IT Risk Assessment Case Study

Contents

Executive Summary

Aztek is a financial services organization from Australia. The company is facing major challenges in IT infrastructure management because of rising costs. The company needs to hire more employees for management of the growing business and in that case, the costs would raise more. In order to save on their IT infrastructure costs, the company is planning to adopt Bring-Your-Own-Device which would allow new employees get their own devices thereby reducing the cost of procurement and maintenance in IT systems for the company. However, with this adoption, the security posture of the company would also get affected. This report would assess the security posture of the company and the impacts of BYOD on the same with an objective to identify and assess the potential risks with the new posture so that steps can be taken to improve it as per BYOD needs.

The report would first explore the security risks faced by finance industry and the best practiced used for protecting IT systems from these security risks. It would explain the impacts of risks on IT projects and would explore how industrial or government compliance procedures can affect these projects. This would include considerations of industry standards like Workplace Privacy Act and processes used for surveillance. Understanding of standards would help identify governance practices that can be used for strengthening the security posture of Aztek post implementation of BYOD (Engine Yard, Inc., 2014).

The report would explore the vulnerabilities and risks that Aztek is likely to face with the deployment of BYOD devices in the system including mobiles and tablets. It would also identify methods that company can use to protect its assets from these risks (European Commission , 2010).

To identify the right cause of action, it is essential to understand the risks and their impacts. For this, cyber security framework would be used which help in identification of methods for assessing security risks that Aztek would would be exposed to. The framework would help form a risk profile of the company, understand security posture of Aztek, and develop an improvement plan for the company. The cybersecurity framework identifies five core functions of security systems that include risk identification, protect company from them, develop response plan and identify recovery strategies. For every risk category or subcategory, specific security measures can be identified (National Treasury, 2011).

For assessing how security risks would affect Aztek, the industry data about BYOD would be analyzed and protective measures used for such systems by other companies in the industry would be explored such that appropriate security measures that can be used to enhance the security posture of Aztek can be identified.

Project Review

The project involves implementation of a BYOD system in Aztek which is a financial organization from Australia. The company is facing financial challenges and is looking for saving IT costs by allowing personal devices of new employees to be used for the purpose of business. Thus, the company has decided to adopt BYOD systems but this approach is likely to modify the security posture or the organization. To remain safe from cybersecurity risks, company would need to strengthen its security systems to suit the security needs after BYOD adoption. The project would involve development and implementation of BYOD scheme (ACHS, 2013).

With implementation of the BYOD scheme, some regulatory policies and procedures have to be followed. Australian Capital Territory of Australia is one of the main areas where regulatory policies are defined. At the organizational level, policy based surveillance can track employee communication such that the management would know how employees are using their systems and if their usage patterns are secure for Aztek (GILBERT, 2014).

There are also some laws at the state, federal and territory levels that have to be followed when concerning employment in the organization. At the organizational level, Aztek can install access control systems on the devices used by users such that the employee communication can be tracked and monitored. This would help Aztek ensure that the confidential data of the company is not shared by employees outside the company. A cover surveillance can be launched on employees which would allow company to track the suspected employee after 14 days notice given (APM Group Ltd, 2017).

NSW Act is one such act which is created for governance of employee management practices. As per this act, employee activities can be tracked including sending and receiving of files or messages but only on the official accounts. The personal accounts and the resources used by employees may not be tracked (Afaq, et al., 2014).

Another useful act is Telecommunications (Interception and Access) Act 1979 . This act talks of the interception by companies on the employee communication between two employees which is done without the knowledge of both employees. The act allows employers to see the content that is being exchanged but not the related personal information such as email addresses, communication time, and the metadata. The way this interception can be carried out is highlighted in the section 5F of the telecommunications act. This provides protection to the employers but only to some extent (Berg, 2010).

A usage policy can be created for IT assets in the BYOD scheme which is formulated as per the rules defined in the regulatory acts which would include considerations of types of surveillance, methods of tracking, and span of interception The Privacy Act (APP 5) suggests following statements can be included in such a policy (Alali & Yeh, 2012):

- The company must have the right to see the content that is being transferred between two employees using official emails
- Employer must not record any personal communication happening between employees through informal methods like chat
- Employees must be aware of the information that is open for the employer to see.

- Certain procedures and access rules can be defined for personal communication
- The company should have defined procedures that would be used for reporting data inside or outside the organization (GILBERT, 2014)

Security Posture of Aztek

With the introduction of the BYOD devices in the Aztek IT network, the security posture of the company would be modified as the private devices of the users would now be connected to the critical infrastructure of the organization. There would be added risks because of addition of BYOD which would change this posture. Thus, the company needs to make considerations for these risks while defining security management strategies for the IT systems of Aztek (Avdoshin & Pesotskaya, 2011).

Finance industry poses some barriers to implementation of BYOD as security risks are higher in the cases. To manage these risks, industries and regulatory bodies in various countries have identified certain security procedures and Aztek needs to follow them for enhance protection. However, regulatory bodies also has certain mandates that would make it difficult for Aztek to keep a high level of control over the mobile devices used by its employees especially when they would be used outside the corporate network. The companies in the finance industry use certain protection measures for BYOD devices such as (Oracle, 2009):

Securing Mobile Devices: Earlier, company had given mobile phone devices to its employees and these devices were procured from the same manufacturer and thus, had same make and features. This made it easy for Aztek to create a unified interface for controlling all the devices remotely and establish standard usage procedure. With BYOD devices in the IT infrastructure of the company, the device configurations make and features would not remain same but would vary significantly and thus, a single unified system cannot be used for controlling or securing these devices (ACHS, 2013). The company would need to consider the change device portfolio while defining security strategies for mobile systems which would be more challenging. The earlier system used for security by Aztek would no longer be able to support the multiple devices belonging to different users who could be having different settings used and applications installed. The current device management system of Aztek would not be sufficient as it would not be able to manage the vulnerabilities and thus, a new measure is needed (Bodicha, 2005).

Aztek can lock the mobile devices for personal uses such that employees would not be able to misuse those posing threats to the security of company's infrastructure. However, this would discourage employees from using their devices if they would not have freedom of usage of their own deice. Thus, a new approach that is acceptable to both employers and employees has to be arrived at (Bhatta, 2008).

Some risks can be faced predominantly in case BYOD devices are used as the part of IT infrastructure of Aztek such as lost or stolen devices, physical access gained by a non-company person, lack of awareness of security implications leading to misuse of devices by employees, and more. If the devices are lost or stolen, any one getting the device can use it for connecting to the company network through VPN which would make it also possible for the user to gain access to the confidential information of the organization which can be dangerous for the company. In such cases, security can be enhanced with pass encryption but even that can be cracked at certain stage (APM Group Ltd, 2017). Thus, the company needs to have a system in place which allows remote wiping of the device from the company network so that the user would not be able to connect to organizational applications remotely. This would reduce the chances of damage from the stolen device (Rule Works, 2017).

There could also be instances that attackers get the device in hand inside or off the office premises in which case, the risk would be even more. In the case, the device used is old then the security threat would rise even more. As the device has been chosen for office use by employee, the company would not have any control over the device age, specifications or configuration settings unless a BYOD policy defines a minimum configuration that a device must have to be used for the official purpose by the employees (CDC, 2006).

When employees are using their own personal devices, they want to have more control over it than the company which is why they may change the settings suggested by company to enjoy freedom of usage. This can result into disabling of some essential security feature thereby increasing risk to the employer. An employer may not have the awareness of the change and can fall prey to security hassles because of reduced protection level (Campbell, 2005).

Some key measures can help company enhance its security posture with the use of BYOD devices such as:

- Identification of risk scenarios for each device considering its configuration
- Use of device management for enforcing security policies (Afaq, et al., 2014)
- Using industrial security standards like data encryption, remote wiping, and communication interception
- Establishing a baseline for installation of software and use of operating systems on the mobile devices used by employees (Chan, Lam, Chan, & Cheung, 2008)

Managing Application related Risks: If malicious software applications get installed in the mobile devices due to some mistake of an employee or by others having access to the device, it would risk the security posture of the company as the hacker can launch attack on the critical infrastructure of the company by connecting through VPN using the device. Every device that is configured in the corporate network must be protected with an anti-virus and anti-malware for which the company can include mandatory measures for their installation in the company policy (Alali & Yeh, 2012). Moreover, it is essential that the devices are managed well by the users failing which the company would face larger risks. Compartmentalization of the company data on devices can help reduce risks further (HP Enterprise, 2015).

Managing mobile environment: The mobile devices must be updated and patch regularly by the users. However, users may not be very particular about such needs and thus, company needs to take the responsibility by sending notifications, updates and reminders to the employees using BYOD devices for regular updates. This would make the environment safer for the company as the updates would patch any new vulnerability as per the increasing threat scenarios (Curtis & Carey, 2012).

A supportive usage policy may be defined by Aztek for the use of mobile devices by employees for the official purpose which would define patching as mandatory procedure to be followed in certain time. Moreover, self-service solutions given to employees for patching or getting support from technical staff of the organization can also help further (Avdoshin & Pesotskaya, 2011).

Risk Assessment

The framework used for managing security in the cyberspace defines certain practices that are cost-effective, reusable, performance based and cost effective. These practices have been identified by a team of security experts and industry professionals working on security systems (Paschke, 2014).

The framework presents a mechanism that can be used for defining the security posture of Aztek, exploring the target state of the company network, prioritizing improvement opportunities, assessing security systems and communicating the security risks to company stakeholders (Delhi Government, 2014).

Aztek managers can create a checklist which could be based on the security categories, functions and industry references for the management of security posture of the company. Some examples of the security functions are asset protection, intrusion detection, data recovery, risk identification and risk response planning. Certain security categories can be identified for inclusion in security policies such as access control. Asset management and intrusion detection (Berg, 2010). There can also be some sub-categories within these such as threat notification under intrusion detection and data protection under access control. All these security themes if taken care in security measures can enhance the security posture of Aztek (E&Y, 2013).

The security framework defines some tiers of security that define different protection levels such as:

Tier 1: At this level, the company would have the partial protection with each device covered but there would not be any integration of the risk based programs and neither processes in the company nor the processes would be formalized (Bhatta, 2008)

Tier 2: Risk management processes are formalized at this stage and activities have priorities based on the security needs and impacts (Paschke, 2014)

Tier 3: The risk management processes and procedures are all formalized and repeatable security measures that can be taken by the company would be defined. The methods defined would be consistent with the level and would help in strengthening the security posture of the company by providing better protection (Health and Safety Authority, 2006)

Tier 4: The company would adapt to the required changes in the security systems in this stage as per the changed security posture and levels of threats that the company would be exposed to. At this level, security processes are integrated and the security practiced become the part of organizational culture (Elky, 2006)

The framework can be used by Aztek for other purposes such as reviewing the security practices and policies already used in the company such that scope for improvement can be defined. The framework would be used as a guide for communicating the risks to the stakeholders as well as for enforcement of the policies (Bodicha, 2005).

Security Profile Review: The security posture of the company would be reviewed in order to understand the practices that company is using for detecting threat, protecting its IT systems, responding to risks and recovering from security challenges (Rule Works, 2017). The current structure of the company is used as per the traditional system of the organization where the devices were connected and were all owned by the company. However, the current need of the company is to alter the security management structure to adapt to the needs of BYOD devices to enhance its level of protection (John Snow, Inc., 2010).

Establishing security program: Aztek can use following steps for establishing security systems:

- Developing the objectives of security measures and scope of the same for the IT systems of Aztek (Security Awareness Program Special Interest Group, 2014)
- Prioritising the objectives defined based on the current IT security needs of the company

- Studying the probable threats to the current system and it vulnerabilities. Aztek can use personal and financial data of the company customers to identify potential loss of data. vulnerabilities would become dangerous for the company when company employees would try connecting their devices to companies applications in an insecure environment and thus, such threats have to be studied for understanding impacts and possible response measures to be taken (Campbell, 2005).
- The security profiling of Aztek would help define risk categories and risk sub-categories such as identity thefts, financial frauds, and unauthorized access (NCSU, 2017). Each of these categories of risks can have different impacts on the organization as explained below:
    - **Identity Thefts**: A stolen data of customers and the company can be misused by the stealer as it can be used for launching an attack on the company or on the accounts of the customers to gain access to the financial data of the users and use identity details to misuse it. This can damage the reputation of the company and thus, lead to loss of trust in customers (La Trobe University, 2017).
    - **Financial Fraud:** Attackers can use the opportunity to modify the financial data which would hide some figures such that the money can be taken by the attacker without the user getting to notice the reduction in account balance. It is only when the amount grows big enough that the user would get the notice of it (CDC, 2006). Once attacker gets to use the credentials of user accounts, direct monetary gains can also be achieved. This can be threatening not just to Aztek but to the entire financial industry as the customers would lose money and thus, trust in financial systems (Chan, Lam, Chan, & Cheung, 2008).
    - **Unauthorized Access:** Unauthorized access by hackers to the user accounts can lead to launch of cyber attacks like DDOS which would cause disruption in service provisions by blocking the same for the genuine users thereby affecting the service capabilities of the company (Curtis & Carey, 2012)
- Aztek can study the profiles of stakeholders for identifying the target profiles that can get affected most by specific categories of risks and these profile users needs to be communicated about the probable threats with steps to remain safe (Engine Yard, Inc., 2014). Various stakeholders and the responsible communication that must be sent to them are listed in the table below:

Risk Category	Stakeholders	Requirements
Identity Thefts	Employees Users	Personal information of users and employees need to be protected from getting stolen or leaked (European Commission , 2010)
Records alteration	Management Employees Users	Customer and users data has to be managed securely without any allowance to user or any other third party person to make modifications without the proper approval of the customer and the company officials (GILBERT, 2014)
Unauthorized access	Customers Management	Customer credentials should be kept safe such that they do not get leaked and misused by a hacker or unauthorized user (HP Enterprise, 2015)

Financial fraud	General Consumers Finance companies Investors	Fraud patterns can be identified and analyzed to understand how the industry is getting affected by the security threats and mutual steps must be taken to identify best protection measures that must be shared and used for increasing security posture of all the companies in the finance industry (Health and Safety Authority, 2006)

- The security gaps in Aztek would be identified assessed and priorities would be created for improvement steps for each gap (Veracode, 2017). Risks can be given priority based on the cost benefit analysis of the suggested improvement and impact of the risk exploitation. The gas would include the existing vulnerabilities in the IT systems and applications of the organization. These could include lack of monitoring and lack of security awareness in the employees (NIST, 2014).
- A security plan would be projected for managing risk in each category and sub-category (IBM Global Technology Services , 2011)

Opportunity Identification: Company staff can explore the practices used by industry companies for securing their IT systems including those using BYOD schemes. With this exploration, best security practices that have worked well with BYOD schemes can be identified and used for the enhancement of the protection of Aztek. Some of the best practices used in the finance industry include (Infrascale, 2014):

- A layered security infrastructure can be used that identifies trusted methods of access from the untrusted methods of access to the company systems through mobile devices (John Snow, Inc., 2010).
- Control mechanisms may be used on the mobile devices such as authentication when employees are connecting to critical resources of Aztek (WatchGaurd, 2013).
- The company should have an awareness and training program launched to tell employees about risks, their impacts and protective measures (NIST, 2014)

Data Security

One major risk that finance industry faces is the loss of the data of the organization and its customers. With proper policies defined for managing different types of access systems such as remote or wireless access, privacy settings, codes of conduct, social media access, ad incidence response plans (MYOB, 2016), risks of losing data can be reduced. Devices can be directly or indirectly secured from these threats using measures like encryption, remote wiping, authorization, sandboxing, and inventory securing. Employees must be provided with sufficient training so that they can identify vulnerabilities and take steps for securing their devices (Paschke, 2014).

Another risk that BYOD environment is increased exposure to the data through the end point devices connected to the system. End point protection measures have to be used with BYOD devices which would need different protection techniques than those used with traditional systems. Two major risks faced by the finance industry are data leakage and productivity reduction because of the

use of BYOD (Microsoft Asia News Center, 2016). Thus, Aztek needs a mechanism that allows tracking the activities at the end point and provide authorization systems for remote data access. If an end point device faces a threat such as after getting stolen, a remote wiping feature can be used such that the device is disconnected with the system which would not allow user to connect with company systems any more. This would protect the unauthentic user for gaining access to the confidential data of Aztek (NCSU, 2017).

The methods people use for accessing data and applications on BYOD devices can also affect the security and thus, company must have a way to check the access methods and define some data protection strategies for overcoming these challenges such as (National Treasury, 2011):

- Employee activities in the cyberspace can be monitored for understanding how they are using company systems and the data through the use of activity logs and usage records (Office of the Privacy Commissioner of Canada, 2015).
- Protecting devices with pass word authentication is the responsibility of the employee using the network and he or she must protect the company's sensitive data from getting leaked through the device (OECD, 2008)
- A minimum level of control over the access gained by the employees must be defined such that the company can enforce security standards on them. These control mechanisms would be applied to the end user devices when they would be used company applications or accessing data such that they are protected (WatchGaurd, 2013).
- Training can be given to employees on secure use of devices and on security aspects such as data storage, administration, encryption, authentication, patching, antivirus protection incident management, application management, asset management, and inventory control (Office of the Privacy Commissioner of Canada, 2015).

Conclusions

The aim of this paper was to explore the case of Aztek which is a financial organization to identify changes in security posture and finding measures that can be used by the company to enhance protection. It was found that the company uses a security structure that is more suitable to an IT infrastructure that is wholly owned by the company and thus, new strategies are required with addition of end point devices as the company is planning to implement BYOD scheme in it. The study of the security posture suggests that the risk of leaking data, loss of control over devices and risking unauthentic access by attackers would be major concerns for the company with BYOD scheme. A cybersecurity framework can be used to develop security management strategies that are suitable for the end point protection. This would include security management methods like surveillance, device management, policy enforcement, and employee awareness to give them responsibility for protection of devices.

References

ACHS. (2013). *RISK MANAGEMENT & QUALITY IMPROVEMENT HANDBOOK.* EQuIPNational .

Afaq, S., Qadri, S., Ahmad, S., Siddique, A. B., Baloch, M. P., & Ayoub, A. (2014). Software Risk Management In Virtual Team Environment. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH , 3*(12), 270-274.

Alali, F., & Yeh, C.-L. (2012). Cloud Computing: Overview and Risk Analysis. *Journal of Information Systems, 26*(2), 13-33.

APM Group Ltd. (2017). *DEFINING RISK: THE RISK MANAGEMENT CYCLE*. Retrieved September 14, 2017, from https://ppp-certification.com/ppp-certification-guide/52-defining-risk-risk-management-cycle36

Avdoshin, S. M., & Pesotskaya, E. Y. (2011). *Software Risk Management: Using the Automated Tools.* Russian Federation.

Berg, H.-P. (2010). *Risk Management: Procedures, Methods and Practices.* Salzgitter, Germany: Bundesamt für Strahlenschutz.

Bhatta, G. (2008). *Public Sector Governance and Risks: A Proposed Methodology to do Risk Assessments at the Program Level .* Asian Development Bank .

Bodicha, H. H. (2005). How to Measure the Effect of Project Risk Management Process on the Success of Construction Projects: A Critical Literature Review . *The International Journal Of Business & Management, 3*(12), 99-112.

Campbell, D. (2005). *Risk management guide for small business.* Global Risk Allianz.

CDC. (2006). *CDC Unified Processes Practice Guidance for Risk Managment.* CDC.

Chan, A., Lam, P., Chan, D., & Cheung, E. (2008). Risk-Sharing Mechanism for PPP Projects – the Case Study of the Sydney Cross City Tunnel. *Surveying and Built Environment*, 67-80.

Curtis, P., & Carey, M. (2012). *Risk Assessment in Practice.* COSO.

Delhi Government. (2014). *HAZARD, RISK AND VULNERABILITY ANALYSIS.* New Delhi: Delhi Government.

E&Y. (2013). *Bring your own device - Security and risk considerations for your mobile device program.* E&Y.

Elky, S. (2006). *An Introduction to Information System Risk Management.* SANS Institute.

Engine Yard, Inc. (2014). *Security, Risk, and Compliance.* Engine Yard.

European Commission . (2010). *Risk management in the procurement of innovation.* European Commission .

GILBERT, P. L. (2014). *Surveillance of workplace communications:What are the rules?* TOBIN.

Health and Safety Authority. (2006). *Guidelines on Risk Assessments and Safety Statements* . Dublin: Health and Safety Authority.

HP Enterprise. (2015). *Cybersecurity Challenges, Risks, Trends, and Impacts: Survey Findings.* MIT.

IBM Global Technology Services . (2011). *Security and high availability in cloud computing environments.* IBM Corporation.

Infrascale. (2014). *BYOD Program Best Practices for Data Protection & Security .* Infrascale.

John Snow, Inc. (2010). *Developing a Risk Management Plan.* USAID.

La Trobe University. (2017). *Video 4: Project Risks*. Retrieved September 14, 2017, from https://lms.latrobe.edu.au/mod/book/view.php?id=2493632&chapterid=201714

Microsoft Asia News Center. (2016, June 7). *Malware Infection Index 2016 highlights key threats undermining cybersecurity in Asia Pacific: Microsoft Report*. Retrieved from Microsoft News: https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/

MYOB. (2016, September 13). *Protecting your confidential information*. Retrieved from MYOB: http://myob.com.au/myob/australia/myob-security-recommendations-1257829253909

National Treasury. (2011). *Public Sector Risk Management Framework.* Republic of South Africa.

NCSU. (2017). *Risk Management* . Retrieved September 14, 2017, from http://agile.csc.ncsu.edu/SEMaterials/RiskManagement.pdf

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* National Institute of Standards and Technology.

OECD. (2008). *Malicious Software (Malware): A security Threat to Internet Economy.* OECD.

Office of the Privacy Commissioner of Canada. (2015). *Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?: Privacy and Security Risks of a BYOD Program.* Office of the Privacy Commissioner of Canada.

Oracle. (2009). *Managing Risk with Project Portfolio Management in the Oil and Gas Industry During an Economic Downturn .* Oracle.

Paschke, C. (2014). *Bring Your Own Device Security and Privacy Legal Risks.* Information Law Group.

Rule Works. (2017). *The risk management cycle*. Retrieved September 14, 2017, from The risk management cycle

Security Awareness Program Special Interest Group. (2014). *Best Practices for Implementing a Security Awareness Program.* PCI.

Veracode. (2017). *APPLICATION SECURITY SOFTWARE*. Retrieved May 19, 2017, from https://www.veracode.com/products

WatchGaurd. (2013). *BYOD: Bring Your Own Device – or Bring Your Own Danger?* WatchGaurd.