Module 6: Change Management Policy Assignment

Kyler Kent

School of Continuing Studies, Georgetown University

MPCR-7990-101: Capstone

Dr. Rosemarie Pelletier

October 8, 2023

Module 6: Change Management Policy Assignment

Request for Changes

As a private sector CISO of Ackme, I recommend the following changes to the Change Control Approval Board. This document is a formal RFC (Request for Change):

1. EOL systems should be upgraded and patched ASAP
    1. Change request reasons and rationale: EOL (end-of-life systems) are described as the "point of entry" by attackers (Georgetown University, n.d.-b, para. 2). These systems are best described as not receiving regular updates from their manufacturer or developer and continue to maintain a persistent vulnerability within the organization.
    2. How system functionalities can be improved: they will simply be upgraded. EOL hardware will need to be disposed of. EOL software can be potentially upgraded, depending on hardware requirements and capabilities. For example, some systems may have an older TPM (trusted platform module) that supports an older version, such as version 1.2, and cannot be upgraded to the latest operating systems, such as Windows 11 (Microsoft, 2021). Therefore, software requirements may necessitate hardware upgrades.
    3. Benefits to Ackme's mission: This will prevent both a point of entry and point of persistence used by the ransomware attackers, helping to secure Ackme's overall CIA (Confidentiality, Integrity, and Availability). Availability is critically important for Ackme's business profits and revenue as a publicly traded company as well as for its BSEE (Bureau of Safety and Environmental Enforcement) compliance issues (Georgetown University, 2020, p. 2).

2. All changes and upgrading should occur for each platform individually
    1. Change request reasons and rationale: This is to mitigate as much downtime as possible. If all platforms are brought down for upgrades, then Ackme's downtime will be exacerbated and Ackme may suffer excessive losses. Each platform is estimated to cost at least $300,00 per day of downtime (Georgetown University, n.d.-a, paras. 3,9). To best mitigate this cost, platforms should be administered individually in case of total system failure or interruption.
    2. How system functionalities can be improved: these will be specified throughout the series of change requests in this document.
    3. Benefits to Ackme's mission: this change will protect Ackme's availability as much as possible. The ransomware attack has effectively compromised Ackme's availability on at least 4 platforms (Georgetown University, n.d.-a, para. 1). Ackme must ensure its change management policy reflects the continuity needs of the organization and counters any impairment of availability of its oil and gas operations. Additionally, it should be noted that Ackme's loss of availability was potentially one of the attacker's goals in the attack and was also successful (Georgetown University, n.d.-e., para. 5). Therefore, Ackme's change management will benefit its own goals and potentially counter the attacker's goals.
3. Golden images should be upgraded and not be EOL
    1. Change request reasons and rationale: Ackme cannot afford to be using obsolete system images to restore. In fact, there is evidence Ackme is restoring systems to what appears to be the same state in which they were exploited, thus allowing the

attackers to re-enter at any time (Georgetown University, n.d.-e). Golden images represent the baseline for the organization and if the baseline is vulnerable, Ackme is setting up its organization during its recovery phase for another attack, which is actually a probability for ransomware victims (Arntz, 2023, para. 2). Additionally, poor recovery methods are cited as a reason for ransomware "reinfection" (Arntz, 2023, para. 4). "Unpatched vulnerabilities" are also a common reason (Arntz, 2023, para. 2). Therefore, Ackme cannot afford to be using a faulty golden image to restore systems to.

2. How system functionalities can be improved: restoration capabilities will be dramatically improved at Ackme as they will not be artificially making systems vulnerable again.
3. Benefits to Ackme's mission: Ackme will directly benefit from the CIA (confidentiality, integrity, and availability) triad in that they will not be restoring systems and putting them in vulnerable states to attacks like ransomware attacks.

4. Perimeter devices shall be forensically analyzed and prepared for replacement.
    1. Change request reasons and rationale: there is evidence that perimeter devices are in question of being compromised (Georgetown University, n.d.-e., para. 5). This necessitates a forensic evaluation to determine if they are truly compromised. Inspection will occur on each device individually and the forensic examiner and system or network administrator will make the decision to replace them if no indicators of compromise are found.
    2. How system functionalities can be improved: perimeter devices will be upgraded, patched, or replaced through this process. This may result in system

improvements, such as increased stability, reliability, and availability as well as reinforcing system security controls.

3. Benefits to Ackme's mission: Ackme will enjoy increases to its CIA (confidentiality, integrity, and availability) triad as perimeter devices will become more secure and reliable. Additionally, it will provide Ackme and its cybersecurity team with the peace of mind knowing they evaluated not only ground zero, but the surrounding systems to comprehensively analyze and prevent another ransomware attack.

5. Reporting (Task R-5, NIST SP 800-37r2)
    1. Change request reasons and rationale: this change aligns with our desire to align with the NIST Risk Management Framework (RMF) on Task R-5 via Authorization Reporting (NIST, 2018, p. 69). Vulnerabilities, risks, and changes will reported to a centralized system for auditing and review.
    2. How system functionalities can be improved: vulnerabilities will be much more conspicuous to senior management and change management officials to track changes over time and potentially prevent a repeat ransomware attack or disaster.
    3. Benefits to Ackme's mission: Ackme will enjoy improved security and benefits to its CIA triad (confidentiality, integrity, and availability) triad.
6. System disposal strategy (Task M-7, NIST SP 800-37r2)
    1. Change request reasons and rationale: this requires that we have a good strategy in place when disposing of legacy and EOL hardware and software. This will ensure data confidentiality is preserved after we terminate hosts and endpoints.

2. How system functionalities can be improved: this may be automated, such as a wiping or imaging stick inserted that runs a script and performs a DoD-compliant software wipe of hard drives before they are manually disposed of and sent to an incinerator.
3. Benefits to Ackme's mission: primarily Ackme's confidentiality is preserved by these actions.

Change Management

Ackme changes shall follow the following change management procedures moving forward to aid in recovering from the ransomware incident (see Figure 1):

1. Request for change (RFC)
    1. Serious vulnerabilities and issues requiring urgent attention should be "emergency requests" in order to get fast approval. We anticipate a swathe of these in response to the ransomware incident.
2. Impact analysis
    1. The pros and cons will be weighed of a change request in order to protect or benefit Ackme while mitigating risks or losses.
3. Approve/deny
    1. Ackme's Change Control Approval Board will ultimately decide to approve or deny the change.
4. Implement change
    1. The requested change will be implemented according to the change schedule. Emergency change requests will receive a fast-tracked response.
5. Review/reporting (Ramos, n.d.).

1. Changes will be reported to a centralized change board in order to document them and ensure implicated parties are aware of the changes.

Figure 1

Change Management System Diagram

Note. Adapted from Ramos (n.d.) 8 elements of an effective change management process. Smartsheet. https://smartsheet.com/8-elements-effective-change-management-process.

Implementing such a plan will ensure full transparency of change management at Ackme and enable organized change requests.

Furthermore, throughout the change management process, Ackme shall implement the NIST Risk Management Framework NIST SP 800-37 r2. Implementing a change management process and having it delegated by a Change Control Approval Board aligns with the authorize phase of the RMF, especially Tasks R-2 and R-4 (NIST, 2018, p. 69). Task R-2 is the Risk Analysis and Determination task and Task R-4 is the Authorization Decision task (NIST, 2018, p.

69). In making these change management decisions, the risk is being determined by an "authorized official" and includes "risk tolerance" fulfilling TASK R-2 (NIST, 2018, p. 69). Additionally, Task R-4 is being fulfilled as there is ultimately a decision to authorize the change made by the authorized person/s via the Change Control Approval Board (NIST, 2018, p. 69).

References

Arntz, P. (2023, September 11). The main causes of ransomware reinfection. *Malwarebytes*. Retrieved October 8, 2023, from https://www.malwarebytes.com/blog/news/2023/09/the-main-causes-for-ransomware-reinfection#:~:text=Ransomware%20reinfection%20arguably%20could%20be,to%20a%20repeat%20ransomware%20attack.

Georgetown University. (n.d.-a). *Module 3: In the Thick of a Ransomware Attack* [Slide show; Canvas]. Georgetown University Canvas. https://georgetown.instructure.com/courses/175977/pages/module-3-in-the-thick-of-a-ransomware-attack?module_item_id=3283361

Georgetown University. (n.d.-b). *Module 4: Do or Do Not* [Slide show]. Georgetown University Canvas. https://georgetown.instructure.com/courses/175977/pages/module-4-do-or-do-not?module_item_id=3283367

Georgetown University. (n.d.-e). Module 6: Systems Recovery [Slide show]. Georgetown University Canvas. https://georgetown.instructure.com/courses/175977/pages/module-6-systems-recovery?module_item_id=3283379

Georgetown University. (2020). H. Ackme Oil & Gas Background Material. In *Google Drive*. Retrieved September 7, 2023, from https://drive.google.com/file/d/1TDoFQQWPZTgWTncVxTrKOfP2rMGkz_Re/view

Microsoft. (2021, August). *Enable TPM 2.0 on your PC - Microsoft Support*. microsoft.com. Retrieved October 8, 2023, from https://support.microsoft.com/en-us/windows/enable-tpm-2-0-on-your-pc-1fd5a332-360d-4f46-a1e7-ae6b0c90645c

NIST. (2018). Risk Management Framework for Information Systems and Organizations. In *NIST* (NIST SP 800-37r2). U.S. Department of Commerce. Retrieved October 8, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Ramos, D. (n.d.). 8 elements of an effective change management process. *Smartsheet*. https://smartsheet.com/8-elements-effective-change-management-process