Research Note

Arrayent's Inherent Risks

Kyle Simpson

December 2017

Keywords: Cloud Security; Internet of Things; Third Party Risks

Abstract: Risk is an inherent part of every business, and in the ever-evolving global economy, managing risk effectively and appropriately is crucial to maintaining competitive advantage as a company. This paper examines Arrayent, an Internet of Things (IoT) cloud service company that manages dozens of large companies including Whirlpool, Maytag, Liftmaster, and Febreeze; and makes recommendations of risk mitigation paths given the company's potential control failures.

Arrayent is a third-party cloud service that partners with companies to help them connect their products to the Internet of Things (IoT). Arrayent's platform "transforms traditional products into connected devices, acquires and transmits usage and device data in formats that power business intelligence systems, and enables device interoperability through cloud-to-cloud integration with third-party ecosystems."[1] This essentially boils down to Arrayent being a cloud connection service that offers consumers "a way to interact with their connected product," and allows companies to outsource their data collection and management.[1] Using Whirlpool as an example, Arrayent uses the sensors in washing machines manufactured by Whirlpool, collects any and all data Whirlpool may be interested in, and presents this data in a portal that Whirlpool can use to make informed decisions based on insights from their own data. By outsourcing their data collection, Whirlpool can spend more time on the manufacturing and customer relations side of their business, freeing up resources they can dynamically allocate elsewhere.

Being a cloud-based company, and a company that works heavily with third-party businesses, there are inherent risks that are present. In a meeting with two House of Representatives subcommittees, Bruce Scheiner, a cybersecurity researcher, commented that there is a clear relationship between cost and vulnerability potential. Products that are frequently replaced (such as smartphones) are patched more often since these companies want to maintain a content, consistent customer base. Products that are infrequently replaced (like refrigerators) are patched less frequently since there is a longer life-cycle and less turn-around. Scheiner puts it simply, saying that, "If there is not a profit or cost benefit for the manufacturer to patch a less frequently replaced product, then there is no drive for the manufacturer to patch it regularly."[2] Since Arrayent typically collaborates with businesses that specialize in the long-lasting category of product Scheiner references, there is already an inherent operational risk for Arrayent that is based on the partner company's willingness to provide long-term support for their products. In conjunction with this overarching operational risk, there are three specific risk areas to examine: 1) the risks associated with systematic failures, 2) the risks associated with external fraud, and 3) the risks associated with internal fraud.

[1] "Company Overview of Arrayent, Inc." Bloomberg. N.D. Accessed Nov. 2017 <www.bloomberg.com>.
[2] "Managing the Risk of IoT: Regulations, Frameworks, Security, Risk, and Analytics." *ISACA Journal*, 2017, pp. 19-16.

Systematic Failure

The operational risk associated with systematic failures has two primary focuses: IT system failures and information security failures. With IT system failures, a number of things could go wrong. There is the obvious risk which is having company technology stolen and used for malicious purposes, but there is also the possibility where a system is not properly created and something as simple as an unexpected transaction tears apart the system. The point of faulty software also relates to the potential for an information security failure, and is where much of Arrayent's potential for risk lies. Being a cloud-based service that interacts with many third-party clouds, there is a strong potential for a hack in one of the third-party clouds that can then be used to hack Arrayent's cloud. This method is essentially how Equifax's data was breached, and is a common occurrence with large companies that employ third parties. Back in September when it was announced that Equifax was hacked, it was made clear that it was one of Equifax's subsidiaries that was breached, giving the hacker access to all the data in the Equifax network. The event of a third-party hack is a circumstance we can be sure Arrayent has considered, but it is currently unclear what their risk mitigation strategy looks like for this kind of event.

External Fraud

Second, the primary operational risk associated with external fraud is phishing. Phishing has become more and more of a problem, especially in relation to elderly communities. When you think about who is primarily buying expensive appliances, and who is often pressured into buying "industry leading" technology, it is mostly the elderly, who are then even more of a target for phishing scams. Eric Carson, a researcher who in 2006 published a paper on the frequency of phishing in elderly communities, noted, "up to five million seniors annually are victims of some type of financial fraud."[3] In addition, those raised in earlier generations were often "taught to be polite and trusting," so when a scammer offers to fix their product, elderly are more willing to trust the scammer.[3] Meanwhile, elderly tend to be relatively new to the internet, so these scams are more likely to be effective when those targeted are ignorant to what is occurring. All of these opportunities to be phished represent large potential risks for the company to be hacked from the inside. These risks are difficult for companies to proactively mitigate without specific customer training sessions, which for most businesses are out of the question, and become a strong factor in determining what users have access to in any customer portal. Ultimately, the potential for external fraud should be a large factor in the cybersecurity needs of any company, and Arrayent is one such company where external fraud should be a top priority.

Internal Fraud

Finally, there are two primary operational risks associated with internal fraud: misappropriation of assets in response to an event, and insiders aiding fraudsters. Insiders aiding fraudsters is relatively self-explanatory. This would be a scenario where an employee, or even a group of employees, knows some vulnerability within company procedures, and gives this information to someone outside the company who is looking to gain access to data or break the internal system. We see many instances of this risk in the banking world, where employees find ways to smuggle money between the lines of a ledger, or help to clean money, for an external organization. Misappropriation of assets in response to an event can also be an incredibly dangerous problem, and is one that could take up its own short paper. The way in which a business responds to an emergency is incredibly important, and any negligence within the company at this stage could spell disaster. For example, last week Equifax was hacked for a second time, and there are surely investigations looking into misappropriation of assets. The fact that one of the three big credit firms was

[3] Carlson, Eric L. "Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow." *The Elder Law Journal*. 2006.

hacked twice in the span of three months is to be of large concern for customers, and should be a concern for management of the company. It is important to note that this assertion is just speculation, and there is currently no proof that there was any form of misappropriation of assets within Equifax or any of its related companies. The use of Equifax's press release is simply an example for where misappropriation of assets could be investigated, and again, there is currently no evidence that misappropriation of assets is present anywhere within the company.

Best Practices

With all of these potential operational risks in mind, what are some best practices for companies who want to mitigate or avoid these risks? Starting with internal ways to mitigate risks, controls are a great way for companies to manage procedures and can be implemented at many different places within the company. A few tried and true controls include: *directive controls* where things like IT configuration settings and corporate policies are managed, *recovery controls* where data backups are performed in the event of system failure, and *automated controls* where access permissions and password requirements are managed.[4] These are three basic controls to help prevent potential internal fraud, and there are many more ways companies can institute types of controls, so businesses should not feel limited by these three examples. If Arrayent were to implement a few of these techniques throughout their company, they would surely increase trust between themselves and their consumers.

Moving into ways to mitigate system failures, the best way to prevent IT issues and cyber threats is simply to design and implement risk mitigation strategies throughout the entire company, and not just in certain sectors. Again, system controls are a great way to manage some of the network activity, but the best way to avoid system failures is to design and implement a better system. Finally, external fraud. It is safe to say that there is no way to eliminate the potential for external fraud, and that the best way to handle the potential for external threats is, again, to have a robust internal structure capable of thwarting such intrusions Having strong internal software and procedures to manage risk are truly the best way for a company to handle threats from any front.

During the process of researching and writing this analysis, Arrayent was acquired by Prodea, an even larger cloud-based IoT service. Prodea's focus has been around creating "a generic framework with the ability to communicate with devices, move media, create interactive experiences for end users, execute service logic, and enable end-to-end service management and control."[5] Essentially, this acquisition has placed Prodea/Arrayent in a strong position to control much of the IoT service platform that, as we have seen with other businesses controlling large parts of any market, can be fantastic for creating a strong industry standard, but can also be a large organizational risk if the company is breached. One would expect that Prodea and Arrayent are currently working diligently to create new frameworks to manage both repositories of data, and hope that both companies prioritize the safety of customer data when designing any new systems.

Conclusion

As we have now seen, operational risks thwart every part of a business. Often, there is no way to completely eliminate a risk, so the best strategy is to try to prevent it and develop risk mitigation strategies that will be implemented throughout the company to be deployed in response to a risk. One can hope that there will soon be greater regulations enforced to ensure that companies are following more strict risk mitigation practices, but it is also important to recognize that general regulations are never one-size-fits-all. One can likewise hope that Prodea and Arrayent are successful in the merging of their two companies, and that their customer base will ultimately benefit from a strengthened cloud platform with increased security precautions.

[4] Searle, Annie. "Enterprise Risk Management." *Informatics 312, Autumn 2017,* Week #3A Slideshow, p. 7.

[5] "IoT Services Platform." *Prodea*. Accessed Nov. 2017 <www.prodea.com>.