Final Project: Wilbur's Widgets GAP Analysis

Vince Rosas

Southern New Hampshire University

Executive Summary

Author: Vince Rosas

This report was created to provide Wilbur's Widgets with an overview of their current security posture and highlight any missing or insufficient security policies. Wilbur's Widgets currently has a weak security posture. The company is currently using out of date software, does not update their software regularly, non-technical staff does not receive regular security policy training, and IT staff is not empowered to make the necessary changes to properly secure the network and systems. Wilbur's Widgets needs to update their existing security polices with current industry best practices as well as adopt new policies to further secure the company's infrastructure, data, profits, employees, and clients.

Contents

Background, Scope, and Study Overview

Company Background:

Wilbur’s Widgets is a small business that creates and sells the widget. They have 82 employees across their various departments as well as a CEO and board of directors. Wilbur’s Widgets is in the manufacturing industry. Their widget is a widely used product and there are many other companies and nations who want to acquire the plans to make their own widgets. Consultants have been brought in to help Wilbur’s Widgets analyze their existing security policies and recommend changes that will increase the information security posture of the company and help prevent future data breaches.

Scope of Document:

The scope of this report is the organization’s entire security framework. The existing policies and practices leave the company open to many points of intrusion. The lack of training of non-IT personnel leave the company open to many forms of social engineering attacks such as phishing scams.

Overview:

This GAP analysis will look at current security policies and identify what policies are necessary but missing or unenforced.

Gap Analysis and Results

Security Posture:

The IT staff does not currently have the ability to train the other employees on best practices or coach them on securing their terminals. There are some security policies in place, such as incident response, email, password guidelines, and more, but because IT staff cannot train employees they are not well understood by the other staff. All these issues, and others, combine to form a very weak information security posture. The company is willing to accept a high amount of risk of data loss by favoring current profit margins over long-term security and profitability.

Policy Errors and Gaps

There are multiple gaps in the current policies for Wilbur's Widgets. The existing policies do not cover all possible situations. They are currently missing multiple common policies as well, such as an Acceptable Use Policy, Physical Access Policy, E-waste policy and Security Training, among other things.

Technology analysis:

Currently, Wilbur's Widgets is using outdated technology with respect to their operating system. This is due to lack of policy enforcement as well as a lack of proper software update policies. Lack of proper backup and storage policies also lead to data being scattered across multiple drives, with unnecessary duplication of data and multiple versions of the same information. Data needs to be consolidated to ensure the correct data is accessible and that proper backups can be made with the most up to date version of company data.

Staffing Analysis

The current staffing levels in the IT department are inadequate and the staff they do have is not empowered to enforce the policies that are in place. While there are IT security staff in place, they are not dedicated to security but also handle general IT requests as well. The IT security group should be split off from the general IT Department and managed by a Chief Information Security Officer (CISO). Additional staffing would enable the IT security group to dedicate their time to security and become more proactive. They should also be empowered to enforce policies. This can be done by auditing logs and enforcing through technical means as many policies as possible.

Additional staffing should also be added to the general IT department, this would reduce their workload and allow them to handle requests quicker and more effectively and offset the loss of the two staffers lost to the IT security group.

Implementation Issues:

An issue that could arise in the implementation of new and updated security polices is lack of authority. If management does not empower the appropriate staff in the implantation and enforcement of these policies, then the policies will not be implemented properly or at all and will become unenforceable. Secondly, if employees feel that there are no consequences for not following the new and updated policies, then they will continue to follow old habits and the policies will be ineffective. Lastly, if the new policies are too complicated or cumbersome to the average employee, then employees will be less likely to follow the new and updated policies.

Recommendations

Findings

The analysis of Wilbur's Widget's policies has found multiple gaps in coverage. There are not enough policies in place to protect the company, its data, employees, or clients. Some of the current policies that do exist are ineffective or unenforced. One of the most glaring gaps in policy is the lack of software updates and the refusal to keep operating systems on currently supported versions. This one gap opens the company to innumerable threats because of the number of unpatched threats that exist for that operating system. The lack of additional policies leaves the company open to additional threats from outside malicious actors as well as legal and financial liabilities should a breach occur.

Policies

The following policies are recommended to be implemented in addition to the existing policies. An Acceptable Use Policy, Physical Access Policy, Clean Desk Policy, Personal Mobile Device Policy, Electronic Waste Policy, Data Backup and Recovery Policy, and Security Training Policy. See Table 1for an explanation of each policy as well as the reason for each policy.

Defense of Policies

Each of these policies is designed to protect the company from external and internal threats, as well as limit the liability of the company should a breach occur. The Acceptable Use Policy details how company systems and information are to be accessed and used. There needs to be clearly documented and enforced AUP so that users can know and understand what they are and are not allowed to do with company information and services.

The Physical Access Policy dictates how access to the company's physical locations will be controlled. Physical access needs to be controlled to protect company systems and data. Without restricting physical access, information and systems become much more vulnerable. Like the Physical Access Policy, the Clean Desk Policy will help protect physical access to company information and systems. By maintaining a clean desk, this limits accidental data exposure and limits the likelihood of unsecured data being stolen.

The Personal Mobile Device Policy dictates how personal devices such as personal laptops, cell phones, and tablets, can connect to company resources. By having a policy in place, it will limit the ability of attackers to gain access through unsecured personal devices or ensure that personal devices meet a minimum-security standard before connecting to the corporate network. The Electronic Waste Policy will help ensure that data is disposed of properly. If devices are not disposed of properly, confidential data could be retrieved from them by malicious actors.

The Data Backup and Recovery Policy will create clear guidelines on how often backups will be created, how long they will be retained for, as well as the procedures for restoring data. This policy will protect the company should a breach occur, and data be stolen or deleted. It will also allow the company to resume normal operations as quickly as possible should a catastrophic event occur. Lastly, the Security Training Policy will detail who will receive security training, how often, and what kind of security training each person will receive. It will also detail what would happen when a breach or exception to one of the policies occur.

All these policies serve to protect the company breaches and limit the attack surface of the company. The also have the secondary affect of limiting the legal liability of the company should a breach occur. By having the policies in place and enforcing them, should a breach occur due to someone not following the policy, the liability falls on the person who broke the policy.

Controls

The company should strive to adopt and become ISO27001 certified. While this is not a necessary certification, it shows that the company is dedicated to the protection of their data, their client’s data, and their employee’s data. The certification shows the company’s commitment to protecting the confidentiality, integrity, and availability of their data and systems. It covers a wide range of events, not just data breaches. Even if the ISO27001 certification is not achieved, the steps taken to attempt the certification will be beneficial in securing company data and physical locations.

Implementation Plan

To implement the new policies, a coalition will be formed to develop the policies, drive implementation, and raise awareness and adoption. The coalition will be comprised of the CEO, two members of the board of directors, three members of IT, one being the IT lead, one from the IT security department and one in the general IT role. It will also include leads from each of the following departments: Sales, Manufacturing, Inventory Control, Research and Development, Marketing, and Human Resources. Each lead will be responsible for providing input on what they see as risks to the business as well as obstacles they see in implementing and enforcing the new policies. Each department lead will also be responsible for gathering input from their direct reports on possible pain points in implementing the new policies. Human Resources will also be responsible for tracking incidents of policy violations.

Once the initial policies are created, time will be given for department leads to gather input from their direct reports. A company-wide meeting will be held to introduce the new policies and a brief overview of the new policies will be given. Each employee will then receive a copy of the new policies and be given time to submit feedback to their managers. Department managers will be responsible for collecting and evaluating the feedback received and follow up with their direct reports. Once the feedback period has ended, management will meet to discuss the feedback received, evaluate, and update the policies accordingly.

Once the policies have been updated, the final policies will be distributed to all employees for training by the IT staff and department leads. The IT department will be empowered to audit company owned IT equipment on a random basis to ensure compliance. When a device passes the audit, the employees responsible for that device should receive positive marks on their employee records which are then included in future performance evaluations which can lead to better raises or bonuses for employees. This will incentivize employees to follow the new policies and they will also be incentivized to encourage their coworkers to follow the policy.

There will also be a minimum of quarterly full audits of all company owned devices. These will be performed by the IT security employees with the results submitted to IT management, the CEO, and the board of directors. The random and quarterly audits will provide successes to leadership who can then communicate those wins to employees. This will give the employees a look into the success of the policies and feel pride that the policies they helped create are working and securing the company. Lastly, security checklists should be created for employee use during training and additional ones provided to them for their day-to-day activities. Employees should be encouraged to use and follow these checklists until they can perform these security tasks without needing to refer to the checklists.

Policy Lifecycle

Each policy will follow a life cycle that requires regular re-assessment. By following the life cycle, each policy will be reviewed regularly to ensure compliance with current government standards and industry best practices. It will also allow the policies to be updated for changes in technology and needs of the business. As the business grows, roles may shift to new departments or personnel or outsourced to other companies to reduce the company's risk, expenses, and liabilities. See Table 2 below for details on the policy life cycle plan.

Desired future state:

The desired of Wilbur's Widgets is the implantation of the described polices and procedures. The changes made to Wilbur's Widgets security policies will help secure the company from future risks of data losses or data breaches. It will also reduce the company's threat surface, minimizing the chance of an attack. This will also reduce the legal and financial liability of Wilbur's Widgets.

Appendix 1: Tables

Table 1: Recommended Policies

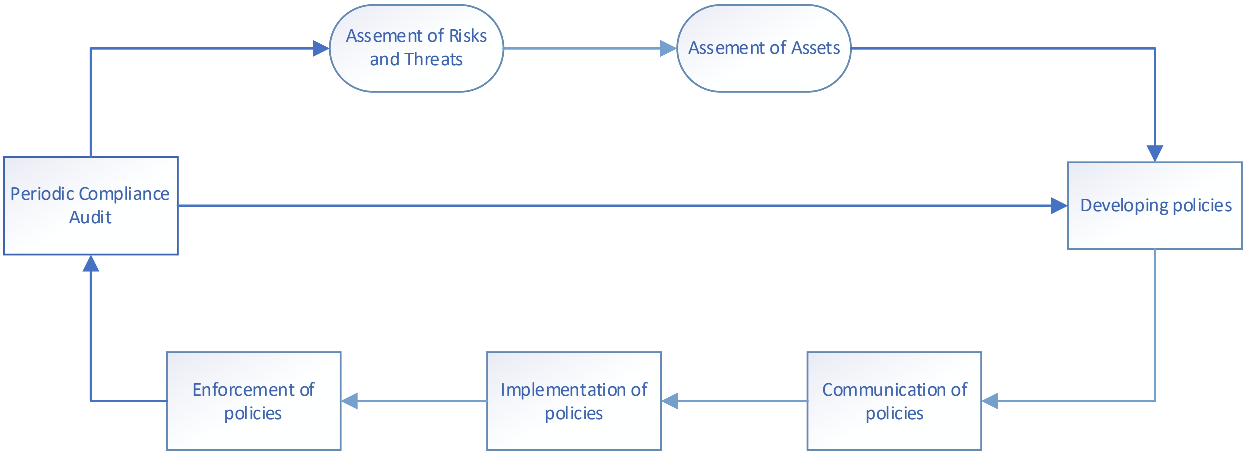
Acceptable Use Policy	The acceptable use policy will detail the rules for accessing and using Wilbur’s Widgets technology. This includes desktops, laptops, servers, mobile devices such a tablets and phones, and the network. It will detail what activities are allowed and not allowed on Wilbur’s Widgets technology. By detailing what type of activities are and are not allowed on company equipment and networks, the company will aim to protect itself from liability if illegal or unapproved activities take place. This policy also aims to reduce the risk of computers or the network being infected by malware.
Physical Access Policy	The physical access policy aims to increase the physical security of Wilbur’s Widgets locations. The policy will establish standards for allowing, denying, and logging of physical access to company locations. This policy will apply to external and internal access. This policy will detail visitation hours and policies, who has access to secure internal locations such as offices, server rooms, and manufacturing areas, and how long logs will be stored for. This policy is to ensure the physical security of company property and reduce the incidences unauthorized access and create an audit process in the case of a physical breach or theft.
Clean Desk Policy	This policy is to ensure that no sensitive information is left out to be stolen or viewed by unauthorized personnel. It will detail what information is and is not allowed to be left unattended on employee desks. This policy is to reduce the risk of data theft. It will also reduce the liability of the company by mandating what information is not allowed to be left exposed.
Personal Mobile Device Policy	This policy is to detail the use of personal mobile devices on company property and their interaction with company resources such as the company network and company data. This policy will dictate how and when personal devices such as mobile phones, tablets, and laptops will be allowed to access

	the company network and data. This policy will ensure that users who need access to company information and networks on non-company devices follow established security practices and that users do not access company information or networks without permission. This policy also seeks to limit the company's legal liability in the instance a user accesses company data or networks without permission and a breach, theft, or malware infection occurs.
Electronic Waste Policy	This policy will describe how electronic devices such as, but not limited to, company issued computers and cell phones, will be recycled when they are no longer usable or are replaced by newer equipment. This is important because if a company issued laptop, desktop, or mobile device is not completely cleared of data before destruction, recycling, sale, or donation, a malicious actor could use data recovery tools to steal company information. By ensuring complete and proper deletion of data, this will reduce the company's risk of data theft and reduce the company's liability.
Data Backup and Recovery policy	This policy will be used to create the scheduled backup policy of company data. This will ensure that should data loss or theft occur that it can be restored quickly minimizing downtime. It will ensure that should data be stolen and deleted from company it is not lost permanently. This will reduce the damage done by data breaches, natural disasters, and data mismanagement such as accidental deletion. This will also assist in police investigations by establishing data ownership in cases of corporate espionage. This will protect the company from liability in cases of accidental deletion of company data as well.
Security training	This policy will be used to create a schedule of security training. These trainings will be held on a regular basis to ensure employees are aware of and understand current policies. Refresher training sessions will be scheduled as management sees fit in instances of policy violations. Additional trainings will be scheduled when additional policies are

	created, or existing policies are updated significantly. Because these policies are the frontline of defense against breaches and data loss, it is important that users are properly trained. By ensuring users are trained it will reduce the risk of these incidents occurring and reduce the company's liability should an incident occur.

Appendix 2: Figures

Figure 1: Policy Lifecycle overview


Assement of Risks and Threats
Assement of Assets
Periodic Compliance Audit
Developing policies
Enforcement of policies
Implementation of policies
Communication of policies