**Research Report #2: Emerging Issues Risk Analysis & Report**

CSIA 300 Cybersecurity for Leaders and Managers

Olufemi Akinyemi

Professor Nedim Goren

December 8, 2019

**Introduction**

The Entertainment Team (ET), Marketing & Media (M&M), and Resort Operations (RO) are three of the major operating units at Padgett-Beale. These teams are in support of the procurement of a new cloud-based event management platform that provides end-to-end management for events (conferences, concerts, festivals). The teams have highlighted several benefits of the new platform, including the provision of customized RFID bands to be worn by attendees, which adds ease for tracking. There is also a potential reduction in counterfeit tickets which will limit revenue losses. The employment of RFID technology will also provide automatic identification and tracking without extra staff, resulting in cost savings. “Data collected can be used for analytics to benefit future event planning, and for follow up and direct marketing after the event”, (RFID4U, n.d). Furthermore, attendees’ credit card or debit card accounts can also be connected to the bands to easily make and process purchases. (Stabile, 2015). The teams also relied on the fact that RFID technology has been around for a while and over the years, become less expensive and more robust. (Advancing Identification Matters, 2018).

While the members and heads of the operating teams are in full support of adopting the platform, several other high-level managers have expressed concerns over the use of customizable RFID wrist bands for managing and tracking attendees. This analysis and report is in response to the Chief Privacy Officer’s request for more information about the potential privacy and security issues of the RFID system, based on proposed use cases. One of the use cases of concern is with individuals attending a music festival or other event where IDs must be checked to establish proof of age (legal requirement for local alcoholic beverage consumption). “Privacy organizations have long criticized the use of RFID chips in documents and items that could be used to track people's movements, determine their identities or make inferences about their habits”, (Martínez-Cabrera, 2012). Key security and privacy concerns with RFID implementation surrounds the collection of information. What information is collected? Where does it go and where is it stored? Who has access to it? These are strong security and privacy related questions that will limit or impose additional responsibilities upon Padgett-Beale. (RFID Journal, n.d). Data leakage or disclosure, hacking attacks, third-party security procedures and practices, location tracking and monitoring and theft or misplacement are reasonable security and privacy concerns arising from implementation of this new technology.

**Analysis**

At Padgett-Beale, one of the proposed use cases of customizable RFID wristbands is for individuals attending music festivals or other events where IDs must be checked to establish proof of age (legal requirement for local alcoholic beverage consumption). At such events, issued wristbands can be scanned “to do things like pay for food or drink, get access to VIP areas, or even upload posts to social media. The bands will allow for the collection of data which can later be used to sell, promote, brand further, find sponsors, and much more”, (Bowler, 2017). This will let event organizers know when attendees are coming in and leaving, how they move around the venue, where more resources should be allocated, the types of interactions taking place and products being consumed. (Bowler, 2017).

This use case requires Padgett-Beale to collect, store, process, and transmit various types of private/personal information or data. A key 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”, (Chu, 2017). While this may seem like a small amount of storage capacity, it is enough to store wearers “names, address, credit card numbers, date of birth, and whatever identifying information the local administrator wants to track”, (Chu, 2017). Additional information can include physical location data, email address and even social media information. This personal information is used for proper identification purposes, especially under the specified use case. A wearer’s date of birth is critical to identifying and verifying his/her age, which is legal requirement for serving alcohol beverages. (Anonymous, 2013).

Privacy is a serious and important concern that always emerge when RFID technology and its various applications are discussed. This is mostly due to the fact that, “RFID tag embedded chips often contain important personal information and usually this kind of private information can hurt one’s privacy seriously if leaked”, (Jung & Lee, 2015). The RFID wristbands will contain personal/private information that will raise reasonable privacy concerns. Without adequate security implementation, wristbands can be accessed and the information they hold will be leaked to unauthorized parties, jeopardizing the privacy of guests. Information such as the linked credit card or debit card account can lead to fraudulent charges, while other personally identifiable information may even facilitate identity theft, stalking and more. (Meingast, King & Mulligan, 2007). Leakage can occur from poor implementation or improper storage of information after collection. During processing and transmission, improper handling can equally contribute to data leakage as well.

A major security consideration with privacy repercussion is that RFID technology is not tamper or hack-proof. One prevalent hacking method employed against RFID systems is the use of rogue RF readers by unauthorized entities. It is no secret that hackers and other malicious entities are usually after anything that provides valuable information that can be exploited. Rogue RF readers can be used to obtain access to the personal information stored on wristbands without the knowledge of the wearers or Padgett-Beale. Two popular methods access employed via rogue readers include skimming and eavesdropping. “Skimming occurs when the data on the RF transponder is read without the owner’s knowledge or consent using an unauthorized reader. Eavesdropping is the opportunistic interception of information on the chip while the chip is accessed by a legitimate reader. While similar to skimming, eavesdropping may be feasible at longer distances, given that eavesdropping is a passive operation”, (Meingast, King & Mulligan, 2007).

Furthermore, the involvement of third-party presents both security and privacy concerns. Information shared with third-party may not be approved by guests which may make them feel their privacy is being violated. For this implementation, the service is cloud-based and offered by another party who may participate in the collection of data and even analyze or use it. This relationship must be disclosed to the guests and the manner of usage by the service provider. Data confidentiality is difficult to ensure in relationships with third-parties. While Padgett-Beale may be following regulations governing data security and privacy with regards to storage, processing, transmission, use and even retirement, the platform provider may not be. The company must remember that “even if a security risk is due to a third party’s lax security, in the mind of the customer it will be the main organization that bears responsibility”, (UpGuard, 2017). This is a legal issue also, as liability responsibilities may fall on Padgett-Beale.

Another major privacy concern with RFID wristbands is the tracking or monitoring ability it provides. Some event goers may not want their location to be tracked or their purchasing habits at events monitored by organizers. The design of RFID technology requires the chip in wristbands to always respond to the reader’s query. “Most RFID wristbands use passive tags that operate at high frequency, they cannot track wearers actively, however, a wearer’s last known location can be tracked and recorded”, (Chu, 2017). This can used to determine the physical locations where the specific wristband has been, thus, enabling wearer’s movements to be tracked or monitored. (Khattab, Jeddi, Amini, & Bayoumi, 2016). Some guests may view this tracking or monitoring as a violation of location privacy.

Finally, RFID wristbands are not immune to getting lost or stolen. A physically misplaced or stolen wristband may fall in the wrong hands resulting in security and privacy problems for the owner. Like all lost or stolen electronic devices, the physical device can easily be replaced, however, exposure and exploitation of the data is where the big concern lies. Account funds and personal information may be at risk if a lost or stolen RFID wristband is not deactivated in-time. (Intellipay, n.d).

Padgett-Beale’s planned implementation of the event management system with RFID wrist bands may be impacted by some relevant data security and privacy laws. The postposed wristbands will contain sensitive personal data that must be secured and kept confidential. 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”, (Jolly, 2017). The FTC has broad authority that allows it to address a wide range of practices affecting consumers, including the ones that emerge with the development of new technologies or business models. In addition, the current EU data protection laws provide some regulations to be followed when applications are employed to process personal data. The EU data protection laws requires “fair and lawful processing, retention of personal data for only as long as necessary and collection of data which is relevant and not excessive for the purposes it has been collected”, (Archer & Salazar, 2005). Another provision is informed consent, which requires Padgett-Beale to disclose and make clear the details of how the information in a RFID wristband will be used.

In addition, Padgett-Beale may have to comply with regulations set forth by the Payment Card Industry Data Security Standard (PCI DSS). This is a global data security standard that any businesses must adhere to in order to collect, store, transmit and process card holder information. (Rouse, 2009). This data security standard covers objectives that must be implemented to secure customer data. Several states also have their own RFID regulations and laws that may impact the company’s proposed use case. For example, the HB-203 is approved in New Hampshire. This bill requires “warning labels on consumer goods and identity documents containing RFID tags or other tracking devices, as well as regulating the use of RFID for tracking individuals, and establishing a commission on the use of tracking devices in government and business”, (RFID Journal, n.d).

**Recommendations**

Before the technology is put into use by Padgett-Beale, some best practices for security and privacy should be implemented to mitigate associated risks. Here are recommendations to cover categories including people, processes, policies, and technologies:

* Encryption: Encrypting data stored in RFID wristbands will help in maintain confidentiality. “Even if a rogue reader could get a chip to “talk,” encryption would prevent the reader from understanding the message”, (Federal Trade Commission, 2005). Payment card information and other personal data must be encrypted. Something like the use of a password or pin must be used whenever information is to be retrieved from the wristbands to decrypt the stored data. This will also help in the event of lost or stolen wristbands, as disclosure or access to personal data will not be possible without using the correct password or pin. In addition, data in-transit between wristbands and readers should be encrypted as well.
* Informed Consent: Guests should be informed of the use of RFID technology in wristbands and the collection, storage, usage, processing of data that will result from their participation at events. It should be ensured that participants clearly understand that their participation equals consent to relinquishing some expectation of privacy and/or security. This is disclosure and consent acquisition are especially critical where third-parties may be involved, such as the proposed case use. (Archer & Salazar, 2005). The potential for tracking and monitoring should be disclosed to mitigate feelings of location privacy violations and liability claims.
* Due Diligence (third-party data storage and processing evaluation): “Due diligence is always recommended, even when a technology is mature, because it brings rigor to your business case analysis and helps you reduce risk”, (DataFlows Dimensions, Inc, n.d). entering business with third-parties can open the door to many risks and data protection compliance pitfalls, therefore, identifying these risks is a critical step to take before starting the relationship.” With the increasing use of cloud storage, unsecured cloud instances managed by third-parties are a frequent cause of data exposure. When dealing with third-party cloud solutions, it’s important to understand not just how the data will be stored, but also how it will be handled when the relationship ends”, (UpGuard, 2017). Enforcement of minimum required security standards and monitoring should be established.
* Usage Policy: The usage policy should “describe the authorized and unauthorized uses of RFID technology in the organization and the personnel roles assigned to particular RFID system tasks”. This policy should be integrated in Padgett-Beale’s privacy policy, “which addresses topics such as how personal information is stored and shared”, (Karygiannis, Eydt, Barber, Bunn & Phillips, 2007). The policy should clearly communicate expectations and requirements and enable management to exercise legal or disciplinary actions against employees or entities who fail to comply.
* Employee Training: Untrained/undertrained staff is a source of privacy and security risks that needs to be mitigated. Training “provides personnel with the skills and knowledge necessary to comply with, identify and report violations of RFID usage, IT security, and privacy policies, as well as agreements with external organizations”, (Karygiannis, Eydt, Barber, Bunn & Phillips, 2007). .

**Summary**

Padgett-Beale is considering the implementation of a new cloud-based event management platform that provides end-to-end management for events (conferences, concerts, festivals). While the three major operating teams are in full support of the implementation, several managers and the CPO have raised privacy and security concerns. The potential for personal/private information leakage, RFID hacking, third-party data protection pitfalls, location privacy violations via tracking and monitoring, and misplacement or theft of customizable RFID wristbands are all reasonable privacy and security issues that can be mitigated through recommended best practices. Encryption data stored in wristbands and in-transit, receiving informed consent, performance of due diligence (third-party data storage and processing evaluation) on the cloud-based platform provider, implementation of a usage policy with compliance enforcement and performing appropriate employee trainings are best practices that should be put in place before implementation and continued thereafter. These recommendations are critical to mitigating the privacy and security concerns associated with the use case discussed.

**References**

Advancing Identification Matters. (2018). Radio Frequency Identification (RFID) 101. Retrieved

December 4, 2019, from <http://www.aimglobal.org/?page=rfid_basics>

Anonymous. (2013). Wristbands for Beer Festivals. Retrieved December 4, 2019, from

<https://www.eventwristbands.com/blog/Wristbands-for-Beer-Festivals.html>

Archer, Q., & Salazar, G. (2005). RFID: a threat to privacy? Retrieved December 7, 2019, from

<http://www.computerweekly.com/opinion/RFID-a-threat-to-privacy>

Bowler, J. (2017). RFID Wristbands: The Good, the Bad and the Ugly. Retrieved December 7, 2019, from <https://blog.printsome.com/rfid-wristbands-good-bad/>

Chu, W. (2017). How RFID Wristbands Work, Decoded. Retrieved December 7, 2019, from

<https://www.wristbands.com/blogs/blog/how-rfid-wristbands-work>

DataFlows Dimensions, Inc. (n.d.). THE DATAFLOWS APPROACH TO RFID DUE

DILIGENCE. Retrieved December 7, 2019, from <http://www.dataflows.com/RFIDduedil2.shtml>

Intellipay. (n.d.). Snowbombing Cashless FAQ's. Retrieved December 6, 2019, from

<https://snowbombing.pay.intellifest.com/info/FAQ>

Jolly, I. (2017). Data protection in the United States: overview. Retrieved December 7, 2019,

from <https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=%28sc.Default%29>

Jung, K., & Lee, S. (2015). A systematic review of RFID applications and diffusion: key areas

and public policy issues. Retrieved December 7, 2019, from <https://link.springer.com/article/10.1186/s40852-015-0010-z>

Karygiannis , T., Eydt, B., Barber, G., Bunn, L., & Phillips, T. (2007). NIST SP 800-98,

Guidelines for Securing Radio Frequency Identification (RFID) Systems. Retrieved December 4, 2019, from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-98.pdf>

Khattab, A., Jeddi, Z., Amini, E., & Bayoumi, M. (2016). RFID Security Threats and Basic

Solutions. Analog Circuits and Signal Processing RFID Security, 27-41. doi:10.1007/978-3-319-47545-5\_2

Martínez-Cabrera, A. (2012). Privacy concerns grow with the use of RFID tags. Retrieved

December 5, 2019, from <https://www.sfgate.com/business/article/Privacy-concerns-grow-with-the-use-of-RFID-tags-3175330.php>

Meingast, M., King, J., & Mulligan, D. K. (2007). Security and Privacy Risks of Embedded

RFID in Everyday Things: the e-Passport and Beyond. Retrieved December 6, 2019, from <http://www.bing.com/cr?IG=1107B5B9F7CA4F63942FE732B490A640&CID=11AAEB47BA6266AC0540E0E7BBCD67D9&rd=1&h=VZgvU3RLgszDUfxboJVbkIA6SyH37Ttq3bkYHw4H17c&v=1&r=http%3a%2f%2fciteseerx.ist.psu.edu%2fviewdoc%2fversions%3fdoi%3d10.1.1.83.8403&p=DevEx,5034.1>

RFID Journal. (n.d.). Are there laws governing the use of RFID? Retrieved December 5, 2019,

from <http://www.rfidjournal.com/faq/show?135>

RFID4U. (n.d.). Event Management Case Study. Retrieved December 7, 2019, from

<http://rfid4u.com/wp-content/uploads/2015/12/Event-Management-Case-Study.pdf>

Rouse, M. (2009). What is PCI DSS (Payment Card Industry Data Security Standard)?.

Retrieved December 6, 2019, from <http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard>

Federal Trade Commission. (2005). RFID Report: Applications and Implications for Consumers.

Retrieved December 7, 2019, from <https://www.ftc.gov/sites/default/files/documents/reports/rfid-radio-frequency-identification-applications-and-implications-consumers-workshop-report-staff/050308rfidrpt.pdf>

UpGuard. (2017). Five Things to Know About Third Party Risk. Retrieved December 7, 2019,

from <https://www.upguard.com/articles/five-things-to-know-about-third-party-risk>

Stabile, R. (2015). Are RFID chips ruining festivals? Retrieved December 5, 2019, from

<https://m.axs.com/are-rfid-chips-ruining-festivals-67816>