Acme Corporation Security Posture Report

Carson Bird

University of Michigan, Flint

CYB 303: Security Operations

Dr. Mario Booker

December 12, 2024

Table of Contents

Executive Summary

The security posture report process of Acme Corporation is written in a way to go over the summary of Acme Corporation as a whole, the methodology of the report, the types of assets owned by Acme, a risk assessment of Acme Corporation, main security controls found within the corporation, A vulnerability assessment of Acme, and lastly, a conclusion to the security posture report. Each main section of the report will be sectioned off into subsections going over more specific topics of the main sections.

This report is being done in order to review and report key findings of Acme Corporation with respect to their cyber security posture. Some of the key findings of the report include the total key assets owned by Acme Corporation, which total up to $1,010,630,580.18. The top five risks associated with Acme. These are DDoSing, Phishing, fair-use legal action, data breaches, and on end-user devices. Security implementation will be deeply divided into. This will mainly go into depth about testing frameworks, patch management, and more. The vulnerability assessment of Acme will look over a wide range of potential vulnerabilities. This will range from key assets, such as building protection, to remedies for said vulnerabilities. Some recommendations of these findings include more advanced password management, advanced and frequent employee training, encryption of company data, and a set plan in place for incidents

(such as the use of segmentation). Lastly, the conclusion will touch on key points discussed in the security posture report.

By implementing the findings of the security posture report, Acme Corporation will be able to further strengthen its already hardened security within the company. This report will be considered a means to a beginning, with continued future posture reports being done annually.

Introduction of Acme Corporation Security Posture Report

Methodology of Acme Corporation Security Posture Report

This posture report will be split into the main sections of an introduction of the Acme Corporation, an asset inventory report, Acme Corporation security controls, a vulnerability, and finally a conclusion of the whole report. Within each main section, it will start with a section methodology in order to better understand the main section structure. Then there will be multiple subsections going into a deep dive of specific aspects that fall under the main section. Each main section will then end with a section conclusion giving an overview of the section.

However, the main sections of the introduction section and conclusion will not follow the above main section methodology. The introduction section will contain the security posture report methodology and a brief overview of Acme Corporation. The conclusion of the report will have a quick analysis of the main section's findings as well as a reflection of Acme’s security.

Overview of Acme Corporation

Acme Corporation is a technology company located in North America. It was founded by Jeffery Donahu on April 1st, 2011. Jeffery Donahu invented a super affordable and high-throttle system to store data. The corporation became public on February 13th, 2014, with an average share price of $45.62. Acme averages 6.4 billion dollars of revenue a year.

Acme specializes in the storage and streaming of videos. They are considered one of the top five streaming companies in North America. They have locations in Texas, Illinois, New York, Colorado, and Michigan. Currently, they employ over three thousand employees. While they do have an in-house cyber and physical security team, They recently partnered with a world-leading cybersecurity firm in order to streamline the safety of company assets. This shift has seen a reduction of cyber attacks and data breaches.

Asset Inventory Report

Methodology of Asset Inventory Report

ID Number:	**Type:**
O1	Windows
O2	Linux
O3	macOS

This asset report was conducted by the subsidiary Acme Corporation Office Zeta from the span of March 11th, 2023, to June 7th, 2023. This report includes asset IDs, type of asset, model of asset, manufacturer of asset, and price and amount of said asset. Furthermore, assets with operating systems will have one of three tags appended to the asset ID. Denoting between Windows, Mac, and Linux operating systems.

Acme Corporation Location Overview

Acme Corporation currently owns two data centers and five branch offices. These data centers are used for distributing content such as live streams, music, and videos. The five branch offices maintain the public and private sides of the company. They are located in different regions of the United States in order to serve the large variety of consumers Acme provides its services too. The figure below shows the subsidiary name and current address of the subsidiary.

Acme Corporation Subsidiaries:	**Location:**
Data Center Alpha	1234 W. Maple St., Chicago, IL 60610
Data Center Omega	9102 N. Elm Dr., Dallas, TX 75201
Office Alpha	5678 S. Oak Ave., Chicago, IL 60616
Office Omega	3456 E. Cedar Blvd., Dallas, TX 75204
Office Beta	789 Broadway Ave., New York, NY 10003
Office Gamma	2345 Pine Lane, Boulder, CO 80301
Office Zeta	4567 Grand River Ave., Detroit, MI 48208

Acme Corporation Data Center Assets

Data Center Alpha and Omega hold some of Acme's most important assets. In order to protect said assets, Acme has built around each property a ten-foot-tall metal fence topped with barbed wire. A plethora of lights and cameras are placed around and within the compound. Each entrance is guarded by an in-house security agent who checks employee IDs. In order to gain access to the building, one must swipe their ID card and enter an assigned PIN. Once employees will go through a metal detector.

Alpha and Omega both contain twenty, forty-two unit server racks full of top-of-the-line server units. Windows and Linux operating systems are deployed through each facility. Equipped to each server rack is a singular industrial cooling system. As added protection, each data center is equipped with roof-mounted air conditioning systems constantly running at 45 degrees Fahrenheit, as well as multiple backup generators. One SAN array, ten physical firewalls, three backup servers, and five load balancers are allotted to each facility. In total, the data centers have $6,042,141.38 worth of assets.

Asset ID:	Type:	Model:	Manufacturer:	Price:
D00001 - D00040	Server rack	NavePoint 42U Server Rack Cabinet, 800mm depth, Fan Compatible Top, Perforated Door (Commercial Series) - 00406222	NavePoint	$1,500.00 X 40 units
D00041 - D00461 (O2)	Server	PowerEdge R450 Rack Server (AP9562)	Dell Technologies	$3,129.00 X 420 units
D00462 - D01722 (O1)	Server	PowerEdge R450 Rack Server (AP9562)	Dell Technologies	$3,129.00 X 1260 units
D01723 - D01763	Cooling system	SmartRack Portable Server Rack Cooling Unit, 12,000 BTU, 120 V, TRP SRCOOL12K	Tripp Lite	$1,443.00 X 40 units
D01764 - D01765	SAN	PowerVault ME484 storage expansion enclosure with 28 20tb hdd SAS USE 12gb s 7.2k 512e 3.5in hot-plug - ME484	Dell Technologies	$141,895.69 X 2 units
D01766 - D01786	Firewall	SonicWall High Availability Security Appliance (TZ370)	Dell Technologies	$565.00 X 20 units
D01787 - D01797	Load balancer	S5810-48TS, 48-Port Gigabit Ethernet L3 Switch, 48 x Gigabit RJ45, with 4 x 10Gb SFP+ Uplinks, PicOS®, Support MLAG, Broadcom	FS	$1,579.00 X 10 units
D01798 - D01804	Backup server	Quantum Scalar i6000 Base Tape Library Control Module. Add Slots and Drives (TO9)	Quantum	$59,770.00 X 6 units

Acme Corporation Branch Office Assets

The Acme branch offices handle some of the most integral duties within the corporation. To ensure things run smoothly and efficiently. Each office is equipped with three forty-two unit servers, again consisting of a mix of Windows and Linux operating systems, and physical firewalls. Each branch is monitored by a third-party security agency, and regular auditing is done

to ensure the branches are secure. In total, the branch offices have a combined asset total of $2,018,240.

Asset ID:	**Type:**	**Model:**	**Manufacturer:**	**Price:**
B001 - B015	Server rack	NavePoint 42U Server Rack Cabinet, 800mm depth, Fan Compatible Top, Perforated Door (Commercial Series) (00406222)	NavePoint	$1,500.00 X 15 units
B016 - B436 (O1)	Server	PowerEdge R450 Rack Server (AP9562)	Dell Technologies	$3,129.00 X 420 units
B437 - B646 (O2)	Server	PowerEdge R450 Rack Server (AP9562)	Dell Technologies	$3,129.00 X 210 units
B647 - B662	Cooling system	SmartRack Portable Server Rack Cooling Unit, 12,000 BTU, 120 V, TRP SRCOOL12K	Tripp Lite	$1443.00 X 15 units
B663 - B668	Fire wall	SonicWall High Availability Security Appliance (TZ370)	Dell Technologies	$565.00 X 5 units

Acme Corporation End-user Devices

Acme Corporation prides itself on the ability to reach all devices. This means that the company must also own all devices. In total, Acme owns eight hundred desktop computers, two hundred laptops, consisting of both macOS and Windows operating systems, and fifty tablets. To ensure these devices are being used according to code. A zero-trust procedure is in place. This ensures the security of the network and its devices. The company holds a no-phone policy, ensuring nothing malicious happens within company grounds. In total, Acme owns $1,263,076 worth of end-user devices.

Asset ID:	**Type:**	**Model:**	**Manufacturer:**	**Price:**
EU00001 - EU00800 (O1)	Desktop computer	OptiPlex Micro Form Factor, 7020 Plus	Dell Technologies	$989.00 X 800 units
EU00801 - EU01600	Desktop monitor	Dell 24 Monitor, SE2422H	Dell Technologies	$99.99 X 800 units
EU016001 - EU02400	Desktop mouse	Lenovo 300 USB Mouse GX30M39704	Lenovo	$7.99 X 800 units
EU02401 - EU02500 (O1)	Laptop	ThinkBook 16 Gen 7 AMD ( ) - 21MW0005US	Lenovo	$1,399.00 X 100 units
EU02501 - EU02600 (O3)	Laptop	Apple MacBook Air M3 (13”) - MRXN3xx/A	Apple	$1099.00 X 100 units
EU02601 - EU02650	Tablet	iPad Pro 13-inch (M4) - A2926	Apple	$2,394.00 X 50 units
EU02651 - EU03450	Desktop keyboard	Dell Multimedia Keyboard-KB216, US International (QWERTY) - Black, 739P7	Dell Technologies	$19.99 X 800 units

Acme Corporation Network Infrastructure Assets

In order to stay connected, fiber optic cables run from each branch and data center. Each facility is equipped with top-of-the-line switches, WAN routers, NICs, optical transceivers, and wifi routers. In case of an emergency, information can be routed between the different locations to ensure interconnectivity. In total, the network infrastructure has a price of $77,799.80.

Asset ID:	Type:	Model:	Manufacturer:	Price:
N001 - N020	Switch	Force10 S4810-ON	Dell Technologies	$796.97 X 20 units
N021 - N040	WAN router	Dell Edge Gateway 3200	Dell Technologies	$1,484.03 X 20 units
N041 - N060	NICs	NVIDIA Mellanox MCX516A-CCAT ConnectX®-5 EN Network Interface Card, 100GbE Dual-Port QSFP28, PCIe3.0 x 16, Tall & Short Bracket	Mellanox	$809.00 X 20 units
N061 - N080	Optical transceivers	Cisco SFP-10G-LR 10GBase-LR SFP+ Transceiver Modules 10 Gbps	Cisco	$400.00 X 20 units
N081 - N100	Wifi routers	Nighthawk WiFi 7 Router RS500, 12Gbps	Netgear	$399.99 X 20 units

Acme Corporation Security and Monitoring

Acme Corporation went away with their in-house security and monitoring in 2014. Currently, a third party ensures that Acme's virtual and physical assets stay protected. This includes threat detection, content filtering, vulnerability scans, and regular penetration tests. Since 2014, Acme has had five small-scale attacks that were swiftly defended against. The corporation allocates $1,229,323 annually to this third party.

Acme Corporation Business Applications

Acme Corporation developed an enterprise resource planning system in 2012 to adjust the expansion of the company. It is used to track employee time cards, payroll, as well as department budgets. Office Beta is the company's leading office in handling customers. This includes email responses, bug fixes, and marketing. In 2019, Acme went away with their

in-house collaboration suite instead to use the Microsoft-developed software, such as Microsoft Teams. The pride and joy of Acme is the video storage system that was created by Jeffery Donahu in 2013. In total, it is valued at $1,000,000,000.

Acme Corporation Asset Report Conclusion

Acme Corporation's assets have grown by fifteen percent in the last five years. Accounting for all major assets combined plus the annual payment to the third party providing security. Acme has a total of $1,010,630,580.18 worth of assets as of June 7, 2023.

Risk Assessment of Acme Corporation

Methodology of Risk Assessment

This section of the report will go over the main risks associated with Acme's IT infrastructure. Each risk will be defined as a risk type, a rating (1–5, where 1 is very unlikely and 5 is very likely), and an impact rating (1–5, where 1 is minimal impact and 5 is severe impact). As well, each will be defined by why each rating was applied. The top 5 highest scoring risks will have their own section dedicated to strategies in order to mitigate said risks from happening, an explanation on how said strategies will work, and lastly, any challenges associated with the strategy.

IT Infrastructure Risk Types

In the world of a technology-based company, there will be a multitude of risks associated with the company. The main seven risk types will consist of: physical security, data security, network security, business continuity and disaster recovery, compliance and regulatory risks, operational risks, and third-party/vendor risks. Physical security risks are associated with assets such as physical locations, i.e., data centers and offices, equipment, etc. Data security risks include user and company data being lost. Network security risks are considered protection of

resources within a network. Business continuity and disaster recovery are the risk of the company not being able to function in turn of a scenario such as natural disasters or cyber attacks. Compliance and regulatory risks include legal risks associated with running a corporation. Operational risks, which encompass internal and external needs to keep Acme running. Lastly, third-party/vendor risks are considered when working with outside vendors and third-parties associated with Acme Corporation.

Acme IT Infrastructure Risks

Acme Corporation faces a variety of risks involving its IT infrastructure. These risks can be categorized into seven different risk types. These risk types are: physical security, network security, data security, business continuity and disaster recovery, compliance and regulatory risks, operational risks, and third-party/vendor risks.

Physical security plays an important but common overlooked role in IT infrastructure security. Unauthorized access to data centers can cause the potential for hurt employees or property to be stolen/damaged. This could also lead to malicious acts taking place inside the data center.

Network security is the process of protecting information held within an infrastructure as well as the resources of the infrastructure. Two of the most common types of network security threats include malware being installed on end-user devices and Distributed Denial of Services (DDoS) attacks occurring. “A distributed denial of service attack is designed to overwhelm victims with traffic and prevent their network resources from working correctly for their legitimate clients.” (Nazario, 2008) Malware being installed on end-user devices such as computers could cause data to be withheld or breached, compromising network traffic. DDoS

Attacks on a network could cause widespread outages on the network. With Acme primarily being a video streaming and storage provider, this could cause severe consequences.

Data security, and most importantly, data breaches. Could cause some of the most extreme consequences for Acme. With millions of users private information being stored and collected on Acme servers. A data breach could cripple the trust and resources the corporation provides. Potentially leading to legal action. On the other hand, credential fraud, such as account sharing and credit card fraud, is a commonly seen risk within Acme Corporation. With proper measures, this can be detected and reduced.

Acme Corporation has locations all over the United States; the risk of business continuity and disaster recovery on the IT infrastructure of the corporation should also be considered. With two important locations being located in Texas, flooding, hurricanes, and tornadoes should be considered. While this is very likely to happen, it is important to consider what might be done in case a natural disaster disrupts the IT infrastructure.

When dealing with user data as a video streaming and storage company, compliance and regulatory risks will occur. Fair-use laws could be broken in the case of something being uploaded that does not lie under its guidelines. Stream-ripping is one of the most common risks associated with providing streaming services. While common, this can also lead to extensive legal battles.

Operational risk, such as an employee account being compromised to phishing, can lead to important devices and accounts being compromised. Operational risks such as phishing heavily rely on the need for employees to midgate this.

Lastly, the risks associated with third-party vendors, mainly them being compromised, are serious yet not very likely. Acme relies on a third party to provide cybersecurity functions for

the corporation. Since the third party is one of the leading companies, the risk of this occurring is low. If this is compromised, this could lead to the whole IT infrastructure of Acme being liable to severe risks.

Acme IT Infrastructure Risk Assessment Table

Risk Type	**Risk**	**Likelihood Rating**	**Impact Rating**	**Justification**
Physical Security	Unauthorized access to data centers	1	3	Strict access to facilities, but potential consequences
Network Security	Malware on end-user devices	4	3	Frequent threat, but easy to avoid (security policies)
Data Security	Data breach	3	5	Could it possibly happen? If it does, sensitive data could be leaked
Business continuity and disaster recovery	Natural disaster	2	3	Not likely to happen but could potentially cause issues such as flooded buildings
Compliance and regulatory risks	Stream ripping	5	2	Very likely to happen but some mild legal action will occur
Operational risks	Phishing	5	4	Frequent threats could lead to employee accounts being compromised
Third-party and vendor risks	Third-party outsourcing breach	1	4	Potential to happen; if it did occur, the cyber security systems outsourced could lead to catastrophic problems
Network Security	Distributed Denial of	5	5	Frequent threats could cause severe disruption in IT infrastructure

	Service (DDoS)			
Data Security	Credential fraud	4	2	Very likely to occur, can be detected and reduced
Compliance and regulatory risks	Fair-use/Legal action	4	4	Very likely to occur, could cause expansive legal battles

Acme Risk Mitigation Strategies

In order to ensure these risks are not realized, strategies can be implemented. In no particular order, the highest scoring risks associated with the IT infrastructure of Acme Corporation would be malware on end-user devices, data breaches, phishing, DDoSing, and fair-use/legal action.

Malware on end-user devices as stated before has the potential to cause severe issues. The best way to avoid malware being downloaded on end-user devices is by following a strict employee-user policy. This could include tagging in and out of which devices are being used and by whom. Proper employee training can prepare employees for steps to take in order to spot malicious software or websites. Implementing a restricted download policy for devices can also help. On top of this, implementing a firewall and top of the line antivirus programs can help prevent this. Many aspects of this strategy—making sure employees follow them—aren't that simple. Human error can lead to these countermeasures falling completely useless.

Data security, mainly data breaches, are considered the highest threat if one comes to fruition. This can happen for a variety of reasons, but most commonly it is from a bad actor infiltrating the network. The best way to counter this risk is to make sure data is encrypted in 256-bit encoding. Then making sure the encryption key changes every 24 hours. This would

ensure that it was virtually impossible for hackers to decode the information that was stolen. The limitation to this is the cost associated with setting it up and maintaining it on a large scale.

Phishing attacks are one of the most common attacks that could put Acme at risk. Employee training and proper testing of employees can lead to phishing attacks becoming less common. Proper training should be frequent with a fake company sending phishing emails to employee emails. This would allow Acme to focus on training employees who need help with recognizing phishing attacks. Implementing anti-phishing software on computers can also help catch phishing emails. Human error is the biggest contributor to why this strategy might fail.

Disturbed Denial of Service is another one of the highest threats Acme Corp. could fall victim to too. It is important to install load balancers and restrict network traffic using a zero trust policy. Load balancers would detect and migrate network-related services if too much traffic is overloading a server. Restricting traffic can be done by only allowing certain users or user locations to access the network. Then, make sure the user on the network is constantly verifying itself to be allowed on the network. This would make sure if a botnet was to attack a network, the system would balance the users and start to shut off connections to non-verified users. The biggest risk involved with this strategy would be the possibility of the botnet having root access to PCs already located in the network. In order to gain false verification and be granted permission to the network.

Lastly, the risk of fair use/legal action is a very common and highly impactful risk when running a video streaming and storage company. Using an AI to screen videos for copyrighted material, such as music, can help avoid the risk of being sued for copyright infringement. Allowing companies to file DMCA requests to take down potentially copyrighted material can allow the liability of being sued to diminish. The most important thing to make sure of is that in

terms of service, it is recognized that Acme is not liable for any stolen virtual property. This would ensure that, in case of litigation, legal action can be dismissed. The biggest risk of this strategy not working is if these policies are not enforced correctly. This would lead to even more serious legal action.

Acme Corporation Risk Matrix

Risk Assessment Matrix						
Likelihood	**5**				Phishing	DDoS
	4			Malware end-user devices	Fair-use/ legal action	
	3					Data breach
	2					
	1					
Low	**High**	**1**	**2**	**3**	**4**	**5**
Medium	**Very High**	**Effect**				

Acme Risk Assessment Conclusion

As a leading company in the tech space, Acme Corp. must be considerate of every risk that may compromise the IT infrastructure. The physical security, network security, data security, business continuity and disaster recovery, compliance and regulatory risks, operational risks, and third-party/vendor risks. Should be documented, and proper protocols should be taken in order to ensure operations run smoothly.

Acme Corporation Security Controls

Methodology of Security Controls

This report will be sectioned into five distinct security implementation-related sections, going over security controls, policy development, employee training, vulnerability scanning, and penetration testing. The final section of this report will be a conclusion of the said implementations.

Acme Corporation Security Controls

Security controls are put in place to protect Acme's information and other assets safe from threats and risks. The three main areas of this security fall into the categories of network security controls, endpoint protection, and access control. Without these Acme can be at risk to viruses, malware, DDoSing attacks, and other hacks. Many of these security controls act as a virtual first line of defense for the corporation.

Network security controls are implemented to keep the network and devices connected to it safe. Many household computers come preinstalled with Windows as their operating system. Within the Windows OS there is a firewall called "Microsoft Defender." This allows the computer to only allow safe network connections while filtering out malicious connections. While extremely helpful as a layer of protection, at Acme more security must be implemented to protect such a costly network system.

Acme currently uses the SonicWall TZ370 High Availability Security Appliance as a physical firewall for its server rooms. This next-generation firewall includes redundant power systems, 10/5/2.5/1 GbE interfaces, SD-Branches, and SD-WAN capability. The TZ370 runs on the ground-breaking SonicOS 7.0; this operating system is designed to protect and control network traffic. Unknown threats are sent to the SonicWall cloud-based Advanced Threat Protection using a multi-engine sandbox in order to analyze the threat. The firewall also includes

deep packet inspection, content filtering, anti-virus, and anti-spyware protection. Each firewall and coinciding servers are separated into its own virtual local area network. This ensures that if one VLAN is compromised, none of the other VLANs are at risk.

End-point protection is the protection of all in-house devices, such as laptops and desktops. These are implemented with the third-party company antivirus and firewall software. This third-party company handles a majority of Acme's cybersecurity functions. Some functions of this third-party software include, but are not limited to, whitelisting of applications, real-time threat detection, zero-trust network capabilities, scanning, and more. This can be all monitored by people of appropriate authority within the third-party company. Updates for this software are released biweekly to maintain integrity. These updates are pushed automatically to devices with a 24-hour window. Each device is given the ability to roll back updates within 5 minutes of the update being installed.

Access control is one of the most important but widely overlooked sides of Acme's security control system. Starting with one of the most simple yet important aspects of access control is Acme's password policy. Each employee is required to have an encrypted hash password and physical password key for said encryption. These physical encryption keys are kept behind three layers of security. In order for an employee to gain access to them, they must pass a biometric door lock and be buzzed in through the man trap. Then be given the key by the onsite decryption key manager. Every 14 days, the hashed password and key are changed. After logging into the system, the user must complete a two-factor authentication.

The network runs on a zero-trust protocol. Requiring users of the network to constantly verify they are allowed to be on it. No device from outside the location of the specific Acme building is allowed to access the employee side of the network. This allows for non-authorized

access to swiftly be taken care of. These are monitored as well by the third-party cybersecurity company.

Acme Corporation Policy Development Framework

In the last ten years, a lot of things in the digital world have changed. With this, Acme Corporation's policies for employees have evolved too. Some core policies of Acme are the acceptable use policy, information security policy, and access control policy. These policies allow for a sturdy foundation for some of Acme Corp's other policies, such as the incident response and management change policy.

Acceptable use policy is the umbrella policy for all employees on how they should conduct themselves online. This policy is in place to keep the company and its employees safe and productive. Some key rules in this include not using user-end devices for personal needs, not accessing pornographic sites while on the network, using work email for work usage only, and more. If these rules were not followed, it could lead to the potential risk of a phishing attack or worse on an end-user device.

Information security policies aim to protect the coveted information of users, employees, and the corporation itself. The main facet of this policy is the risk assessment methodology. Currently, Acme operates in conjunction with the third-party cybersecurity company to handle this methodology. This involves identifying key risks held within Acme and seeing how deeply this could affect operations. Besides this risk assessment, there are a plethora of security controls implemented in the corporation's framework. Some of these include the training of all administrative employees, the usage of firewalls and other security software, and making each physical Acme facility secure.

Access control policies go over who and where can use and access Acme's network.

This policy is separated between customers, employees, and administrative users. Customers are allowed to use Acme's network to stream and upload videos too. They do not have access to any non-surface-level software or information. Employees will have a bit more access to the network, while still limited. This is based on a need-to-know basis and still has the zero trust policy implemented into it. Lastly, administrative users will have a wide variety of controls over the network. This is monitored at a higher rate than any of the other levels of access. Employees and administrative users are not permitted to access any of Acme's network from outside specific locations.

Acme Corporation Employee Security Training Program

Employees are considered the first line of defense within Acme. This is why Acme has implemented a comprehensive employee training program. The first step in the security training program is with new hire orientation. This orientation goes over what to expect and be expected of as an employee of Acme at the most basic level. Some of the things talked about in this orientation are the appropriate usage of end-user devices, going over how to stay safe when accessing the internet, and how the password system works. This ensures that each new employee has basic knowledge of security fundamentals.

After this is down, biweekly each employee will be assigned to do an interactive one-hour paid security program. This program will go over deeper security concepts based on their access control level. This could consist of threats and risks, recent incidents, and how to mitigate them. After each session, the employee will take a short quiz on what they learned. If the score is not satisfactory, more training will be required.

Every month, each employee will have to attend a three-hour seminar and training session provided by the third-party cyber security company. This seminar will go over the flaws

seen by the company and what needs to be improved upon. Employees will be given fake scenarios in teams and asked to solve the scenario. After this is done, any unsatisfactory groups will be assigned more training if needed.

On the daily, employees will be sent a newsletter that goes over basic security fundamentals to think about. On the other hand, random fake third-party phishing attacks will be conducted on employees. If an employee fails the fake attack. They will be subjected to an interactive video course on how to stop phishing attacks. Employees who successfully pass A hundred or more fake phishing attacks will be rewarded with a salary bonus. This is seen to encourage employees to stay vigilant of security concerns.

Acme Corporation Vulnerability Management Program

Acme Corporation Vulnerability Management involves the scanning requirements and remediation process of all vulnerabilities within Acme. This is done in partnership with the third-party cyber security company. This is done to make sure that the network is kept up-to-date and secure. Any issues with it can be remedied through the specific process constructed to fit Acme's needs.

Acme Corp. requires one weekly and one monthly vulnerability scan. The weekly scan consists of a scan of the network infrastructure, server environments, and the web environment. This is done to make sure that no vulnerabilities are visible on a surface level. Monthly scans consist of deep internal scans of the infrastructure, database, and all in-house internal software. These scans take roughly five hours to complete. This scan can find deep issues in the network, source code of software, and more.

If an issue is found within the scan, a remediation process will immediately be taken into effect. The third-party cyber security company operates 24/7 in order to assure no vulnerabilities

go unchecked. The risk-based priority approach consists of critical prioritization; this must be remedied in less than 24 hours. High-priority issues must be resolved in less than three days. Medium issues must be addressed within a week. Lastly, low-priority issues must be resolved within two weeks. After these issues are resolved, a deep scan will be done to make sure there are no new issues associated with the vulnerability. After each scan and remediation, a log will be made explaining the vulnerability and how said vulnerability was remedied. This process allows Acme to go back and see how well certain vulnerabilities might have been taken care of in order to collect data for the future.

Acme Corporation Patch Management

The management of patches to Acme's security control framework is highly important. If a patch to a bug in a system is not remedied, it could lead to potential exploits or an unenjoyable user experience. The patches should be prioritized based on the severity of the vulnerability. This ensures that critical patches are deployed to parts of the infrastructure that matter the most. After each patch, there should be a process of testing in order to make sure the issue was solved and didn't cause any new ones. Rollouts of patches should be down weekly, while severe risks should be addressed and patched immediately.

Acme Corporation Penetration Testing Framework

Penetration testing is the process of probing a network, or software, etc., for vulnerabilities by actively trying to exploit it. This is usually done in a way to predict threat actor actions before a threat actor takes action. Once a penetration test is finished, issues found will go through the remediation process. Acme's cyber security partnership handles all penetration tests done. Some of the testing scopes focused on by the cyber security company are external network, internal network, and application security.

External network testing consists of probing the internet-facing systems for vulnerabilities that could be exploited. This is mainly done on the Acme video streaming website. This is also done on the cloud-based storage, where users can upload their own videos.

Internal network testing consists of probing the inside of Acme's infrastructure. Such as trying to compromise servers, elevate privileges on servers in order to be used in a malicious manner, trying to gain access to information not permitted at a certain access control, and more.

Application testing is done to ensure that the applications provided by Acme, such as their mobile and web-based video streaming applications, can't be breached. Some concerning Web-based vulnerabilities are the potential for cross-site scripting or SQL injection. This can be done to trick users into downloading malicious content. The mobile application could potentially be breached, and user data could be stolen.

These penetration tests are conducted monthly on each aspect provided by the framework. Every three months, the partnered cybersecurity company will outsource the penetration test to another cybersecurity company in order to gain a deeper level of testing completed. This makes sure the standard in-house testing is not overlooking any flaws. Recently, AI has been being used to continuously test certain web and mobile applications for vulnerabilities. After each test is completed, a comprehensive report is written and shared with administrative members of Acme.

Acme Corporation Security Implementation Conclusion

Acme Corporation prides itself on the implementation of these distinct security sections: security controls, policy development, employee training, vulnerability scanning, and penetration testing. While these implications are working well for the corporation, with the nature of the evolving technology field, more security protocols will be implemented.

Acme Corporation Vulnerability Assessment

Methodology of Vulnerability Assessment

This vulnerability assessment will talk about some of the key assets Acme owns. Afterwards, Acme's security controls will be talked about. This includes admissive, technical, physical, and incident response. Next, the assessment will go over common vulnerabilities associated with Acme and the likelihood of them occurring.

Acme Corporation Key Assets

Acme Corporation prides itself on all the assets the company has. The most notable assets of Acme are its two data centers located in Dallas and Chicago and its five offices located in Chicago, Dallas, New York, Boulder, and Detroit. Each data center consists of 840 servers each (operating with Linux and Windows operating systems). As well as multiple firewalls, backup servers, and SAN arrays. Between all the branch offices, there are a total of 630 servers.

On the network side of Acme's infrastructure, they implement top-of-the-line switches, WAN routers, NICs, optical transceivers, and wifi routers. Considering the massive amount of employees Acme has, they also own a plethora of end-user devices. Some of these include the 800 desktop computers, 200 laptops (Windows and Mac-based operating systems), and 50 laptops. In total, Acme Corporation has about $1,010,630,580.18 worth of assets as of June 7th, 2023.

Acme Corporation Security Controls: Practical Application

Security controls are put in place to protect Acme's information and other assets safe from threats and risks. These security controls are separated into four categories: administrative, technical, physical, and incident response. Some physical security controls include the SonicWall TZ370 High Availability Security Appliance as a physical firewall for its server rooms. These

Next-generation firewalls include redundant power systems, 10/5/2.5/1 GbE interfaces, SD-Branches, and SD-WAN capability. The TZ370 runs on the ground-breaking SonicOS 7.0; this operating system is designed to protect and control network traffic. Each building is physically secured with metal chain fences, barb wire on top, active lights and cameras, and biometric ID and man traps in order to enter the building, and lastly, house security guards. This ensures the wrong people do not enter the buildings.

Technical security controls include all the third-party company antivirus and firewall software. This third-party company handles a majority of Acme's cybersecurity functions. Some functions of this third-party software include, but are not limited to, whitelisting of applications, real-time threat detection, zero-trust network capabilities, scanning, and more. One of the most simple yet important aspects of access control is Acme's password policy. Each employee is required to have an encrypted hash password and physical password key for said encryption. These physical encryption keys are kept behind three layers of security. In order for an employee to gain access to them, they must pass a biometric door lock and be buzzed in through the man trap. Then be given the key by the onsite decryption key manager. Every 14 days, the hashed password and key are changed. After logging into the system, the user must complete a two-factor authentication.

The administrative access controls are mostly handled by the third-party cybersecurity company. They oversee all the updates and important cyber security-focused aspects of business within Acme. This includes training Acme employees, monitoring who is on each network, and looking for threats on the network.

Just like the administrative access controls, the incident responses are handled by the third-party company as well. This ensures that any incident is sectioned off and taken care of. If

an incident is reported, the remediation process will begin. The risk-based priority approach to remediation consists of critical prioritization; this must be remedied in less than 24 hours. High-priority issues must be resolved in less than three days. Medium issues must be addressed within a week. Lastly, low-priority issues must be resolved within two weeks. After these issues are resolved, a deep scan will be done to make sure there are no new issues associated with the vulnerability.

Common Vulnerabilities of Acme Corporation

With Acme being a large company consisting of hundreds of end-user devices and servers, there is the potential for vulnerability. One of the biggest threats to the Acme network is the potential for discarded denial of service attacks (DDoS). These occur when a network is being used by too many users; this can then lag the server, making it potentially useless while said attack is occurring. With thousands of people accessing Acme's services each day, this could help protect these users from malicious users. This vulnerability has the potential to happen a lot and can cause devastating losses to Acme.

Another vulnerability is that one of Acme's key features is the ability to upload users' videos to Acme's cloud-based storage. If any malicious code was uploaded to the cloud. It could potentially be used to steal information. This could be super harmful to all user data and information stored on Acme's infrastructure. This is likely to be attempted if a way is found to do so.

Data security, mainly data breaches, are considered the highest threat if one comes to fruition. This can happen for a variety of reasons, but most commonly it is from a bad actor infiltrating the network. A data breach would leave Acmes secure information at risk. This could lead to legal action, loss of virtual assets, and more. While potentially likely to happen, this could

become a worst-case scenario for Acme. If any vulnerability is to be exploited, this will most likely be the outcome.

Employees can also be a massive vulnerability to a company's security. If an employee fell for a phishing link, it could lead to a compromised end-user device and network. Employees could also unknowingly share information that could lead to harm within the company, such as a coworkers password, etc. Phishing links and other employee scams can be very commonplace in the workplace and are an easy threat to avoid. It could be the leading cause to the start of a data breach or a variety of other vulnerabilities being discovered.

Remediation of Acme Corporation Vulnerabilities

Employees, being on the front line of Acme, should be trained accordingly. Common training should be done to help employees spot phishing attacks, conduct themselves online according to corporation standards, and provide a good first line of defense. This can be done using interactive games, seminars, and short daily learning videos. Fake phishing emails should be sent out to regularly test employees on their ability to spot real phishing emails. If an employee fails this test, more training should be provided. Acme should implement a secure password and two-factor authentication system for all employees. This single handedly could bring down the risk of any of these vulnerabilities from happening.

DDoSing attacks can be reduced by implementing load balancers and network segmentation and implementing a zero-trust protocol on the network. This would ensure that if a network were to be overloaded, it could be handled properly without affecting any other parts of the network. Zero-trust would only allow users that were constantly verified to be allowed on the network to keep access. So if any suspicious user was active, they would be kicked off the network.

The feature to upload videos could easily be remedied by only allowing users to upload specifically configured files, such as an MP4 or MOV file. These uploaded files should still be scanned before being uploaded to ensure there were no malicious files in the upload for a variety of reasons. Once everything is verified, the files could be uploaded to the system.

Data security should be the biggest concern when it comes to Acme, since so much user data, such as passwords, and other information is saved on the cloud. All information should be kept encrypted with a rotating encryption and key. This would make it virtually impossible for someone to decode the information unless they gained access to the key. The key should only be accessed by people who are at that security clearance level. On top of this, all software should be routinely scanned and updated to ensure the safest level of security. Automated scanning could be utilized to do this seamlessly. “Automated vulnerability scanners operate by systematically examining systems and networks for known vulnerabilities. They utilize extensive databases that contain information about security flaws, misconfigured, and outdated software versions.” (Zahid, 2023) If any new software was to be released, it should go through extensive black-and-white box testing to ensure its security. Acme should use third-party cybersecurity company software to keep their end users and servers safe.

Vulnerability Assessment Conclusion

Vulnerabilities are everywhere when it comes to information technology. The best way to avoid these vulnerabilities is to maintain a secure environment of access controls. These can prevent some of the worst possible vulnerabilities from occurring. It is important for Acme to assess itself for new vulnerabilities and fix them.

Acme Corporation Security Posture Report Conclusion

Security Posture Report Conclusion

The posture report of Acme corporation aims to identify the assets owned by Acme, a risk assessment of Acme Corporation, main security controls found within the corporation, A vulnerability assessment of Acme. Some of the key findings of the report include the total key assets owned by Acme Corporation, which total up to $1,010,630,580.18. The top five risks associated with Acme. These are DDoSing, Phishing, fair-use legal action, data breaches, and on end-user devices. In order to mitigate these main risks, concise network security and proper training can be implemented.

The three main areas of access control security within Acme Corporation fall into the categories of network security controls, endpoint protection, and access control. The network runs on a zero-trust protocol. Requiring users of the network to constantly verify they are allowed to be on it. No device from outside the location of the specific Acme building is allowed to access the employee side of the network. End-point protection is the protection of all in-house devices, such as laptops and desktops. These are implemented with the third-party company antivirus and firewall software. Access control can be secured by requiring each employee to be required to have an encrypted hash password and physical password key for said encryption.

For employees, an acceptable use policy is in place. This is the umbrella policy for all employees on how they should conduct themselves online. Employees are considered the first line of defense within Acme. This is why Acme has implemented a comprehensive employee training program. The first step in the security training program is with new hire orientation. Then they will have daily, biweekly, and monthly training in different forms.

Security controls are put in place to protect Acme's information and other assets safe from threats and risks. These are separated into four categories. Technical security controls

Include all the third-party company antivirus and firewall software. The administrative access controls and incident response are mostly handled by the third-party cybersecurity company. If an incident is reported, the remediation process will begin by categorizing them into low to high priority and fixing accordingly. These security controls are maintained in order to lower the risk of vulnerabilities in the corporation.

While there are still potential security risks and vulnerabilities within Acme Corporation. Continuous assessments and posture reports can help strength and find new ways to harden Acme. Prioritizing security over maximizing profits will lead Acme to grow even larger as a national technology company and a leader in the cyber security industry.

References

Nazario, Jose. (2008). "DDoS Attack Evolution." ***Network Security*****, Elsevier, Retrieved December 12, 2024, www.sciencedirect.com/science/article/abs/pii/S1353485808700862.**

Zahid, H. (2023). ***Understanding the cyber threat landscape: Comprehensive vulnerability assessment techniques*****. ResearchGate. Retrieved December 12, 2024, https://www.researchgate.net/profile/Haseena-Zahid/publication/384356350_Understanding_the_Cyber_Threat_Landscape_Comprehensive_Vulnerability_Assessment_Techniques/links/66f571709e6e82486ff08891/Understanding-the-Cyber-Threat-Landscape-Comprehensive-Vulnerability-Assessment-Techniques.pdf**