Cybersecurity Strategy & Plan of Action

**Introduction**

The PBI-FS/Island Banking system has the cybersecurity issues of ignorance of social engineering, untrained officials, lack of clear policies, system and software updates, password management, leaving operations running, being on the lookout for unusual emails, and phishing scams. The new organization is at risk of similar cyber-attack from internal and external sources from the arrangement of the Island Banking Services IT Infrastructure bought by the Padgett-Beale.Inc. The structure of the infrastructure makes it vulnerable and employees or clients using the utilities may find shortcuts to get into the data center, or disrupt the internet required for crucial operations (Enriquez Álvarez, 2019). The organization may also have problems when the managers from Island Banking Services use similar passwords as the previous organizations or passphrases that may give easy access to people with malicious intent or those who had accomplished the cyber-attack on Island Banking Services.

Table 1. Risk Profile Table

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Risk | Category | Severity | Applicable Laws, Regulations, Standards | Risk Mitigation Strategy (description) | Implementation: Required Technologies, Products, or Services | NIST Cybersecurity Framework Category and Sub Category Identifier (e.g. ID.AM-1) | Sub-Category Description |
| 001 | Theft of customer information from online transactions | Technology | 4 |  | Encrypt all communications between customers and the company’s online ordering system. | Implement Transport Layer Security; purchase and deploy digital certificates to use to encrypt communications. | PR.DS-2 | Data-in-transit is protected. |
| 002 | Ignorance of social engineering | People | 5 |  | Educate the employees on social engagement and the dangers of falling under psychological manipulation | Train employees | PR.AT-1 | All users are informed and trained |
| 003 | Lack of back up data | Confidentiality | 3 |  | Back up data and information for east retrieval | Acquire data saving facility for backup | PR.DS-4 | Adequate capacity to ensure availability is maintained |
| 004 | Lack of clear policies | People | 3 |  | Formulate clear policies that hold employees responsible for their actions | Punish employees that endanger the company data | PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) |
| 005 | AP theft  | Availability | 4 |  | Monitor incoming and outgoing wireless data and store it for later use | Review suspicious activities | PR.PT-4 | Communications and control networks are protected |
| 006 | VPN login cracking | Authentication | 3 |  | Input security cameras to prevent brutal VPN login cracking | Enhance physical and system security | DE.CM-2 | The physical environment is monitored to detect potential cybersecurity events |
| 007 | Power saving attacks | Availability attack | 5 |  | Providing ample power | Ensure the building has access to enough power | DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed |
| 008 | masquerading | Confidentiality | 2 |  | Installing Artificial intelligence systems that match employee IDs and their appearance | Use advanced technology | DE.CM-1 | The network is monitored to detect potential cybersecurity events |
| 009 | War driving | Access Control Attack | 4 |  | Use of multi-factor authentication | Practice the use of multi-factor authentication | PR.IP-8 | Effectiveness of protection technologies is shared |
| 010 | Identity theft | Authentication attack | 3 |  | Protecting packet capturing tools | Blocking entry through unknown packets  | DE.CM-8 | Monitoring for unauthorized personnel, connections, devices, and software is performed |
| 011 | Wireless network viruses | Integrity attack | 4 |  | Installing antivirus software | Getting antivirus software from trusted dealers | DE.DP-5 | Detection processes are continuously improved |
| 012 | Session hijacking | Confidentiality attack | 2 |  | Enhancing security during wireless transactions | Denying access to foreign devices seeking to gain access | DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed |
| 013 | Password speculation | Authentication Attack | 3 |  | Avoid using common password suggestions from online platforms and password dictionary | Implement strong password usage | DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events |

Internal issues such as greedy employees may pose a threat to the PBI-FS as it is difficult to identify employees capable of carrying out cybercrimes against their employer and clients they serve. The greediness of employees often arise from unsatisfactory pay and lack of motivation to uphold the company's ethical policies and standards. Social engineering involves the psychological manipulation of people to give up important information and make security mistakes and occurs through human interactions (Almuhammadi,& Alsaleh,2017). The employees at PBI-FS are at great risk of social engineering as it occurs when one least expects it and utilizes psychological manipulation to lure the unsuspecting employees into making security mistakes such as giving up important information. An existing employee can have a newly hired islander in charge of guarding the passwords to the vault believing they have clearance from the managers to access private and crucial information of client's confidential information.

Untrained officials and employees are a current risk to the merger as they may cause the company great loss by falling under the manipulation of experienced employees and masters of trickery. The new organization lacks clear policies that indicate the price of crimes aiding or attempting cybercrimes, as observed in the previous banking company (Packin, 2017). These policies help hold employees responsible for their criminal activities, such as manipulating newly employed personnel. The new organization also has no clear set routines to update the systems and software used to run and manage client information. Updating systems and software getting used at the organization will keep clear of malware and viruses used by cybercriminals to attack organizations.

Updated systems and software often fix bugs that may get used by cybercriminals and existing employees to gain access to restricted information about client details and the organization's information that is sensitive and makes the organization vulnerable. Newly employed Islanders may lack knowledge on systems operation and feel free to take breaks while leaving crucial systems running. Workmates may take advantage of such gaps and get access to private information such as vault passwords or client lists that may have gotten forgotten running by new employees taking a bathroom break or a lunch break (Almuhammadi,& Alsaleh,2017). Running systems get used as entry points to carry out criminal activities in the organization.

Unusual emails are another point of entry for cyber security issues such as the introduction of malware and ransomware that take control of the organization's entire files and documents, thus crippling out the new merger when no backup data has gotten taken into account. Finally, the account may get security concerns through phishing scams that lure employees into clicking click-baits containing computer viruses that may hold and render the organization crippled, like its predecessors. Scams come in the form of enticing news the employees may get interested in, and they are accessing this information through company servers and networks.

These click-baits introduce malware and ransomware into the organization's systems, making them susceptible to cybercrimes and loss of important information such as client data. Many of these challenges involve the help of inside information, namely employees, to cripple down the organization and its clientele. The presented risks include technological, process, availability, integrity, and confidentiality categories of risks. The technological category relies on technology to avoid and improve performance, and the people category requires the employees to get extra careful in their transactions at the new business to improve and maintain management. The confidentiality category requires the managers and employees to maintain critical and private information such as passwords and client data under strict control and access. Generally, companies will chose a few individuals and will entrust with passwords and access to the organization's confidential material.

All kinds of information are available on online platforms, and employees need to exhibit professionalism and restriction when accessing some of these sites. Online platforms get used as sites for click-baits, thus having distracted employees venturing their job descriptions and inviting in viruses and malware through innocent browsing through a boring period at work (Packin, 2017). The workers also require professional training to avoid distractions and boredom as excuses to venture into sites beyond work that may invite viruses and malware into the merger's company online presence. Updating software and the system may get tricky, leading to those in charge of updates clicking on the wrong software or program, thus introducing viruses or malware that may interfere with the functioning of the overall system and the security of the client confidentiality held.

Newly employed islanders may have little to no information about technological requirements such as updates and constant monitoring of spam emails to avoid introducing viruses and malware capable of destroying the organization's operations. The new organization requires training the new and existing employees about various methods that people, processes, integrity, and availability may get used to compromise existing knowledge of the clients and the organization's private matters.by the company (Enriquez Álvarez, 2019). Technology is another category of risk that the new organization may face. Technology may get tricky if employees are of an elderly age that does not appreciate changes in their usual schedule. This factor hinders the managers from updating the system and software, which is a requirement in keeping the system and software up to date; making it susceptible to malware and virus that compromises the company's safety and client's private information.

The banking business is among the most regulated industries in the United States with banks playing an important role of taking deposits, allocating loans, and operating the payment system. The current United States bank regulatory framework meets the federal level requires chartered banks across the states to have at least one federal supervisor. There are laws and regulatory guidance that apply to financial services industries and companies like Island Banking Services such as the Federal Reserve System in the central bank of the United States that regulates monetary processes. Financial services also apply to Federal Deposit Insurance Corporation that regulates the primary state-chartered thrifts that insurer’s banks and thrift deposits. The policy also gives power to FDIC-banks over certain institutions and businesses. The Office of Comptroller of the Corporation regulates and supervises all national banks and federal savings for individuals, federal branches, and agencies of foreign banks.

The consumer Financial Protection Bureau has authority to develop consumer protection regulations that may be applied to banks and non-banking associations to ensure law compliance enforcement for institutions with over $10bn. The final bank regulation and policy is the Financial Stability Oversight Council that oversees and empowers important non-banking institutions that are under the supervision of Federal Reserve. The Risk Management and the Cybersecurity Framework in the NIST security framework involves detecting, responding, protecting, recovering, and identifying points of improvement. The process eliminates possible cyber threats that may bring the organization as done to the previous company (Almuhammadi,& Alsaleh,2017). Detecting points of cybersecurity threats is an initial step in protecting the new company from falling into the traps of cyber expert’s out to rob and destroy what got build by others. Cybersecurity issues getting spotted as an early stage ensures that the managers have an ample time formulating suitable strategies to prevent catastrophic failure of the merger.

Responding to detected issues of cybersecurity is the immediate step that involves updating systems and software in the new organization. It would also involve training newly employed islanders and employees with little knowledge with mobile banking and issues to ensure that every employee understands what is at stake at the new company and how to eradicate these challenges and find a solution for problems getting faced by the company. Protection is the next step in the framework as it is crucial to protect client confidentiality and information that would become dangerous on the wrong hands (Packin,2017). Protecting the system makes it easy to recover any lost data and information stored on precious devices and platforms that would enable the organization to run the systems smoothly after an interruption. Recovering information from existing back-up points enables the organizations to quickly pick up after an incidence of cybersecurity that would require the client’s and employers to become more careful with the handling of data and information that is critical and crucial to the organization.

Points of improvement may get observed from the working of the current system that involves existing employees, newly hired islander, and the managers from the failed bank. The collaboration of these three units will see to the improvement of identified points in attempt to improve its importance. The proposed plans of actions include the hiring of expert cyber teams to manage troubles of technological and interpersonal personnel that take into consideration every possible risk involved in the new organization and creating new and effective strategies to deal with the ideals. Resources should get directed to high risk areas of training and educating newly employed staff about the workings of the bought systems that enabled them to understand the working of the organization better. A team equipped with the knowledge of the risks, and issued involved in running the merged organization will ensure that previous mistakes do not get repeated and everyone becomes on high alert on the issues presented in the new organization.

**References**

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, *7*(3), 51-62.

Packin, N. G. (2017). Regtech, Compliance and Technology Judgment Rule. *Chicago-Kent Law Review, Forthcoming, Baruch College Zicklin School of Business Research Paper*, (2018-06), 03.

Enríquez Álvarez, L. F. (2019). La visión de América Latina sobre el Reglamento General de Protección de Datos (Coyuntura).