have turned to in times of cyber crisis. Mandiant's expert cybersecurity consulting services could help News Corporation usher in a new standard for security across its company.

Mandiant Corporation has become the global leader in incident response and computer forensics solutions services. Founded in 2004 by Kevin Mandia, a former cyber analyst with the United States Air Force, Mandiant Corporation has seen explosive growth over the past nine years, as an increasing number of companies have turned to Mandiant for expertise in addressing

their security needs. Headquartered in Alexandria, VA, and operating offices all over the country, Mandiant has provided security response for over 30% of Fortune 100 companies and regularly consults for a number of state and federal government agencies.³¹ Today, as a result of its unique threat analysis and intelligence procedures, Mandiant prides itself on being the only security company that can both 1) tell a company when it has been compromised, and 2) tell what the material impact of the breach is.³² Mandiant made headlines when it published a report exposing APT1 and the source of the hacks on U.S. media companies in February 2013. In the wake of that hacking episode, News Corporation and other media companies engaged Mandiant to conduct investigations into the incident.³³

But while incident response is the service that gained Mandiant fame among U.S. media companies, Mandiant offers a number of other products and services to help prevent cyber intrusions of company networks. For instance, if companies lack the security expertise to protect their own security, Mandiant can provide training and software to its clients' information technology personnel to make sure they have the most advanced tools available to prevent cybercriminals from penetrating their networks. Additionally, Mandiant hires out its own people to provide 24 hour surveillance of clients' networks, monitor for any signs of suspicious activity, and keep clients' networks secure.³⁴

But no matter how secure a company's defenses are, there will be breaches, and when those intrusions occur, Mandiant can provide its clients with rapid intelligence on where the

³¹"Mandiant, A New Name for a Fast-Growing Company." *Businesswire.com*. Berkshire Hathaway, 14 Feb. 2006. Web. 07 May 2013.

<http://www.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view>.

³² "Mandiant." *Mandiant.com*. Mandiant Corporation, 2013. Web. 07 May 2013.

<<https://www.mandiant.com/company/>>.

³³ Holland, Steve. "Mandiant Goes Viral after China Hacking Report." *nbcnews.com*.

³⁴ "Mandiant." *Mandiant.com*.

threat is coming from, how long it has been occurring, and what information the attackers are attempting to steal. For clients who engage their services, Mandiant consultants respond to cyber intrusions as they occur, boot hackers out of our clients' computer networks, and patch defenses to prevent future breaches. From incident response to program development to intelligence subscriptions to vulnerability assessments, Mandiant provides its clients with a variety of services to protect them against cybercriminal activity. Media companies could improve their cybersecurity in a number of ways by engaging Mandiant's consulting services.

However, while Mandiant's services might be more comprehensive than hiring extra personnel or following SANS 20 Critical Controls, those services also come with a greater price tag. For the most part, Mandiant provides unique service packages to each client, so the company does not make its pricing structure public. However, according to Mandiant's Media Relations Coordinator, a corporate subscription to Mandiant's Intelligent Response threat analysis application software costs \$125,000 plus recurring fees of \$25,000 for support and maintenance.³⁵ Additionally, according to a publically posted contract between Mandiant and the South Carolina Department of Revenue, Mandiant consultants charge a rate of \$300/hour to conduct incident response, clear networks of intruders, and shore up defenses. The total bill for Mandiant's services in that case totaled \$840,000.³⁶ Given the massive size of News Corporation, the variety of data that needs to be secured, and the number of endpoints across News Corp's global network, the price tag for Mandiant's consulting services could be very

³⁵ Helmick, Susan. "Mandiant Pricing and Revenue." Message to the author. 2 May 2013. E-mail.

³⁶ Adcox, Seanna. "SC Revenue Director Says Agency's Completed Top 2 Security Recommendations, Working on Others." *The Republic*. The Associated Press, 23 Apr. 2013. Web. 02 May 2013.
<<http://www.therepublic.com/view/story/9e3eb057764c46d4aa83414adb8ed556/SC-XGR--Hacked-Tax-Returns>>.

substantial. However, given that over 30% of Fortune 100 companies have called upon Mandiant to help shore up their cybersecurity, the high price tag may be worth the quality network defense that will result.

Recommendations:

News Corporation is in a unique position to take initiative with increasing its commitment to information security. The company has already had to endure several incidents of past cyber attacks, ranging from website defacing to DDoS attacks to data theft, so News Corporation executives know the damage that cybercrime can cause. While Congressional legislatures have not yet passed information security regulations for media companies, News Corporations executives are already aware of the vulnerability of their company, and their industry, to cybercrime. Additionally, News Corporation, like all media companies, is moving an increasing amount of its media activities online as it fights to engage media consumers on mobile devices. This migration to digital technology increases the amount of information that can be compromised across News Corporation's diverse brands. Finally, while other news companies have struggled financially in recent years due to the Financial Crisis and the major media transition from print to digital, News Corporation has been performing very well in recent years, with its stock price near its all-time high of \$32.19.³⁷ With its history of cyber problems, its continued migration to digital media, and its substantial profits from recent performance, News Corporation has the motive and the means to undertake cybersecurity reforms to increase the security of the company.

Given the options available to News Corporation, News Corp executives should undertake all cybersecurity measures that are available to them. First, while News Corporation

³⁷ News Corporation. "Stock Information." *NewsCorp.com*. News Corporation, 7 May 2013. Web. 07 May 2013. <<http://investor.newscorp.com/stockquote.cfm>>.

already has information security personnel and a Chief Security Officer, News Corp executives should add a seat at the boardroom table and appoint a Chief Information Security Officer.

While this move will give a central authority for cybersecurity issues at News Corporation, it will also demonstrate to employees across the various brands of the very large company that News Corporation is restructuring itself to take cybersecurity seriously. By designating a chief executive for information security, News Corporation can foster an attitude of respect for information security among its employees throughout the company, which can help immensely reinforce security.

Additionally, News Corporation information security personnel should assess the security of the company's network by conducting a coordinated assessment with the SANS Institute's 20 Critical Controls. While the News Corporation network is undoubtedly very complex, with many different devices connected to many different servers in the offices of News Corporation's many different media brands, information security personnel should start with the first controls and take inventory of all hardware and software connected with News Corporation's network. With this map of the network, information security personnel can better address the other steps in the 20 Critical Controls, and it will help identify vulnerabilities, which can be pressure tested through vulnerability testing.

Of course, implementing the 20 Critical Controls across a global corporate network like News Corporation's can be a massive undertaking, and as long as News Corporation is going to be expending human and financial resources on improving the security of its network, it should bring in an outside perspective to ensure that it is securing itself properly. To obtain this outside perspective, News Corporation should talk with Mandiant Corporation about engaging Mandiant's cybersecurity consulting services. While News Corporation has its own in-house

information security personnel, history has demonstrated that its network has stayed vulnerable over time and has been attacked in different ways time and time again. By hiring the cybersecurity professionals from Mandiant, News Corporation security personnel would get expert perspective on how to properly reform their network security and what they can do to prevent future attacks. Additionally, News Corporation security personnel (and, hopefully, its CISO) will have access to the latest intelligence on new threats evolving in the Internet, and it will be able to counter these threats before they harm the company. While Mandiant's services are expensive, given News Corporation's recurring troubles with cybercrime in the past and the fact that the company has been bringing in substantial profits over the past several quarters, News Corporation's decision to invest in Mandiant's cybersecurity consulting services would be both a wise and feasible move for News Corporation to make. By restructuring its top level management to include a new CISO position, beginning an initiative to take inventory of its entire corporate network, and engage consultants from Mandiant to ensure the integrity of its cybersecurity reforms, News Corporation can go from a vulnerable target for cybercriminals to a model of quality and security for other corporations in the media industry to follow.

Conclusion:

Cybercrime is a major problem for all types of individuals and corporations around the world, and it is only growing in magnitude. Increasingly more computers and mobile devices connect people to the Internet every day, and as the media industry takes an increasing amount of its activities online, it will have more information in cyberspace for cybercriminals to exploit. The current legal environment surrounding cyberspace does not give companies guidance for how to deal with this issue, and the low rates of prosecution only incentivize more cybercriminal activity to take place. The media industry needs to take action to protect its proprietary

information, customer data, and intellectual property from the cybercriminals who are constantly trying to steal them. As a media company that has survived several cyber incidents in the past and has realized its vulnerability to cybercrime, News Corporation should leverage its currently strong financial performance and take steps to become a model of cybersecurity for the media sector in the United States. In order to take cybersecurity more seriously, News Corporation should have a hiring surge of information security personnel, designate a chief-level position of Chief Information Security Officer; begin a full network audit by implementing the SANS Institute's 20 Critical Controls, and engaging consultants from Mandiant to oversee cross-company cybersecurity reforms.


While the media industry has proven to be one particularly vulnerable target of cybercrime, information security issues are not specific to the media industry alone. Every company that handles commercial transactions, transfers communications, or even stores data on Internet-connected devices and networks is vulnerable to cybercrime. As the world moves farther into the Information Age, the U.S. economy is being built upon a digital infrastructure that is vulnerable to criminal activity. Both the federal government and private companies need to do their part to protect the security of this infrastructure and the economy. Congress should pass meaningful legislation that helps regulate Internet traffic, increases punishments for cybercriminals, and makes it more difficult for cybercrime to undermine U.S. Internet activity. Until that happens, companies will be on their own to shore up their own cyber defenses and to protect their information from cybercrime. By investing time, money, and human resources in cybersecurity initiatives, News Corporation can increase its cybersecurity across all its brands, become a model of cybersecurity for other companies to follow, and continue its strong performance into the digital age of media.

Appendix 1:
Example of Spear-Phishing Email³⁸

Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketmail.com>
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next week?
We need to finalize the press release.
Details [click here](#).

Kevin Mandia

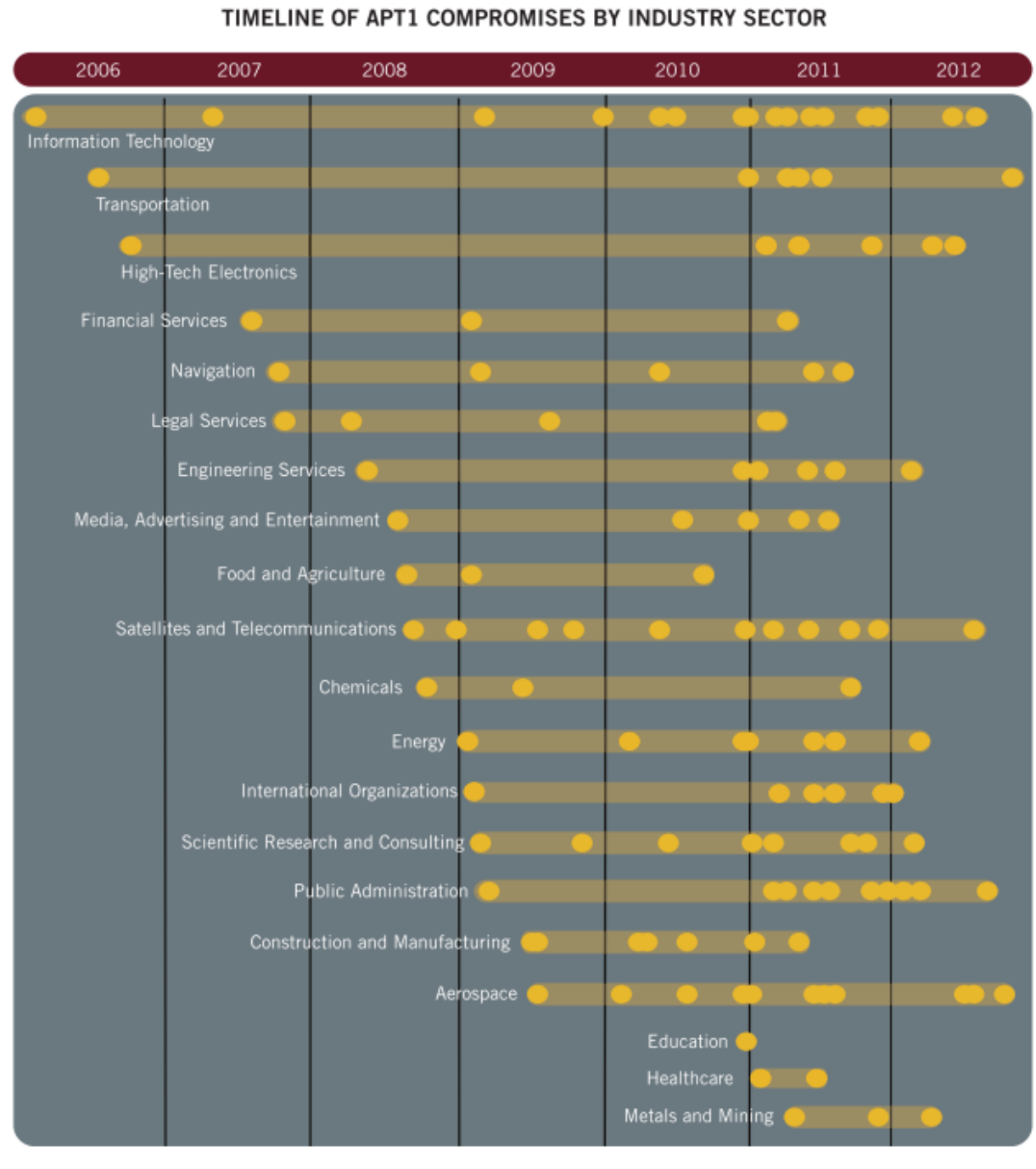
Name	Type
 employee benefit and overhead adjustment keys.pdf ...	Application

³⁸ Mandiant Corporation. *APT1: Exposing One of China's Cyber Espionage Units*. Mandiant.com. 19 February 2013. 30 April 2013.
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. Page 22.

Appendix 2:
News Corporation's Quarterly Income Statement for FY 2012³⁹

In Millions of USD (except for per share items)	3 months ending 2012-12-31	3 months ending 2012-09-30	3 months ending 2012-06-30	3 months ending 2012-03-31	3 months ending 2011-12-31
Revenue	9,425.00	8,136.00	8,370.00	8,402.00	8,975.00
Other Revenue, Total	-	-	-	-	-
Total Revenue	9,425.00	8,136.00	8,370.00	8,402.00	8,975.00
Cost of Revenue, Total	5,869.00	4,848.00	5,233.00	5,216.00	5,583.00
Gross Profit	3,556.00	3,288.00	3,137.00	3,186.00	3,392.00
Selling/General/Admin. Expenses, Total	1,666.00	1,610.00	1,642.00	1,580.00	1,614.00
Research & Development	-	-	-	-	-
Depreciation/Amortization	310.00	300.00	310.00	294.00	281.00
Interest Expense(Income) - Net Operating	-	-	-	-	-
Unusual Expense (Income)	65.00	152.00	2,873.00	4.00	-122.00
Other Operating Expenses, Total	70.00	78.00	15.00	3.00	26.00
Total Operating Expense	6,565.00	5,581.00	10,005.00	7,118.00	7,475.00
Operating Income	2,860.00	2,555.00	-1,635.00	1,284.00	1,500.00
Interest Income(Expense), Net Non-Operating	-	-	-	-	-
Gain (Loss) on Sale of Assets	-	-	-	-	-
Other, Net	-	-	-	-	-
Income Before Tax	2,860.00	2,555.00	-1,635.00	1,284.00	1,500.00
Income After Tax	2,458.00	2,296.00	-1,509.00	1,003.00	1,127.00
Minority Interest	-77.00	-63.00	-44.00	-66.00	-70.00
Equity In Affiliates	-	-	-	-	-
Net Income Before Extra. Items	2,381.00	2,233.00	-1,553.00	937.00	1,057.00
Accounting Change	-	-	-	-	-
Discontinued Operations	-	-	-	-	-
Extraordinary Item	-	-	-	-	-
Net Income	2,381.00	2,233.00	-1,553.00	937.00	1,057.00

³⁹ News Corporation FY2012 Income Statement. finance.yahoo.com. Web. 29 April 2013.
<<http://finance.yahoo.com/q/is?s=nwsa>>.

Appendix 3: APT1's Timeline of Cyberattacks by Industry⁴⁰

⁴⁰ Mandiant Corporation. *APT1: Exposing One of China's Cyber Espionage Units*. Mandiant.com. 19 February 2013. 30 April 2013.
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. Page 23.