**Return on Investment**

Jose Flores

CSOL-550-01-FA22: Management and Cyber Security

Dr. William Hess

November 22, 2022

**Cybersecurity Investment**

As technology continues to advance, so will the threats. Cybersecurity is an organization's investment because it creates a strong network and provides protection (Stedman, 2022). Although cybersecurity does not actively gain revenue, it reduces the chances of losing assets. Cybersecurity return on investment (ROI) comes in various forms, such as reduction in risk, compliance, and meeting business objectives. The ROI calculation is expressed as the organization (Revenue - Cost) = Profit (Brathwaite, 2022). The amount of money saved through cybersecurity implementation is described as “Revenue,” and the security control cost is defined as “Cost.” The RIO of cybersecurity will be based on how adequate security controls can prevent incidents and save the company money by avoiding fines or recovering from damages.

**Reduction in Risk**

An organization may suffer from security breaches or incident damage that are expensive to recover from. Investing in cybersecurity will reduce the occurrences by implementing security controls and advising on policy changes. BioHuman suffers from 15 data breaches due to phishing emails and five system misconfigurations due to access controls. Every data breach is estimated to be about $5,000 to fix. Every system misconfiguration costs about $2,000 to discover and fix. The Annual Loss Expectancy (ALE) is calculated by the Annualized Rate of Occurrence (ARO) and the Single Loss Expectancy (SLE) (CompTIA, 2022).

BioHuman ALE is as follows:

ALE = ARO x SLE

ALE = (15 data breaches) x ($5,000)

ALE = $75,000 (Data Breaches)

ALE = (5 System Misconfigurations) x ($2,000)

ALE = $10,000 (System Misconfigurations)

ALE = $10,000 + $75,000

ALE = $85,000

BioHuman spends an estimated $85,000 annually due to data breaches and system misconfigurations. Investing in cybersecurity will help reduce this cost by decreasing the ARO and implementing new security controls. An example of security control that will decrease the ARO is installing firewalls as a buffer between users, networks, and computers. This type of technical security control will reduce the ARO and can be implemented in upcoming years. Additionally, a firewall can be configured to implement an access control list to allow or deny traffic based on IP address. Awareness and training is an administrative security control that may be implemented to help users identify phishing emails and avoid them. Additional administrative security control is the separation of duties and least privilege policies. These policies will decrease the ARO of system misconfigurations because the wrong users will not have access to the system directories and will have basic access.

The technical control security control will cost an estimated $10,000 but will reduce the ARO of data breaches by 10 for a total of 5 per year.

Data Breach Security Control Calculations

RIO = (10 data breaches) x ($5,000)

RIO = $50,000

RIO % = [(RIO - (Cost of Control) / (Cost of Control)] x 100 (Kolochenko, 2015)

RIO % = [($50,000 - $10,000) / $10,000] x 100

RIO % = 400%

The administrative security control will cost an estimated $1,000 but will reduce the ARO of system misconfigurations by 3 for a total of 2 per year.

System Misconfiguration Security Control Calculations

RIO = (3 System Misconfigurations) x ($2,000)

RIO = $6,000

RIO % = [(RIO - (Cost of Control) / (Cost of Control) ] x 100

RIO % = [($6,000 - $1,000) / $1,000] x100

RIO % = 500%

Both Security Control Calculations

RIO % = [(RIO - Cost of Control Total) / (Cost of Control Total) ] x 100

RIO % = [( $56,000 - $11,000) / $11,000] x 100

RIO % = 409%

BioHuman's ROI percentage is 409%, implementing two security controls. With the initial investment in security controls, BioHuman saved 409%, estimated to be about $45,000. BioHuman may reduce risk by reevaluating its risk acceptance and mitigating it with security controls. Although security controls save a ton of money, hiring the right staff to implement and manage the security control is paramount (Touhill, & Touhill, 2014).

**Compliance**

Cybersecurity plays a vital role in complying with multiple laws and regulations. Depending on an organization’s field and region, they must abide by different regulations such as Health Insurance Portability and Accountability Act (HPPA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR). BioHuman handles credit card information from various clients and must follow PCI DSS. The PCI DSS regulation has six goals and 12 main requirements to comply with (Cole, 2017). Three of their requirements are restricting access to cardholder data, protecting stored cardholder data, and maintaining an information security policy. To meet these requirements, BioHuman must invest in cybersecurity professions and equipment. The cybersecurity professional will be able to advise and implement security controls to meet these requirements needed by PCI DSS. They can advise in creating a role-based access control (RBAC). An RBAC restricts access to employees based on their duties and responsibilities (Rosencrance, 2021). An example of a type of equipment that can use to meet these requirements is a hardware security module (HSM). An HSM is a physical device that provides crypto processing to protect data at rest. These implementations will ensure BioHuman stays in compliance with PCI DSS regulations. Breaking PCI DSS compliance can result in a fine ranging from $5,000 to $100,000 monthly (Baykara,2022). Investing in cybersecurity professionals and equipment can help avoid heavy penalties.

**Business Objectives**

Meeting business objectives is paramount for all departments in a business. In cybersecurity, business objectives involve recovery time objectives (RTO), recovery point objectives (RPO), and data availability. An RTO is an allowable time the computer, system, or network can be down after an incident (Kerner, 2021). An RPO is the organization’s tolerance level for the amount of data lost before it is considered significant damage. Data availability is the ability to access your system and data without interruptions. The organization defines RTO and RPO and is incorporated with a disaster recovery plan (DRP). They are measured in time, so it is critical to invest in cybersecurity professionals to ensure they can recover the data/system promptly. BioHuman's business objectives are to reduce the time of RTO and RPO. A cybersecurity professional will advise implementing redundancy and creating a DRP with playbooks. Redundancy includes frequent backups and servers, reducing the RPO and RTO. Frequent backups will ensure that the data is available at the earliest convenience to continue the business. Multiple servers will establish continuity when one server goes down by kickstarting the next server. Creating a DRP with playbooks will create a step-by-step procedure for employees to do when an incident occurs. Instead of panicking and being lost, the playbook will give directions on what needs to be done and how it should be done.

**Overall**

Cybersecurity is an investment toward the future of BioHuman because it reduces risk, meets compliance, and meets business objectives. To minimize risk, security controls can be implemented to strengthen the system and reduce breaches. Depending on the laws and regulations an organization must comply too, cybersecurity professionals can adjust and advise to meet those standards. Lastly, cybersecurity meets BioHuman’s business objectives by implementing redundancy and creating a DRP with playbooks. Cybersecurity does not bring in revenue; instead, they save money by avoiding repairs, penalties, and fines.

Reference

Baykara, S. (2022). *What are the PCI compliance fines and penalties?* PCI DSS GUIDE. Retrieved November 21, 2022, from https://www.pcidssguide.com/what-are-the-pci-compliance-fines-and-penalties/

Brathwaite, S. (2022). *How to calculate the return on investment (ROI) of Cybersecurity*. SecurityMadeSimple. Retrieved November 22, 2022, from https://www.securitymadesimple.org/cybersecurity-blog/how-to-calculate-the-roi-of-cybersecurity

Cole, B. (2017). *What is PCI DSS compliance (Payment Card Industry Data Security Standard Compliance)?* TechTarget. Retrieved November 20, 2022, from https://www.techtarget.com/searchsecurity/definition/PCI-DSS-compliance-Payment-Card-Industry-Data-Security-Standard-compliance

CompTIA. (2022). CompTIA *Exam objectives*. CompTIA. Retrieved November 20, 2022, from https://www.comptia.org/training/resources/exam-objectives

Kerner, S. M. (2021). *What is a recovery time objective, and how does it work?* TechTarget. Retrieved November 22, 2022, from https://www.techtarget.com/whatis/definition/recovery-time-objective-RTO

Kolochenko, I. (2015). *How to calculate ROI and justify your cybersecurity budget*. CSO Online. Retrieved November 20, 2022, from https://www.csoonline.com/article/3010007/how-to-calculate-roi-and-justify-your-cybersecurity-budget.html

Rosencrance, L. (2021). *What is role-based access control (RBAC)?* TechTarget. Retrieved November 20, 2022, from https://www.techtarget.com/searchsecurity/definition/role-based-access-control-RBAC

Stedman, C. (2022). *The ultimate guide to cybersecurity planning for businesses*. TechTarget. Retrieved November 22, 2022, from https://www.techtarget.com/searchsecurity/The-ultimate-guide-to-cybersecurity-planning-for-businesses

Touhill, G. J. & Touhill, C. J. (2014). Cybersecurity for Executives – A Practical Guide. The

American Institute of Chemical Engineers, Inc. Published by John Wiley & Sons, Inc., Hoboken, New Jersey. ISBN 9781118888148.