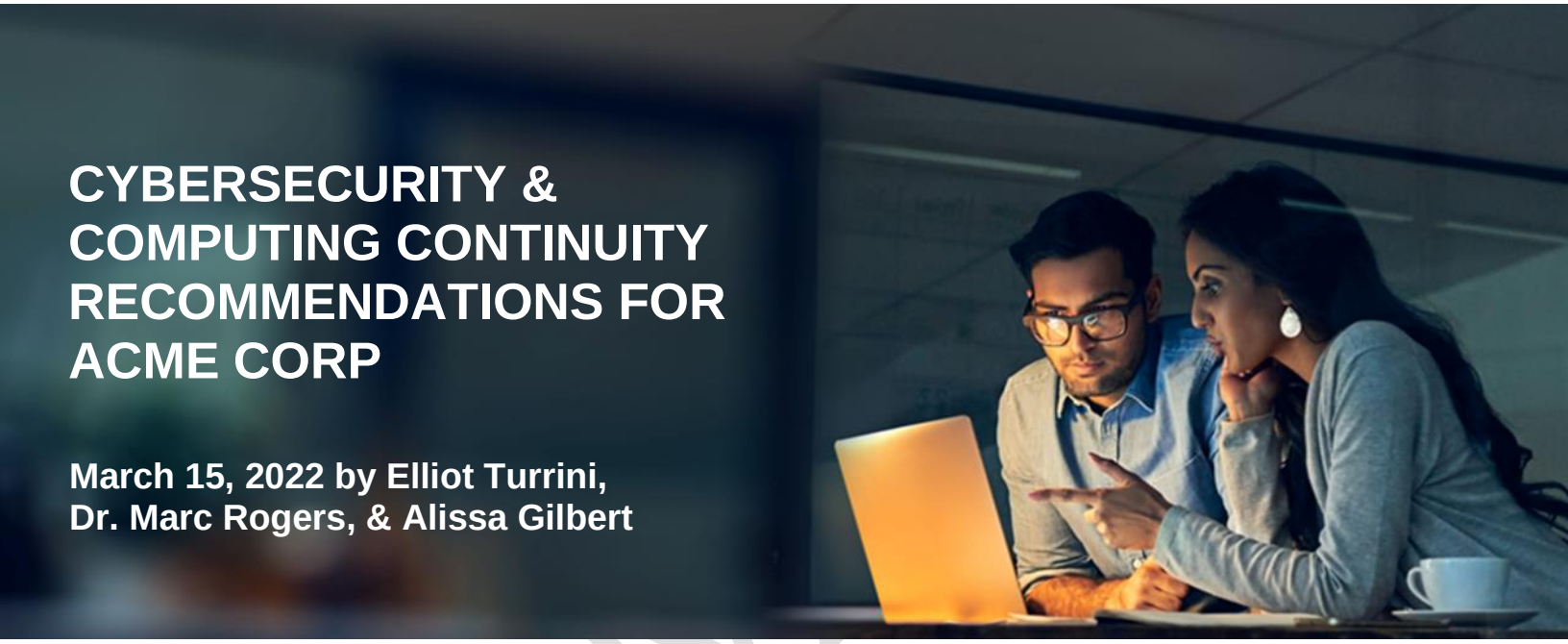


CYBERSECURITY & COMPUTING CONTINUITY RECOMMENDATIONS FOR ACME CORP

March 15, 2022 by Elliot Turrini, Dr. Marc Rogers, & Alissa Gilbert

SAMPLE HIGH-LEVEL CYBERSECURITY & COMPUTING CONTINUITY ROADMAP

Project Scope: Acme Corp engaged Practical Cyber to review its "unique business model and current mitigation efforts" and provide a "a customized and prioritized High-Level Cybersecurity & Computing Continuity Improvement Roadmap ["Roadmap"] . . . [that] will (1) succinctly summarize the current efficacy Client's cybersecurity and computing continuity and (2) set forth clear, prioritized improvement recommendations . . . ."

Practical Cyber's review focused on Acme Corp's Cybersecurity and Computing Continuity. It did not extend to the other 3 cyber risk mitigation tools.

Cybersecurity refers to the technologies, people, and processes used to protect your computing operations and digital data from attack. Computing Continuity refers to the technologies, people, and processes that restore your computing operations and digital data after cyber-incidents.

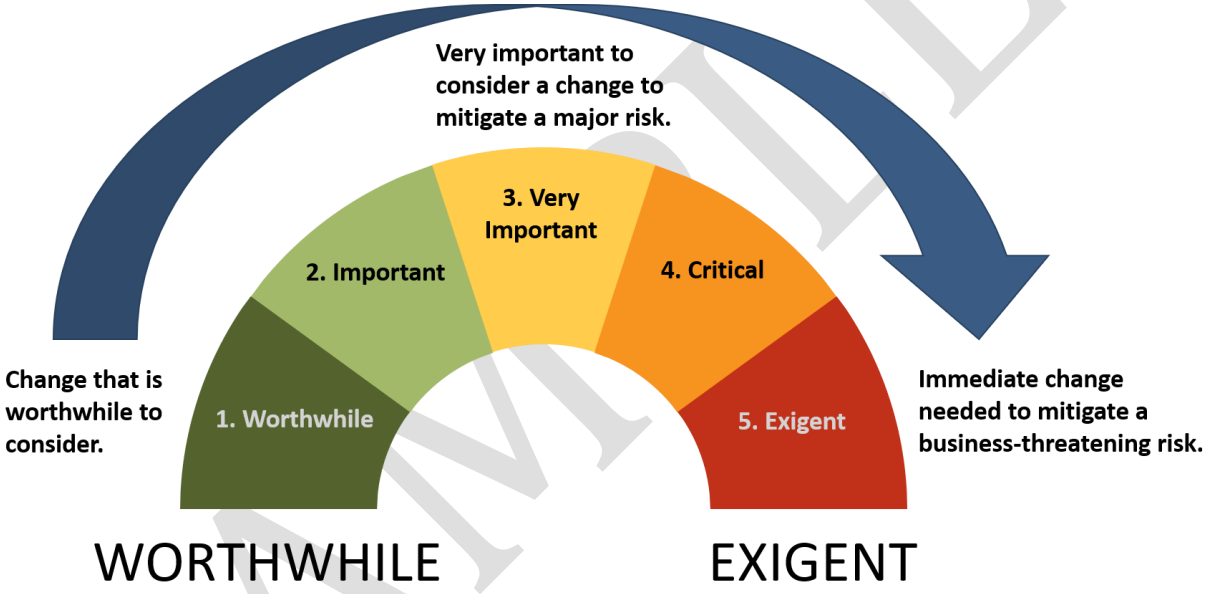
Methodology: To assess Acme Corp's current Cybersecurity and Computing Continuity mitigation efforts, Practical Cyber did the following:

- Interviewed Acme Corp representatives many times via a series of written questions and answers and online meetings.
- Reviewed Acme Corp materials it provided.
- Independently researched the technologies and processes that Acme Corp is using and might benefit from using.

Practical Cyber did not independently verify Acme Corp's factual assertions – a task that requires a much more rigorous and expensive process than this type of High-Level Roadmap. Rather, Practical Cyber based its analysis and recommendations upon the information that Acme Corp provided.

Caveat: The efficacy of Practical Cyber's recommendations depend heavily on the accuracy of the information that Acme Corp provided.

Priority Ratings for Recommendations: Section 2 sets forth recommendations for ways Acme Corp can improve its Cybersecurity and Computing Continuity. For each recommendation, Practical Cyber included a priority rating of 1 to 5:



List of Practical Cyber's Prioritized Recommendations

Use the hyperlinks for expedient navigation.

Level 1-5	Recommendation Title
5 – Exigent	Improve Data Loss Prevention
4- Critical	Improve Security for Proprietary Software
4 – Critical	Create Continuously Accurate Computing Asset List
4 – Critical	Create Customized Incident Mitigation Protocols
4 – Critical	Improve Computing Continuity
3 – Very Important	Improve its Detect & Analyze System

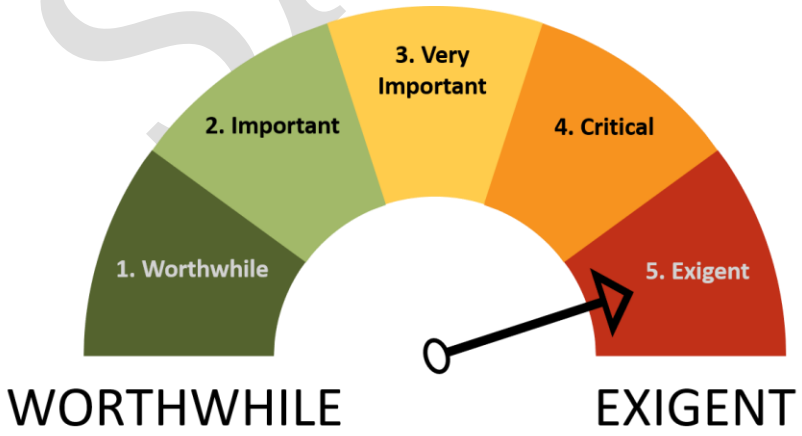
3 – Very Important	Improve Access Controls
3 – Very Important	Revise and Consolidate Policies
3 – Very Important	Improve Mobile Device Management
3 – Very Important	Improve Employee Security Training
2 – Important	Improve Patch Management
2 – Important	Improve Malware Detection
2 – Important	Add Additional Network Defenses
2 – Important	Improve Email Security
2 – Important	Improve Social Media Security
1 – Worthwhile	Encryption for Business Information
1 – Worthwhile	Improve Security for Third-Party Vendors/Consultants
1 – Worthwhile	Improve Removable Media Security

2. PRIORITIZED RECOMMENDATIONS

Overall, Acme Corp should be commended for implementing a reasonable degree of Cybersecurity and Computing Continuity. Nonetheless, Acme Corp should strongly consider implementing Practical Cyber's initial set of prioritized Cybersecurity and Computing Continuity recommendations detailed below. And Practical Cyber welcomes the opportunity to help Acme Corp cost-effective make these prioritized improvements.

IMPROVE DATA LOSS PREVENTION

Priority: Level 5 – Exigent.



Current Situation: Acme Corp has not yet implemented a Data Loss Prevention system across all systems – e.g., Office365, MS Office Products, and data stores – with readily administrable data classification as Appendix A introduces.

Specific Suggestions: Acme Corp should consider the following:

1. Evaluate internal resources that can be applied to creating and implementing a DLP system.
2. Create a data classification system. See Appendix A.
3. Enable DLP including a platform that permits DLPs and implement DLPs across all systems
4. Use DLP to prevent forwarding sensitive documents and files outside of the Acme Corp domain.
5. Further educate employees on the need for DLP and how to implement it.
6. Establish DLP remediation processes and procedures.

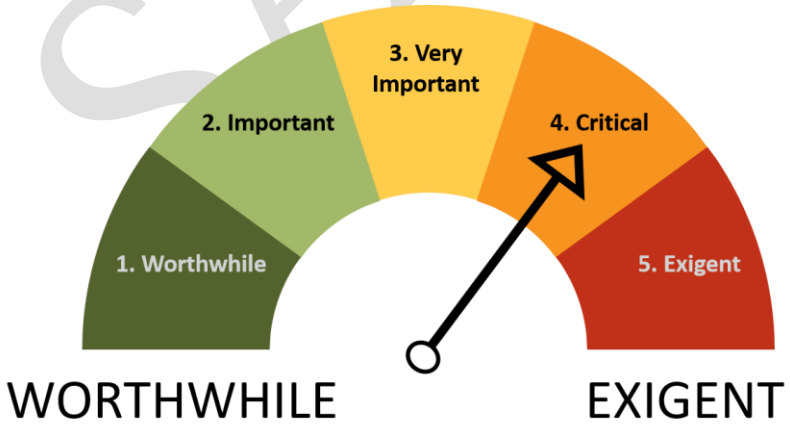
Benefits from Implementing this Recommendation: Implementing a comprehensive DLP system will provide Acme Corp the following benefits:

- Better prevent data exfiltration.
- Improves other security areas.
- Improves Acme Corp's overall business continuity.
- Increases effectiveness of confidential system.
- Improves defenses against insider threat.

Helps secure computing devices by improving mobile device management.

IMPROVE SECURITY FOR ACME CORP'S PROPRIETARY SOFTWARE

Priority: Level 4 – Critical



Current Situation: Securing software has two basic elements: (1) securing the software development environment and (2) using secure coding practices. Acme

Corp has hired a third-party software development company to manage ongoing software projects, which were originally coded by a team led by Sergey Dzekunov. The original software team still has some access to the code and related proprietary data. Bob and has team do not have information relevant to Acme Corp's coding practices or the security measures the third-party software development company has implement for its development environment. As to Sergey's team, the following is true:

- Control of the code has been turned over to the third-party development company;
- Sergey still has access to the development code from an un-managed endpoint;
- Sergey is not required to follow baseline cybersecurity and computing continuity requirements/procedures that the rest of the organization must use.

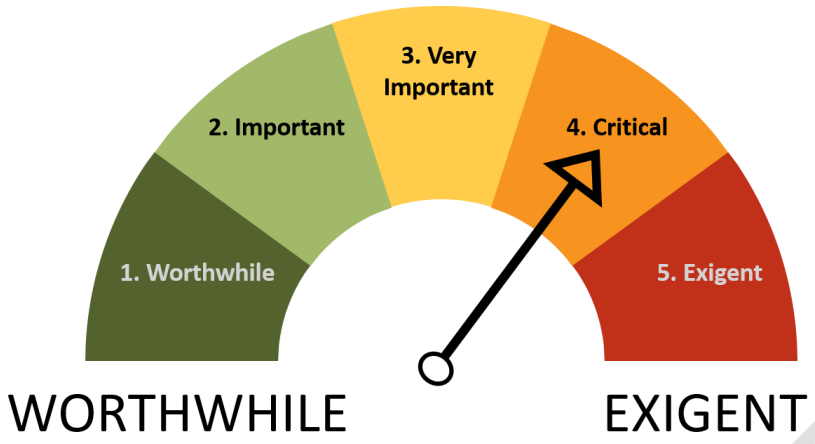
Specific Suggestions:

- Evaluate Acme Corp's secure coding practices – a task that requires a third-party expert such as Practical Cyber.
- Evaluate the security measures that the third-party development company is using to protect its software development environment and Acme Corp's code. This company's security measures directly impact Acme Corp.
- Require Sergey and his team to follow all Acme Corp's cybersecurity and computing continuity requirements/procedures.

Benefits: Acme Corp's proprietary software is the lifeblood of its profitability. Therefore, protecting it from cyber-attack is critical. To do so, Acme Corp should implement Practical Cyber's suggestions, focusing on both (1) securing the software development environment and (2) using secure coding practices.

CREATE CONTINUOUSLY ACCURATE COMPUTING ASSET LIST

Priority: Level 4 – Critical.



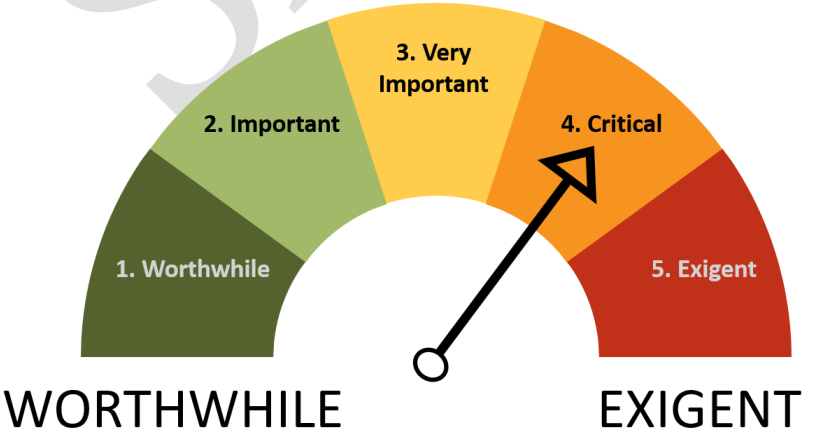
Current Situation: Acme Corp has not yet created a system to continuously and accurately list all computing assets. This list should cover desktops, laptops, network printers, networking devices (routers, switches, etc.), storage devices, mobile devices, Iot devices (e.g, Ring cameras), and other connected devices.

Specific Suggestions: Acme Corp should consider creating a policy that defines how it will cost-effectively create and maintain this list, and then diligently apply this comprehensive policy.

Benefits from Implementing this Recommendation: A continuously accurate computing asset list is a major part of detecting/repelling cyber threats and identifying and remediating cyber vulnerabilities. Any computing device with a vulnerability might be the reason that Acme Corp suffers an expensive cyber-incident. Therefore, Acme Corp should have and leverage a continuously accurate computing asset list.

CREATE CUSTOMIZED INCIDENT MITIGATION PROTOCOLS

Priority: Level 4 – Critical.

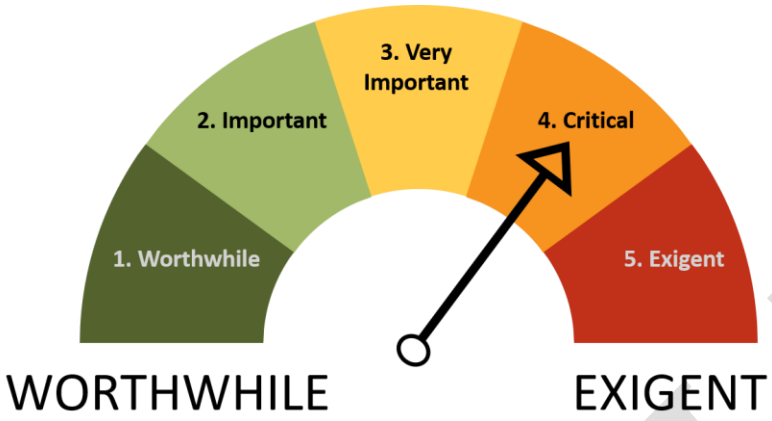


Current Situation: Acme Corp has a series of policies that relate to how it should mitigate the financial harm from cyber-incidents: Business Continuity Plan, Continuity of Operations Plan, Disaster Recovery Plan, Security Incident Response, Security Response Plan.

Recommendation: Promptly and effectively identifying cyber-incidents and then cost effectively mitigating the harm from all unprevented cyber-incidents should be a high priority for all companies, including Acme Corp. Acme Corp's balkanized approach is not nearly as effective as creating a single set of Customized Incident Mitigation Protocols – as Appendix A explains. Practical Cyber therefore, highly recommends that Acme Corp engage Practical or other similarly competent expert to lead the creation of Customized Cyber-Incident Mitigation Protocols. Normally, the minimum price for this service is $10K, but Practical Cyber will reduce the price to $8K because of its relationship with Acme Corp if Acme Corp also engages Practical Cyber to revise and condense all its Cybersecurity and Computing Continuity policies (See next recommendation). The total cost for customized Cyber-Incident Mitigation Protocols and revised and condensed polices is $13K.

IMPROVE COMPUTING CONTINUITY

Priority: Level 4 – Critical.



Current Situation: Computing Continuity refers to the technologies, people, and processes that restore your computing operations and digital data after cyber-incidents. Acme Corp has a broad Business Continuity Policy that does not specify how Acme Corp will regularly test and then recreate its computing operations after cyber-incidents. Acme Corp currently uses the following Computing Continuity technologies and processes:

- Onsite server that stores all work files, and an automated backup of that onsite server in the cloud.
- Backs-up its development files to the Git repository anytime code is changed.
- Backup are made whenever files are changed or at the server's next backup.

Overall, Acme Corp's Computing Continuity is reasonable

Specific Suggestions: Acme Corp should consider the following:

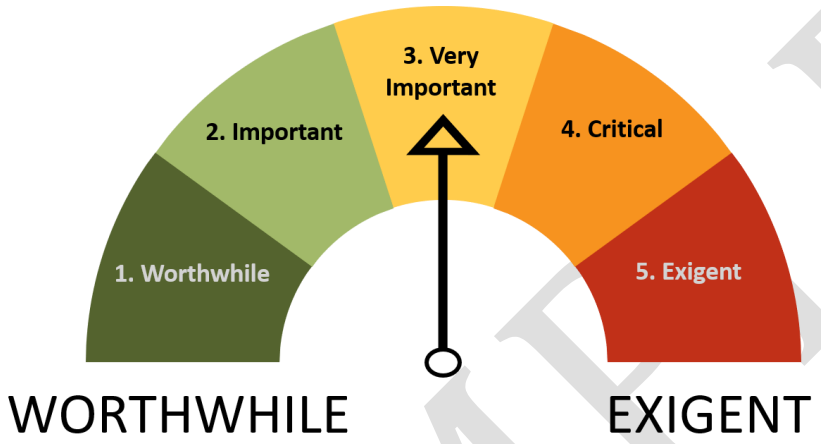
- Revise is Broad Business Continuity Policy into a more effective Computing Continuity Policy that specifies regular testing and lays out recreation procedures in more detail.
- Helps protect its data storage from ransomware because the spread of ransomware is dependent on what systems it can access. Having a plan to stop backups, restore known good ones, and following computing continuity plans help mitigate harm from ransomware.
- Implement a data loss prevention plan (DLP)
    - Restrict users from using private backup services in favor of using Acme Corp resources.
    - Prioritize backups which are business critical or have a high sensitivity level.

Benefits from Implementing this Recommendation: In light of the growing ransomware threat, effective computing continuity is essential. It starts with a

concise, intelligent computing continuity policy, which specifies the (1) computing continuity technologies and procedures – including regular testing – and (2) how the organization will recreate computing operations in a timely, business-focused approach. Our low-cost recommendations will sufficiently improve Acme Corp's computing continuity to justify the additional expense.

IMPROVE ITS DETECT & ANALYZE SYSTEM

Priority: Level 3 – Very Important.



Current Situation: Overall Acme Corp has implemented a fairly effective Detect & Analyze System, which comprises the technologies, processes, and people that detect and analyze cyber vulnerabilities and cyber threats. For its Detect and Analyze system, Acme Corp is currently doing the following all overseen by Bob has his team:

1. Using BlackPoint's MDR to detect, analyze, and automatically respond to cyber threats.
2. Using EventTracker to monitor logs from operating systems and Active Directory events.
3. Using Nodeware for 24/7 vulnerability scanning.
4. Manually review logs and other information – including but not limited to reviewing firewall logs.

Appendix B explains in more detail the value of a highly effective Detect and Analyze system as part of how Acme Corp should use customized Cyber Incident Mitigation Protocols to protect itself from the potentially very expensive financial harm inflicted by almost inevitable unpreventable cyber-incidents.

Specific Suggestions: Acme Corp should consider the following:

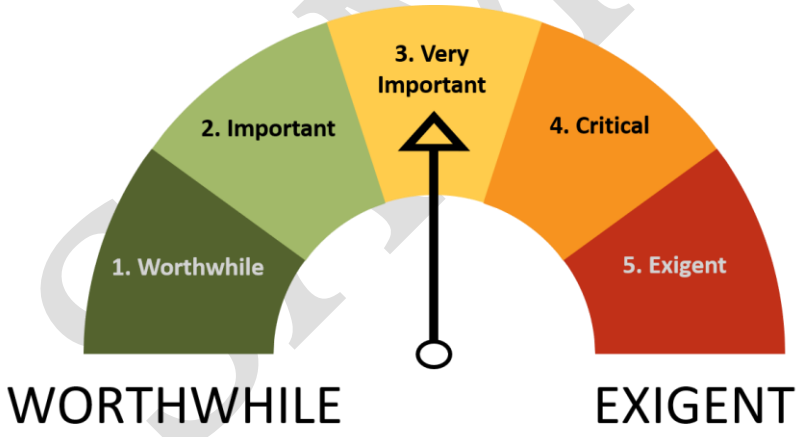
1. Create a continuously accurate computing asset list. See other recommendation.

2. Monitor for large file transfers by properly implementing DLP.
3. Replace Event Tracker with a log management aggregator such as BlackPoint's LogIC, and automate the comparison with the BlackPoint MDR.
    - BlackPoint MDR comes with time-limited log retention; but it is not perfect system. Logs needed for necessary investigation may not be stored.
    - LogIC is an add-on to the already existing MDR service which will add features over Event Tracker as new assessments and audits.
4. Review MDR logs on a quarterly basis and use lessons learned to "adjust" the MDR to more accurately reflect Acme Corp's normal computing activity.
    - This might include changing thresholds of acceptable/unacceptable activity or behavior
5. Implement DLP. See other recommendation.

Benefits from Implementing this Recommendation: Some cyber-incidents are unpreventable, and many go undetected. The quicker and more comprehensively that Acme Corp detects cyber-incidents, the better it can mitigate the related financial harm. Our Detect and Analyze suggestions provide sufficient benefit to Acme Corp to justify the additional cost of implementation.

IMPROVE ACCESS CONTROLS

Priority: Level 3 – Very Important.



Current Situation: Acme Corp has already implemented a reasonable series of Access Controls, which help protect its resources and computer environment. However, there are additional low-cost access control improvements that we suggest below.

Specific Suggestions: Acme Corp should consider the following:

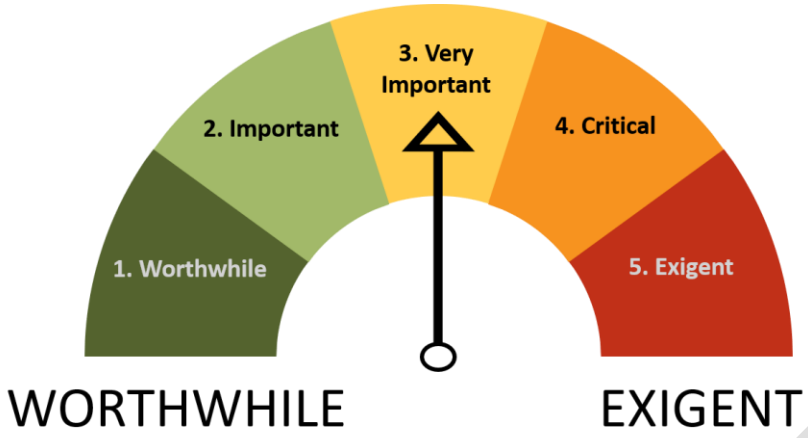
1. Remove local admin from users.
2. Use MFA with backup passphrases and keep them in a password manager.

   a. Any process or application that has MFA capability should have MFA enabled.
   b. Prohibit users from resetting their own MFA. They should go through some authentication process.
3. Automate off-boarding
   a. Right now MacCyte does this manually
   b. You can automate the process to remove the person from all systems – e.g., using Active Director to push out all the changes.
4. Review orphaned accounts on a monthly basis.
5. Continue role-based access controls – this includes all employees and contractors (particularly the software developers).
6. Document their access control policies and procedures for third-party service providers – such as SalesForce, NetSuite, Atlassian, and Solidworks.
7. Document their access control policies and procedures for elevated privileges
   a. Make sure Acme Corp's C-Suite understands the importance of its role in approving elevated computing privileges.
   b. Need an internal employee backup/alternate for the CFO's elevated privileges.
8. Background checks for all people working on Acme Corp's IT and/or providing software development services to Acme Corp.
9. Yearly access control audit by independent expert.
   a. This is part of SOC 2 compliance and good cybersecurity
10. Enable Microsoft Credential Guard.
11. Use one-time passwords instead of assigning a new user role.
12. Disable network access control (NAC) from credential spraying.
13. Ensure NAC for all IoT devices.

Benefits from Implementing this Recommendation: Implementing these low-cost suggestions will improve Acme Corp's Access Controls in ways that will cost-effectively enhance Acme Corp's ability to prevent unauthorized access to its computing operations and digital data.

REVISE AND CONSOLIDATE POLICIES

Priority: Level 3 – Very Important.



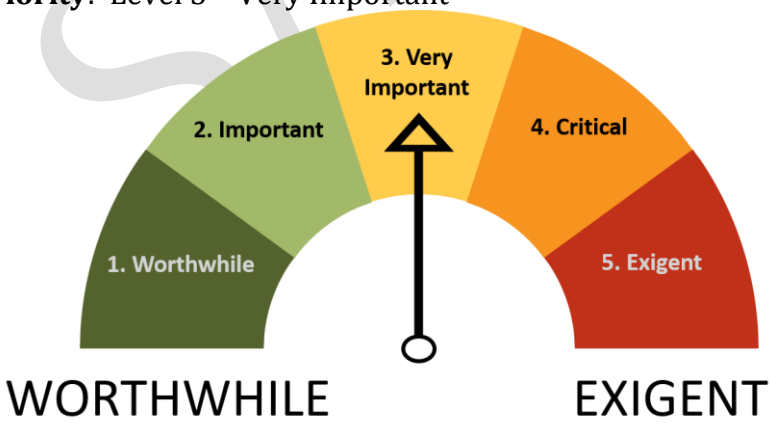
Current Situation: Acme Corp has 51 separate policies relating to Cybersecurity and Computing Continuity – some focused on what Bob and his team should do, some on management action, and some on employee action. Some of these policies have overlaps.

Specific Suggestions: Acme Corp should consider engaging an expert to revise and consolidate its policies based on the changes it has made over time and any changes it will make based on this Roadmap. Practical Cyber will do this work for a fixed price of $5,000. This does not include customized Cyber Incident Mitigation Protocols, which require much greater effort.

Benefits from Implementing this Recommendation: Having customized, concise Cybersecurity and Computing Continuity policies is an essential part of cost-effectively mitigating Acme Corp's cyber risks; as well as an important part of any SOC 2 audit.

IMPROVE MOBILE DEVICE MANAGEMENT

Priority: Level 3 – Very Important



Current Situation: Overall Acme Corp's mobile device management is reasonably designed and implemented – except that it is not deployed all on devices.

Specific Suggestions:

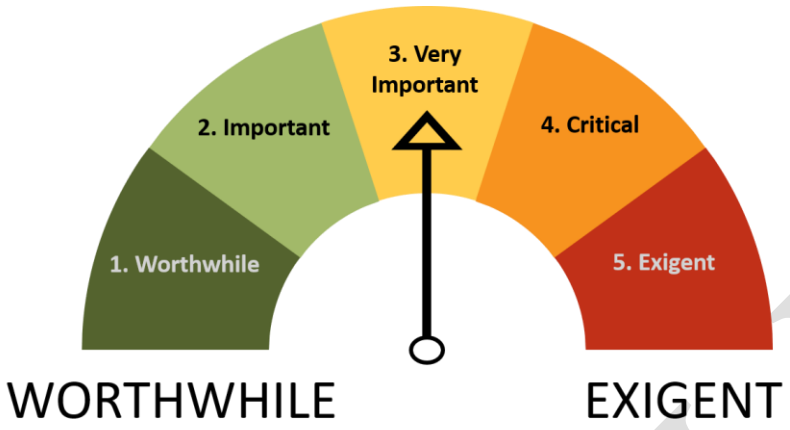
- Finish deploying your MDM to all devices.
- Centralize RMM (Remote monitoring management) by having all mobile devices on one system such as Intune.

Benefits: Acme Corp will gain the following benefits from our low-cost recommendations –

- Help prevent attacks through employee's cellphone e.g. mobile malware.
- Ability to remove sensitive data from a device remotely.
- Utilize access control for apps for proper authentication to digital assets such as documents and spreadsheets.
- Enforce application updates, renew certificates, and segmentation from personal apps
- Provide automatic backup of mobile files.
- Ability to remote wipe a lost or stolen device.
- Helps ensure device compliance with updates and security patches.

IMPROVE EMPLOYEE SECURITY TRAINING

Priority: Level 3 – Very Important



Current Situation: For employee training, Acme Corp currently uses KnowBe4 phishing training and Domain Technology Partners ("DTP"). DTP training occurs annually, phishing training occurs monthly. However, as with almost every training program, improvements can be made.

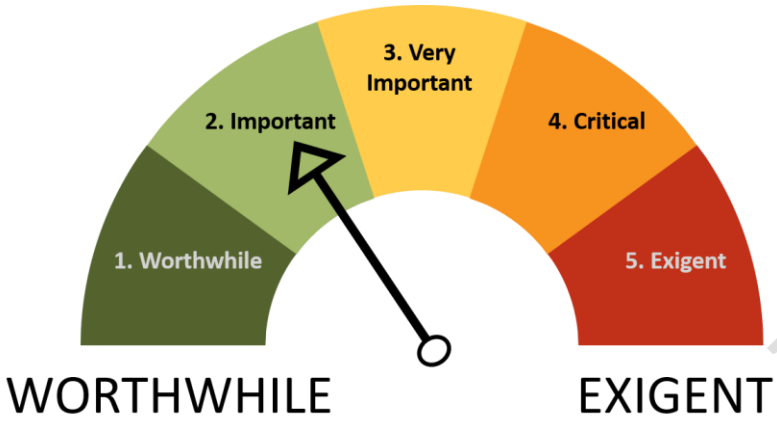
Specific Suggestions:

- Increase annual training to monthly but apply a non-intrusive, prioritized approach that doesn't over-burden employees.
- Expand training to include proper security hygiene and not phishing alone. These practices include proper credential handling, data loss, malicious attachments or services, clean desk policy, how to update personal devices, and other practices.
- Support from upper-level staff to encourage a proper security culture among employees. Employee security practices often depend on the type of management support for the training.

Benefits: Employee insecure behavior is one of the greatest vulnerabilities for companies like Acme Corp. An employee opening a single malicious email can trigger a very expensive cyber-attack such as ransomware or a data breach. Improving employee security, therefore, will significantly help mitigate Acme Corp's overall cyber risks.

IMPROVE PATCH MANAGEMENT

Priority: Level 2 – Important



Current Situation: Overall Acme Corp's patch management systems is reasonably designed and implemented. The system currently includes:

- Bob and his team reviews, applies, and tests new patches weekly using a test environment:
  - Workstations are patched weekly; and
  - Servers are patched weekly or monthly and rebooted monthly
- Bob and his team further review all patches on monthly basis and as needed.

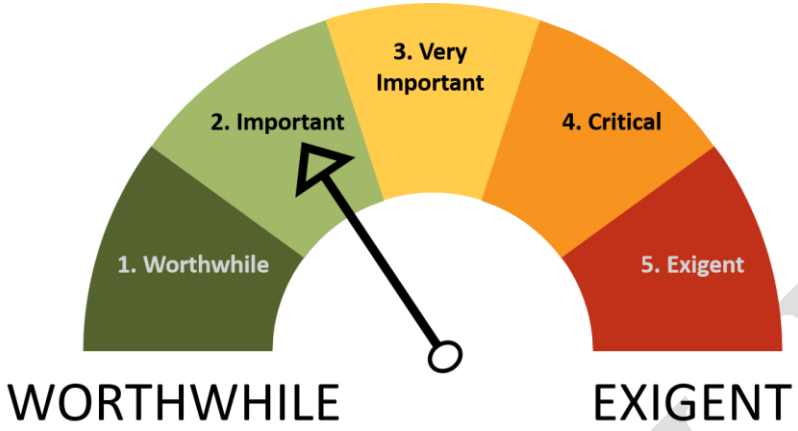
Specific Suggestions:

- We recommend that anytime the network topology changes – excluding mobile phones – that patches are applied immediately not weekly.
- Every Acme Corp department should use a change management system – for example HR & marketing are not following the current change management system.
- Add a change management system to the software development environment.
- Review change management procedures
  - Ensure software development lifecycle and CI/CD pipelines are defined and put in policies
  - Implement items from lessons learned

Benefits: Diligently patching computing technologies is a critical part of cybersecurity. A single unpatched computing asset – e.g., a server – can lead to a very expensive cyber-attach such as ransomware, data breaches, or IP theft. Our suggestions will help Acme Corp diligently patch systems and technologies not currently covered.

IMPROVE MALWARE DETECTION

Priority: Level 2 – Important



Current Situation: Overall Acme Corp's current malware detection system is reasonably implemented. Acme Corp uses Webroot and Microsoft InTune on all known computing assets. Having a continuously accurate computing asset list will help Acme Corp maximize the benefits of its malware detection by helping Acme Corp ensure that anti-malware software is properly deployed all on its computing devices.

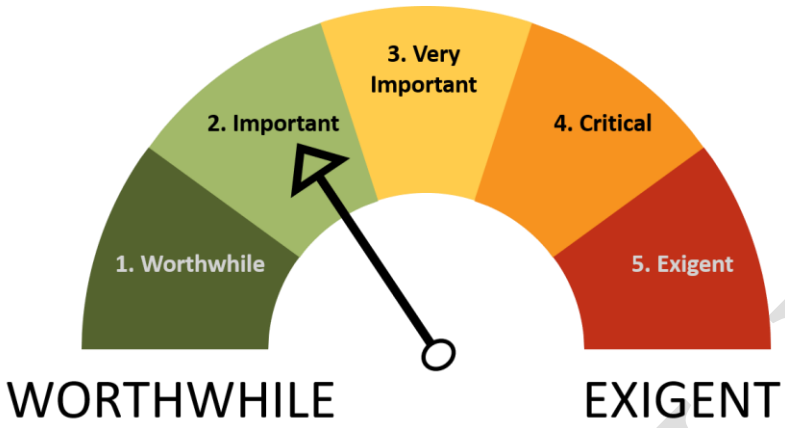
Specific Suggestions:

- Enable InTune along with Webroot. InTune works with mobile phones, and enabling it will not cost more money.
- Enable Microsoft Exploit-Guard. But, we recommend that Acme Corp maintain an accurate asset list, and deploy malware detection on all appropriate assets (i.e., computing devices).

Benefits: Our low-cost suggestions will improve the overall efficacy of Acme Corp's malware detection, which is an important benefit. One vulnerable computing device can lead to malware infecting many other of Acme Corp's computing devices and overall computing operations.

ADD ADDITIONAL NETWORK DEFENSES

Priority: Level 2 – Important



Current Situation: Overall Acme Corp's current network defenses are reasonably implemented.

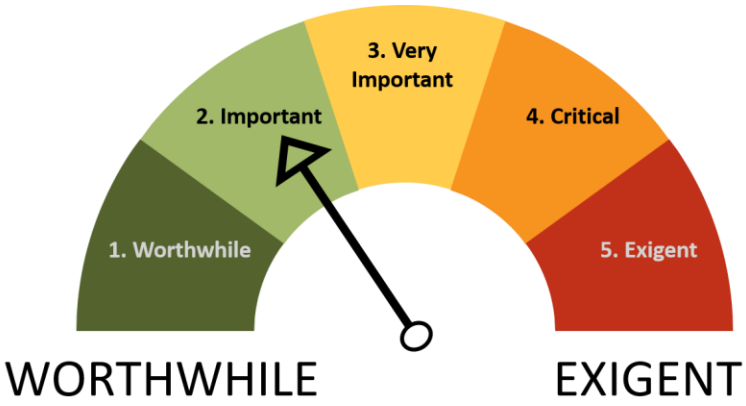
Specific Suggestions: The following are low-cost suggestions to improve Acme Corp's network defenses --

- Disable LLMNR
- Disable Windows proxy auto-discover.
- Don't allow external devices to have network access
- Every two weeks, review VPN logs to look for suspicious activity
- The MDR should send alerts for most suspicious VPN activity. Disable SMB version 1, and enforce SMB signing

Benefits: These low-cost recommendations will further impede the ability of hackers to traverse your network.

IMPROVE EMAIL SECURITY

Priority: Level 2 – Important



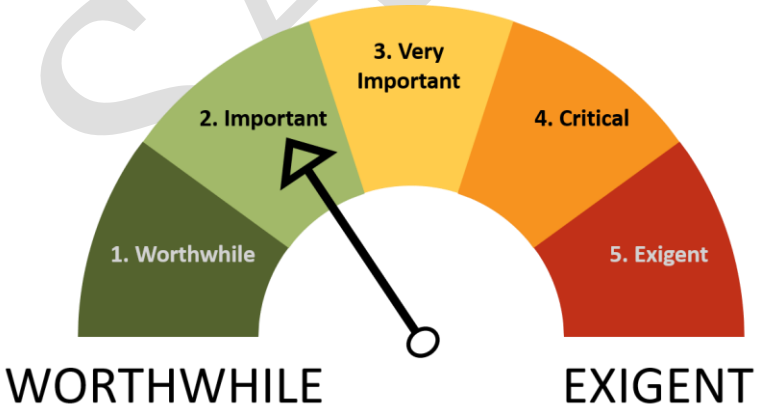
Current Situation: Overall Acme Corp's current email security is reasonably implemented. Acme Corp uses security awareness training, SPAM filtering, and DNS filtering to remove potentially harmful emails from the Acme Corp environment.

Specific Suggestions: Acme Corp should consider centralizing email security with products Acme Corp already has, such as using Exchange Online Protection or Microsoft Defender for Office 365 plans. Additionally, Acme Corp should adopt more strict standards for SAT (see above).

Benefits: Because emails are the most common – and a highly effective – method for launching cyber-attacks, email security is paramount. Our suggestions will improve Acme Corp's email security by providing reports, threat information, and automated investigation and response. It will also consolidate efforts and potentially reduce costs.

IMPROVE SOCIAL MEDIA SECURITY

Priority: Level 2 – Important



Current Situation: Overall Acme Corp's current social media security is reasonably implemented. Acme Corp's credentials are not monitored or stored in a central

repository for others to access securely. Individual departments such as marketing handling their own social media security.

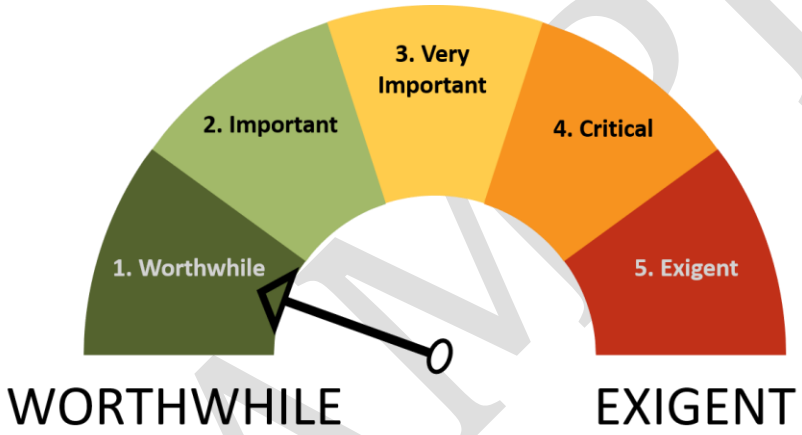
Specific Suggestions:

- Acme Corp should consider credentials through a credential manager such as LastPass.
- Acme Corp should enforce security procedures for accessing and utilizing social media accounts. These accounts should be managed by the IT security team and not individual departments.

Benefits: Properly security social media decreases your cyber-attack surface. Reducing this surface in this way helps protect Acme Corp from reputational damage inflicted by its social media accounts.

ENCRYPTION FOR BUSINESS INFORMATION

Priority: Level 1 – Worthwhile



Current Situation: Overall Acme Corp's use of encryption for business information is reasonably implemented. The encryption includes:

- Using Bitlocker to encrypt the data on the hard drives of the Microsoft workstations and laptops
- Encrypting backups
- Using FileVault to encrypt the data on the hard drives of the Mac computers.
- Bob and his team are doing a manual monthly audit of Acme Corp computers.

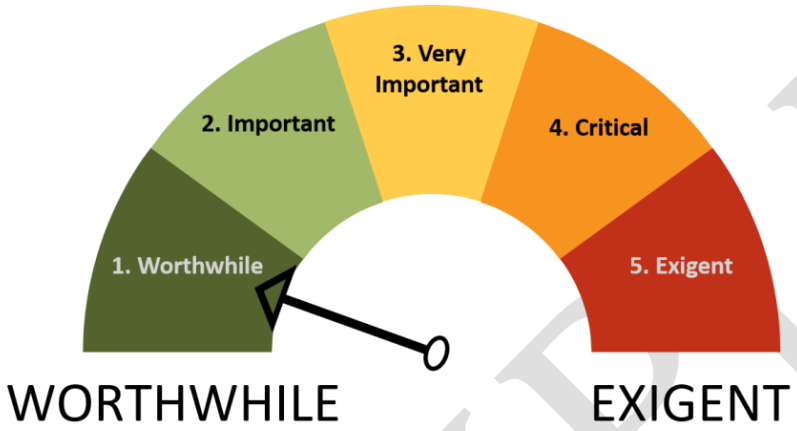
Specific Suggestions:

- We recommend backing-up the Bitlocker or FileVault encryption key in a universal but secure location such as a password manager.
- Ensure all communications and storage procedures are using the most modern and secure protocols – such as using SFTP over FTP for file transfer.

Benefits: Encrypting business information is a low-cost, vital part of ensuring that cyber-attacks cannot exfiltrate valuable, unencrypted files. Our low-cost recommendations will enhance the overall encryption system.

IMPROVE SECURITY FOR THIRD-PARTY VENDORS/CONSULTANTS

Priority: Level 1 – Worthwhile



Current Situation: Overall Acme Corp is reasonably secure its interactions with third-party vendors and consultants. Acme Corp allows third-parties to connect to Acme Corp resources through multiple API connections. Consultants do not have access to Acme Corp resources, but do have corporate emails. API connections traffic is still subject to security scanning and auditing. Acme Corp has a written policy for third-party vendors and consultant interactions.

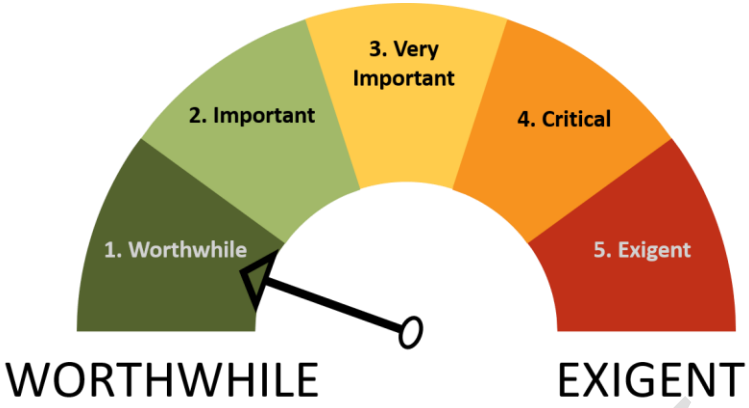
Specific Suggestions:

- Acme Corp should review is API connections quarterly and assess their need for access.
    - In addition, Acme Corp should be privy to ongoing cybersecurity breaches and media to ensure one of the third parties is not compromised.
        - Practice least privilege and remove unused API connections.
- Ensure input is validated and does not allow for data leaks or exploitation and use rate limits to deter denial of service attacks.
- Ensure traffic is encrypted to prevent a man-in-the-middle cyber-attacks, which is when the attackers insert themselves in the middle of some form of digital data transfer.

Benefits: These additional, low-cost improvements will be worthwhile supplements to Acme Corp's already reasonable efforts.

IMPROVE REMOVABLE MEDIA SECURITY

Priority: Level 1 – Worthwhile



Current Situation: Acme Corp does not have a technical control for removable devices; though there is a policy in place. Employees learn about the dangers of unknown removable media through Security Awareness Training.

Specific Suggestions:

- Formalize the removable device policy and further implement its procedures – e.g., the practice of preventing the use of removable media.
- To provide a technical control for this recommendation, data loss prevention should be implemented.
- Audit occurrences of attempted data exfiltration and connected removable media quarterly.
- Permissible removable devices should be logged and audited quarterly, looking for large amounts of data transfer.

Benefits: Enhances employee security behaviors and helps prevent data exfiltration.

APPENDIX A: DATA CLASSIFICATION

Data classification is an important part of cyber and privacy risk mitigation, helping organizations do the following:

- Identify and categorize your sensitive and regulated data,
- Determine how your organization produces, distributes, and stores such data,
- Apply customized and prioritized security protections (e.g., adjusting security controls, limiting access, and selecting the right encryption,
- Ensure regulatory compliance such as GDPR, HIPAA, NIST SP 800-53, and PCI DSS.
- Streamline search and e-discovery
- Reduce storage and maintenance costs by enabling you to eliminate unneeded data.

There are five basic steps to data classification:

1. Establish a data classification policy, including objectives, workflows, data classification scheme, data owners and handling.
2. Identify the sensitive data you store.
3. Apply labels by tagging data.
4. Use results to improve security and compliance.
5. Data is dynamic, and classification is an ongoing process.

How Practical Cyber will can help Acme Corp address data classification

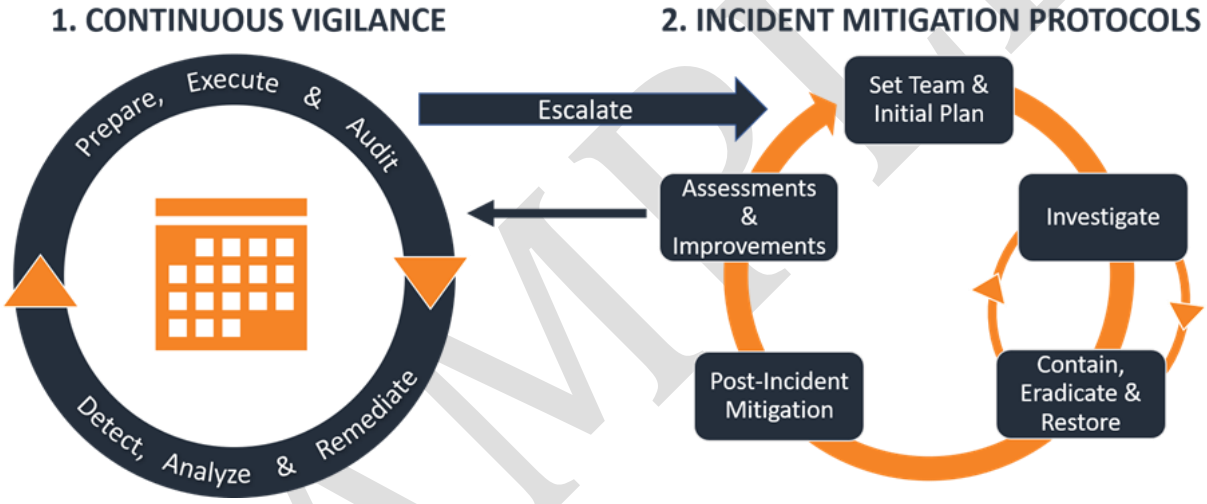
Practical Cyber can help Acme Corp "Establish a data classification policy, including objectives, workflows, data classification scheme, data owners and handling." This includes advising Acme Corp about (1) how its data classification system will impact its cyber and privacy mitigation, (2) helping Acme Corp select its data classes, and (3) the benefits of using an automated, mandatory system/rules/process to classify all new data, and (4) the need to make its data classification system dynamic.

Practical Cyber will not take responsibility for (1) identifying a Acme Corp's sensitive data or (2) applying labels by tagging data -- because those tasks are best handled by the Acme Corp's staff. It will provide high-level advice about these tasks.

APPENDIX B: CUSTOMIZED INCIDENT MITIGATION PROTOCOLS

No Cybersecurity is 100% effective, even defense-in-depth strategies that cost far more and go far beyond Acme Corp's efforts. Today's cyber-attacks can cripple Acme Corp's operations; and prompt detection of attacks can save Acme Corp millions. Therefore, it is vital for Acme Corp to promptly detect evidence of cyber-attacks, and to react swiftly and effectively.

Unfortunately, traditional incident response plans are not sufficiently effective. This led Practical Cyber to develop a better approach – namely Customized Incident Mitigation Protocols, which are a vital part of effective cyber risk mitigation – as this graphic introduces.



Continuous Vigilance: Continuous Vigilance focuses on everything you should do to mitigate cyber risks before an exigent incident requires immediate remediation. It includes the following --

> **Prepare, Execute & Audit:** This refers to all your efforts to create, execute, and audit your comprehensive set of cyber/privacy risk mitigation checklists (as explained in Section 2 below).
> **Detect & Analyze:** Involves the systems, software and people needed to promptly and efficiently identify, analyze, and classify cyber/privacy vulnerabilities and incidents (e.g. cyber-attacks or malfunctions). The goals are (1) to identify vulnerabilities and properly remediate them before they are exploited and inflict harm and (2) to accurately identify and classify

incidents, minimize false positives and cost-effectively escalate only material incidents to your Incident Mitigation Protocols.

Escalate: The process for escalating material cyber incidents to your Incident Mitigation Protocols.

2. Incident Mitigation Protocols: This focuses on reducing the harm from cyber incidents escalated to your full Incident Mitigation protocols. The proper execution of the detect, analyze, and escalate elements is vital to the success of your Incident Mitigation Protocols. Those elements collaborate to ensure that you properly identify and escalate incidents that might inflict significant harm.

After you escalate an incident to your Incident Mitigation Protocols, your multidisciplinary team should deploy the following Incident Mitigation elements:

Set Team and Initial Plan – This identifies the team members responsible for each escalated incident, who then create an initial investigation plan based on the detection and analysis evidence. Teams need to be set in real-time, because each incident is different, and some personnel might not be available.

Investigate – This focuses on executing your initial investigation plan, which should help you obtain the information needed to contain, eradicate, and/or restore operations. Sometimes, you will proceed directly to the contain, eradicate, and restore phase.

Contain, Eradicate, and Restore – These are grouped because some or all these elements might be needed after the Initial Investigation. Contain means stopping the damage/harm. Eradicate means removing any malicious code and/or unauthorized access or any other source of harm. And restore means restoring operations mostly using your computing continuity plan.

Loop between Investigate and Contain, Eradicate & Restore – This is part of the diagram because when the initial attempts to contain, eradicate & restore are inadequate, a second investigative plan should be created and implemented.

Post-Incident Mitigation – This focuses on reducing any post-incident harm such as by regulatory notifications, privacy notifications, and public relations issues.

Assess and Improve – This focuses on improving your overall cyber and privacy mitigations systems by incorporating lessons learned from each instance of detection, analysis, escalation, and incident mitigation.

When properly and promptly executed, your Incident Mitigation Protocols can literally stop the loss of millions of dollars. It is essential for cost-effective mitigation of cyber risks.