*Setting a **Higher Level of Excellence** in Information Security & Compliance Services.*

Minding your P's and V's | by Stan P. Skwarlo, CISA, CISSP

Congratulations! Your boss has tasked you with creating a Patch Management Policy to address a recent IT Audit finding. So, you think to yourself "No problem, I'll just Google an example - or even better, request a template from 10-D Security and knock it out." Just when you think this is the easiest thing you've done all week, your boss comes back and nonchalantly states, "Actually our remediation tracker says, 'Vulnerability Management Policy', so create that instead." "Ok, fine," you think, "I'll call it whatever you want, it's the same thing anyway." Or is it? A quick web search for definitions reveals there is indeed a difference:

- Vulnerability Management- A security practice specifically designed to proactively mitigate or prevent the exploitation of IT vulnerabilities.

- Patch Management - A strategy for managing upgrades and updates to software applications and technologies. Includes the acquisition, testing, and installation of patches to a computer system in order to fix known vulnerabilities.

A check of the FFIEC Information Security Handbook confirms that while separate, both are required in the Information Security Program. Vulnerability Management (i.e. vulnerabilities) appears under section *11.A Risk Identification*, and Patch Management under section *11.C Risk Mitigation*. The fact that one deals with risk identification and the other with risk mitigation implies they go hand in hand - you can't patch what you don't know about. Does this mean separate policies are required? As far as the handbook content is concerned, the answer seems to be "yes," since vulnerability and patch management have different objectives; however, it doesn't necessarily mean separate documents. Some organizations choose to maintain a single comprehensive document containing all relevant Information Security policies, while others opt for individual policy documents. Regardless of how these policies are documented, the important part is making sure each has a clearly defined objective and specific guidelines for achieving compliance.

To keep the policy concise and less susceptible to frequent changes, detailed tasks should be reserved for procedures. Additionally, it is a good idea to refrain from referring to individual staff members, specific system brand names, etc. The policy's owner(s) and target audience (for whom the governance applies) should also be defined. For example, in larger organizations the Information Security Officer (ISO) may have overall responsibility for vulnerability management with support by IT, business unit application owners, etc. In this case the ISO would be assigned ownership and involved stakeholders included in the target audience.

Now that we have a little more insight to these processes and some basic policy development strategies, we can begin drafting our policies beginning with Vulnerability Management. The first step is to define the objective. According to our definition above, the purpose of performing vulnerability management is to proactively mitigate vulnerabilities; but how is this achieved? Answering that question will provide us with our objective. Think about the main tasks associated with vulnerability management; identification, analysis and remediation, collectively these make up our stated objective: Identification + Analysis + Remediation = Objective: *To identify, analyze, and remediate security vulnerabilities.*

The specific functions and guiding principles required for achieving the objective are represented as provisional policy statements. For example, tracking assets, performing vulnerability assessments, monitoring alerts from security systems, evaluating external threat intelligence are all functions of vulnerability identification. Analytical functions include evaluating assessment results, determining risk ratings, and reviewing authoritative vulnerability information (e.g. CVE[i] database). Remediation includes, mitigation verification (e.g. re-scanning), risk acceptance approval, status tracking, and metrics reporting. Put this all together, and here is our resulting Vulnerability Management Policy:

Vulnerability Management

Objective:

To identify, analyze, and remediate security vulnerabilities across all <*organization*> systems.

Policy Statement:

- The institution will conduct routine scans of devices, systems, and applications connected to networks to identify operating system and application vulnerabilities. (*Identify)*

- An individual will be assigned responsibility (e.g. ISO) for ensuring routine initiation and review of the results of internal vulnerability scans of devices, systems, and applications. Procedures are in place to evaluate, test, and mitigate where appropriate, identified vulnerabilities. (*analyze*).

- The results of vulnerability scans and review must be reported to management in accordance with the Information Security Policy.

- Remediation of vulnerabilities will be performed in accordance with stated objectives of the IT Risk Management policy (provides specific IT risk mitigation directives, including conditions and requirements for risk acceptance).

- If a solution or remediation is not available to address a vulnerability the responsible party (e.g. ISO) must approve any compensating controls in accordance the IT Risk Management Policy.

Using the same methodology, we can knock out our Patch Management Policy. This of course is where the rubber hits the road in terms of preventing the exploitation of vulnerabilities. Referring to the patch management definition above, the purpose is simple: to fix vulnerabilities. To do this requires the acquisition, verification, and installation of security patches, and in some cases, configuration changes. Like vulnerability management, these are the collective actions that must be accomplished to fulfill the purpose of patch management, Acquire + Verify + Install = Objective: *To acquire, verify, and install security patches that mitigate security vulnerabilities.* The specific functions and guiding principles required to acquire security patches includes the use of automated software for all Microsoft products and supported third-party software. Vendors are solicited manually for all other systems and applications. Application and/or functional test groups are used to verify system (and patch) performance. To the extent possible, testing may only be conducted on “non-production” systems and/or off hours on production systems. Security patch and/or system failures must be recorded and subjected to a risk assessment. The installation of security patches (and updates) of production systems occurs during non-business hours. Putting these together results in the following Patch Management Policy:

Patch Management

Objective:

To acquire, verify, and install security patches that mitigate security vulnerabilities.

Policy Statement:

- The institution will maintain patch management processes and procedures detailing how patches identified, tested, and applied to information resources and systems.
  Note: Unless otherwise stated procedural documentation is contained in the <Name of IT Procedures Document>.

- The institution will maintain patch management standards that outline what type of patches are applied and when patches are applied.

- The institution will maintain an accurate inventory of systems and ensure operating systems (OS) and application security patch levels are maintained in accordance with best practices and/or software vendor recommendations. Specifically,
  - Microsoft systems (servers and workstations) will be configured to automatically check for Critical, High, and Moderate priority patches and apply them according to procedures. At a minimum within thirty (30) days of publication. Low priority patches will be applied during regular maintenance windows, within a ninety (90) day period.
    - Emergency patching must be approved and documented in accordance with established IT procedures.
  - Network devices (routers/switches) are patched by a third-party service provider with oversight by institution IT staff according to procedures.
  - Non-Microsoft system updates and patches are obtained directly from third-party application/software vendors, tested, and installed in accordance with established procedures.
  - Antivirus system updates dates and patches are obtained from the vendor and server/ clients are updated as needed.
  - Core system updates and patches obtained directly from the <core provider> upon completion of testing and installed in accordance with established procedures.
  - The institution will conduct a thorough risk assessment and implement alternative mitigating measures to the extent possible in cases where security patching is not possible. Such must be documented and approved in accordance with the <Institution's Risk Management Policy>.

- The institution will conduct internal and external audits/assessments to verity the effectiveness of the patch management system at least annually.

Finally, in today's fast paced IT environments, it's easy to take the fundamentals for granted especially when it comes to such routine practices like vulnerability/patch management. While it may seem unnecessary to think about these

functions independently since they are so closely aligned, doing so may help drive accountability and corrective action when something goes wrong. For example, is an unpatched system the result of a vulnerability not being identified in a scan or did the patch just not install properly? Establishing policies to govern these practices separately helps define areas of responsibility and provides direction for what needs to be done. Of course, often easier said than done; however, like us auditors like to say - everything starts with a good policy!

[i] CVE database CVE® is a list of entries—each containing an identification number, a. description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S.