# SECURITY ASSESSMENT REPORT FOR:

# ACME INC.

PREPARED FEBRUARY 4, 2021 BY GRIMMICK TECHNOLOGY

# INTRODUCTION

## ABOUT THIS REPORT

This report was prepared for Acme Inc. by Grimmick Technology & Media LLC as part of a “Mini Security Assessment” service. Through interviews with Acme’s senior management, and open-source intelligence gathering (OSINT), the author compiled information regarding the organization’s overall security posture. This includes not only technical safeguards, but business practices, employee behavior, and more.

The primary objective of this service and the accompanying report is to help Acme achieve a reasonable level of security without significant adverse impacts to the organization’s financial health, efficiency, or day to day operations. To meet this objective, each recommendation in the report was evaluated for cost, administrative complexity, and security impact. Only recommendations that have a “Medium” security impact or greater were included in the report. The report is further organized by “Top Recommendations” and “Additional Recommendations & Thoughts For The Future”. “Top Recommendations” provide an immediate impact to security at a relatively low level of cost and complexity, and should be implemented in the near-term. “Additional Recommendations” include both operational and security benefits, but may be more expensive or complex to implement. Some such recommendations could gain a higher level of importance as the company grows. Centralized Device Management, for instance, could be considered a “Nice to Have” at 4 company-owned devices, but becomes increasingly necessary at 40 devices.

While the “Mini Security Assessment” performed does not directly measure compliance or conformity with any particular security standard, regulation, or framework, the recommendations contained in this report are heavily influenced by best practices specified in the Center for Internet Security (CIS) Critical Security Controls, the National Institute of Technology (NIST) Cybersecurity Framework (CSF),  the US Department of Defense’s Cybersecurity Maturity Model Certification (CMMC), and others.

It’s important to note that while the recommendations outlined in this report represent industry-accepted best practices that should greatly increase security posture at Acme, cybersecurity is a complex and ever-changing field with no “silver bullet”. The defense-in-depth approach advocated here works to reduce and mitigate cyber risks, but some level of residual risk will always remain so long as technology is employed to carry out business functions.

## RISKS, THREAT ACTORS, AND ATTACK VECTORS

The guidance in this report is influenced not only by best practices and security frameworks, but by Acme’s unique risk profile. In building this profile, we must consider several factors, including Risks, Threat Actors, and Attack Vectors. As no two organizations are exactly the same, the risk profile – and the most appropriate measures for reducing and mitigating risks – will naturally vary. Let’s take a deeper look at what these terms mean:

**Risk**

“Risk” consists of multiple elements: a specific weakness or vulnerability, the likelihood or ease with which that weakness can be exploited, and the impact of such an exploit on the organization. A large enterprise may carry out very formal and detailed risk assessments that evaluate risk on a per-asset basis, along with any expected cost or financial hit to the organization for each eventuality. In this instance, our goal is not to quantity every specific risk that Acme may face, but rather build a “big-picture” risk profile to aid the organization in assessing and improving its overall security posture. Risks are in a state of constant flux as an organization changes and grows.

**Threat Actor**

“Threat actor” is a blanket term encompassing any individual or group that could potentially use digital technology against the organization with some form of malicious intent. The capabilities, motives, and techniques of a threat actor vary wildly. At the low-end, a single disgruntled former employee with little technical knowledge could use insider knowledge against a lightly defended organization. The extreme opposite is an Advanced Persistent Threat (APT), a well-financed and highly sophisticated group capable of developing their own custom malware and defeating the most advanced defenses in use today. APTs are frequently backed by nation-states for political or espionage purposes, but can also be linked to organized crime.

**Attack vector**

“Attack vector” refers to the mechanism or channel through which a threat actor exploits risk. Attack vectors aren’t necessarily technical in nature. Twitter, for instance, saw its internal support tools fall into rogue hands in 2020 thanks in large part to a series of convincing phone calls from a 17 year old in Florida. By pretending to be a member of the company’s IT department and simply asking employees for their credentials, this particular threat actor was able to completely sidestep millions of dollars worth of security controls by choosing a unique attack vector.

# ACME’S RISK PROFILE

Through the elements listed above, we can develop a profile uniquely tailored to Acme. Let’s start from the back and work forwards. As the company is a remote team that primarily utilizes cloud and SaaS services, the most likely attack vectors are also in the cloud. This means that security controls that might be appropriate for other types of organizations might play less of a role in the overall security program. An expensive firewall or network monitoring appliance, for example, is much less helpful without a centralized network to protect/monitor.

From a threat actor perspective, Acme’s most pressing concerns should be opportunistic attackers of low to moderate skill level, insiders who act either unwittingly or deliberately, and more skilled actors looking to leverage the company in supply chain attacks against its larger clients. The chance of a directly targeted attack by an APT group is low; such groups usually target institutions of major geopolitical, military, or advanced technological consequence. While smaller targets have been swallowed up as “by-catch” in some previous APT campaigns, the low likelihood of being of great interest to a nation-state or organized crime group combined with the great cost and complexity in combating such a well-resourced attacker means the most prudent course of action at the present time is to focus on less advanced but more likely threat actors.

Risks can be expressed in very granular, quantitative ways, at a very high level, or somewhere in between. In risk analysis, spreadsheets and tables are frequently used to help illustrate and understand risk. The table below represents just a few potential risks based on Acme's unique Risk Profile, along with their potential qualitative impacts:

| Risk | Threat Actor(s) | Attack Vector(s) | Potential Impact |
|---|---|---|---|
| A company account on a cloud service or SaaS account is compromised | Opportunistic (Low to High Level)<br>Insider (Unwitting or Deliberate) | Malware, credential stuffing, phishing, social engineering | Reputational damage<br>Downtime costs related to discovery and remediation<br>Data Loss<br>Regulatory Consequences |
| A company-owned device is lost or stolen | Opportunistic (Low to High Level)<br>Insider (Unwitting or Deliberate) | Physical theft | Data Loss (if unencrypted)<br>Loss of Productivity |
| The company's devices or accounts are leveraged in a supply chain attack against a large client | Insider (Low to High Level)<br>Advanced threat (targeted)<br>Corporate Espionage | Phishing, Social Engineering, Malware | Potential Legal Consequences<br>Major Reputational Damage<br>Remediation Costs |
| A ransomware attack encrypts data in a cloud service | Advanced threat (opportunistic or targeted) | Phishing, Malware | Lost Productivity<br>Potential Regulatory Consequences |

The recommended actions and controls contained in the rest of this report are intended to address risks such as these.

# 1. DEVICES AND DEVICE ADMINISTRATION

Acme's current fleet of company owned devices includes a mix of Mac, PC, and Linux devices. The machines are managed directly by employees on an ad-hoc basis. Employees have administrator accounts and can install software and make configuration changes at will. Sophos is currently used for Endpoint Protection, and is believed to be installed and up-to-date on all company devices. Employee use of devices is governed by a technology usage agreement, but does not appear to be enforced through a technical basis at the present time.

## TOP RECOMMENDATIONS:

### I. ESTABLISH A BASELINE SECURITY CONFIGURATION ON DEVICES

**Cost: Low | Complexity: Low | Security Impact: High**

An organization's endpoints – the laptops, tablets, and other devices used in the course of day to day business – are frequently targeted by attackers as an initial attack vector. Sneaking malware onto an old HR laptop or commandeering a long forgotten printer gives the attacker a foothold from which to launch more sophisticated and damaging attacks. Endpoints are often configured to emphasize convince and usability by default, rather than security (think about all the terrible default password you've seen over the years). "Hardening" the company's devices can greatly increase the organization's overall security posture at a minimal level of expense and complexity. At a minimum, this should include:

1. **Disabling any unneeded services.**
   Services like file sharing, remote login, and remote management can present high security risks as they represent a potential means for an unauthorized third party to access systems or data. The underlying protocols for these services have been subject to widespread abuse in the past, and enabling remote access in combination with a weak password could open the door for a brute-force attack that most antivirus software would miss. In most instances, these services should be disabled on all devices that employees use for standard tasks. Sharing of files or other resources is better accomplished through dedicated servers or cloud services like Dropbox.

**Remediation:** Currently enabled services can be viewed from the “Sharing” section of the Settings application on Apple Devices, and the “Network and Sharing Center” in most versions of Windows 10.

**More info:** Commonly Exploited Protocols: Server Message Block (SMB)**,** Digging Deeper into Vulnerable Windows Services

## 2. Enable on-device Firewall for all machines.

Historically Firewalls were hardware devices used to protect corporate networks from outside attacks. In this scenario, little need was seen for adding additional protection on company owned machines behind the firewall. However, very few organizations today operate solely with computers permanently attached to a centralized corporate network. All modern desktop operating systems now include a robust software firewall to block unwanted and suspicious connections at the device level. It’s especially important to enable these software firewalls on devices that frequently roam on untrusted networks, like coffee shops.

**Remediation**: The Firewall can be enabled from the  Firewall tab of the Security and Privacy section in the Settings app on macOS or from the Update & Security Section of the Windows Settings application.

**More info:** About the application firewall, Turn Microsoft Defender Firewall on or off

## 3. Enabling Automatic Updates of Both Operating System and Applications

All software, even the most carefully designed, is subject to bugs and vulnerabilities. Software is created by humans, which are by their very nature imperfect beings and therefore not capable of producing perfectly flawless code. While many bugs are harmless, some present very serious security implications. Major software vendors are doing a better job of promptly patching their products, but the time gap between a flaw becoming public knowledge and threat actors exploiting that flaw in vulnerable systems has shrunken dramatically. Many high-profile security incidents in recent years, such as the Equifax Data Breach of 2017, began with an attacker exploiting a known but unpatched flaw. For these reasons, it’s extremely important to keep both operating systems and other software, such as web browsers, up-to-date. All operating systems and many applications now include automatic patching functionality. In complex Enterprise environments, patching is sometimes delayed or carried out manually to ensure compatibility with legacy systems and applications. As Acme does not have legacy applications or systems, Automatic patching should be enabled on all machines.

**Remediation:** Automatic Updates can be enabled from the “Software Update” section of the Settings App on macOS, or from the “Update & Security” Section of the Windows Settings application. Individual applications will have automatic update settings in various places.

**More info:**  How to manually update apps on your Apple device, Windows Update: FAQ,

### 4. Enable Full-Disk Encryption (FileVault, BitLocker, etc)

Full Disk Encryption does not directly prevent many types of security incidents, but can play a significant role in mitigating the threat or impact. A threat actor who gains access to an encrypted drive – whether remotely or through the physical theft of a device – stands very little chance of accessing the data without a decryption key. Although Acme’s data primarily resides in the cloud, it’s possible that copies of client or customer data could be stored locally in browser or email cache files. End devices

may also contain data useful in carrying out a multi-stage attack on cloud services, for example user credentials stored in a web browser. Encryption technologies like FileVault and BitLocker are now seamlessly integrated within operating systems, and are held in such high regard that activating them can actually relieve an organization of the duty to notify consumers or regulators in the event of a Data Breach, provided the encryption key is not also accessed. For these reasons, encrypting the entire volume is recommended on all Acme machines. However, care should be taken to document and securely store recovery keys in the event an employee forgets their password or leaves the company.

**Remediation:** FileVault can be enabled from the "FileVault" tab of the "Security & Privacy" section of the Settings app in macOS. On Windows 10, BitLocker can be enabled from the Update & Security section of the Settings app. Full Disk Encryption on Linux is dependent on the distribution in use.

**More Info:** Use FileVault to encrypt the startup disk on your Mac, Turn on device encryption

# II. CONFIGURE EMPLOYEE ACCOUNTS AS STANDARD USERS

**Cost: Low | Complexity: Low | Security Impact: High**

In many organizations employees have full administrative access on all machines, and are capable of installing software and changing system configuration settings. This presents a major security risk. Employees may install vulnerable or insecure software without informing management, but a greater risk comes from outside parties gaining access to employee accounts. A successful phishing attack or social engineering ploy would give an attacker a high degree of access, including the ability to install backdoors, exfiltrate data, and perform further reconnaissance against the organization. Malware also frequently inherits the privilege level of whatever user account was active at the time of infection. For example, if a user visits an infected website or opens a poisoned Office document while running as administrator, the malware would inherit full administrative access to the machine.

To counter these types of threats, a model known as the "Principle of Least Privilege" is recommended. In this model, user accounts possess the minimum level of permissions and access needed to perform their job functions. As the day-to-day responsibilities for most Acme employees do not include the need to install software or make major configuration changes, implementing the Principle of Least Privilege would provide a major security boost with little to no impact on efficiency. For employees that do require administrative access, it is recommended that separate accounts be maintained: one for day-to-day operations, and another used solely for administrative purposes.

**Remediation:** In macOS, user account types can be changed from the "Users & Groups" section of the Settings app. In Windows 10, user account types can be changed from "Accounts" section of the Settings application. Permissions in Linux work slightly differently, but in general running as the "root" or "superuser" should be discouraged unless strictly necessary.

**More info:** Implementing Least-Privilege Administrative Models, Least Privilege (CISA)

# III. ESTABLISH AN INVENTORY OF ASSETS

**Cost: Low | Complexity: Low | Security Impact: Medium**

In the wake of widely publicized security events and vulnerabilities, organizations often want to know whether they might be impacted. Without an accurate knowledge of software installed on company devices, the organization may not be able to reliably answer that question. This can become a serious issue in the wake of a fast-moving attack. In light of the ability for employees to install software on company machines, it is possible that additional applications have been installed without the knowledge of management. These applications may present a security risk outright, the applications could have vulnerabilities that allow for compromise, or they may change settings on the device.

In mid to large sized organizations, complete inventory management solutions are used to discover and track assets. Smaller organizations may not require such a comprehensive approach, but a basic understanding of the hardware and software currently in use at the organization is beneficial from a security standpoint. On the hardware side, a simple spreadsheet consisting of device, serial number, and installed operating system version would suffice.

Having a basic list of software installed on all company-owned devices is also highly recommended. Even popular software such as Zoom can have very serious flaws and vulnerabilities, and without some idea of what programs (and which versions of those programs) are installed, it can be difficult for an organization to know where they might be vulnerable.

**Remediation:** A list of installed applications can be viewed from the built-in “System Information” app on macOS. From the Apple menu in the top left, select “About This Mac”, press the “System Report button, and then select “Software -> Applications” from the left side NavBar. In Windows 10, a list of installed software can be viewed by opening the “Settings” application and navigating to “System -> Apps and Features”. Many third-party utilities, such as Belarc, also provide similar capabilities, as do the RMM/MDM tools mentioned in the next section.

# IV. IMPLEMENT DNS FILTERING FOR ALL COMPANY-OWNED DEVICES

**Cost: Low | Complexity: Low | Security Impact: Medium to High**

DNS Filtering utilizes a foundational component of the Internet – the Domain Name System (DNS) – to provide additional protections against phishing, malware, and command-and-control callbacks. As devices resolve domain names, such as example.com, to their underlying IP address, DNS Filtering services check the domain being requested for unwanted or malicious content. If there is a security risk or other condition that violates policy, the service will simply not return the true IP address for the malicious domain, preventing any connection from ever being made. DNS filtering can also be useful in limiting the scope of an attack that bypasses other controls: Almost all types of ransomware, viruses, spyware etc. will “phone home” to an attacker’s infrastructure to fetch additional instructions and attack payloads, or to exfiltrate data out of the victim’s network. DNS filtering providers regularly add known Command-and-Control (C2) domains to a block list as new campaigns are discovered, which can work to mitigate what might otherwise be a successful attack.

**Remediation:** Enable a DNS Filtering service and configure networks and/or endpoints to use the service.

**More info:** How Does DNS Filtering Work?

# ADDITIONAL RECOMMENDATIONS & THOUGHTS FOR FUTURE:

## I. IMPLEMENT A CENTRALIZED MANAGEMENT SOLUTION.

**Cost:** Medium to High | **Complexity:** Medium to High | **Security Impact:** Medium to High

Centralized management solutions go by many names: Mobile Device Management (MDM), Remote Monitoring and Management (RMM) etc. Whatever the name, the benefits are the same: centralized administration, management, and monitoring of company-owned assets. This can decrease administrative burden and increase security. The company can rapidly roll out new software to the entire fleet of devices, ensure all devices are configured in a secure fashion, and carry out any support activities remotely. Lost or stolen devices can be locked, tracked, or remotely wiped. As new employees are onboarded, new devices can be automatically provisioned. Different MDM/RMM solutions have different capabilities, costs, and levels of complexity. Implementing an MDM/RMM solution could also facilitate easier implementation of many of the other recommendations in this report.

As Acme continues to grow and distribute devices to new team members, manually provisioning and administering devices will become untenable. The cost of an MDM solution becomes offset by the reduced administrative burden and increased security (provided the solution is used to adhere to best security practices, of course).

**Remediation:** Implement an RMM or MDM solution.

**More info:** Google Endpoint Management, Apple Deployment Platform Guide

# 2. CLOUD SERVICES AND SAAS APPLICATIONS

The ongoing shift toward cloud and Software-as-a-Service (SaaS) applications has many advantages from both an efficiency and security perspective. For instance, the company does not need to update a large number of applications or secure the physical infrastructure required for those applications. However, threat actors have modified their tactics in response to the growing reliance on cloud services. This section contains recommendations and guidelines for dealing with cloud threats.

# TOP RECOMMENDATIONS:

## I. ENABLE MULTI-FACTOR AUTHENTICATION (MFA) ON ALL ACCOUNTS AND SERVICES

**Cost: Low | Complexity: Low to Medium | Security Impact: Very High**

Multi-factor Authentication (MFA), also known as Two-Factor Authentication (2FA) is widely considered to be one of the best ways to enhance organizational security. It is no longer considered simply an "enhanced" security measure, and is now viewed as essential for nearly all organizations. Lack of MFA has been labeled a "bad practice" by the Cybersecurity and Infrastructure Security Agency (CISA) for MFA is now mandatory across most Federal Agencies and contractors, as well as many state and local governments, and is also required for compliance with standards like PCI-DSS. Even when compliance is not an issue, many cyber insurance providers now require MFA to be in use as a condition of coverage.

MFA comes in several different flavors. In the most common implementation, a one-time use code is sent to a phone number or email address during the login attempt. While it's often used, SMS or email-based options represent the least secure forms of MFA and have been subject to many known abuses. Authenticator apps like Ping, Duo, Authy, or Google Authenticator are a far better option. The most tamper resistant form of MFA comes in the form of physical security keys or tokens. Unfortunately, the choice of which MFA variety to use is often made for us by the application, site, or service we're using. Only a handful of banks, for example, offer anything besides SMS based multi-factor authentication despite the known weaknesses of this approach.

It should also be noted that MFA can also be used in conjunction with several of the other recommendations listed in this document, such as Single Sign-On and Conditional access, both of which are discussed further in subsequent sections.

**Remediation:** Enabling MFA varies by platform, but is often found in the security or account settings section of an administrative portal.

**More info:** Multi-factor Authentication (CISA), The Best Way to Use Two-Factor Authentication, How to implement Multi-Factor Authentication (MFA),

# 3. IDENTITY AND ACCESS MANAGEMENT

Identify and Access Management (IAM) consists of the processes, policies, and technologies used to provision and maintain user accounts for company employees. At present, this appears to take place on a manual ad-hoc basis, with employees using separate logins for each service and application that the company uses. There does not appear to be a password policy in place, and there is no account monitoring. While full IAM solutions can be prohibitively expensive and complex, implementing some best practices in the area of account management can greatly increase security at minimal expense or loss of productivity.

# TOP RECOMMENDATIONS:

## I. DEVELOP AND ENFORCE A PASSWORD POLICY

**Cost: Low | Complexity: Low to Medium | Security Impact: High**

Passwords have long been viewed as insufficient to safeguard data and computing resources - even the earliest known implementations of passwords on computing systems fell victim to attacks. However, modern computing power and access to nearly infinite resources in the cloud has made password cracking feasible on a scale not previously seen. In 2021, a massive compilation of real-world passwords from previous data breaches was posted online, and quickly became available throughout the hacker and security researcher communities. The file contained over **8.4 billion** passwords, which works out to an average of more than two passwords for every Internet user on the planet. Modern password cracking tools are highly effective, and capable of rapidly trying numerous permutations of any dictionary word. For example, using common character substitution rules,“p@ssw0rd”, “pa$$word”, and “password!” could all be tried in a completely automated fashion, making it unlikely they’d last much longer than a simple “password”.

The precise details that should make up a password policy – length, inclusion of special characters, etc – are a matter of some debate in the security community, but there is an overall consensus that more complex passwords are better. In recent years, there’s been a shift towards passphrases instead of singular words: “ILoveGoingToTheBeachOnSundays” would be considerably more difficult to crack than “p@$$w0rd”, even though the former does not contain any special characters.

While Multi-Factor Authentication (MFA) can greatly diminish the threats posed by weak passwords, it is not foolproof and is increasingly being sidestepped or defeated by clever attackers. Acme should adopt a password policy requiring some level of complexity, and in particular prohibiting the reuse of passwords from personal sites. Where possible, this policy should be enforced through technical means. Google Workspace, for example, includes a setting for “enhanced security” in the

**Remediation:** Develop, disseminate, and enforce a password policy to all employees. Where possible, enforce this policy through technical means.

**More info**: Passwords Evolved: Authentication Guidance for the Modern Era, Password administration for system owners, Enforce and monitor password requirements for users, CIS Password Policy Guide: Passphrases, Monitoring, and More

## II. USE A DEDICATED PASSWORD MANAGER

**Cost: Low to Medium | Complexity: Low to Medium | Security Impact: High**

In conjunction with the first recommendation, use of a dedicated password manager can greatly enhance security and reduce user frustration. Password managers generate high-quality passwords on a per-site basis, alleviating many of the concerns raised in the previous recommendation. Business plans from providers like LastPass and 1Password also allow some centralized management, so that if an employee forgets a password or is otherwise locked out of an account, management can reset it remotely.

It's important to note that many password managers built into web browsers, for example Google Chrome, are not considered secure because an attacker with access to the user account can dump them with little difficulty. Dedicated password managers store credentials in a more secure fashion, and generally keep the passwords encrypted until a "master password" or other form of authentication is used to verify user identity.

**More info:** Password manager buyers guide (NCSC)

## III. DEACTIVATE UNUSED ACCOUNTS AND SERVICES

**Cost: Low to Medium | Complexity: Low | Security Impact: Medium to High**

Cyberattacks frequently leverage old or forgotten assets and accounts. The 2021 Colonial Pipeline Ransomware attack that interrupted gasoline supplies throughout the Eastern United States, for example, is thought to have begun after the credentials to an old VPN account were leaked on the dark web. To counter this threat, it's a good idea to have a formal process for deactivating or archiving accounts when no longer needed, such as when an employee leaves the company. It's also a good practice to perform a periodic review of open accounts and services that may no longer be needed.

**Remediation:** Deactivate any unused accounts or services through the settings or administration sections of relevant cloud/SaaS applications.

# ADDITIONAL RECOMMENDATIONS & THOUGHTS FOR FUTURE:

## I. IMPLEMENT AND UTILIZE SINGLE SIGN-ON (SSO)

**Cost: Low to Medium | Complexity: High | Security Impact: Medium to High**

Single Sign-on (SSO) refers to the practice of maintaining one single account per user that is used across multiple services. In such a case, a user's identity is stored centrally and users are redirected to a centralized login page when trying to access the various services. This has many benefits from both an efficiency and security perspective. Users would only need to remember a single username and password, security policies can be uniformly applied, and suspicious login attempts can be more easily detected.

Unfortunately SSO can be difficult and complex to implement. There are a variety of options available at various price points, each with unique capabilities and configuration requirements. Each service used by the team would also need to integrated with the chosen SSO solution, which can

range from a one or two-click process to a multi-step process for each service. Integration with other security and authentication components, such as authenticators, present another potential pain-point.

Despite the potential complexity, Acme should consider implementation of SSO. A well-designed and holistic SSO implementation offers both prevention and mitigation opportunities: MFA, conditional access, and other techniques present the opportunity to block attacks, and the possibilities for account monitoring and suspicious login detection can limit the fallout of any successful attack.

**More info:** How does single sign-on work?, Overview of Google identity management

## II. LOG AND MONITOR ACCOUNT ACTIVITY

**Cost: Low to Medium | Complexity: High | Security Impact: Medium to High**

As some of Acme's biggest potential risks lie in a cloud or SaaS account being compromised, logging and monitoring access to cloud services is recommended. The extent to which this is possible depends on the particular cloud platform or application. At a minimum, audit logs should be retained in order to assist with any response or remediation efforts that may need to take place following a security incident. Without such logs, it may be nearly impossible to adequately investigate and remediate the incident.

Several services and solutions also exist for performing more detailed monitoring and proactive "threat hunting" based on authorization logs. Some such services are fully automated, while others add human analysts to review and notify the appropriate personnel in case of suspicious activity.

**Remediation:** Maintain audit logs and implement some form of account monitoring.

**More info:** Monitor usage and security with reports, Five Tips for Monitoring Your SaaS

## III. IMPLEMENT AND UTILIZE CONTEXT-AWARE ACCESS/CONDITIONAL ACCESS

**Cost: Low to Medium | Complexity: High | Security Impact: Medium to High**

In most authentication systems, authorization is granted in a completely binary form: either the user authenticates correctly and may proceed, or the user fails to authenticate and is denied access. Context-Aware Access or Conditional Access brings more granularity to this process. Adding additional conditions that need to be met for authorization to be granted helps prevent and mitigate certain types of attacks. For example, authentication can be dependent on geolocation so that a hacker in another part of the world would be denied access even if they had stolen an employee's legitimate username/password. Enterprises are now leveraging conditional access to restrict access only to devices with up-to-date software. Policies can be applied on a granular level as well, which might include more restrictive controls for sensitive data or accounts.

Conditional/context-aware access is considered a more mature security practice, and many organizations fail to implement it due to administrative overhead and complexity. Some solutions can simplify the process to a degree, though may do so through a proprietary process.

**Remediation:** Enable and/or implement a context-aware or conditional access solution.

**More info:** Context-Aware Access overview, Conditional Access Explained

# 4. POLICIES AND PROCEDURES

An organization's overall security posture depends on much more than just technology. The policies, procedure, and people of the organization can be just as important, and in many cases even more important. This section contains recommendations based upon interviews with staff and a review of Acme's current relevant policies and procedures.

## TOP RECOMMENDATIONS:

### I. IMPLEMENT SECURITY AWARENESS TRAINING

**Cost:** Low to Medium | **Complexity:** Low to Medium | **Security Impact:** Very High

Security Awareness Training may provide the largest return on investment (ROI) of any control discussed in this report. A well-educated and security conscious workforce often succeeds where expensive technical solutions fail. To understand why, picture a house protected by a very expensive high-end security system. Would a would-be thief stand a better chance of success through trying to outwit motion sensors and cameras, or by dressing up as a pizza delivery person in order to convince the homeowner to open the front door? Attackers know that targeting human error and emotion is often more successful than hunting for vulnerabilities. By some estimates, up to 95% of data breaches begin with a human and not technical issue.

Some organizations take a "check-box" approach to training, viewing it as nothing more than a compliance requirement. This is an error, as the effectiveness of the training program can be heavily dependent on the engagement and attentiveness of the employees. Training should be viewed through both a formal and informal lens; formal training or courseware can be used to introduce key topics, with other opportunities like phishing simulations, games, and even posters used for reinforcement purposes. In both cases, gamification and interactivity can be beneficial.

The exact makeup of a security awareness program can vary, however it is important that the overall tone of the program convey a sense of teamwork and security consciousness. Employees should never be made to feel like they will be retaliated against for reporting a security incident.

**More Info:** The Importance of Security Awareness Training, Security Awareness Planning Kit, StaySafeOnline.org

### II. CREATE OR UPDATE SECURITY POLICIES

**Cost:** Low to Medium | **Complexity:** Low to Medium | **Security Impact:** Medium

Security policies have many functions, from describing an organization's overall appetite for risk to spelling out in detail what kinds of activities are allowed on company owned resources. Despite their importance, a surprising number of organizations have no security policies of any kind. This puts the organization and its employees at a significant disadvantage. Smaller organizations may not require

the myriad of specialized policies that are found in large enterprises, but at a minimum all organizations should have a policy that includes:

1. **The organization's overall attitude towards security.** Security policies should communicate senior management's intent towards information security.
2. **Roles and responsibilities:** Who's responsible for overseeing security? What responsibilities do employees have for reporting an incident?
3. **How will the policy be monitored and enforced?** Policies need to be adhered to in order to be effective. For that to happen, policies need to be

**More info:** Security Policy Roadmap - Process for Creating Security Policies, How to Create a Good Security Policy, Security Policy: Development and Implementation

# III. DEVELOP AN INCIDENT RESPONSE PLAN

**Cost:** Low to High | **Complexity:** Low to High | **Security Impact:** Medium

An Incident Response Plan is a resource that employees can turn to when they believe a security incident has occurred. In large enterprises, these plans can be very complex and involve parts of the company ranging from legal to public relations to HR. Smaller businesses may not require anything on this scale, but having a basic plan in place is useful for any size organization. Even some basic instructions for employees can help maximize the speed of response and minimize any fallout. At a minimum, this plan should cover:

1. **Who is responsible for handling an incident**

The midst of a cyberattack is not the time to be asking "who do I report this to?". Employees, contractors, and any other stakeholders should have a pre-defined point of contact to report an incident, and there should be a clearly defined chain of command. Well-meaning employees attempting to handle the incident themselves can inadvertently make the situation worse. The thresholds at which senior management becomes involved depends on the organization.

2. **How to report an incident**

Should the incident be reported by phone? Email? What details should be included? At a minimum, including the machine the incident occurred on and software/service affected are helpful in quickly pinpointing the root cause of the incident. At an organizational level, it's also helpful to have a plan for who would be responsible for contacting law enforcement, legal representation, and state regulators if required.

3. **Steps to take in the immediate aftermath of an incident**

The response to a cybersecurity incident will vary depending on the severity of the incident. Certain situations, like ransomware attacks, call for an immediate halt to all activities. In the case of the most serious cybersecurity incidents, there may be a desire or requirement to perform digital forensics on the data and/or equipment impacted by the attack. Electronic forensic evidence can be very transitory, and if there is any suspected illegal activity or sophisticated attacks, any use of the device in question should immediately be discontinued.

# 5. BACKUP AND DISASTER RECOVERY

Backup is often not viewed as a part of a cybersecurity program, but it is actually a very critical component. Having an intact backup of important data can mean the difference between arranging a painful ransom payment to an offshore hacker or resuming business as usual in just a few clicks. Business Continuity and Disaster Recovery (BCDR) is the modern business-grade evolution of consumer backup solutions, offering robust capabilities but also introducing new complexity. As suggested by the name, BCDR addresses other types of risk beyond cyber. Natural disasters, accidental deletion, and other types of incidents can be addressed and mitigated through these types of solutions. This section contains recommendations and best practices for BCDR and similar solutions.

## TOP RECOMMENDATIONS:

### 1. IMPLEMENT A BCDR SOLUTION WITH OFF-SITE BACKUP

**Cost:** Medium to High | **Complexity:** Medium to High | **Security Impact:** Medium

Acme Currently does not currently appear to have a comprehensive backup solution in place. While much of the company's data is stored in cloud where cloud service providers are maintaining their own backup infrastructure. This provides some level of redundancy, however nearly all of these providers recommend maintaining separate backups. The terms of service of providers like Google, AWS, and Microsoft all absolve the provider of any responsibility in case of user error or cyberattack targeting an individual customer. Accidental deletion, cloud ransomware, and insider attacks are very real threats.

Traditionally, there was a strong recomendation to maintain an off-site backup. As Acme's data is already "in the cloud", the risks of data loss associated with natural disaster and physical access are diminished. However, it is still advisable to maintain copies of data that are separate from the primary provider. For example, as Acme makes heavy use of Google services, it may not be advisable to use a backup provider that also uses Google's cloud infrastructure.

**More info:** Why Small Businesses Should Consider Business Continuity Planning, What is BCDR: Business Continuity Planning & Why is it Important?

## II. REGULARLY TEST BACKUP SOLUTIONS AND CREATE A RECOVERY TARGET

**Cost:** Low | **Complexity:** Low | **Security Impact:** Medium

Organizations of all sizes frequently implement a backup or disaster recovery solution without ever testing the solution. This can be a disastrous mistake. The immediate aftermath of a ransomware attack is not the time to learn that a procedure wasn't working as expected, or that a particular setting hadn't been configured correctly. A complete test of the backup solution should be conducted at least annually, with spot checks or sample recoveries performed quarterly if possible.

Beyond making sure the backup solution works, organizations should be mindful of the time involved in completely recovering their systems. Moving large amounts of data out of remote backup site over commodity Internet connections can be excruciatingly slow, especially for complex environments. There is no "correct" amount of time for how long a recovery should take; each organization needs to weigh the costs of expediting recovery against the lost productivity involved from a protracted process.

**Remediation:** Test any implemented backup solutions on at least an annual basis, and decide on an acceptable time period for recovery.

**More Info:** Computer Security Incident Handling Guide, An Incident Response Plan for Startups

## III. FOLLOW THE "THREE-TWO-ONE" RULE

**Cost:** Low to Medium | **Complexity:** Low to Medium | **Security Impact:** Medium

A long-prescribed best practice when it comes to disaster recovery, the "three-two-one" rule holds that there should be three copies of important data, on two different physical mediums, with one of those backups off-site. The cloud has muddied this rule somewhat, as a large deal of data is now perpetually offsite and accessed only on demand. Still, maintaining some degree of redundancy is important in ensuring business continuity. Even in the age of cloud backup, maintaining a separate, fully offline copy of data can help to mitigate any threat posed by ransomware, as the program will not be able to encrypt any data that it does not have access to.

**Remediation**: Establish redundancy in backup procedures.

**More info:** What Is the 3-2-1 Backup Rule?, The 3-2-1 Rule for Cloud Backup

## III. MAINTAIN APPROPRIATE SECURITY CONTROLS OVER BACKUPS

**Cost:** Low | **Complexity:** Low to Medium | **Security Impact:** High

All backups, regardless of the medium or location, should retain the same security controls as the original data whenever possible. To give a simple example, this means that if the original data is encrypted, the backup(s) must also be encrypted. It's highly important to secure access to the decryption keys. The same access controls as the original should also be applied; if only management has access to HR data, HR backups should not be accessible to the company as a whole. If backups are kept in a physical medium like an external hard drive or tape storage, physical access to the storage should also be controlled.

In the age of ransomware, the concept of immutability has also become important. An immutable backup is one that cannot be changed or altered once the backup is created. This prevents ransomware from encrypting sensitive files and data, as encryption is a form of modification. The

technical mechanisms that are used to implement immutability can vary from provider to provider, and it's important to understand that even a solution advertised as immutable may not be 100% immune to ransomware.

**Remediation:** Ensure appropriate security controls are implemented for all backups.

**More info:** The Five Tenets of the Most Secure Backup

# 6. INSURANCE, COMPLIANCE, AND REGULATORY ISSUES

Acme does not currently appear to full under any special compliance or regulatory requirements such as HIPPA, PCI-DSS, or CMMC. However, companies of any size can be subject to state Data Breach Notification laws, which require any business or agency in the state to notify a resident of the state when the resident's personal information is acquired by an unauthorized third party. Beyond this, larger clients may have contractual cybersecurity requirements for any vendors or partners they work with.

## TOP RECOMMENDATIONS:

### I. OBTAIN CYBER INSURANCE COVERAGE

**Cost:** Medium to High | **Complexity:** Low | **Security Impact:** Medium

While many of the recommendations in this report are designed to thwart or mitigate cyberattacks and data breaches, there is no "silver bullet" that ensures an incident will never occur. The fallout from a data breach, ransomware attack, or other type of incident can be particularly devastating for smaller businesses. Cyber insurance policies aren't an excuse for poor security practices any more than auto insurance is an excuse to drive recklessly. But just as a cautious drive still carries auto insurance to be prepared for the unexpected, a well-protected business should consider cyber insurance to provide some level of protection in a worst-case scenario.

Cyber insurance policies can vary significantly in cost and coverage. Some aren't much more than expanded Errors and Omissions (E&O) policies, while others might go so far as to assist with

notification of customers and regulators in the event of data breach. Coverage can be either first-party, which applies only to the directly insured organization, or third-party, which covers impacts to the organization's clients, customers, or partners. However, insurers are introducing increasingly stringent requirements or limiting coverage based on an organization's security practices following a large jump in ransomware and data breach claims. Implementing and then documenting the recommendations in this report may prove beneficial when applying for cybersecurity coverage.

**More Info**: Cyber Insurance | Federal Trade Commission, How Cyber Liability Insurance Can Rescue A Small Business, Cyber insurance explained: What it covers and why prices continue to rise

## II. UNDERSTAND CALIFORNIA DATA BREACH NOTIFICATION OBLIGATIONS

**Cost: Low | Complexity: Low | Security Impact: Medium**

As stated in the introduction to this section, California has a Data Breach Notification Law that applies to all organizations doing business within the state, regardless of size. In addition to notifying any impacted California residents, a breach involving the personally identifiable information (PII) of more than 500 people must be reported to the state's Office of the Attorney General (OAG). In recent months, California's Attorney General has signaled that increased enforcement of this measure could be on the way. While no business wants to experience a data breach, being prepared for the eventuality is prudent. There are guidelines for how individuals must be contacted, as well as what kind of communications are acceptable.

As part of planning for times of disaster and crisis, it may be helpful to have a draft of such a notification prepared. There are several templates available online. It's also worth noting that the law contains an encryption safe harbor, relieving the organization of any notification requirements provided the decryption key is not also compromised.

**More info:** Data Security Breach Reporting, California Data Breach Notification Statute Summary


# PREPARED BY GRIMMICK TECHNOLOGY AND MEDIA, LLC

grimmicktechnology.com
100 W Broadway
Suite 3000
Long Beach, CA 90802
(562) 283-5573
info@grimmick.tech