Hiren Shah

Research Report #2 – Emerging Risks

**Introduction**

Padgett-Beale is ready to deploy a new cloud-based event management system that provides a plethora of software services to aid in events such as conferences, concerts, and festivals. The major operating units at Padgett-Beale, the Entertainment Team (ET), Marketing & Media (M&M), and Resort Operations (RO), are eager to implement the new event management system. The operating teams noted several benefits of Radio-Frequency Identification (RFID), including automatic check-in for attendees, cash free payment option, reduced likelihood of theft, and easy connection to social media accounts (ID&C). Padgett-Beale can improve their competitive advantage by analyzing the data collected from the RFID wristbands to increase profits, optimize cloud capabilities, and process transactions and authorizations for cashless payments for goods and services (Lockton, 2005). The head of Corporate IT has given approval for the new system because it leverages cloud-computing capabilities. However, the project has come to a halt since the Chief Financial Officer (CFO) and the Chief Privacy Officer (CPO) have requested more information about the advantages of RFID and its potential issues regarding privacy and PCI compliance. This report will provide analysis of managing adult attendees at music festivals with RFID bands linked to social media accounts (Facebook, Twitter), credit card accounts and security and privacy issues that may potentially arise.

**Analysis**

At Padgett-Beale, one of the proposed use cases of customizable RFID wristbands is for individuals attending music festivals or concerts where IDs must be checked to establish proof of age (legal requirement for local alcoholic beverage consumption). Padgett-Beales’ Entertainment Team can manage adult attendees at music festivals by utilizing a token that is attached to each wristband which enables attendees to have access to cashless payments, social media, etc. “Additionally, the ability to ‘wear’ the RFID token in a form of a wristband means less hassle for attendees’ and decreased risk of lost tickets or theft.” (Token) The RFID wristbands also offer some form of child safety, “RFID systems also offer ways of increasing child safety. A parents' RFID wristband can be linked to their child's, preventing minors from gaining access to certain areas or leaving a perimeter without their parents.” (ID&C) There are many advantages of RFID wristbands, however it is important to explore the possible security and privacy risks involved with them.

**RFID Sniffing**

“An important element in how RFID wristbands work is storage capacity. The largest passive RFID tags can store up to 3720 bytes, or 3.72 kilobytes of information. That may seem like a small amount, but that is enough to store your name, address, credit card numbers, date of birth, and whatever identifying information the local administrator wants to track” (Chu, 2017). With all this data storage and information sharing, Padgett-Beale should be concerned about the rise in RFID sniffing, which is when attackers use a complex mobile device of their own to steal information on users’ wristbands (Wing, 2015).

**Reverse Engineering**

Reverse engineering is when a hacker will disassemble the chip to figure out how the device receives the data. This type of attack is rare, since the hacker would need to have complex knowledge and experience to successfully take apart and put together an RFID device. (Smiley, 2016) These embedded chips often contain important personal and sensitive information that could be detrimental to the individual if the information is leaked.

**Eavesdropping & Replay**

Eavesdropping is when a hacker uses an unauthorized RFID reader and listens to conversations between a tag and reader to obtain important data (Smiley). In a replay attack, “an attacker intercepts communication message flowing between the reader and the tags and he records the tag’s response that can be used as a response to reader’s request. An example of reply attack is a perpetrator recording communication between access card reader and a proximity card, which can be used to access a secure facility.” (Wing)

**Denial of Service**

A Denial of Service attack is the broad concept of an RFID system failure that is associated with an attack. These attacks are usually physical attacks like jamming the system with noise interference, blocking radio signals, or even removing or disabling RFID tags. (Smiley)

**Viruses**

[RFID tags](https://www.atlasrfidstore.com/rfid-tags/) currently do not have enough memory capacity to store a virus; but in the future, viruses could be a serious threat to an RFID system (Wing). “A virus programmed on an RFID tag by an unknown source could cripple an RFID system when the tagged item is read at a facility. When read, the virus would transfer from tag to reader and then to a company’s network and software – bringing down connected computers, RFID components, and networks.” (Smiley)

**Tracking**

Another major concern with RFID devices is the tracking capabilities that it provides. Not everyone wants to have their location known or every purchasing habit monitored by event organizers. Hence, it is important to realize that when wearing an RFID device, it will capture the last known location of when it was in the range of the RFID reader’s field, which stores the identification of the object and locate its position (Wing).

**Laws**

Padgett-Beale should be aware of some of the security and privacy laws that relate to the RFID wristbands which may impact their decision to use or not use RFID devices. It is critical to keep the information retained from the wristbands confidential at all times. Consumer privacy and security for personal data is regulated by the Federal Trade Commission (FTC), in the United States. “The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorized disclosure of personal data” (FTC). Some basic security laws from the FTC require businesses to provide information on how to disable tags, how to label tags and when to inform attendees when an RFID is nearby (Brulia, 2019). The EU is data protection law is working to implement a data protection framework called PIA. “The PIA process is designed to uncover the privacy risks associated with an RFID Application and evaluate the steps taken to address those risks. These impacts (if any) could vary significantly, depending on the presence or lack of personal information processing by the RFID Application. The PIA Framework provides guidance to RFID Operators on the measures adequate to mitigate any likely data protection or privacy impact in an efficient, effective and proportionate manner.” (RFID)

Furthermore, Padgett-Beale may have to comply with regulations set forth by the Payment Card Industry Data Security Standard (PCI DSS). The data security standard covers rules that must be held compliant to secure the customers data. It is important to note that each state may have their own specific rules and regulations. RFID laws, in regard to PCI DSS are still being considered and implemented gradually in each state. However, there are guidelines for risk and controls to help mitigate any security issues. The purpose of the Federal Communications Commisions (FCC) is to “regulate private-sector telecommunications by establishing technical standards that minimize the likelihood that devices that transmit or receive radio frequency (RF) energy will interfere with each other.” (Mo, 2019). And they have set in place some labeling laws in certain states that, for example, some manufacturers have to provide a Supplier Declaration of Conformity (SDoC) just to prove that they are not operating any devices that emit radio waves more than the amount recommended by the FCC (Mo, 2019).

**Recommendations**

**Data Encryption**

Encryption makes it extremely improbable for an untrusted party to read the contents of a message. Encryption could improve RFID security because data transfer between tags and trusted readers could be encrypted so that rogue readers cannot intercept the message (RFID Facts). It is important to make sure that all payment card information and personal data are all encrypted.

**Privacy Policy**

Implementation of a privacy policy will be critical to determining how the RFID system will store and manage customer data and information. “The RFID privacy [and usage] policy should also address privacy issues associated with the tag identifier formats and the potential disclosure of information based on solely on the tag identifier format selected.” (Karygiannis) The policy should be clearly written as to explain the requirements and expectation of use for the wristbands and “enable management to exercise legal or disciplinary actions against employees or entities who fail to comply.” (Karygiannis)

**Training and Education**

Anyone that will be involved in operating the RFID devices should participate in a pre-developed security training program offered by Padgett-Beale. It is obvious that if we all know about the risks associated with RFID, then it will be easier to try and mitigate those risks, rather than coming in with no knowledge. “The training program should cover the RFID privacy policy and teach operator how to properly use the system and the appropriate security measures.” (Karygiannis)

**Informed Consent**

Padgett-Beale should make sure to inform the guests of the technology in the RFID devices and the data collection, usage, storage, and processing that may inevitably put peoples’ information at risk. “The guest should be aware of the RFID tags and how their information will be used and stored.” (ID&C) If the device is to keep records of tracking and location, it should be clear to the guests that this information will be used for the interest of Padgett-Beale to avoid location privacy violations.

**Social Media Security**

In order for Padgett-Beale to have outstanding security measures in place, following the EU PIA framework for RFID can reduce unauthorized access. The PIA Framework provides guidance to RFID Operators on the measures adequate to mitigate any likely data protection or privacy impact in an efficient, effective and proportionate manner.” (RFID) Maintaining a strong information security framework can help mitigate most internal and external risks involved with the information stored on the RFID devices.

**Conclusion**

To summarize, Padgett-Beale has an important decision to make regarding RFID wristbands that may impact future businesses and processes. In order to make the best decision moving forward, Padgett-Beale needs to be aware of the privacy and security risks, the laws the govern the privacy and usage, and the best practices to prevent any unauthorized access. RFID devices has many advantages, and it will help Padgett-Beale run operations smoothly and with less infrastructure, and with its cloud-based capabilities, it might be cost effective. New technology brings risks, which leads to mitigation strategies. Make sure to always be aware of risks involved with RFID devices and be ready to act swiftly if unauthorized access occurs to one of the guests.

References

Brulia, V., Jung, D. (2009). Privacy and RFID Technology – Legal Issues Retrieved from <http://www.personal.psu.edu/users/v/j/vjb5014/index.html>

Chu, W. (June 5th, 2017). How RFID Wristband Work, Decoded. Retrieved from <https://www.wristbands.com/blogs/blog/how-rfid-wristbands-work>

Mo, C. (December 24th, 2019). RFID Products Regulations in the US: An Overview. Retrieved from <https://www.compliancegate.com/rfid-products-regulations-united-states/>

FTC. (2016). Data Privacy and Security Update (2016). Retrieved from <https://www.ftc.gov/reports/privacy-data-security-update-2016>

Lockton, V., Rosenberg, R.S. RFID: The Next Serious Threat to Privacy. *Ethics Inf Technol* **7,** 221–231 (2005). <https://doi.org/10.1007/s10676-006-0014-2>

ID&C. (2020). 8 Benefits of Using RFID Wristbands for Resorts & Attractions. IDC band. Retrieved from <https://www.idcband.com/en-us/blog-us/8-benefits-of-using-rfid-wristbands-resorts-attractions/>

RFID. (2017). All You Need To Know About RFID … For End Users. Retrieved from <http://www.rfidineurope.eu/privacy>

RFID Facts. (2020). RFID Fact Sheet. Society and Technology Group. Retrieved from <https://rfid.cs.washington.edu/posters/RFID-fact-sheet.pdf>

Smiley, S. (2016). 7 Types of Security Attacks on RFID Systems. Atlast RFID Store. Retrieved from <https://www.atlasrfidstore.com/rfid-insider/7-types-security-attacks-rfid-systems>

Token Team. (January 4th, 2018). The Beginner’s Guide To RFID Technology For Events. Token Systems. Retrieved from <https://www.gettoken.com/beginners-guide-rfid-technology-events/>

Wing. (February 12th, 2015). Top 10 RFID Security Concerns and Threats. Retrieved from <https://securitywing.com/top-10-rfid-security-concerns-threats/>