20

Cyber Threats in the Health-Care Industry

Bertrand Monnet and Philippe Very

In addition to its numerous positive impacts, the development of information technologies in health care exposes the sector to a variety of major risks emanating from hackers, organized criminals, and terrorist organizations. In addition, the proliferation of connected devices raises specific issues and new possibilities for breaching the security of the IT systems belonging to the sector's various stakeholders. In this chapter, we examine these threats, analyze the objectives of cybercriminals, and present recommendations for preventing and dealing with cybercrime. We consider the industry at large, including providers of medical services, pharmaceutical firms, and their customers.

B. Monnet (✉)
Criminal Risk Management Chair, EDHEC Business School, Roubaix, France
e-mail: Bertrand.MONNET@edhec.edu

P. Very
Department of Strategy, EDHEC Business School, RoubaixNice, France
e-mail: Philippe.VERY@edhec.edu

L. Menvielle et al. (eds.), *The Digitization of Healthcare*,
DOI 10.1057/978-1-349-95173-4_20

20.1 Cybercriminal Techniques

There are many definitions of cybercrime. We use the United Nations' (UN) definition, according to which: "cybercrime is defined as a broad range of illegal activities committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" (United Nations 2015). While the UN definition refers to a computer system or network, current technological progress requires the definition to be extended to encompass any connected object. In the "internet of things," any object—mobile phone, household appliance, medical device—can be assigned an IP address and thus communicate using technology such as Bluetooth, radio frequency identification (RFID), or near field communication (NFC). In the health-care industry, for example, information about patients' health can flow though computers and mobile phones between doctors, patients, and hospitals; connected devices are also facilitating autonomous treatment at home. Any connected device can provide a gateway for entering a private network or developing an illicit activity focused on a target. The more connected devices, the higher the risk of security breaches.

Consequently, the health-care industry with its numerous participants and network entry-points can be particularly vulnerable. Criminal elements use diverse techniques to target organizations in the industry. Cyber security providers and auditing firms regularly publish cybercrime reports (see for instance KPMG 2015). Our focus will be on the main attacks perpetrated by elements external to the industry.

20.1.1 Intrusion

As described to the authors by an experienced hacker,[1] many companies' information systems (IS) can be penetrated using two main tactics: social engineering and by exploiting the technical weaknesses of their operating

[1] Interview—Paris—May 2016.

systems—particularly in the case of Windows for computers or Android for mobile phones. The first component of social engineering involves sending emails that contain malware embedded in attached documents or links to numerous employees of the targeted company (phishing) or by sending these malicious emails to employees who are specifically targeted for their level of access to the company's strategic data (spear phishing). Once the malware has been downloaded onto the employee's computer and if designed for this purpose, it can explore the parts of the IS to which the infected computer has access, and then gain access to critical data. The second component of social engineering involves scanning employees' passwords to use their access rights to penetrate the company's IS; this second technique being facilitated by a poor level of password security. Security breaches underpinned by social engineering techniques are based on human failures. The proliferation of electronic devices connected to the IS (tablets, watches, glasses, cars, etc.) makes this first technique more dangerous, especially as the employees equipped with these devices tend to be top executives.

The second way to penetrate the IS of a targeted organization is to exploit its structural weaknesses. No IS is perfect, and skilled hackers have been scanning all of them for years, to identify the weaknesses of their code-based design. They find breaches that enable them to enter a targeted IS. Once these structural security breaches—or backdoors—are identified, hackers can use them to travel inside their target without breaking the door but merely by opening it with the key they have found. They can open the door as often as they like.

20.1.2 Saturation

The second type of cyber-attack to be considered for the health-care sector involves saturating the Web interfaces of targeted organizations. Such attacks can severely disrupt operations if Internet is strategically important for the organization concerned, or if its website servers are connected to other servers that support critical data. This Denied Disposal of Services (DDOS) technique is based on simultaneously connecting thousands or millions of computers (that the criminal

controls remotely) to the targeted organization's website. If the website's servers are not designed to support this many simultaneous connections, they quickly "crash" under the number of requests they try to address.

Intrusion and saturation are the main techniques employed by cybercriminals. They can be used for various purposes or types of crime. It is therefore worth understanding the objectives behind such criminal activities.

20.2 Objectives of Cybercriminals

The objectives of the various types of cybercriminals using the above techniques to gain access to an organization's IS can be classified into three main categories, according to the Monnet and Very typology (2010): destruction, predation, and competition. Some acts target specific organizations within the health-care industry.

20.2.1 Destruction

The first data to be considered here are pharmaceutical company data. The destruction of critical data, such as results of research protocols carried out on strategic future drugs and products, can severely threaten the performance and sustainability of these companies. Once cybercriminals have penetrated the IS, they can try to destroy critical data contained in accessible servers. The first potential perpetrators of this first type of data destruction are legal stakeholders and primarily competitors that may resort to these cyber techniques on isolated bases for economic reasons. Putting ethical behavior aside, it can clearly be in a pharmaceutical company's interests to destroy the added value and even the future products of a competitor by cyber-destroying its critical data. As already observed in cases of espionage—but not as yet in cases of data destruction—the attacking company does not carry out the attack itself, but tends to solicit aid from two different sources. The first source is usually a firm of specialized business and forensic intelligence consultants, which in addition to its legitimate services of data

protection, can organize efficient cyber-attacks through its own internal resources or hired hackers. The second source may be the intelligence services of the attacking company's host country. There may be economic and/or political advantages for a government—American, Chinese, Russian, French, or other—in destabilizing key stakeholders in the economies of competing states, regardless of any existing diplomatic and military alliances. This form of data destruction through cyber-attack has already been observed in the nuclear and mining industry and raises an additional threat of economic warfare in which the pharmaceutical industry could prove to be a collateral victim.

In addition to data destruction, cybercrime can entail more dramatic consequences for the health-care sector, since the digitalization of this industry could potentially lead to cyber-attackers killing patients. Three possibilities are to be considered here. The first involves accessing the IS of hospitals or clinics that have digitalized the management of pharmaceutical treatments, and then modifying the data related to types or doses of drugs to be administered to targeted patients to kill them. The second one, which is rather similar, functions by taking control of patients' medical devices—insulin pumps for example—again to kill them. The third option consists of developing larger-scale intrusions, without any specific targeting of patients, to commit a new form of terrorist attack on a large number of vulnerable victims without the terrorist having to resort to any guns or explosives.

20.2.2 Predation

The digitalization of the health-care sector has greatly increased—and in some cases created—vulnerability for its stakeholders in the face of several types of criminal predation and particularly theft, which is the simplest type. Cybercriminals can access huge volumes of sometimes highly valuable data through the techniques presented above. There are two main categories of data to be considered here. The first concerns scientific and commercial data belonging to pharmaceutical companies and which can not only be destroyed but also stolen by non-ethical competitors aided by private and public sources as described above.

These acts can be qualified as espionage. The second category concerns the medical data of millions of patients, stored in servers belonging to hospitals, clinics, and public administrations. These data can be of high commercial value for companies seeking to address demands related to these patients' diseases. Community Health Systems, based in Franklin, Tennessee and an operator of 206 hospitals in 29 US states, fell victim to this kind of theft in 2014, when it had 4.5 million data items concerning American patients (details of first names, social security numbers, addresses, phone numbers, birthdates, etc.) stolen from it. Investigations proved that the theft was committed by Chinese hackers. Note also that this kind of information theft may also be valuable to non-ethical insurance companies looking to illicitly select their customers according to their health.

The second type of criminal predation liable to be augmented by health-care sector digitalization is extortion. Extortion involves the predator forcing its victim to give it money under the pressure of major threats. Hospitals, pharmaceutical companies, and other private stakeholders in the sector are already exposed to forms of physical extortion and forced to pay out millions of dollars in numerous regions controlled by criminal organizations like the Italian mafia, the Japanese Yakuza, or the Chinese Triads. However, the concept of digital extortion also needs to be considered, especially for the health-care industry. After entering a pharmaceutical company's IS, a criminal organization can copy critical data on key research programs, and threaten to release the details on the Web if the company does not pay a ransom. But the most common form of digital extortion is based on ransom wares, or in other words malwares infecting corporations' strategic servers and encrypting large volume of data. Once the data has been made inaccessible, the criminal organization demands a ransom in exchange for releasing a decryption code to the victim. This form of extortion successfully targeted the Hollywood Medical Presbyterian Center, a Los Angeles hospital, in February 2016. Ransom ware was used to encrypt data stored in the hospital's servers, thus blocking its administrative services for a week until the hospital agreed to pay a US$17,000 ransom (in bitcoin form).

In the same vein, saturation or intrusion has the potential to hinder the emergence of virtual surgery, a technology that allows specialist

surgeons to control robots located on a remote site location and thus perform surgery on patients anywhere in the world. The potential exists for cybercriminals to interrupt such operations and demand ransom money.

20.2.3 Competition

Digitalization will also increase the health-care sector's vulnerability to the already-major threat of counterfeiting. Although precise estimates are clearly impossible to make, the World Health Organization considers that about 10% of the drugs sold worldwide each year are fake. This criminal economy generated an estimated US$200 billion in revenues in 2014 or the equivalent of 10–15% of the pharmaceutical industry's overall revenues (SANOFI 2015). Drug counterfeiting is extremely profitable: each US$1,000 invested in it generates US$500,000 for the criminal organizations involved. Internet plays a key role in the growth of this form of criminal competition for pharmaceutical companies. Although 60% of fake drugs are sold in emerging countries, mostly on street markets, 40% are sold in developed countries, where it is difficult for the criminal organizations to insert them into the pharmaceutical sector's legal channels. Most of the fake drugs are therefore sold on these markets through online drugstores. The growth of online drug sales is clearly dangerous for the industry: 96% of online pharmacies sell illicit drugs, either always or at times. In addition to the economic prejudice it causes, this form of criminal competition, which is accelerated by digitalization, has dramatic human consequences: in 2013, a total of 122,350 malaria patients died after taking fake drugs for the disease (SANOFI 2015).

20.2.4 Cybersecurity: Some Recommendations

Despite this dark picture of health-care industry digitalization, solutions exist to mitigate the impacts of cybercrime on the industry. Firstly, all the sector's stakeholders need to enhance and permanently update the technical protection afforded to their IS by hiring specialized IT security

providers. Most of the sector's stakeholders have already moved to act on this first solution. However, it does not afford them enough protection on its own, as cybercriminals usually become capable of overriding most of these security measures.

As one weak entry point is sufficient to allow intrusion to a network, all inter-connected participants in the industry must upgrade their protection via a race to the top, so that all partners enjoy the same high level of protection. Security is not an issue for isolated participants, but for networks as a whole. An important first step for the whole of the industry is to mitigate the risks of backdoors being created in their IS. They therefore need to define and use "a less common IS" that is capable of ensuring the necessary degree of efficiency within the network.

However, the most important security measure is not technological, but strictly managerial. It relies on the sector's ability to disseminate a security culture among all of its stakeholders. Since social engineering is the most common tactic used by cybercriminals, all of the industry's employees must be informed and trained, so as to diminish the ability of hackers to enter their organization through the organization's own employees. A number of simple and fairly cheap-to-implement actions are probably the most efficient means to fight cybercrime. These may range from rules for creating and changing passwords, to guidelines for the use of social networks at work and lists of websites to avoid.

20.3 Conclusion

The exciting technological progress embraced by the health-care industry raises new security issues. The industry is particularly exposed to cyber threats thanks to its complexity and the number of organizations and individuals participating in it. In addition, the medical industry's efficiency now relies on the multiple connections that interlink the industry's participants, devices, and systems. And this vulnerability is set to remain high because, like for doping, security solutions are not invented until after a new threat is identified. In other words, hackers and other cybercriminals will always stay one step ahead of the game,

thus meaning that 100% security is illusory. " . . . As we know, there are known knowns. There are things we know we know. We also know there are known unknowns. That is to say, we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know" (Rumsfeld 2002).

References

Donald, Rumsfeld, US Secretary of Defense. 2002. Speech "*known unknown,*" February 12.

KPMG. 2015. *Health Care And Cyber Security: Increasing Threats Require Increased Capabilities*. http://www.kpmg-institutes.com/institutes/healthcare-life-sciences-institute/articles/2015/08/health-care-and-cyber-security.html

Monnet, Bertrand, and Philippe Very. 2010. *Les Nouveaux Pirates de l'Entreprise: Mafias et Terrorisme*. Paris: CNRS Editions.

SANOFI. 2015. *Report Lutte contre la contrefaçon des médicaments*. November.

United Nations. 2015. http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf