Chapter 10
Blockchain and Cybersecurity

The Rise of Cybersecurity Threats

Computer exploitation is on the rise. Advanced adversaries are becoming more capable and destructive. Organizations must become increasingly effective at mitigating their information security risks. Effective cybersecurity is more important than ever as immeasurable amounts of personal and potentially incriminating data are currently stored in websites and social media platforms. The Internet is full of powerful hacking tools and hackers are using them extensively to cause damage to individuals and organizations. Attacks are becoming stealthier, having a greater financial impact, and causing broad damage. Reports of organizations being hacked and suffering reputational damage have become commonplace. According to Symantec, cybersecurity threats in some categories rose to 600% in 2017 (Symantec 2019). A continuous stream of cybersecurity breaches in 2017 underscores our inability to provide adequate security for our online information. Organizations are spending significant time, financial, and human resources to combat cyber threats and combat cyberattacks, however some companies are still getting compromised. The traditional prevention approach to security architecture has failed to prevent hackers from intrusions. Blockchain technology is that proactive approach to security needed to enhance the capabilities of organizations to detect and prevent threats that will inevitably slip through existing defenses.

Americans are increasingly installing the smart home devices like Google Home and Amazon Echo, thermostats, doorbells, and other household devices. These devices connect to the Internet and can be controlled and monitored remotely via smartphone apps. According to a data report, the number of smart speakers like Amazon Echo and Google Home installed in U.S. homes almost doubled—from 36 million in 2017 to 66 million in 2018. The majority of owners use these speakers to stream music or answer questions. Nearly 40% are used to help control owners'

M. Attaran, A. Gunasekaran, *Applications of Blockchain Technology in Business*, SpringerBriefs in Operations Management,
https://doi.org/10.1007/978-3-030-27798-7_10

connected smart homes. Of U.S. smart speaker households, 35% owned multiple devices in 2018 (Kinsella 2019).

These smart home devises are providing unprecedented convenience for homeowners on the go, but they also represent new frontiers for Internet hacking. While there are no statistics about the number of smart devices that have been hacked, experts anticipate the problem will grow along with the proliferation of smart devices. There are numerous reports of hacked smart home devices. According to the Chicago Tribune, in January 2019, a Lake Barrington, Illinois couple overhead a male voice speaking to their 7 month-old baby through the baby monitor. They also noticed their Nest thermostat had been cranked up to 90 degrees. Then the same man's voice began yelling vulgarities at them from the downstairs Nest security camera. It turned out that the couple's devices had been hacked, giving the hacker almost full control (Marotti 2019). The hacker could watch, listen, talk, and change the temperature via devices on the network. This is just one example of the dangers that occur as the smart home devices expand and security concerns around it multiply.

There are several reasons why home devices may be vulnerable to hacking (Marotti 2019):

- These devices are designed for convenience. Manufacturers are concerned about implementing security steps that consumers may find frustrating.
- Manufacturers are not as well versed in how to securely connect their device to the Internet.
- Some consumers fail to follow the security steps for connecting the device to the Internet and adequately securing them.
- Most consumers are not considering these devices as something that needs protection the same way laptops or smartphones do.

Blockchain and Cybersecurity Risks

Blockchain technology can reduce cybersecuity risks in different ways. The technology provides a hack-proof authentication that protects user and company data from cyberattacks. It provides data integrity in the financial industry that both stakeholders and regulators need. Supply chains such as pharmaceuticals, electronics, diamonds, and luxury items need transparency to work correctly. Blockchain improves transparency in supply chains, can identify counterfeits, and provides a global solution.

The most promising blockchain real-world cybersecurity use cases are listed below (Singh 2018; Marr 2018).

- **GuardTime.** A cybersecurity blockchain project that aims to create "keyless" signature systems to secure the health records of one million Estonian citizens.

- **REMME.** A cybersecurity blockchain project with the goal to improve the current standards of security for both users and companies by replacing logins and passwords with SSL certificates stored on a blockchain.
- **Blockverify.** A blockchain-based anti-counterfeit solution to identify counterfeits and offer a non-duplicate environment. It also provides the integrity required to run the supply chains with 100% transparency. Blockverify is used for electronics, pharmaceuticals, and luxury items.
- **PeerNova.** A blockchain-based technology that provides financial institution a way to verify and secure data, and address their audit, reconciliation, and compliance.

References

Kinsella B (2019) CIRP reports that U.S. smart speaker installed base rose to 66 million in 2018 with Amazon holding 70% share compared to google and apple. *Voicebot.ai.* February 5. Retrieved April 19, 2019, from https://voicebot.ai/2019/02/05/cirp-reports-that-u-s-smart-speaker-installed-base-rose-to-66-million-in-2018-with-amazon-holding-70-share-compared-to-google-and-apple/

Marr B (2018) 35 amazing real world examples of how Blockchain is changing your world. *Forbes*. September 25, Retrieved March 12, 2019, from https://bernardmarr.com/default.asp?contentID=1302

Marotti A (2019) Why are you looking at me? I see you watching me Smart devices like Nest getting hacked in digital home invasion. *Chicago Tribune*. February 8. Retrieved April 16, 2019, from https://www.chicagotribune.com/business/ct-biz-nest-cameras-hacked-20190204-story.html

Singh N (2018) Real world Blockchain use cases – 46 Blockchain applications. July 6 Retrieved, March 25. https://101blockchains.com/blockchain-applications/

Symantec (2019) Internet security threat report. Vol 24, February. Retrieved March 25, 2018, from https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf