Microsoft Xbox: Information Risk Management

Jacob John Williams, 15008632

1.0 Abstract

This document has been constructed to detail the possible threats to video game platforms, including an analysis of attacks on the infrastructure, such as intrusions and distributed denial of service attacks, but also insider threats, such as leaks. The purpose of this document is to guide the priority and implementation of information security practices and physical security implementations. After analysing previous incidents, threat actors and communities will be identified, then after this the threat will be measured using a combination of FAIR and the ISO series.

2.0 Introduction

The games industry is fraught with peril when it comes to information risk management. In the fourth quarter fiscal presentation (Microsoft, 2019) it was reported that the active user base of the Xbox Live service had reached 65 million, and the closest competitor Sony's Playstation network reporting through an official announcement (Sony, 2020) that it had reached 103 million monthly active users. With each user on the platform there comes new information, usernames, passwords, emails, addresses, and possible credit card information.

All of these details are sensitive, and as a result have need of being assessed for potential risk to them, as there is entirely the possibility of them being stolen whether it is via an external intruder or an internal threat. The users of such platforms trust us with said data and as a result we should be able to prove that said trust is not misplaced, and that they have the confidentiality they are owed. Furthermore, each user is a paying customer, and in the growing market of online platforms we should be able to guarantee the consistent availability of the online service we provide. This creates the risk of our online service lacking its availability.

This report will explore relevant incidents to the online games platform industry, delving into the intrusions suffered by our competitors and us in the past, from this we can derive who or what exactly it is that poses a risk to our platforms and what we can do about it.

3.0 Incidents

Perhaps one of the most high profile incidents in recent years is the 2011 Playstation Network hack, an incident that caused the service to be unusable for nearly an entire month, but also resulted in the theft of 77 million users personal data, which included names, addresses, emails, and passwords (Bonner, 2012). It was later added that Sony that possibly up to 12,000 credit card details had been stolen, albeit in encrypted form. The event was so catastrophically large that it caused the push for upheaval in how insurance policies should operate in regards to cyber information risk, with Connecticut Senator *Blumenthal (2011)* writing to congress demanding they apprehend those responsible and also audit Sony in order to find evidence of wrongdoing. Sony is widely criticised for its delay in response, a week of silence exists between the taking down of the Playstation network and the first announcement communicating the nature of the downtime. In the aftermath of the event, it was reported that it was "the biggest internet security break-in ever" by Reuters. Despite the initial silence and the overwhelming amount of data stolen, Sony was able to recover, bringing its service back up nearly a month later with *"additional security measures that strengthen against unauthorised activity"* (Sony 2011a). It is possible the reason Sony made such a remarkable recovery is due to its actions after the week of silence, after acknowledging the attack Sony was increasingly vocal about its current course of action releasing numerous public statements on actions being taken and actively taking responsibility. Additionally, Sony provided a "Welcome back campaign" that included a free month of their service and select entertainment products free to download (Sony, 2011b), and to address the credit card theft, Sony announced it would provide a free year of Identity Theft insurance for those affected (Sony, 2011c). It is believe that through these incentives and the transparency of Sony, that they were able to limit reputational loss. After the fact, Sony reported the outages had cost them 171 million dollars (PCMAG, 2011), however it is assumed this lacks the hidden damages that usually occur with the loss of personally identifiable information, as detailed by Deloitte (2016).

Briefly mentioned earlier, in an age where online services being constantly available is a must for financial and reputational success, it is no surprise that a considerable risk comes from the potency of a distributed denial of service attack. 2014 was a year full of such attacks, mostly performed by the infamous "Lizard Squad", who took down the Playstation Network, Xbox Live, and Blizzards BattleNet numerous times. For the most part the attacks are shortlived, being able to return the services in a couple of hours. One particular attack stands out amid the rest however, "Lizard Squad"'s attack on the Playstation Network and Xbox Live during Christmas day, which resulted in the services both being down for nearly two days (Daily Mail, 2014). It is fortunate that during the event the threat agents were extremely vocal in admitting they were the ones perpetrating the attack, as this led to mass reporting of the blame being with the hacker group rather than the platforms. Otherwise this event could have been extremely damaging, it is detailed in the FAIR model that the secondary loss factor of time can have a tremendous impact on loss, one could assume that if "Lizard Squad" had stayed quiet that the financial and reputational loss would have been significantly more severe than it was.

A more contemporary example of threats comes from the recent developments in the next generation of consoles, lead competitor Sony suffered a leak of the specification of its next generation console, the Playstation 5, and not

through any form of hacking. Whilst the credibility of the rumour around how the leaker acquired the data is questionable, the fact that the leaked specification line up with the official statement lends credibility. According to T3 (2019) the leaker was somebody who had *"been at a Sony meeting due to the nature of his work"* and sent messages containing the details to a friend, who then leaked the details to Reddit. Such a threat is what is usually referred to as an Insider Threat, where an actor within the company leaks information, usually for personal reasons. In the case of this leak, the leaking of data may be the best case scenario as the specifications were admirable. But the event that a leak takes place and the general reaction is negative could have disastrous effects, furthermore, insider threats have been known to leak things other than the details of upcoming products, things such as user personal details.

4.0 Assets and Personnel

One of the key assets we must acknowledge is actually a collective. The data centres that host Microsoft Azure and subsequently a significant portion of Xbox Live services and online game servers. These servers present perhaps the most risk of all assets, albeit in different forms. The data centres could come under numerous forms of attack, distributed denial of service, insider threats, and external hacking campaigns. All of these pose a significant possibility to breach the confidentiality, integrity, and availability of the platform and therefore must be of the highest concern when it comes to securing our assets, a lesson to be learned from Sony's PSN hack mentioned prior. If such an attack was performed on our system to a similar degree, the results could be devastating. This is why first and foremost one must focus on the securing of the network, but also the creation of a plan to recover and resurge in case such an event does occur. Within these data centres the assets of the physical security must be carefully considered, their placement and routine updating is critical to ensuring the security of data. Following this, the machines on these internal networks can pose a threat through unneeded high privileges and the programs utilised on them.

Furthermore, the personnel that work in the data centres or with systems related to them need to be identified and have appropriate actions taken to secure the operations they perform. Performing this will have a boosting effect on the overall security of the data centres outside of the physical security measures implemented within. Additionally, another type of personnel must be acknowledged as a fairly significant security risk, those being external personnel. Recently majority of the leaks have allegedly come from external contracts rather than direct employees. These differ slightly from the average insider threat in terms of how to deal with them and the difficulties dealing with them can create.

Another form of personnel one must consider are those that are required to be forward facing to the community, these personnel must be appropriately trained and informed of what explicitly can and cannot be said. Incompetency in this personnel can lead to accidental leaking, especially in the current atmosphere of journalists asking particularly probing questions in order to garner details.

5.0 Risk Analysis

In order to perform an effective analysis and combat of threats and risks, we will be drawing inspiration from different sources as they are relevant. There is no golden technique for identifying threats and risks and implementing controls, therefore combining them as deemed appropriate in the context of the industry is the most effective method for developing a system that works for us. In this case, we will be using the FAIR model (2005) to identify threats and risks, since FAIR has its basis in analysing threat actors, communities, estimating risk. Building from that, we will be utilising ISO270001 to determine implementable controls as it details broad spectrum controls that it deems relevant to every industry.

5.1 Threat Actors / Communities

Within the FAIR model it is useful to identify the types of people that could be affecting your system in order to discern possible threats and risks. Threat actors usually act for different reasons but often through the same mediums, through these mediums we can create what FAIR calls Threat Communities. By creating this categorization we can consider attack vectors and the differing ability and rationales of threat actors in the same threat community.

The first type of threat community to look at is an external one, that of cybercriminals. The cybercriminals threat community is extremely diverse and this presents a difficulty when analysing them. The rationale of cybercriminals we may encounter would be similar to that of "Lizard Squad" where the primary intent is to cause disruption and chaos, they have no external dependencies, their preferred target is infrastructure, and their target characteristic is whatever will gain them recognition. A deviancy of this type of threat community could be the community being motived by ideology, since "Lizard Squad" did claim via tweet to be attacking Sony at one point because of their *"endless cash flow"* and to *"end the greed"* (Naked Security, 2014).

Building from what was established in the Assets and Personnel section. There are numerous threat actors to be identified in the internal threat community of employees. The typical insider threat can come in two forms, the first being motivated by a need for revenge is more likely to want to cause damage to infrastructure than anything else, the possibility for collateral damage with this actor is high. The second is an employee motivated by financial interest, this actors target is data they can sell, this sort of attack is often precise and therefore doesn't present the same collateral damage that the previous does. Leakers can occur in any internal threat community, to the point where one could argue they warrant their own threat community. Leakers in the context of the games industry are rarely motivated by financial interest, but instead are motivated by indirect recognition for their actions or a form of revenge by leaking certain details that could put organisations in awkward situations. The final type of actor within the employee threat community are those that are forward facing, these are rarely motivated for malicious reasons, and leaks occurring from these individuals is often due to the lack of training or general incompetence.

5.2 Measuring Risk

The key risk to look at is the possibility of Distributed Denial of Service on the Xbox Live platform, therefore preventing users from utilising the service. In 2014, "Lizard Squad" was able to perform multiple DDOS attacks in a single year, but wasn't able to perform them consistently, often awaiting and planning the attacks for certain occasions. Due to this infrequency, the threat event frequency for this threat would be moderate, occurring between 1 and 10 times per year. Lizard Squad and the threats like them can be regarded as being skilled individuals, their attacks were coordinated and effective for the most part. The threat capability of a DDOS performed by a skilled actor is very high, such an attack can disrupt the key availability characteristics of our platform and therefore cause dissatisfaction in customers.

There are not many effective controls for preventing against DDOS. One is already implemented simply by geographical divisions, each continent has its own data centres and there can be multiple on a single one. This non-centralised format can mean that whilst one centre is getting attacked, traffic can be redirected to another. Or in the event that all the data centres in a region are attacked, only that region loses access. In order to attack all the data centres across the globe, the threat actor would need access to a botnet of previously unseen scale. The second most effective control for countering a DDOS event is an effective response strategy, having trained employees to respond to these sorts of events and communicating effectively with the community can limit reputational damage and return the service to working condition relatively quickly. Therefore, factoring the accepted level of risk and the controls we can evaluate the Control Strength in response to DDOS events as Very High (90%). Building from this we can discern the Vulnerability level as produced by the FAIR model as a moderate (60%) vulnerability. The events are significant and can be impactful, but with an appropriate distribution and response we can limit the vulnerability. The loss event frequency for such an event is therefore only moderate, whilst the event certainly has the possibility to incur substantial loss, the proper response and utilisation of controls should mean to limit the impact the event has financially or reputationally. Concluding, the probable loss magnitude of such an event if responded to effectively should only be moderate, perhaps costing around $100,000 in a significant event lasting 5 hours or more.

More analyses like this can be view in tabular form in Appendix A.

6.0 Evaluation of Methodologies

The FAIR model is effective in utilising a conjunction of quantitative and qualitative approaches to advising the gauging of threats and risks. Using quantitative measures with qualitative labels allows for the effective translation and communication of deep analyses to the decision makers in relatively simplistic and effective terms. Instead of trying to confuse and scare decision makers into performing certain actions it offers a more honest view of the ones perspective of the threats and risks. FAIR can be used with data or without it, it operates on the basis of formulating statistics for decision makers in fields where there "is a lack of good information" (FAIR, 2005), this was proposed numerous years ago however and now there is a significant amount of recorded data detailing the sorts of threats and risks companies can face. Luckily FAIR establishes that if in the possession of relevant data, you can use it to inform your analysis instead of estimating. Whilst the FAIR model presents a fantastic way to formulate threat and risk analyses, it does little to inform users of controls to be implemented, and where it does, is rather vague. This is where the BSI Standards ISO/IEC 27000/1 can be utilised, it offers essentially the inverse of FAIR. The standards detail Information Security Management Systems with a heavy focus on the implementation but no so much the identification and analysis of threats and risk. This isn't to say that there is nothing within the standards that detail threats and risk, the problem there in lies that it does not provide a particular method of quantifying them, and provides very little on anything like the concept of threat agents and communities. This is why the FAIR model was utilised to identify and analyse threats and risk, then the ISO/IEC 27001 was used to identify relevant controls. Using a hybrid of the two methodologies in areas they are strong in there in creates a stronger, unified implementation.

7.0 Conclusion

There is no way to totally erase the threats and risks that appear alongside your business, as almost all models will tell you, implementing controls is more akin to reducing the chances in which you will encounter the threat or risk, or reducing the impact they might have. But this in of itself is subject to opinion, within the FAIR (2005) model it details an entire section affirming the analyses of risk is impossible to make entirely objective, as human decision making is always fuelled by some form of subjectivity, be that in the analyses or the interpretation of the analyses. It is believed the analysis of events in this report is honest and truly reflects the risks and threats within the video game service industry. Something one must acknowledge however is that the threats and risks to video game services change as the perspective of the community changes, bad press can give rise to more threats from the hacking community and the release of new hardware can lead to the possibility of different kinds of intrusions. In finality, utilising a conjunction of methodologies in order to cover all of the strengths and weaknesses of each other appears to be the best way to approach information risk management, this way you can have in depth analyses whilst also complying to the international standards and all in all making your business safer.

8.0 References

Blumenthal, R. (2011) Letter to Congress, 28 April.

Bonner, L.B. (2012) Cyber Risk: How the 2011 Sony Data Breach and the Need For Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches. *Law & Policy* [online]. 40 (40), pp. 257-277. [Accessed 05 March 2020].

British Standards Institution (2017) *Information Technology - Security Techniques - Information Security Management Systems - Requirements (ISO/IEC 27001:2013).* London: BSI Group.

British Standards Institution (2017) *Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary (ISO/IEC 27000:2016).* London: BSI Group.

Daily Mail (2014) *Please let us Play! Thousands of Playstation and Xbox gamers who are STILL locked out of networks plead with hackers who 'ruined Christmas' to let them log on to games.* Available from: https://web.archive.org/web/20200306130533/https://www.dailymail.co.uk/news/article-2887270/Hackers-calling-Lizard-Squad-ruin-Christmas-gaming-fun-millions-taking-Sony-Playstation-Microsoft-Xbox-servers.html [Accessed 05 March 2020].

Deloitte (2016) *Beneath the surface of a cyber attack: A deeper look at business impacts.* London: Deloitte. Available from: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html [Accessed 20 February 2020].

GameInformer (2011) *[Update] Sony Confirmed Thousands of Credit Cards Stolen During Hac*k. Available from: https://www.gameinformer.com/b/news/archive/2011/05/02/thousands-of-credit-cards-stolen-during-second-sony-hack.aspx [Accessed 05 March 2020].

Microsoft (2019) *Fourth Quarter Fiscal Year 2019 Results* [press release]. 18 July. Available from: https://view.officeapps.live.com/op/view.aspx?src=https://c.s-microsoft.com/en-us/CMSFiles/SlidesFY19Q4.pptx?version=57904466-7e87-bcd6-1a59-9e4c5e26a761 [Accessed 06 March 2020].

Naked Security (2014) "Lizard Squad" hackers force PSN offline and Sony exec from the sky. Available from: https://web.archive.org/web/20200306124759/https://nakedsecurity.sophos.com/2014/08/26/lizard-squad-hackers-force-psn-offline-and-sony-exec-from-the-sky/ [Accessed 05 March 2020].

PCMAG (2011) *Playstation Hack to Cost Sony $171M; Quake Costs Far Higher.* Available From: https://uk.pcmag.com/news/106573/playstation-hack-to-cost-sony-171m-quake-costs-far-higher [Accessed 05 March 2020].

Reuters (2011) *Sony CEO apologises for data theft; shares fall 2pct*. Available from: https://www.reuters.com/article/uk-sony/sony-ceo-apologises-for-data-theft-shares-fall-2-pct-idUKLNE74505420110506?type=companyNews [Accessed 05 March 2020].

Risk Management Insight (2005) *An Introduction to Factor Analysis of Information Risk (FAIR)*.

Sony (2020) *PLAYSTATION™NETWORK MONTHLY ACTIVE USERS REACHES 103 MILLION* [Official Announcement]. 06 January. Available from: https://web.archive.org/web/20200306153156/https://www.playstation.com/en-us/corporate/press-releases/2020/playstation-network-monthly-active-users-reaches-103-million/[Accessed 06 March 2020].

Sony (2011a) *Playstation Network Restoration Begins* [Official Announcement]. 17 May. Available from: https://web.archive.org/web/20160212074828/http://uk.playstation.com/psn/news/articles/detail/item369506/PSN-Qriocity-Service-Update/ [Accessed 05 March 2020].

Sony (2011b) *Some Playstation Network and Qriocity Services To Be Available This Week* [Official Announcement]. Available From: https://web.archive.org/web/20200305175323/https://blog.eu.playstation.com/2011/05/01/some-playstation-network-and-qriocity-services-to-be-available-this-week/ [Accessed 05 March 2020].

Sony (2011c) *Sony Offering Free 'AllClear ID Plus' Identity Theft Protection in the United States through Debix, Inc.* [Official Announcement]. Available from: https://web.archive.org/web/20200305183545/https://blog.us.playstation.com/2011/05/05/sony-offering-free-allclear-id-plus-identity-theft-protection-in-the-united-states-through-debix-inc/ [Accessed 05 March 2020].

T3 (2019) *PS5 tip-off reveals consoles insane power as "Sony meeting" infiltrated.* Available from: https://web.archive.org/web/20200306151119/https://www.t3.com/news/ps5-tip-off-reveals-consoles-insane-power-as-sony-meeting-infiltrated [Accessed 05 March 2020].

9.0 Appendices

Incident	Threat Event Frequency	Threat Capability	Controls	Control Strength	Vulnerability	Loss Event Frequency	Probable Loss Magnitude
Distributed Denial of Service Attack	Moderate: 1 - 10 incidents a year.	Very High	Response Strategy Geographic Distribution	Very High (90%)	Moderate Vulnerability (65%)	Moderate (50%)	Significant ($100,000+)
Critical Network Breach / Vulnerability	Very Low: One event every 10 years.	Very High	Response Strategy. Event Logging (A.12.4.2). Admin and operator logs (A.12.4.3). Controls against Malware (A.12.2.1). Restrictions on software installation (A.12.6.2). Network Controls / security / segregation (A.13.1.1/2/3).	High (It should be assumed the top percentile of threat actors would be using zero days, therefore intrusion detection may prove to be reactive rather than predictive)	High (80%)	Very Low (Such an event should rarely occur, despite this events will almost always result in significant loss)	Severe ($10,000,000+)
Product leak (Insider)	Low (Such leaks only usually occur leading up to announcement)	Low (previous events have appeared to be opportunistic)	Screening (A.7.1.1) Terms and conditions employment (A.7.1.2) Information Access Restriction (A.9.4.1) Physical Entry Controls (A.11.1.2)	High	Very Low	Very Low	Very Low / Negligible
Product leak (Community Facing Employee)	Low (See above)	High (Reporters are trained to probe information)	Classification of Information (A.8.2.1) Labelling of Information (A.8.2.2) Confidentiality or Non-disclosure agreements (A.13.2.4)	High	Very Low	Very Low	Very Low / Negligible