Report on Improving Cybersecurity by using Monitoring Software for West Valley Business Products

for

Steve Smith
Senior Manager
IT Department at West Valley Business Products

by

Jacklyn Kohls
HR Assistant
Human Resources Department at West Valley Business Products

August 2019

Introduction

The use of technological tools to improve the company's efficiency has become necessary to keep up with technological advancements. While technology has helped make its data more manageable and accessible, West Valley Business Products must be cautious of the risks associated with its use.

Currently, there is a lack of enforced cybersecurity among the employees within the company. Employees have sometimes engaged in risky internet behavior by connecting to faulty web hosts or accessing private documents in unauthorized locations. Some of them may be aware of the risks they are taking and others may believe that the data is already secured because the company has not stated otherwise. Either way, this puts West Valley Business Products at risk of a data breach and is therefore an issue that needs to be addressed immediately.

This report will address the pros and cons of a possible solution to the cybersecurity issue mentioned, diving into further detail about the company's inadequate state of cybersecurity and how to improve it. The best possible solution, according to cybersecurity professionals, involves the installation of software that monitors employee internet usage and prevents interception from outside sources.

Issues with Cybersecurity at West Valley Business Products

West Valley Business Products' privacy and security policies are well known among its employees, however these policies have not guaranteed the prevention of employees engaging in behavior that could result in compromised data. It has been discovered that a small number of employees have accessed product inventory, financial documents and online client accounts while connected to unsecured wifi networks. It has also been reported that two employees have allowed other people to use their laptops with confidential information stored to them, giving these other people access to the company's data. This is all considered employee engagement in risky behavior that could lead to a potential data breach in the near future if it continues. Since the policies and rigorous training have obviously not had enough of an effect on the employees, it's time that the company find a more effective solution: installing an advanced cybersecurity software that monitors all employee online behavior associated with accessing the company's data.

To illustrate the typical employee activity among businesses that is similar to West Valley Business Products' employee activity, The Right Technologies Unlock the Potential of the Digital Workplace by Aruba provides statistics from a 2017 study. It was found that 70% of employees admitted to some kind of risky online behavior over the past year despite that 92% of employees claimed to be aware of the potential impact of a company data breach. 70% is significantly high and West Valley Business Products is on track to meet this percentage if no action is taken to prevent risky employee behavior.

Possible Solution for Cybersecurity Issues

The 2017 State of Cybersecurity by Forcepoint encourages the use of an intelligent, integrated system that allows IT professionals to see the type of behavior their users are engaging in and how they are engaging in it. West Valley Business Products can improve cybersecurity by installing this type of software that monitors and controls internet access by employees as a way to prevent them from engaging in risky behavior and protect them from outside invasions. Employee behavior is often changing or unpredictable within the company and has been difficult to keep track of when the company upgrades devices that allow data access such as laptops, tablets and smartphones. The applications that are used on mobile devices to track shipments, enter private client information and access financial records should be monitored to protect confidentiality. An advanced cybersecurity software has the ability to monitor all of this information and who has access to it while keeping up with technological advancements to ensure protection when there are device upgrades and software updates. The idea is that this cybersecurity software will always be one step ahead and have the ability to pinpoint the source of the risky behavior that occurs.

Cybersecurity Program Breakdown

Providing network security for West Valley Business Products' IT department would involve the integration of technologies, policies, cultural changes and intelligent systems into one cybersecurity program, as defined in the 2017 State of Cybersecurity by Forcepoint. This type of program would have the ability to observe the behavior of all IT users, such as all of the employees who access the company's confidential information on their devices. Then, it will determine whether their behavior is risky or not and have the ability to intervene before a data breach can occur. The program would focus on:

- Protecting employees from compromise as they access the web from any location on any device.
- Providing network security by viewing employee actions throughout the network and defending the network from attackers.
- Identifying the employees that engage in the riskiest behavior and determining which ones need to be investigated and dealt with accordingly by the company.
- Providing complete security for employees to easily transfer sensitive information across all devices within the protected network.

An intelligent cybersecurity program that integrates all of the above listed protection would ideally put an end to the potentially compromising cyber behavior within the company. This would then allow for easier management from West Valley's IT professionals and aid in the overall flow of the company or organization.

Potential Advantages of Installing the Cybersecurity Software

A cybersecurity program that integrates all of the technologies listed above would be ideal for a company such as West Valley Business Products since all of the company's records and data exist within one shared drive among employees who have IT access. Many of these employees are on salary and continue to work remotely after hours in order to meet certain deadlines. This means that employees may try to connect to unstable wifi networks or accidently share information with the wrong person by letting them use their device. In addition, they no longer are in the presence of the policies that exist within their normal work environment so they are more likely to forget them and unknowingly engage in risky behavior. The 2017 State of Cybersecurity suggests that understanding human behavior and intent may be more significant than securing technology. Being that West Valley Business Products values the protection of both its data and its employees, it is in the company's best interest to understand its employees' behavior. This is where the cybersecurity software will come into play and target the intent behind the employees' behavior while being able to stop it in its tracks.

Potential Disadvantages of Installing the Cybersecurity Software

West Valley Business Products employees may feel threatened by a cybersecurity software that monitors their every move on the web. They may feel that they cannot be trusted to handle the company's data and therefore may feel that the program is in violation of their privacy when they are working remotely. There has been an increase in employees working remotely within the company as there has been elsewhere, according to the 2017 State of Cybersecurity, and this significantly affects the IT management style. Between 2012 and 2016, the percentage of employees working remotely increased from 39% to 43% and they have spent more time working remotely than before. Those percentages will continue to increase over time and it is important that employees' privacy is respected if they are given the ability to work from remote locations. It is important that West Valley Business Products focus on employee retention in addition to cybersecurity and it may be better to handle the security issue by checking in with employees more regularly as opposed to installing a program to do that for them.

Conclusion

Cyber protection can greatly benefit a company such as West Valley Business Products who are heavily reliant on technology as a means of client data entry and financial data storage. External harddrives and the folders within those harddrives have replaced file cabinets and file folders that were previously only physically accessible to employees. Instead, all stored information is easily accessible to employees with IT access in practically any location they choose to work from. An advanced cybersecurity program that can easily monitor this activity and determine the source of risky cyber behavior could easily prevent a company data breach from occurring while protecting its employees in the process.