Splash's Berwick Vulnerability Assessment

MIS211 – Cyber Security and Governance

Disclaimer

This report, including any recommendations contained therein, was prepared for the purpose of academic assessment in Deakin University's unit:

- MIS211 – Information Security, Governance and the Cloud.

It should not be relied upon or used in any way as a basis for making any "real-life" commercial decisions.

The assistance of **Splash's Learn to Swim- Berwick** in providing us with access to its staff and records in the course of researching the report is gratefully acknowledged.

Dept. of Information Systems and Business Analytics
Deakin Business School, Faculty of Business and Law
Deakin University

LETTER OF CONSENT
MIS211 – Assignment – INFORMATON SECURITY MANAGEMENT REVIEW REPORT

Dr Graeme Pye
Dept. of Information Systems and Business Analytics
Deakin University
1 Gheringhap Street
Geelong 3220
Phone: (03) 5227 2312
Email: graeme.pye@deakin.edu.au
01 / 08 / 2023

Dear Graeme,

I/we hereby give permission for the following students:

Bruce Rachon
Juned Khan
Jack Perry

to review the IS security Management aspects of our business organisation:

Splash's Learn to Swim - Berwick

In order to fulfill the Assignment requirements for MIS211.

I/we have read the Assignment requirements and understand that the students will behave responsibly and professionally in this review at all times.

I/we expect to receive a copy of the final assignment report, containing the results of the review, during the week beginning 18th September 2023.

Yours sincerely,

..... (Signed)
LAURA SIM ..... (Please Print Name)

Executive summary

This report and the interviews which were held for it revealed many poor practices which are currently used at Splash's Learn to Swim. These findings suggest a potential high-risk environment for their data, which includes both customer and staff information.

Splash's has access to personal information of staff and customers; this needs to be protected to keep data safe and secure. Through the interviews we found that they do not follow a particular IS security procedure which allows them to protect their data and know what to do in case of an attack. There were many issues found that can have devastating results such as a vulnerability to phishing emails, poor password practices and sharing accounts to name a few regarding their practices on devices.

These software problems coupled with their physical assets and practices to keep them safe are inefficient and unsafe. Splash's needs to adhere to an IS policy such as the ones suggested by the ACSC where they can focus on the essential eight model to keep their business safe.

Although the findings point to many problems which could be considered high-risk, with that in mind this report discusses the implications of poor practices and the mitigations which can be put in place to stop and prevent potential attacks.

Table of Contents

Introduction

This information security management review was conducted at Splash's Learn to Swim – Berwick, to increase the awareness of staff regarding the security of their data for both staff and clients. The business offers swimming lessons for all age groups, with classes ranging from either private, semiprivate or group settings. Our aim is to provide management with what we believe to be vulnerabilities in their

network, and how to mitigate them to create a safer environment for data to be stored and therefore, create a stronger security model for their business.

This report will contain findings related to data-handling, access control, knowledge of their security policy and potential threats which can violate said security. In addition, our recommendations on how they can implement better practices that can impact data.

Report body – Business background and context

Business profile and services provided

Splash's Learn to Swim was founded in 1988 with the goal of enhancing the survival skills of their students and teaching a lifelong love of water. With over 30 years of experience in the aquatic industry, they have gained a very high reputation amongst other swimming schools.

Splash's offers weekly half-hour lessons to people of all ages, whether it is for beginner level swimmers or higher. To ensure clients get the most out of their lessons, teachers follow a lesson plan. These range in difficulty based on the level of student or the theme of the week, whether it is to challenge students, reinforce their skills or to instill in them an understanding of water-safety. It is important to note that these lesson plans are the intellectual property of Splash's and are unique to them as a business.

Mission and vision statement

Splash's Learn to Swim – Berwick has a mission statement, which is, "to provide children with a life-long love of swimming". This is a vision that is delivered by a large staff team including teachers, assistants, customer service team, help desk team and a management team. All teams work cohesively to ensure the quality of lessons offered to customers is of the highest standard.

Strategic objectives which can influence IS security strategy

Splash does not currently have any strategic objectives which influence their information security. However, protecting athletes, customer, and employee's data, keeping a competitive edge, increasing customer engagement through safe digital experiences, and disaster planning can be some of the key goals. Although for a small level business or sports organizations additionally essential may include compliance, cyberthreat prevention, security training, third-party risk management, and innovation. It is important to consider reputation management, cost control, scalability, incident response, and sustainability. It is essential to customize based on the organization's size, finances, risks, and to regularly analyze and modify as threats change.

Organizational resources which may influence IS sec strategy

Splash's utilizes a lot of resources which can impact their information security. They have a lot of hardware inside of the building, including desktops, tablets, personal devices (Phones & Laptops) and open server racks (located in the manager's office).

When customer service is performing tasks which require the usage of customer data, they use UDIO which is a class scheduling management system software. It stores information related to customers and staff. When it comes to managing their intellectual property, they are thorough and keep very few digital copies to ensure its integrity.

Upon completing the interview, we found many common practices in the office which left much to be desired in terms of security. Though they do have a good grasp of data encryption, their practices regarding password management and security were lack-luster. Additionally, their lack of access controls for staff and having no distinct usage of authentication overshadowed the positive practices.

Though resource constraints are evident in small sports organizations when compared to larger equivalents, essential resources have a considerable impact on Information Security (IS) policies. Financial resources, staffing expertise, technology infrastructure, data assets, vendor relationships, physical security, regulatory knowledge, alignment with strategic objectives, leadership commitment, risk assessment tools, incident response planning, security training, testing, insurance coverage, legal support, reputation management, and environmental considerations are all examples of these. Due to limits, efficient resource allocation and personalized tactics are critical for maintaining effective IS security while remaining cost-conscious and flexible to organizational needs.

Report body – IS Security Management Review/Analysis

Does the business have formal or informal IS policies or procedures to follow

Australian businesses must meet requirements when it comes to cyber security. These depend on the size of a business, however there is a rather easy step businesses can take, which is to look at the policies presented by the ACSC. The Australian Cyber Security Centre has made many documents available to help small to large businesses, with the essential eight model of cyber security being a rudimentary checklist. This model is what should be considered the bare minimum to keep data secure.

Small and medium businesses like Splash's "make up 98% of all Australian businesses," according to the Australian Bureau of Statistics. Now more than ever the need to keep strong policies and procedures for cyber security is integral to keeping customers and a business safe. Cyber threats and attacks are only getting more frequent which means more data being stolen. Consequently, the need for strong IS security policies is imperative for all businesses.

Upon completion of the first interview, the facts point to Splash's having more of an informal IS security policy rather than a formal one. Having a formal IS security policy should be a focal point for any business, so it came as a surprise to learn of the practices and procedures in their workplace.

It has become clear that Splash's does not possess any formal procedure or framework regarding the security of their data which is stored on site. However, the opposite can be said when it comes to their client data, which is stored in a third-party cloud service. The use of UDIO is a great step for them as a business, as it is a secure cloud service which has up to date encryption standards offered on AWS. The client data and staff data are stored there, so when our team asked if they had MFA enabled on UDIO, we were quite surprised to hear it was not the case.

When it comes to small and medium businesses, they must follow the essential eight of cyber security, MFA being one of the eight requirements to keep a business secure. Upon further investigation, the computers which are available to work on for customer service often have shared accounts. Their password manager allows auto-filling the password once a recognized email is entered which could lead to an attack.

Upon further questioning and research into their business practices and getting access to some of their software, we found that some of their operating systems and applications were out of date and not secure. It seems that their practices regarding email filtering are nonexistent as they are currently receiving phishing emails - where the only safeguard is to rely on the common sense of an untrained employee, when the context regards information security. With new employees being trained, it is likely that a mistake will be made sooner rather than later.

This leads to another section of the essential eight provided by the ACSC, which is restricting admin privileges. Currently most staff members have access to data/information they should not be privy to, hence it is important for Splash's to follow a good procedure regarding their privilege management. Due to the attempts to attack the business through phishing, it would not be impossible for someone to gain access to important data due to the lax privilege controls implemented by Splash's when using UDIO.

The informal policy which they follow is to "call the IT guy". This is highly impractical as they rely too heavily on an individual instead of following a process to prevent an attack, reacting to it and reporting the attack. This process should be something that the staff should be trained to do or at least be made aware of actions that can be taken to mitigate potential threats.

To reiterate, Splash's does not follow any formal procedure by having poor password practices, lack of phishing email filtering and reliance on an individual when they do encounter a problem, to name a few. This informal policy is problematic and creates vulnerabilities in how they use their platforms. Having standards such as this can and will cause problems if exploited and the implications of this are dangerous.

If there is no strategy discuss the implication of a lack of strategy

In case of an attack, they would be left clueless, defenseless and most likely would not be aware an attack is happening. If they don't have a plan for the safety of the data and systems in the event of a cyber breach, it could be very damaging even for a small business. For protection, mitigation, and recovery, they need a clear plan. Consequences include uncoordinated responses, data theft, system downtime that lasts too long, financial loss, repeated attacks, low employee morale, and hard to recover from. Hackers could ask for money in return for decrypting data or stopping future attacks. Paying the ransom doesn't mean you'll get your info back, and it can lead to more attacks. Fines and legal action may result from breaking data protection laws.

To avoid these, organizations should create a complete cybersecurity strategy that includes prevention, incident response plans, training, audits, and constant monitoring. Small changes like changing Wi-Fi host passwords, different network connection of all physical and software security, not letting unknown individuals access places they should not, monitoring the business website, will also contribute to a great length. This will help the organization to lessen the impact of any attack. The main goal of cyber security

is to use multiple layers of protection and best practices to make it very hard for attackers to break into the system or get private information as no system is 100% secure.

Review security related measures, training, technologies and processes in place and/or identify any that may be missing

Splashes successfully implemented some security measures and organizational processes to protect their network and consequently employee and client data. While there are some security practices evident, these can be modified to prove more effective as well as implementing additional measures to protect against common small business threats and vulnerabilities.

Measures

All desktops and devices (tablets, etc.) are password protected, offering some form of security against intruders; however, poor password practices are evident. Password/account sharing creates inaccurate logs making it more difficult to identify or resolve an attack. Additionally, all company desktops are accessible via shared login credentials creating a single point of vulnerability for your system. It is suggested Splash adopt a need-to-know security approach, restricting employee access to systems and processes unless necessary to complete their job. Furthermore, it is suggested that all employees who require access to company desktops are provided individual accounts with unique login credentials as well as account restrictions relevant to their job requirements (i.e., employees should not have access to firewall settings unless necessary). Additionally, Splashes are encouraged to individually password protect and/or encrypt valuable desktop files and folders. This adds an additional layer of protection to valuable data in the event of a desktop breach. Next, passwords should not be stored in any physical form where they could be observed and therefore compromised. This creates a large vulnerability in your system, exacerbated by the singular admin desktop account. Alternatively, Splash's employees could use a secure password manager to store and easily access all personal passwords; eliminating the need to write passwords on paper as well as creating complex passwords without concern of forgetting them.

Training

Splash's shows little to no evidence of IS security training processes implemented within the workplace. While cyber-security is not the focal point of the organization, it is important to promote awareness on the topic and educate staff to protect themselves and the business accordingly. It is suggested that Splash incorporate discussing organizational IS security practices and potential threats into their employee induction process to begin promoting organizational awareness. Additionally, it is suggested that Splash hold a cyber-security short training course for current staff, educating them on immediate security measures to implement and threats to be aware of. Splash's are also advised to hold regular team meetings – physically or virtually – where a nominated staff member can discuss common/recent security threats and mitigation techniques, new and upcoming cyber-security standards, general potential security improvements and answering staff questions. Alternatively, to cater to the schedule of a small business; this task could be delegated to a smaller security team or third-party organization who in turn relay this information, summarized, to the workplace. If team meetings are found to be

impractical, Splash's can implement a third-party online service providing employees with weekly online modules regarding relevant cyber security information to promote awareness and education.

Technologies

Splash's uses UDIO; a secure third-party cloud-based software which encrypts data to handle sensitive personal and financial information. This does a good job of securing information once stored within the database, however there are few measures in place to prevent unauthorized access to the UDIO software. Additionally, Splash's implements physical security technologies such as security cameras, door locks and an alarm system to restrict access to their hardware. It is however encouraged that Splash's review the effectiveness of these measures – both immediately and regularly – ensuring equipment is working, cameras are pointed at vulnerable areas and appropriate bodies are alerted when the alarm is activated.

To further secure their system it is encouraged that Splash's implement the following changes:

- Configure firewalls on desktops.
- Install anti-virus software on desktops.
- Implement anti-phishing software on browsers.
- Enable Secure Socket Layer (SSL) on server.
- Implement Multi-Factor Authentication (MFA) where possible.
- Install + configure Wi-Fi cameras which can be viewed remotely.
- Update security configurations on all company IoTs.

Implementing the above changes will aid in mitigating vulnerabilities in your system protecting against malware, phishing scams and eavesdropping attacks. Moreover, updating and regularly monitoring physical security measures will limit adversaries' ability to physically access your system.

Processes

Splash's currently has limited effective security processes in place. Firstly, all employee credentials are manually deleted from the system by the Human Resources (HR) manager after termination. While this is an effective process, it is prone to human error. It is therefore advised that Splash's automate this process to ensure this vulnerability is handled in an effective and timely manner. Splash's provide all employees with UDIO access, an individual account contributing to accurate logs and limiting unauthorized access. Splash's are however advised to enforce minimum password requirements and annual password updates as regular security processes within their organization. Additionally, Splash's are encouraged to adopt a separation-of-duties approach to security, ensuring no one individual has enough access to jeopardies the system. Separating duties increases effectiveness in identifying and resolving an attack as the nature of the attack will be linked to a specific employee's job role.

History of breaches

A cyber breach is defined as unauthorized access to computer systems that results in data compromise and the potential for financial, reputational, and legal harm. Although, Splash's does not have any history

of breaches but, according to Australian bureaus of Statistics (2022), Small and Medium Businesses (SMBs) make up 98% of all Australian businesses out of which 62% of Australia's small and medium businesses were affected by cyber-crime in 2022 and a further 60% of those businesses went out of business within 6 months of being attacked.

Assets and data which could be exposed

The title refers to the potential dangers of data exposure and the need to adopt secure procedures. These threats apply to a range of resources and information, including social media accounts, servers, computers, tablets, and internet connectivity. Unfortunately, because passwords are frequently kept on actual paper documents, the security of these assets is compromised.

Splash's use AWS-standard encryption for both customer and employee data, together with third-party data protection technologies like UDIO, to strengthen their security procedures. Insider risk, specifically unhappy employees who may endanger the security of the data, is a recognized threat.

Billing is a crucial step in financial management, but to effectively reduce risks, it must follow strict financial security rules. To put it simply, unauthorized access to UDIO accounts could have a significant financial impact on the business.

Our concerns also include assets like our company website, social media channels, personnel records, office supplies, paper-based financial records, and HR information.

In short, our study shows how important it is to deal with possible risks of data exposure by using safe practices. These practices include keeping passwords safe, making sure data is better protected, and being aware of the financial risks that come with not having enough security in different parts of our organization's processes and data assets.

ALE – Annual Loss Expectancy

Hardware ALE's

Asset	Threat	Impact	Frequency of Occurrence	Annual Loss Expectancy	Risk Priority
Intellectual Property	Theft/Damage	5	3	$33,333.34	1
Password Practices	Phishing attack	4	3	$3,333.333...	3
Physical Infrastructure	Vandalism	5	3	$33,333.34	2

Intellectual Property

Poor safe-keeping practices regarding their intellectual property leaves them vulnerable to theft, whether it is a disgruntled employee or an insider acting on behalf of a competitor. As there are no safeguards, they are highly vulnerable.

Password Practices

Poor password practices leave the company vulnerable to phishing attacks, employee data breaches and insider attacks. Since desktop documents are not protected beyond desktop passwords, a system breach would leave the majority of employee and company data vulnerable.

Physical Infrastructure

It is very important for an organization to protect its physical infrastructure. It keeps things running smoothly, saves valuable assets, and makes security better against possible threats. When a business doesn't take care of its physical protection, it leaves itself open to disruptions, data breaches, and financial losses.

Software ALE's

Asset	Threat	Impact	Frequency of Occurrence	Annual Loss Expectancy	Risk Priority
Website	DDoS	2	3	$33.33	4
	Data Breach	2	3	$33.33	3
UDIO	Insider Threat	3	3	$333.33	2
Server Rack	Damage/Sabotage	4	3	$3333.34	1

Server Rack

The protection and location of the server rack is minimally safe, it is open and could lead to an accidental attack by spilling liquid or stepping on the cables. The location is right next to a window which could lead to it being stolen if a potential threat actor wanted to take it.

UDIO

Splash uses Amazon Web Services (AWS) to host UDIO. AWS offers strong security by encrypting data and hashing passwords. But protecting UDIO means improving the way Splash uses passwords to stop possible threats and protect the integrity of private data.

Website

Websites generally serve as the face of a company and the entry point for many customers. Although Splash's website doesn't hold sensitive information, it functions as a symbol of the company and damage could potentially discredit the organization.

Information Security Management Recommendations

Password Practices

Passwords are an especially vulnerable area for Splash's. As passwords typically act as the first line of defense against an adversary, it is crucial they are as secure as possible. Poor passwords practices such as

short or common words, re-using and sharing passwords or writing passwords on paper all contribute to an overall significant vulnerability. If necessary, passwords should be stored within secure password management software, eliminating the need to write them anywhere they can be observed and potentially misused. Additionally, passphrases should be used in place of passwords where possible thereby protecting against common password hacking malware. **UDIO**

Splash's chosen cloud-based software; UDIO, is hosted by Amazon Web Services (AWS). AWS employs high level security measures such as data encryption in transit and rest, password hashing and browser/network security. While UDIO effectively employs security methods it's important that Splash's organizational password practices are improved to limit an adversary's ability to infiltrate the software.

Website

Splash's website uses a secure Internet Protocol (IP), HTTPS, to enable the secure transmission of data over networks. While this provides users with a secure browsing session, there are no security measures evident protecting against targeted Distributed Denial of Service (DDoS) attacks. In the event of a website attack, the time taken to identify and resolve the issue could damage the brand image indefinitely. Splash's are therefore encouraged to implement a Web Application Firewall to monitor and filter malicious network traffic.

Physical Security

Splash implements basic physical security measures, however, can improve on these to provide a stronger first line of defense against attackers. Splash should consider:

- Testing all cameras are working and pointed at access points (i.e., server rack, desktops, front door, etc.).
- Install Wi-Fi cameras with remote access.
- Ensure the alarm system alerts the appropriate authorities immediately.
- Secure sever rack to prevent accidental damage and mitigate intentional damage.

Although data is typically stored digitally, the physical protection of these vulnerable devices should not be overlooked. Introducing the above changes will not only limit an attacker's ability to access your system but additionally aid in identifying and resolving any incident that takes place. **Server Rack**

Splashes server rack appears to be an overlooked vulnerability within the organization. There are little to no security measures preventing accidental or intentional damage which could have major implications on Splash's ability to access data (OneDrive) and operate effectively. Moving forward, Splash should consider limiting employee access to the server rack as much as possible, preventing the possibility of any accidental damage. Furthermore, Splash can consider installing a protective barrier and/or gate around the server, further limiting accidental and intentional damage. Alternatively, Splash could consider moving the server rack in its entirety to an inherently more secure location. This would limit and/or eliminate the need to implement previously mentioned security measures. **Intellectual Property**

Splash's create their own unique and invaluable lesson plans which ultimately form the curriculum they follow. Given their unquantifiable significance, the security of these lesson plans should be a focal point

of the company. While storing these documents in physical form does alleviate the stresses of a cyberattack, it also requires the appropriate physical security measures to be implemented. Firstly, Splash are strongly encouraged to store these files in a secure and restricted location (i.e., locked manager's office). This not only limits customers' potential to access them, but further limits the potential of an inside attack. Additionally, Splash are advised to store their lesson plans within a secure and lockable storage system, further mitigating any vulnerabilities.

NIST Framework Recommendation

Small companies that want to improve their security practices can learn a lot from the NIST Cybersecurity Framework. As explained in the NIST "Cybersecurity for Small Business," framework is a complete way to handle cybersecurity risk. First, the framework focuses on how important it is to keep track of all the business equipment, software, and data, as well as to set up clear cybersecurity policies, such as defining roles and responsibilities and making workers more aware of personal and workplace risks.

Additionally, small businesses are told to protect their systems by controlling network access, using security software, encrypting sensitive data, making regular backups, and making sure software is up to date. Detection systems are important, and they need to be constantly checked for unauthorized entry, devices, and software. Any unusual network activity should be investigated right away.

Further, businesses should make a strong response plan that includes alerting the right people, keeping business running, reporting incidents to the authorities, and changing cybersecurity policies based on what they've learned. Lastly, if there is a cybersecurity incident, quick recovery should focus on fixing the systems that were affected, keeping stakeholders aware, and getting things back to normal. By using these frameworks, small businesses can greatly improve their cybersecurity, keep sensitive data safe, and deal with potential threats in a good way.

Conclusion

In conclusion, our assessment of Splash's security standing shows that their security management has serious flaws. The organization faces big risks because it doesn't have official IS security policies, uses bad password practices, and doesn't filter emails well enough. Our suggestions include using strong passwords, making UDIO more secure, making the website more resistant to DDoS attacks or any kind of attack, and better physical security. Also, using the NIST Cybersecurity Framework will give them a complete plan for keeping their processes safe. In an increasingly dangerous digital landscape, urgent action is needed to protect sensitive data and reduce possible threats. This will protect Splash's reputation and ensure its long-term success.

Appendix A

References

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, *10*, 85701-85719. Splash. (2023). *Berwick Swim School.* Splash. https://www.splashs.com.au/berwick/

NIST. (2018). *The NIST Cyber Security Framework*. https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurityframework/cybersecurity_sb_nist-cyber-framework.pdf

UDIO. (n/a). *Make Waves with Class Management Software*. https://www.udiosystems.com/businesstypes/swimming-schools

ACSC. (n/a). *Essential eight*. https://www.cyber.gov.au/resources-business-and-government/essentialcyber-security/essential-eight

ACSC. (n/a). *Small Business Cyber Security Guide*. https://www.cyber.gov.au/resources-business-andgovernment/essential-cyber-security/small-business-cyber-security/small-business-cyber-security-guide