Deloitte.

Cyber & Insider Risk at a Glance: The Pharmaceutical Industry

Abstract

Nothing is more valuable to a pharmaceutical company than the formula for one of its new drugs. Reports of hackers breaking into all sorts of firms and stealing their trade secrets is of enormous concern. Equally troubling, experts warn that theft of trade secrets by company insiders is a larger problem. This article looks at some recent cases of corporate cyber-espionage and insider trade secret theft. It discusses the use of spear phishing and zero-day exploits by sophisticated criminal gangs targeting corporations as well as more traditional, but hard to detect cases of outsiders paying employees to steal secrets. Many of the victims of cyber theft find themselves the target of class action lawsuits and regulatory actions. A quick look at data breach shows a rapidly changing regulatory environment, growing risks of litigation, and some important insurance implications for companies and their top management. This article ends with some areas that companies should consider in tightening up their safeguards against intellectual property theft.

"If you have anything of value, you will be targeted. You won't necessarily know by who."

John Stewart, Chief Security Officer, Cisco Systems[1]

Introduction

In 2011, the UK government estimates its pharmaceutical, biotechnology and healthcare sector suffered £1.8b in losses arising from theft of intellectual property (IP)[2]. The same year, the US government reportedly estimated its economy suffered $500b in harm from intellectual property and trade secret theft[3]. The Obama administration has publicly accused China of orchestrating many of these attacks against US organizations and even took the extraordinary step of indicting alleged members of the Chinese government's elite military hacking team[4].

One Chinese gang allegedly behind attacks on Boston Scientific and other US pharmaceutical companies also developed an exploit deployed specifically against Japanese targets[5]. **According to FireEye, in 2013, Japan was the fourth largest target of such sophisticated cyber gangs that it tracks** [6]. If Japan's pharmaceutical industry incurred damages on a level similar to the UK (whose market is about half the size), this would amount to something on the scale of ¥300b per year[7].

The global market for pharmaceuticals is estimated to hit USD $1.1 trillion this year[8]. Strong demand for new cures and high profits associated with marketing new, patent-protected drugs drive fierce competition in product development[1]. It is not surprising then that criminal elements have increasingly targeted the intellectual property of pharmaceutical companies. The cost of IP falling into a competitor's hands, however, is difficult to calculate[9]. For its 2014 estimate of the global cost of cybercrime, CSIS presented a wide range of $375-575m and specifically noted the difficulty of calculating damages caused by IP theft, adding this difficulty likely produced an artificially low estimate[10].

Despite this challenge, some hard costs are identifiable. Cyber damages expert, the Ponemon Institute, estimates that globally the cost of recovering from a breach averaged $3.5m in 2014[11]. **Ponemon's 2014 review of cyber incidents reported by 26 Japanese companies in 10 sectors showed that the average cost of remediation in Japan is approximately ¥241m**[12]. In addition, the firm found that the adage, "an ounce of prevention is worth a pound of cure", applies to a robust cyber defense. On average, Ponemon found a strong security posture to be the single most important factor in decreasing the cost of cleaning up after a cyber-incident[2].

1. Economist Intelligence Unit, "Cyber Theft of Corporate Intellectual Property: The Nature of the Threat", March 2012.
2. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
3. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html
4. http://usnews.nbcnews.com/_news/2013/03/11/17273068-cybersecurity-threatens-us-china-relationship-white-house-official-says?lite; http://www.reuters.com/article/2014/05/19/us-cybercrime-usa-china-idUSBREA4I0942014051
5. http://www.FireEye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
6. http://www2.FireEye.com/rs/fireye/images/FireEye-advanced-threat-report-2013.pdf
7. http://databank.worldbank.org/data/home.aspx; http://www.efpia.eu/uploads/Figures_Key_Data_2013.pdf, p.22.
8. http://en.wikipedia.org/wiki/Pharmaceutical_industry#cite_note-40 (Link to IMS cite dead).
9. http://csis.org/files/attachments/140609_McAfee_PDF.pdf, p2.
10. http://csis.org/files/attachments/140609_McAfee_PDF.pdf
11. http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
12. http://www.ibtimes.com/uk-joins-investigation-ebay-data-breach-did-company-do-enough-protect-user-data-1589452

Caught unprepared, it is likely that panic grips senior management when a cyber-breach is discovered. **There is a realization that when the breach becomes public, the company possibly faces lawsuits from customers and shareholders, regulatory fines and actions by a variety of national and local bodies, and the potential loss of clients and reputation**. Faced with this situation, a historically penny-pinching management team may find itself gladly opening its purse to pay top dollar to outside consultants to assist in resolving an embarrassing cyber-crisis[3]. The truth is that these cyber incidents are a real risk for companies—and that includes companies in Japan.

Japan is the world's third largest market for pharmaceutical research and development, spending over USD $12b in 2011[13]. The European Federation of Pharmaceutical Industries and Associations estimates that bringing a new drug to market cost on average USD $1.5m in 2011 and took 12-13 years[14]. On average, only 1 or 2 of every 10,000 chemicals synthesized make it all the way to market[15]. Against this backdrop, the value of stealing a potentially successful drug design, particularly one not protected yet, is huge. IP theft offers the unethical competitor the opportunity to bypass the risk and cost of R&D and take a short cut to marketing a profitable drug[4]. With a global manufacturing base and worldwide market, exploitation of stolen pharmaceutical industry is fairly straightforward—more so than in industries where complex, technologically intensive manufacturing processes reduce the pool of partners in a position to exploit stolen IP[5].

Cyber Attacks

Evidence abounds that pharmaceutical companies are the target of sophisticated Internet criminals[17]. The UK Government identified pharmaceutical companies as the primary target of cyber criminals bent on stealing IP[18]. It estimated cyber-theft of IP cost the UK £9.2b, of which it attributed £1.8b to theft of pharmaceutical, biotechnology, and healthcare IP[19]. Surveys of US Cyber attacks consistently find that pharmaceutical IP is a major target of sophisticated cyber gangs[20]. Experts suggest China is using cyber-espionage to support its 5-year economic development plan. That plan includes expanding China's chemical and pharmaceutical sector[21]. Attacks against major US pharmaceutical companies attributed to sophisticated Chinese hacking groups include medical device-maker, Boston Scientific, Abbott Laboratories, and Wyeth, the drug maker acquired by Pfizer Inc. The same group successfully hacked the Food & Drug Administration's computer center in Maryland, exposing sensitive data (including formulas and trial data) for virtually all drugs sold in the US[22].

"What has been happening over the course of the last five years is that China -- let's call it for what it is -- has been hacking its way into every corporation it can find listed in Dun & Bradstreet."

Richard Clarke, former special adviser on cybersecurity to U.S. President George W. Bush[16]

13. http://www.efpia.eu/uploads/Figures_Key_Data_2013.pdf
14. http://www.efpia.eu/uploads/Figures_Key_Data_2013.pdf
15. http://www.efpia.eu/uploads/Figures_Key_Data_2013.pdf
16. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html
17. http://www.ft.com/cms/s/0/a6b09006-e5c9-11e3-aeef-00144feabdc0.html#axzz3CngrmgdR
18. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
19. Ibid.
20. https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf; http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf
21. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html; see also, http://www2.deloitte.com/content/dam/Deloitte/ch/Documents/life-sciences-health-care/ch_Studie_Pharmaceutical_China_05052014.pdf
22. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html

The US National Institute of Standards & Technology promulgated a voluntary Cyber Security Framework in February 2014.

The framework attempts to holistically describe the various policies and measures that a company should implement to protect against cyber-attacks:

- **Identify**: Identify your crown jewels—key data, systems, assets, and capabilities—and the risks they face
- **Protect**: Implement defensive measures designed to defeat or prevent attacks
- **Detect**: Continuous monitoring to detect successful intrusions and to alert in-house responders in real time
- **Respond**: Counter-measures to contain an attack and mitigate damages.
- **Recover**: Decontaminate and restore damaged assets. Maintain key business operations.

Source: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Worldwide, hacking is clearly a pharmaceutical company problem, but it is not just a "big company" problem[23]. In 2011, Cisco found that the percentage of malware targeting pharmaceutical and chemical companies was 422% of the mean[24] and Symantec found that more than half of malware targets employed under 2500 people and 18% employed less than 250[25]. Meanwhile, Cisco's 2014 Cyber Security survey found that for 90% of its corporate respondents, internal machines were making DNS requests for domains associated with malware—a strong sign of an ongoing internal compromise[26]. Based on its review of known intrusions, FireEye warns that the intruder had accessed the network on average 241 days before being discovered[6]. Warning to management: Nobody is too big and nobody is too small and there is a strong likelihood your firm has already been compromised.

A review of recent media reports reveals a number of disturbing elements to modern-day cyber-attacks. First of all, the lone hacker or hacktivist group, while still present, is no longer the most sophisticated threat. Instead, the criminals attempting to steal corporate IP are predominantly state actors such or organized cyber criminals. In its well-publicized report on China's PLA Unit 61398, Mandiant identified Unit 61398 as the hacking group behind numerous, highly sophisticated attacks against US government and private institutions[7]. The group had developed its own zero-day malware and operated an extraordinarily large infrastructure of exfiltration domains and compromised computer cut-outs to facilitate its global hacking operations[8]. The US Intellectual Property Commission pointed its finger at China as well, blaming China-based—in many cases, state-sponsored—hackers for 70% of the attacks against the United States[27]. However, the US identified France, Iran, Eastern European criminal gangs, and Russian state-sponsored and criminal gangs as the perpetrators of sophisticated attacks as well[28].

23. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf
24. Cisco Systems, "Cisco 4Q11 Global Threat Report," 2012, http://www.cisco.com/web/about/security/intelligence/reports/cisco_global_threat_report_4Q11.pdf
25. Symantec, "2011 Internet Security Threat Report," April 2012, 14, available at http://www.symantec.com/threatreport.
26. Cisco Systems, "Cisco 4Q11 Global Threat Report," 2012, http://www.cisco.com/web/about/security/intelligence/reports/cisco_global_threat_report_4Q11.pdf
27. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf, p.3.

Sophisticated hacker gangs successfully utilize two tools to facilitate penetration. Understanding this is essential to developing a robust cyber security strategy.

First, these gangs develop or buy new, unknown exploits to penetrate their targets[9]. In fact, these tools are so valuable that some hackers trade solely in the sale of new "zero-day" exploits, selling them to governments and criminals[29]. The role of an underground market in hacking tools cannot be underestimated. Cisco reported an 87% drop in the number of exploit kits being propagated across the Internet last year after Russian authorities arrested "Paunch", the author of the infamous Blackhole exploit package[30]. He reportedly earned $50,000 a month selling subscription-based access to his zero-day malware to criminals. His "subscribers" used the service to break into computers for various purposes, including the alleged theft of $822m worth of rubles from unnamed banks[31]. Despite this momentary setback, the criminal world continues to get its hands on new "zero-day" exploits that bypass victim's firewalls and anti-virus protections. **This reality has driven a new consensus within the security world that penetration is inevitable and sufficient resources need to be devoted to detecting and responding to successful intrusions**[32].

The second aspect of successful hostile intrusions is the consistent use of spear-phishing (targeted malware-bearing emails appearing to originate from a legitimate sender) and other means to trick unsuspecting insiders into executing malware or otherwise granting criminals access to the target network[33]. In the as-yet-unsolved Francophone attacks, the crime follows a common script: First, the criminals mail the administrative assistant to a senior executive a link to an online invoice (initially bypassing anti-virus protections) and follow up with a phone call from a fluent French speaker pretending to be an executive from another office. The impersonator instructs the assistant to click on the link and open the downloaded attachment. The assistant clicks thru any warnings and unleashes a zero-day malware that allows the criminals access to the network. Once inside, they collect the necessary information to arrange fraudulent bank transfers. In one case, the Francophone perpetrators even called the company's business contingency team with stolen credentials and convinced them to forward the company's calls to a bogus backup call center. The majority of calls were rerouted back to the victim, but the phone call from the bank to verify the criminals' fraudulent transfer was picked up and the transfer approved by another smooth-talking impersonator[34].

Looking at spear phishing across the world, **Symantec has identified executive assistants, senior managers, and PR representatives as the most popular attack vector for criminals employing spear phishing** [35]. Experts also warn that criminals are increasingly using waterholes to spread network-breaching malware[10]. A waterhole is a normal website run by a reputable entity that is hacked and exploited. The bad guys modify that site, so that visitors unwittingly download malware[11].

"Company insiders, not outside hackers, are involved in more than two-thirds of all cyber cases involving theft of intellectual property. . . . Whether driven by opportunism, greed, a desire for revenge, or a combination of all three, these insiders exploit their positions of trust to obtain access to their organization's most valued digital assets." [39]

28. http://www.voanews.com/content/china-russia-israel-france-iran-cyber-threat/1608419.html
29. https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate
30. http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html
31. http://krebsonsecurity.com/tag/paunch/
32. http://www.newyorker.com/magazine/2013/05/20/network-insecurity; https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf, p.1
33. http://www.darkreading.com/vulnerabilities-and-threats/social-engineering-leads-apt-attack-vectors/d/d-id/1100142?
34. http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack
35. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

"Company insiders, not outside hackers, are involved in more than two-thirds of all cyber cases involving theft of intellectual property. . . . Whether driven by opportunism, greed, a desire for revenge, or a combination of all three, these insiders exploit their positions of trust to obtain access to their organization's most valued digital assets."[39]

For example, the US Veteran of Foreign Wars was compromised in February 2014. Visitors downloaded a javascript exploit that tricked the Internet Explorer 10 browser into loading an executable into memory as data, but then executing it and thereby compromising the visitor's computer[36]. Likely to be visited by active duty service personnel, compromising the Veterans of Foreign Wars website was a brilliant way of secretly distributing a compromise to individuals associated with the military. The attack signature led experts to conclude that the group behind it was the same group allegedly based out of China that launched so-called Operation Deputy Dog[37]. The latter was another Internet Explorer zero-day exploit that was used to target Japanese companies[38]. The coding profile of these malware exploits link the same sophisticated hacking groups targeting US companies and government sites to attacks against organizations within Japan as well.

Insider Theft

Despite the fanfare, attackers penetrating a company's network from the outside are not the biggest threat. **Nobody knows the true size of insider theft, but the consensus is that company insiders, not outside hackers, are the biggest thieves of company IP**. In 2012, Dupont saw a formerly trusted employee plead guilty to stealing the formula for producing titanium dioxide, the white pigment used in paper and plastics[40]. Tze Chao, a former Dupont engineer, admitted to stealing the trade secrets on behalf of the Pangang Group, a state-owned chemical company operating a competing facility in Chongquing[41]. Dupont recently suffered a big setback when a federal appeals court ordered a new trial in its litigation against Korean chemical company, Kolon Industries, who it accused of stealing Kevlar production secrets. Dupont won a $931m verdict, alleging that Kolon and five of its executives hired ex-Dupont engineers as consultants, but the relationship was merely pretext for collecting information on Dupont's secret manufacturing processes from the former Dupont employees[42].

Organizations need to do their part to deter intellectual property theft:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.

Source: Federal Bureau of Investigation, The Insider Threat

36. http://www.FireEye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
37. http://www.FireEye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
38. http://www.FireEye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
39. http://www.krollcybersecurity.com/insider_threat_wp_022213_tht_042_2013_final.pdf
40. http://online.wsj.com/news/articles/SB10001424052970203986604577256003717724564
41. http://abcnews.go.com/blogs/politics/2012/02/chinese-espionage-aleged-to-target-dupont/
42. http://www.courthousenews.com/2014/04/10/66975.htm; http://www.crowell.com/files/US-v-Kolon-Indictment.pdf

The criminal prosecution of Kolan and its executives continues and includes allegations that the defendants stole trade secrets from Osaka-based Teijin K.K.'s US subsidiary as well. Dupont and Teijin not alone. In recent years, the Department of Justice successfully prosecuted insiders from Dow, Motorola, and Ford for stealing trade secrets on behalf of Chinese companies[43]. Cases involving theft on behalf of Chinese entities receive widespread attention, but the problem is much more widespread. Employees routinely move corporate information off the company network, taking it home or saving it on Google Cloud. When someone changes jobs, anecdotal evidence suggests this sort of information often ends up on a competitor's network and, in some cases, in their products[44].

Public Reaction

The use of the term, "data breach", connotes a sense of the bad guys penetrating the good guy's defense, but behind the use of this term lurks an emerging legal paradigm: **Companies owe a duty to their customers and partners to protect their network and third-party data contained within**. Under this developing theory of liability, cyber breach is, in fact, a failure to protect that data. As a result, companies victimized by cyber criminals are increasingly finding themselves the target of a myriad of administrative actions and lawsuits.

When 23-year-old Anonymous member, Kody Kretzinger, and his cohorts hacked Sony's Playbox system and corporate networks in 2011, they stole 100m customer records, but apparently no credit card data[45]. These hacktivists did not use the information to commit identity fraud, but to make a point. They were upset that Sony had sued another .hacker, George Hotz, for distributing a jailbreak hack for the Playbox[46]. After disclosing Anonymous' successful intrusion, Sony saw itself named in 65 or so class action lawsuits. Some were consolidated and one was tossed out, but Sony settled another for $15m and had to pay lawyers to navigate all of this. The UK information Commissioner fined Sony £.250K for the breach as well[47].

Target, which suffered the theft of millions of customers' credit cards earlier this year, now believes the attackers initially penetrated their network using credentials stolen from an air-conditioning and refrigeration contractor[48]. Target faces a Department of Justice Probe, a Senate committee hearing, and inquiries from multiple attorneys generals[49]. It is asking a federal judicial panel to consolidate 100 class action suits brought in 39 district courts[50]. A separate class action brought by banks on the hook for fraudulent charges made on the stolen cards also is moving forward[51].

The U.K. Information Commissioner's Office on Friday became the latest agency to start a probe of eBay Inc. to determine if the e-commerce giant did due diligence in handling its recent data breach. . . . The ICO joins similar investigations launched by the U.S. Federal Trade Commission, the Federal Bureau of Investigation and the states of Connecticut, Florida and Illinois.

International Business Times, May 23, 2014[12]

43. http://www.cnbc.com/id/100481542#.
44. http://www.symantec.com/content/ko/kr/enterprise/collateral/white_papers/WP_WhatsYoursIsMine-HowEmployeesarePuttingYourIntellectualPropertyatRisk_dai211501_cta69167.pdf
45. http://www.wired.com/2011/09/sony-hack-arrest/
46. Ibid.
47. http://www.zdnet.com/sony-settles-psn-hack-lawsuit-for-15-million-7000031961/
48. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
49. http://online.wsj.com/news/articles/SB10001424052702304020704579276901918248632
50. http://www.law360.com/articles/522775/target-presses-panel-to-send-data-breach-cases-to-minn
51. http://www.chicagobusiness.com/article/20140325/BLOGS11/140329865/chicagos-trustwave-sued-over-target-data-breach

As Sony and Target management wrestled with these multiple probes, both encountered insurance coverage issues as well. In the case of Sony, its commercial general liability policy issuer, Zurich American Insurance Co., refused to defend and indemnify it against the above litigation and regulatory actions. Zurich won a declaratory judgment in New York state court that its policy did not cover these claims[52]. Target's senior management faces a more personally troubling predicament: At least two shareholder derivative suits have been filed against Target's board and senior executives, alleging that they failed to take adequate safeguards to protect against cyber thieves and mishandled the post-incident response[53]. This sort of litigation is covered by directors & officers insurance[54]. While there is no indication that Target's D&O insurer will not defend these suits, it might be a good time for other firms to confirm that their D&O insurers will step in and litigate derivative suits alleging cyber security-related missteps[55].

In addition to private lawsuits, companies face an ever-growing variety of cyber security regulations and breach notification provisions. California was a leader in data breach notification with a 2003 rule that requires a firm to notify to all residents whose personal data was compromised and to send a sample of those notifications to the Attorney General for incidents involving compromise of 500 or more residents' data[56]. The state just filed suit against Kaiser Permanente for waiting 4 months to notify the 30,000 individual employees whose social security numbers were on a hard drive inadvertently sold to a third party. Florida passed a more stringent notification requirement this fall that adds in reporting to credit bureaus and an annual maximum fine of $500K. In 2011, the SEC Division of Corporation Finance issued guidance for firms disclosing cyber risk in their SEC filings[58]. This year, the European Union also issued a revised ePrivacy Directive, which stipulates not only that communications providers implement cyber security safeguards, but now requires them to notify subscribers in the event subscriber information is compromised[59]. Notably, it provides a notification exception for encrypted data[60]. The EU Article 29 Working Party has advised that good practice across all industries is to notify of a breach and—in some cases—that should be done within 24-72 hours of its detection[61]. Although this EU rule currently only applies to communications providers, the UK Information Commissioner holds much wider fiat. Sony and eBay's recent hacking incidents are just two recent data breaches that it investigated and neither took place on British soil[62]. In addition to breach reporting guidelines applicable to specific industries (such as the financial sector)[63], a firm operating in Japan that suffers a data breach may find itself the target of foreign regulators if the firm held data associated with citizens of the regulator's home jurisdiction and that data was compromised.

52. http://www.insurancejournal.com/news/east/2014/03/17/323551.htm
53. http://www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach/
54. http://www.businessinsurance.com/article/20140608/NEWS07/306089968
55. http://www.rmmagazine.com/2014/04/02/do-insurance-for-data-breaches/ http://oag.ca.gov/ecrime/databreach/reporting
56. http://oag.ca.gov/ecrime/databreach/reporting
57. http://www.infolawgroup.com/2014/01/articles/breach-notice/california-attorney-general-files-lawsuit-based-on-late-breach-notification/
58. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
59. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
60. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
61. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf, p.2; http://www.infosecurity-magazine.com/news/eu-businesses-prep-for-regulations-requiring-24/
62. http://www.theguardian.com/technology/2014/may/23/uk-data-watchdog-ebay-investigation-cyberattack; http://ico.org.uk/news/latest_news/2013/ico-news-release-2013
63. http://www.bahagram.com/files/WLG_Guide_to_Data_Breach_Notifications-Review_Proof.pdf

What can be done?

The pharmaceutical industry boasts an R&D sector that is one of the world's most important sources of innovation and economic growth[13]. Senior executive teams recognize the need to protect the firm's intellectual property, customer data, and other valuable assets. The real question is what are the most cost-effective security measures and how does the firm strike the right balance between deterring attacks, controlling security costs, and promoting a productive work environment. On one level, that question can only be answered by a careful, exhaustive look at what valuable digitized property is held and how it is being guarded. Experts, however, have identified some issues relevant to all companies reassessing their security posture.

For Cyber Security, we believe the following three areas are worth of review:

1. Identify the assets

A firm must identify its essential, most valuable digitized asset. These are the assets critical to business operations and product development:

- What are these crown jewels?
- Where are they held?
- Who has access to them and the networks that they sit on?
- What digitized assets might be attractive to an outsider seeking to steal data?
- What is a firm obligated to protect from a regulatory perspective?

2. Detect

Once a company identifies its crown jewels, they should be segregated and protected. Detect, however, goes beyond traditional security measures such as firewalls, access authentication, and ant-virus tools. All of these protective measures are not good enough to keep out a dedicated, sophisticated gang employing zero-day exploits and social engineering. Companies must assume that these diehard criminals will get into the network. **Accordingly, companies must allocate security budget towards advanced intrusion detection systems that can reliably detect an ongoing intrusion and alert security even where the malware is a zero-day exploit**.

3. Respond & Recover

Technically, two steps in the NIST Cyber Framework, the reality is these two are intertwined. A response cannot be smoothly executed without pre-planning and recovery cannot start until the response has scoped out the damage done. Companies dealing with a serious data breach who have not planned for the occasion are at a serious disadvantage in determining what happened and what was compromised. This, in turn, complicates the task of identifying what business processes are at risk and what needs to be disclosed to the public or regulators. Serious data breaches frequently lead corporate management to hire outside consultants to manage the clean-up effort. We recommend firms recognize this need and prepare for it by pre-selecting a vendor to assist in incident response and recovery. **Working with a cyber-incident vendor to put in place sound logging practices and other measures will facilitate both forensic analysis and mitigation. This will position the firm to ascertain as quickly as possible what happened and to the extent possible, limit the harm done**.

The realization that a company cannot keep all the bad guys out of the network has triggered a paradigm shift in cyber security from prevention to detection.

It is also worth making sure that the legal department understands the regulatory bodies that might get involved and putting in place security practices compliant with applicable standards and regulations. This will assist the firm in dealing with the inevitable regulatory inquiries as well. Particular attention needs to be paid to data breach notification. A plan for executing this must be in place prior to an event if a firm hopes to provide swift notification. **The ability to notify is closely tied to the ability to forensically understand the scope of the attack, so the existence of a well-thought out post-incident response plan will prepare management to swiftly identify who needs to be identified and what needs to be disclosed**.

For insiders, there are a number of issues that seem to reoccur across firms and industries:

1. Lack of training & education

Intellectual property theft is not thwarted just by having people sign non-disclosure agreements that they do not read. Staff needs to be reminded that corporate secrets and other sensitive information cannot be taken off the premises. **It is important to remind employees that saving company data to USBs and the cloud are out of bounds. Employee education is also critical to reducing the spear phishing threat**. It is important that staff know not to click on odd links, downloads executables or even files from unknown sources onto corporate networks. A company should provide an approachable point of contact to alert if something unusual happens.

2. Define who has access & enforce it

Many companies have lax internal controls. This is what enabled Snowden to steal so much. A company should limit who has access to not just key data, but to the physical hardware and, sometimes, even the network that it resides on. Encrypt things to keep out prying eyes. **Access controls need to be enforced and enforced against senior executives and IT staff as well**.

3. HR Practices designed to reduce IP theft

Certain classes of employees represent a higher percentage threat of IP theft. Specifically, disgruntled employees and exiting employees are deemed more likely to copy sensitive corporate documents and take them home or turn them over to third parties. Often, a post-mortem inquiry into a theft will reveal that the employee had multiple performance issues or security incidents prior to the discovery of a major theft, but these issues and events were not noticed or shrugged off. Exiting employees will often start copying large amounts of data in the weeks surrounding official notice. **Logging and other access controls should be in place to monitor exiting employees and other higher-risk employees to enable a firm to look at historical as well as ongoing data transfer behavior of a particular individual**. Of course, these steps need to be undertaken with an eye to relevant labor and privacy laws and should be discussed with legal counsel.

Conclusion

a pharmaceutical company's intellectual property may, in the aggregate, approximate—If not exceed—the value of its tangible assets. For such a firm, in the long run, a smart security posture may pay for itself many times over.

Contacts

Mitsuhiko Maruyama
Partner
Cyber Risk Services Unit Leader
Deloitte Tohmatsu Risk Services Co., Ltd.
+81 90 6492 3648
mitsuhiko.maruyama@tohmatsu.co.jp

Jun Matsuo
Partner
Life Science & Health Care Unit Leader
Deloitte Tohmatsu Consulting Co., Ltd.
+81 80 2003 8644
jmatsuo@tohmatsu.co.jp

Ash Mahmood
SFE, EnCE
Senior Vice President
Forensic & Dispute Services
Deloitte Tohmatsu Financial Advisory Co., Ltd.
+81 80 4182 6048
ash.mahmood@tohmatsu.co.jp

Christian Boettcher
Director
Life Sciences & Health Care
Deloitte Tohmatsu Consulting Co., Ltd.
+81 80 9097 7376
chrboettcher@tohmatsu.co.jp

William “Bud” Roth
Senior Manager
Cyber & National Security
Public Sector
Deloitte Tohmatsu Consulting Co., Ltd.
+81 80 4651 5850
wroth@tohmatsu.co.jp