Communications of the Association for Information Systems

Volume 46 Article 14

3-2020

Cyberespionage Goes Mobile: FastTrans Company Attacked

Janice C. Sipior
Villanova University, Janice.Sipior@villanova.edu

Danielle R. Lombardi
Villanova University

Cathy A. Rusinko
Thomas Jefferson University

Steven Dannemiller
University of Alabama

Recommended Citation
Sipior, J. C., Lombardi, D. R., Rusinko, C. A., & Dannemiller, S. (2020). Cyberespionage Goes Mobile: FastTrans Company Attacked. Communications of the Association for Information Systems, 46, pp-pp. https://doi.org/10.17705/1CAIS.04614

Communications of the Association for Information Systems

Teaching Case DOI: 10.17705/1CAIS.04614 ISSN: 1529-3181

Cyberespionage Goes Mobile: FastTrans Company Attacked

Janice C. Sipior
Department of Accountancy & Information Systems,
Villanova University
janice.sipior@villanova.edu

Danielle R. Lombardi
Department of Accountancy & Information Systems
Villanova University

Cathy A. Rusinko
School of Business
Thomas Jefferson University

Steven Dannemiller
Culverhouse College of Business
University of Alabama

Abstract:

The use of mobile devices, such as smartphones and tablets, in the workplace continues to increase. However, these devices' capabilities make them a prime target for espionage activities. Thus, employees need to understand mobile espionage and how to protect against it. In this paper, we present a teaching case based on two fictitious self-driving car competitors that educators across the world can use in information systems or business courses at the undergraduate or graduate levels. The case introduces students to FastTransportation Company ("FastTrans"), a fictitious American multinational car manufacturing company, who suspects its rival, Wheelz Corporation, a leading ride-hailing company, of engaging in corporate mobile espionage to steal and use trade secrets from its self-driving car division.

Keywords: Mobile Espionage, Security Breach, Teaching Case.

This manuscript underwent peer review. It was received 02/28/2019 and was with the authors for 1 month for 2 revisions. The Associate Editor chose to remain anonymous.

1 Introduction

FastTransportation Company ("FastTrans"), an American multinational car manufacturing company, suspects its rival, Wheelz Corporation, a leading ride-hailing company, of stealing and using trade secrets from its self-driving car division[1]. FastTrans, whose self-driving car Figure 1 shows, believes Wheelz used a FastTrans employee's smartphone to engage in mobile espionage.

Figure 1. FastTrans Self-driving Car (メルビル, 2016)

2 The Situation

While reading an online news site, Paige Presidio, Chief Engineer for the Autonomous Vehicles Division at FastTrans, came across an article about Wheelz' new concept car, "Cruiser". In the article, the author describes the Cruiser as easily navigating San Francisco's 49 mile scenic drive. Marked with blue and white "49 mile scenic drive" signs, as Figure 2 depicts, the route includes downtown San Francisco, the Great Highway alongside the Pacific Ocean, and even the beautiful but crooked flower-lined Lombard Avenue, which Figure 3 shows. The article describes the Cruiser as handling the crooked street nimbly by relying on on-board light detection and ranging technology.

Figure 2. 49 Mile Scenic Drive Sign (Mcmillin24, 2013)

Presidio was aghast. The autonomous vehicles project at FastTrans developed and patented FastTrans' light detection and ranging (FLIDAR) technology. FLIDAR detects the shape of objects around a car by using near-infrared light. Weather, shadows, or direct sunlight do not interfere with FLIDAR's capability to image a three-dimensional map of its surroundings. FLIDAR constitutes the core technology underlying self-driving navigation, and the company expects it to be the factor that makes autonomous vehicles 100 percent safe.

Presidio sought out her Principal Engineer, Francisco Ferrari. She described Wheelz' Cruiser concept car to him. Reflecting on Wheelz' self-driving car project, Presidio said:

> *Wheelz began two short years ago. How could Wheelz possibly have developed a complex light detection and ranging technology, suspiciously similar to FastTrans' FLIDAR? The development timeframe seems impossible*.

After reflecting, she pronounced: "It *is* impossible! Perhaps Wheelz was somehow able to obtain FastTrans' FLIDAR software. But how?" .

[1] FastTrans and Wheelz are fictitious companies.

Figure 3. Lombard Avenue (Sullivan, 2006)

Ferrari remembered:

> *Think back to the time when Wheelz was founded. That's when Aston Martin joined our autonomous vehicles team as a new technical lead engineer. At work, he* always *carries his own personal smartphone with him, and sometimes forgets his corporate issued smartphone.*

Thinking further about Martin, they guessed him to be about the same age as Wheelz's founders. Curious, they looked him up on Facebook and discovered he attended the same university as Wheelz's two founders. Scrolling through his Timeline Album, Ferrari exclaimed: "Look there's a photo of Martin with the two founders" (see Figure 4). The possibility of cyber espionage crossed their minds as Ferrari recalled that the United States (US) Department of Homeland Security detected evidence of cell-site simulators in Washington, DC (Bajak, 2018). Also known as stingrays or international mobile subscriber identity (IMSI) catchers, these simulators act as fake cell phone towers. One can capture phone calls, messages, and location from devices tricked into connecting with them. Presidio reasoned:

> *The US Pentagon bans the use of mobile devices in secure areas on their premises (Deputy Secretary of Defense, 2018) for good reason. And, US Department of Defense personnel are prohibited from using geolocation functions while in designated operational areas (Garamone, 2018). Concerns about fitness trackers, smartphones, tablets, smartwatches and other electronic devices arose from the realization that an interactive online map was pinpointing US troop locations, bases, and other sensitive areas around the world. Governments and intelligence services around the world have long been known to be spying on other countries. The US government has been a target of espionage, but why FastTrans?*

Figure 4. Photo of Martin with the Two Founders

3 High Stakes

As an innovative technology, autonomous vehicles will alter transportation and, in turn, impact car manufacturers and drivers (Sappin, 2018). For automakers, McKinsey & Company has predicted that up to 50 percent of passenger vehicles sold globally in 2030 will be highly autonomous and up to 15 percent fully autonomous (Gao, Kaas, Mohr, & Wee, 2016). Despite a shift towards car-sharing services, sources have projected global vehicle unit sales to continue to grow but the annual growth to decrease about two percent annually (Gao et al., 2016). Whether automakers survive depends on whether they can shift from traditional cars to self-driving cars to respond to this change in consumer demand (Sappin, 2018). For ride-sharing companies, self-driving cars could cut their biggest expense: paying human drivers (Bensinger & Dawson, 2018).

Goldman Sachs Group has predicted that driverless taxicabs will drive the revenue of global ride-hailing and ride-sharing businesses to increase from US$5 billion in 2018 to US$285 billion by 2030 (Welch & Behrmann, 2018). In addition to this growth, operating profit margins could reach 20 percent, more than twice carmakers' current margin. Companies could potentially make even more revenue by offering delivery services, which predicted revenue increases do not consider.

FastTrans has a strong position in the driverless business. Recognizing projected sales trends and future consumer demand, the company has focused on reshaping its business model to include ride-hailing, ride-sharing, and delivery in major markets. The first company to establish a full fleet of autonomous vehicles will benefit from first mover advantage. It matters who gets there first as that company can establish strong brand recognition and customer loyalty before competitors enter the market. Thus, the factors driving a competitor to corporate espionage include predicted growth in industry profitability, high margins, the potential for additional revenue from providing a delivery service, and FastTrans' lead in developing autonomous vehicles.

4 Background on FastTrans

Founded in 1948, FastTrans has its headquarters in Detroit, Michigan (see Figure 5), and has assembly plants worldwide. It produced its first passenger car, the Swift, in 1950. FastTrans quickly grew to offer a range of compact, midsize, luxury, and sports cars. Car industry rankings have consistently placed FastTrans as the ninth largest automobile manufacturer in the world behind Toyota, Volkswagen Group, Hyundai Motor Group, General Motors, Ford, Nissan, Fiat Chrysler Automobiles, and Honda Motor Company.

Figure 5. FastTrans Headquarters (Villanova University Staff Photographer, 2018)

Since the mid-1960s, FastTrans has invested in artificial intelligence and robotics to conduct experiments on automating cars. Its cars include semi-autonomous features, such as forward-collision warning, lane-departure warning, lane-keeping assist, and side collision protection, as standard. Its luxury and sports cars have automatic braking. FastTrans was the first automobile manufacturer in the world to demonstrate a fully autonomous self-driving car on public streets in 2010. One year earlier, Waymo, the self-driving division of Google's parent, Alphabet, a multinational conglomerate and not an automobile manufacturer, accomplished a similar result. Dubbed the "AutoDrive", the car still comes with a steering wheel and brake pedal for safety reasons. The car has driven over two million miles in autonomous mode. Looking to introduce the first line of driverless cars, FastTrans invested 5.75 percent (US$7.475 billion) of its revenues (US$130 billion) in research and development in the past year and has a team of 15 engineers working on its self-driving car project.

Competitors have begun to chase FastTrans in the race to start the world's first driverless business. Pierce Arrow, Head of Buffalo Consulting Company's automotive practice, said:

> *FastTrans has taken the lead among companies now manufacturing autonomous vehicles. The company has developed superior technology. They understand that their business is not focused on manufacturing cars, but on getting people from one place to another.*

5 Background on FastTrans' Competitor Wheelz

Founded in 2016, Wheelz is an on-demand ground transportation company with headquarters in San Francisco, California. Wheelz offers both passenger ground transportation and package delivery services. The Wheelz app serves as an on-demand platform to connect online demand for transportation with offline drivers with cars. Passengers and drivers set up an account with a profile, which maintains their information such as their name, phone number, photos, personal interests and hobbies, car model and license plate, passenger payment method, previous ratings to establish the reputations of both drivers and passengers, and so on. Using the free Wheelz app that both passengers and drivers download to their iOS or Android mobile device, passengers request a ride from a nearby Wheelz driver. Once the driver confirms the ride, the app displays appropriate information to the passenger and to the driver. When the driver successfully completes the drive, the passenger pays the driver's account, rates the service, and may optionally add a tip. The driver also rates the passenger.

Wheelz has worked hard to establish trust in its services and a positive company image. The company encourages drivers to introduce themselves and converse with their passengers. Drivers and passengers must rate each other on a scale of one to five stars to complete the transaction. Neither will be able to enter into another transaction unless they complete the rating. As such, many know Wheelz for promoting social interaction, helping friendships form, creating trust, and providing reliable transportation. The company uses the motto "We are friendly transportation when you need a transportation friend" in its advertising campaigns to promote its trustworthy service and positive company image. Despite its advertising efforts, Wheelz remains in third place among ride-hailing companies.

6 Back at FastTrans the Response Begins

Presidio called Edsel Ford, Chief Information Security Officer (CISO) at FastTrans, to request an internal investigation to determine whether Martin or other FastTrans employees knowingly or unknowingly communicated FLIDAR trade secrets to Wheelz. In sweeping the offices for the autonomous vehicles project at FastTrans, a forensic team discovered smartphone monitoring software on Martin's personal device. The team found that it could eavesdrop on sensitive conversations captured through the microphone, provide visual information about the physical environment through the camera, access corporate systems, track the phone's location, and store data. Although Martin had a corporate smartphone, he continued to carry his own. The team had not yet ascertained whether Martin had fallen victim to device hacking to surreptitiously install spyware or whether Wheelz had planted him as a corporate spy on the project team to steal vital research and development information. Wheelz has denied any wrongdoing. FastTrans has contemplated taking legal action against Wheelz for stealing its trade secrets.

Presidio wanted to understand the situation better. She wondered: "What is corporate espionage? What is spyware? How does spying occur on a smartphone? Where does spyware come from?". She called Reed Roads, Digital Forensics Specialist at FastTrans, who responded to her questions.

7 Documenting the Situation

After their telephone conversation, Roads prepared written documentation as a follow-up to further elaborate on each of Presidio's questions. They decided to prepare this documentation as a necessary step for legal action that FastTrans contemplated, particularly since Roads would likely be called on for expert testimony. We present the detailed documentation that Roads prepared and provided to Presidio in the following subsections.

7.1 What is Corporate Espionage?

Corporate espionage, also known as economic espionage, industrial espionage, or corporate spying, refers to gaining information about competitors using espionage techniques. Obtaining information about competitors may be legal if one uses legal means (even surreptitiously). For example, a company may hire a private detective to attend a trade show in order to overhear proprietary information. Uber's Strategic Services Group (SSG), dedicated to collecting competitive intelligence, reportedly did just that. In January, 2017, SSG members attended the Consumer Electronics Show (CES) in Las Vegas, Nevada, to attend technical presentations in order to obtain information from other companies that would help Uber's Advanced Technology Group develop its own autonomous vehicles (Harris, 2018). In addition, Uber SSG members followed the experimental self-driving vehicles of Alphabet's self-driving car division Waymo for about four days and videotaped them driving on public streets in Phoenix, Arizona. SSG also examined GitHub, a website where software developers post various open source software, in the hope that engineers from Waymo had inadvertently posted some of their secret source code. Additionally, SSG tracked social media accounts (e.g., LinkedIn, Facebook, or Twitter) of key Waymo employees to identify their personal and professional networks to determine which automakers, outsourcers, and suppliers Waymo worked with.

One generally cannot legally acquire trade secrets without the owner's consent. For example, Waymo filed a lawsuit against Uber in which it accused an Uber employee of taking 9,700 megabytes of proprietary technical self-driving car data with him when he left his employment with Google (Harris, 2018). He reportedly used this data to start self-driving truck startup Otto, which Uber acquired, and then brought it to Uber. In the US where both FastTrans and Wheelz have their headquarters, the Economic Espionage Act of 1996 governs corporate espionage involving commercial information. According to this act, "the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information" (Legal Information Institute, 1996). Federal criminal penalties for stealing or misappropriating a trade secret include years of imprisonment and fines up to several million U.S. dollars.

Sources expect espionage activities to primarily target mobile devices in the future (Badenhorst, 2017) and corporate mobile espionage to become more prevalent (Kaspersky, 2018). Indeed, mobile malware continues to rise. Nearly 11 percent of mobile phone customers worldwide reported infections in the fourth quarter of 2017, an increase from about 7.5 percent during the same quarter of 2015 (McMillan, 2018). As Figure 6 shows, over two thirds of respondents to a survey reported that an employee's mobile access to confidential corporate data had certainly or likely resulted in a data breach.

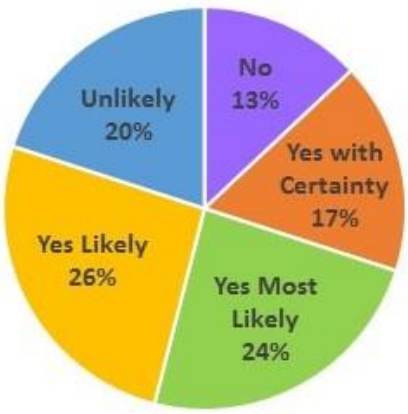

Figure 6. Percentage of Companies Likely to Have had a Mobile Data Breach based on a Survey of 588 IT Managers and IT Security Professionals (Ponemon Institute, 2016)

The prevalence of information technology (IT) has expanded the variety of covert surveillance and tracking tools that one can use to access corporate systems, intercept or eavesdrop on communications, and track employees or other resources. Spyware represents one of the oldest and most widespread tools that perpetrators use. The first lawsuit against spyware occurred in the US in 2004 (Federal Trade Commission v. Seismic Entertainment Productions, Inc., Smartbot.Net, Inc., and Sanford Wallace, 2004).

7.2 What is Spyware?

The U.S. Federal Trade Commission (FTC) has acknowledged that spyware lacks an easy definition because one can use its capabilities for both beneficial and negative purposes (Federal Trade Commission, 2004). People generally regard spyware as a type of malicious software (malware). Malware is a generic term that applies to several types of malicious software that allow one to use a device without the owner's consent. Once installed, an attacker can use malware to control the infected device remotely. For example, the attacker may execute commands to disrupt the device's functionality, send emails or initiate phone calls, change settings, install apps, and gather the victim's personal data. The type of malware known as spyware monitors or gathers information from computers or mobile devices, such as smartphones and tablets, and may assert control over those devices without the user's knowledge or consent (Sipior & Ward, 2008). Adware is a type of spyware that mainly advertisers use to gather user information to deliver customized advertisements and offerings to individual users as they browse the Web. Spyware is usually installed undetected and runs in stealth mode, which makes it difficult to discover or uninstall.

7.3 How Does Spying Occur on a Smartphone?

Given that organizations widely use mobile devices and given the features such devices include, they have become a prime target for corporate espionage. Figure 7 conceptually represents spyware on a smartphone. Data exfiltration through mobile applications poses a primary security threat to organizations (Pradeo Lab, 2018). Mobile devices infected with spyware provide subversives with a powerful espionage tool with which to monitor a user's contacts, communications, travel history, data, and even trade secrets and other intellectual property. Mike Murray, from mobile security firm Lookout, has observed: "It is one thing to compromise someone's computer. It's another thing to have a listening device that they carry around with them 24 hours a day" (McMillan, 2018).

One can remotely control smartphones' features and sensors to secretly capture a wealth of day-to-day real-time data. Attackers most frequently take location data, contact lists, users' profile, users' files, and short message service (SMS) data. Spyware can send the stolen data via data transfer to a remote server or through email. Attackers may then aggregate this data to provide comprehensive information about a person and create deep insights from monitoring and tracking behind company walls. Table 1 summarizes these features and the types of data that one could collect. We discuss each smartphone feature below.

Figure 7. Conceptual Representation of Spyware on a Smartphone (Svay, 2017; Font Awesome, 2018)

Table 1. Smartphone Features and Data Collection

Smartphone feature	Data collected
Microphone	Sounds and oral communications
Touch screen	Touch screen data logs of user interactivity
Camera	Photos and video, which includes exchangeable image file (EXIF) information and potentially geotags
Global positioning system (GPS) and wireless systems	Location information, information passed between two smartphones, or a purchase transaction
Storage	Files, emails, text chats with images, SMS, and others, stored locally and in the cloud

7.3.1 Microphone

A smartphone microphone captures surround sounds and oral communications that occurs face to face, over the phone, through voice interactions with smart speakers and digital assistants, via voice chat, over video conferencing, and through other media. This information is usually timelier, richer, and more sensitive in content than that in documents because one can access it before users commit it to written form.

7.3.2 Touch Screen

A touchscreen logger can capture user interactivity with a smartphone and devices attached to it such as label makers or photo printers. A touchscreen logger can collect information such as passwords and other inputs such as Web form data; which applications (apps), files, folders, and windows that the user has opened; Internet-based activities such as search history, websites visited, or File Transfer Protocol (FTP) downloads; browsing history and bookmarks; emails; messaging apps; chatrooms; and system credentials.

A smartphone's screen is susceptible to visual hackers who may steal the information it displays. Onlookers in public areas may be able to read the screen. Employees need to remain aware of individuals around them while accessing proprietary information where others may be able to view it.

7.3.3 Camera

Cameras capture photos and videos, which spyware can capture and store. Photo and video files include EXIF information, such as date and time the user took the photo, camera used, focal length, and orientation. If a user enables geotagging via GPS, the device embeds the exact location of the photo or video into the file's EXIF data.

7.3.4 GPS and Wireless Systems

A GPS chip and wireless positioning systems can determine the location of a mobile device (i.e., geolocation). The GPS chip uses satellite data to calculate a device's specific location at any time. In some instances, one can augment or assist a weak or unavailable GPS signal using local WiFi networks. One may also identify a device's geolocation through its Internet Protocol (IP) address, media access control (MAC) address, radio frequency (RF) systems, EXIF data, and other wireless positioning systems. One can compile a record of all a device's locations and movements over time. The places a smartphone user frequents can reveal places of work and whom a user meets. News website Quartz recently revealed the persistence of location tracking. Even when users turn location services off, Android software gathers location data and sends it back in encrypted form to Google, which confirmed this revelation (Collins, 2018). If hackers compromised the smartphone with spyware or otherwise hacked it, they could possibly send the encrypted data to a third party who could associate it with each phone through the device's unique ID number.

Bluetooth, near-field communication (NFC), and radio frequency identification (RFID) are types of short-distance, contactless, wireless communication that one can use to send information or make payments. Intercepting a data transmission may reveal the information passed between two smartphones or a purchase transaction sent between a smartphone and an RFID chip-based credit card reader.

7.3.5 Storage

Smartphone storage includes internal storage, external storage, and cloud storage. Users may use internal storage on their smartphone for apps, music, videos, images (such as photos, screenshots, emojis, and stickers), clipboards, contacts, calendar entries, downloads, documents, spreadsheets, usage history, log files, system information, and other information. External storage, such as secure digital (SD) cards, and the cloud expands the storage space available to users, which may place more files at risk.

7.4 Where Does Spyware Come From?

Perpetrators may gain access to mobile devices and sensitive data through three vulnerabilities (Pradeo Lab, 2018): applications, the network, and the device. Table 2 summarizes these vulnerabilities and attack vectors. We discuss each vulnerability below.

Table 2. Vulnerabilities and Attack Vectors to Gain Access to Mobile Devices

Vulnerability	Attack vector
Applications	Malware, spyware, adware, phishing
The network	Public WiFi exploitation, man-in-the-middle attack
The device	Operating system

7.4.1 Applications

Employees use mobile apps on a daily basis to do their work and interact with enterprise data. Hackers most commonly use compromised apps downloaded from app stores to transfer malware to a user's device (La Porta, 2018). Such apps typically look and function like legitimate apps already on the market. However, they secretly install malware, spyware, and adware onto devices, which hackers can use to monitor and track unsuspecting victims. A recent variant of mobile malware, referred to as "Agent Smith", has covertly infected about 25 million devices worldwide (Hazum, He, Marom, MeInykov, & Polkovnichenko, 2019). Disguised as a Google-related app that the user knowingly installs, Agent Smith automatically replaces apps already installed on the device with malicious versions without users' knowledge or interaction. The malware exploits android vulnerabilities to access the devices' resources to show fraudulent ads for financial gain, but one could easily use it for eavesdropping as well.

Hackers could trick victims into installing malware via a malicious email attachment or a link that downloads harmful software. Referred to as phishing, the attacker masquerades as a trustworthy person or organization through email, phone call, text message, chat apps, or social networks to try to fool users into installing malware or divulging sensitive information. For example, employees may receive an email from what looks like their department manager or another trusted sender. An unsuspecting employee may open the email without noticing that the sender's email address does not match the manager's actual address or other details that indicate the threat. The email serves to entice employees to click on a malicious attachment or on a URL that downloads malware to an employee's device.

Malvertising may also dupe users. In malvertising, one inserts malware into advertisements on trusted websites. Malvertising can infect a smartphone in two ways: 1) by users' clicking on the ad (which redirects them to a malicious site rather than the real one) or 2) by users' simply visiting a site that embeds malware in its main scripts. Figure 8 presents the number of detected mobile malware packages as of quarter one in 2018.

Even legitimate apps collect a large amount of data that they do not need to function, such as a user's physical location, calendar, and contacts. These apps may store this data in the cloud with unclear security protections. As such, such apps place details about users' employers at risk of unauthorized access.

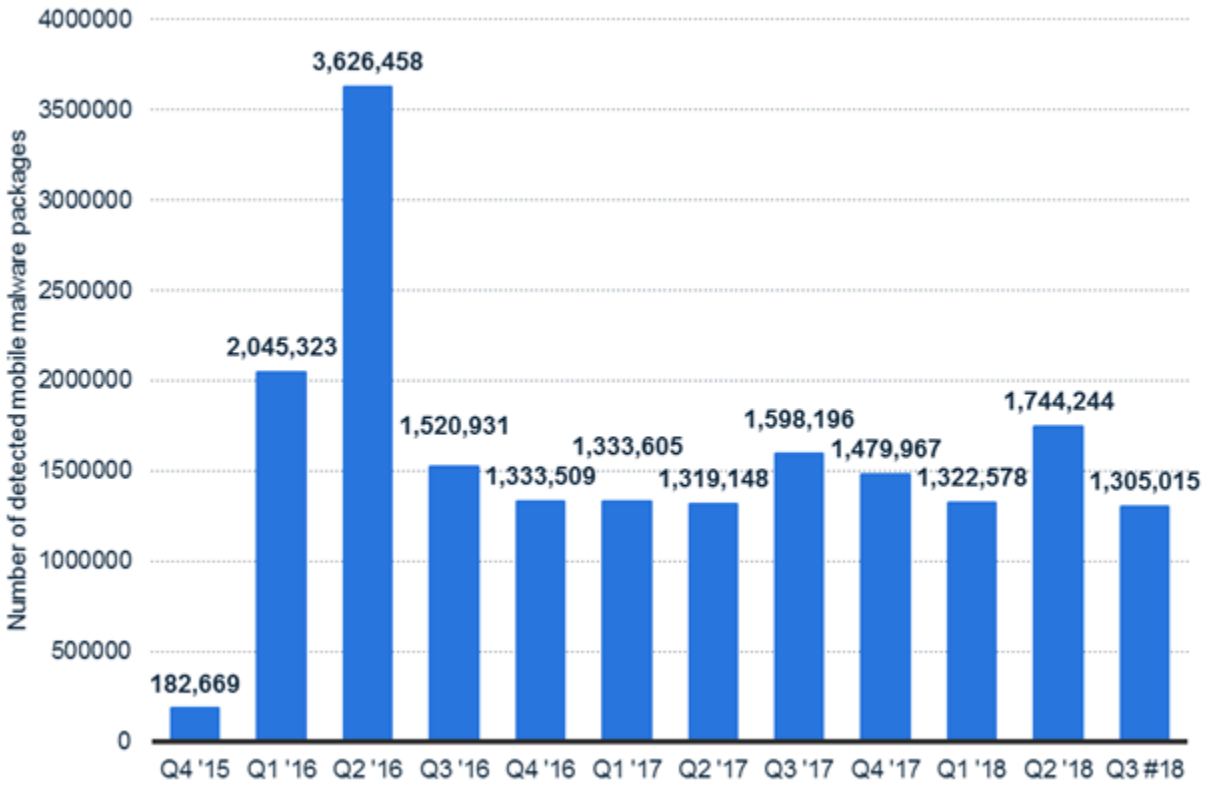

Figure 8. Number of Detected Malicious Installation Packages on Mobile Devices Worldwide from Fourth Quarter 2015 to 3rd Quarter 2018 (Statista, 2018b)

7.4.2 The Network

Unsecured public WiFi is the most common network threat (Pradeo Lab, 2018). Free public WiFi access points have proliferated as restaurants, hotels, airports, and retail stores increasingly provide this service. Figure 9 shows the use of a smartphone at a coffee shop. As a result, attacks through this vector have also increased. One does not need to authenticate to establish a network connection, which creates an opportunity for hackers to access unsecured devices on the same network. These perpetrators can position themselves between a user and the connection point (called a man-in-the-middle attack). In this way, they can intercept data before sending it on to the user/hotspot. Hackers can also exploit an unsecured WiFi connection to distribute malware, spyware, or adware.

Figure 9. Smartphone use at a Coffee Shop (www.Pixel.la Free Stock Photos, 2015)

7.4.3 The Device

Malware may exploit vulnerabilities in the operating system that powers a device's basic functions. While Android has seen more malware than iOS-powered smartphones, hackers target both platforms. Statista (2018) has forecasted that Google's Android would represent 85.1 percent of the mobile operating system market worldwide in 2018 and Apple's iOS would represent 14.8 percent (see Figure 10). In contrast to iOS, Android presents greater corporate security concerns because it poses a bigger target for malware attacks. Additionally, Android is open source software, while iOS is not. When Android emerged, anyone could change the source code to provide enhancements to the mobile experience for users. In recent

years, Google has improved Android's security by implementing controls. Additionally, the security research community has developed tools to evaluate the security of Android applications. By contrast, Apple's iOS places many more restrictions on what developers can do, and Apple does not release its source code.

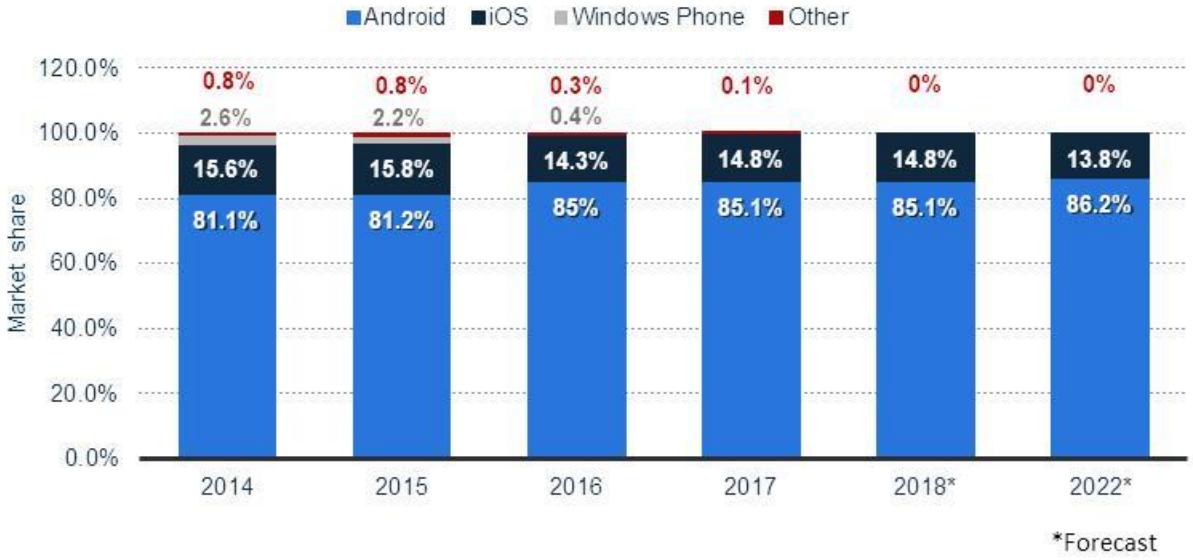

Figure 10. Global Market Share of Smartphone Operating Systems based on Unit Shipments from 2014-2022 (Statista, 2018a)

Hackers may target unattended mobile devices by installing tracking software directly onto the device. Alternatively, a perpetrator could swap in a look-alike battery as Figure 11 depicts, with a chip to hijack the device in order to remotely control it to capture information.

To protect against vulnerabilities, company release security patches on a regular basis. Keeping software on devices regularly updated constitutes the most common solution to reduce malware. However, mobile users may not update their devices in a timely manner, which leaves them vulnerable to exploits. Regularly updating mobile OS poses a greater challenge for organizations that have a bring-your-own-device (BYOD) policy since they do not own the device and, therefore, must rely on employees to take action. Similarly, organizations must rely on employees to not leave their mobile devices unattended at any time.

Figure 11. Medion Brand Battery in a Smartphone (Mabbett, 2017)

8 Use of Mobile Devices by FastTrans Employees

The proliferation of mobile consumer devices in the workplace may provide employees with opportunities to work in innovative and productive ways (Sipior, Bierstaker, Chung, & Lee, 2017). However, these

benefits have certain risks. Employees may have become accustomed to using mobile devices in the workplace but may not consider all the potential risks.

Given mobile devices' growth and changes in the last decade, FastTrans employees have also changed how they use them. FastTrans currently has a corporate-liable Android program for its nearly 25,000 employees. Employees purchase corporate-liable devices with company funds; thus, the organization owns the devices. Originally, the company issued about 30 percent of management personnel with corporate-owned devices. Today, the company issues every FastTrans employee who desires a device with a corporate-owned device. As a result, the company has seen a significant increase in costs associated with the IT department's supporting users and their devices. The company allows only Android-powered devices to access company email; therefore, employees may find themselves using both their Android and another personal mobile device.

FastTrans keeps the software on corporate-liable mobile devices up to date. It issues frequent notices to employees who BYOD to do the same. Employees also receive reminders to refrain from downloading apps from unfamiliar sites and install apps only from trusted sources. With such security measures in place, FastTrans found it had done enough to prevent mobile espionage.

9 Questions

Please develop detailed written responses to each question below. You must acquire more information from FastTrans. What questions would you ask? You also need to undertake additional research regarding mobile espionage to adequately respond to each question. Please state any assumptions that you make.

1) Why do many sources expect corporate mobile espionage to become more prevalent in the future?
2) What smartphone users might be most at risk of corporate mobile espionage?
3) What would motivate Wheelz to risk undertaking mobile espionage? In addition to competitors, who spies on companies or cell phone users and why?
4) What are phishing and malware? How do they relate to each other? What role can these play in mobile espionage?
5) What forms of mobile espionage are legal/illegal?
6) FastTrans is considering banning smartphones from the workplace. Do you agree? What advantages/disadvantages does this approach have in reducing the risk of mobile espionage?
7) What action should FastTrans take in response to the mobile espionage? What are the best practices for an organization to protect itself against mobile espionage?

Acknowledgment

We thank Burke T. Ward (School of Business, Villanova University) for his comments, suggestions, and thorough review of an epilogue.

References

Badenhorst, R., (2017). BizTrends2017: What will the cyber threat space hold in 2017? *Bizcommunity*. Retrieved from http://www.bizcommunity.com/Article/196/726/155541.html

Bajak, F. (2018). APNewsBreak: US suspects cellphone spying devices in DC. Retrieved from https://apnews.com/d716aac4ad744b4cae3c6b13dce12d7e

Bensinger G., & Dawson, C. (2018). Toyota to work with Uber, take stake. *The Wall Street Journal*.

Collins, K. (2017). Google collects Android users' locations even when location services are disabled. *Quartz*. Retrieved from https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

Deputy Secretary of Defense. (2018). *Mobile device restrictions in the Pentagon.* Retrieved from https://media.defense.gov/2018/May/22/2001920731/-1/-1/1/PENTAGON-MOBILE-DEVICE-POLICY.PDF

Federal Trade Commission v. Seismic Entertainment Productions, Inc., Smartbot.Net, Inc., and Sanford Wallace. (2004). Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2004/10/041012comp0423142.pdf

Federal Trade Commission. (2004). *Statement of FTC Commissioner Mozelle W. Thompson before the United States House Committee on Energy and Commerce for testimony on spyware*. Retrieved from http://www.ftc.gov/speeches/thompson/042904mwtspywarestmnt.pdf

Font Awesome. (2018). A solid-weight icon from Font Awesome, a free web icon font [digital image]. *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:Font_Awesome_5_solid_user-secret.svg

Gao, P., Kaas, H.-W., Mohr, D., & Wee, D. (2016). Automotive revolution—perspective towards 2030. *McKinsey*. Retrieved from https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/disruptive-trends-that-will-transform-the-auto-industry/de-de

Garamone, J. (2018). New policy prohibits GPS tracking in deployed settings. Retrieved from https://dod.defense.gov/News/Article/Article/1594486/new-dod-policy-prohibits-gps-enabled-devices-in-deployed-settings

Harris, M. (2018). The tricks and travails of Uber's self-driving car spies. *Wired*. Retrieved from https://www.wired.com/story/uber-waymo-self-driving-car-ssg/

Hazum, A., He, F., Marom, I., Melnykov, B., & Polkovnichenko, A. (2019). Agent Smith: A new species of mobile malware. *Check Point Research*. Retrieved from https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/

Kaspersky. (2018). *Avoiding cell phone spyware infestation*. Retrieved from https://usa.kaspersky.com/resource-center/preemptive-safety/cell-phone-spyware

La Porta, L. (2018). 4 ways hackers are infiltrating phones with malware on Android phones. *Wondera*. Retrieved from https://www.wandera.com/mobile-security/mobile-malware/malware-on-android/

Legal Information Institute. (1996). *18 U.S. Code § 1839.Definitions*. Retrieved from https://www.law.cornell.edu/uscode/text/18/1839

Mabbett A. (2017). Unboxing a Medion LIFE E5020 smartphone [digital image]. *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:Medion_LIFE_E5020_-_2017-10-11_-_Andy_Mabbett_-_06.jpg

McMillan, R. (2018). Mobile-phone malware is rising. Blame spies. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/mobile-phone-malware-is-rising-blame-spies-1528369200

Mcmillin24. (2013). *49-mile scenic drive shield for the route in San Francisco, California* [digital image]. *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:San_Francisco_CA_49-Mile_Scenic_Drive.svg

Ponemon Institute. (2016). *The economic risk of confidential data on mobile devices in the workplace*. Retrieved from https://info.lookout.com/rs/051-ESQ-475/images/Ponemon%20Report%20Enterprise%20FINAL.pdf

Pradeo Lab. (2018). Mobile threat report. *Pradeo*. Retrieved from https://www.pradeo.com/media/Mobile_Security_Report_S22018.pdf?submissionGuid=3f4a8492-98d7-470c-a4c9-b05cea1d690c

Sappin, E. (2018). Will self-driving cars end the big automakers? *Forbes*. Retrieved from https://www.forbes.com/sites/forbesnycouncil/2018/04/13/will-self-driving-cars-end-the-big-automakers/#2bebba7b356d

Sipior, J. C., & Ward, B. T. (2008). User perceptions of software with embedded spyware. *Journal of Enterprise Information Management*, *21*(1 & 2), 13-23.

Sipior, J. C., Bierstaker, J., Chung, Q., & Lee, J. (2017). A bring-your-own-device case for use in the classroom. *Communications of the Association for Information Systems*, *41*, 216-214.

Statista. (2018a). *Market share worldwide smartphone shipments by operating system from 2014 to 2022.* Retrieved from https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/

Statista. (2018b). *Number of detected malicious installation packages on mobile devices worldwide from 4th quarter 2015 to 3rd quarter 2018.* Retrieved from https://www.statista.com/statistics/653680/volume-of-detected-mobile-malware-packages/

Sullivan, J. (2006). Lombard Street in San Francisco seen from the *Coit Tower* [digital image]. *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:Sanfran_61_bg_032605.jpg

Svay, M. (2017). Smartphone—the Noun Project icon from the Noun Project [digital image]. *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:Smartphone_-_The_Noun_Project.svg

Welch D., & Behrmann, E. (2018). Who's winning the self-driving car race? *Bloomberg*. Retrieved from https://www.bloomberg.com/news/features/2018-05-07/who-s-winning-the-self-driving-car-race

www.Pixel.la Free Stock Photos. (2015). Hands-coffee-smartphone-technology [digital image]. *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:Hands-coffee-smartphone-technology_(23698591814).jpg

メルビル. (2016). RX-8 2010Y-MODEL TYPE-S [digital image]. *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:RX-8_2010Y-MODEL-SIDE.jpg

About the Authors

Janice C. Sipior is a Professor of MIS at Villanova University. Her academic experience includes faculty positions at University of Warsaw, Poland; Moscow State Linguistic University, Russia; University of North Carolina at Greensboro, USA; and Canisius College, USA. She serves as Editor-in-Chief of *Information Systems Management* and Associate Editor of *Information Resources Management Journal*, and previously served as Chair of the Association for Computing Machinery's Special Interest Group on Management Information Systems (ACM SIGMIS). Her research interests include ethical and legal aspects of information technology, system development strategies, and knowledge management.

Danielle R. Lombardi is an Assistant Professor at Villanova University. She received her doctorate from Rutgers University and a B.S. in Accounting from The College of New Jersey. Prior to her career in academia, she was an audit manager at PricewaterhouseCoopers and CohnReznick. Her research interests are primarily behavioral and involve judgment and decision-making. She also explores the role of technology related to decision-making. Her publications have appeared in *Accounting Horizons*, *Advances in Accounting*, *Journal of Emerging Technologies in Accounting*, *Current Issues in Auditing*, *Accounting Historians Journal*, and *Journal of Information Systems and Technology Management*. She serves as a reviewer on several journals and is a committee member for the Auditing Section of the American Accounting Association.

Cathy A. Rusinko is Professor of Management and Coordinator of Sustainability in the School of Business and Kanbar College of Design, Engineering, and Commerce at Thomas Jefferson University. Her research explores technology and innovation management in manufacturing and service industries. She also does pedagogical research on integrating sustainability and other innovations in higher education, and was a guest editor of *Journal of Management Education*. She is author of over 50 papers, publications, and presentations and an invited industry speaker. She earned a PhD in Management and Organization at The Pennsylvania State University, and worked at General Electric, U.S. Department of Agriculture, and U.S. Department of Defense prior to her academic career.

Steven Dannemiller is currently pursuing his PhD at University of Alabama. Previously, he earned his Master's in Accounting and MBA at Villanova University.