NO STINKIN' PATCHES

REMEDIATION

COMPATIBILITY

TIMELINESS

VULNERABILITIES

INSTALL GOAL:
90% - 10 DAYS

IoT

CUMULATIVE UPDATES

REBOOT

SERVICE PACKS

PRINTERS

STATISTICS

COMPUTERS

CYBERSECURITY
STATE OF
SOUTH DAKOTA

JIM.EDMAN@STATE.SD.US

AUGUST 2018 - JULY 2019

Patch Management: Executive Summary

Cybersecurity involves many different facets of technology and human behavior. A critical component of the technology regard is endpoint management - keeping computing devices at current software levels. While a patch management program is not a stimulating, headline-grabbing task, it remains a vital component to an organization's cybersecurity posture. Like blocking and tackling in football – it's the fundamentals that lead a team to victory.

Often, stakeholders realize the value of patching only after unpatched systems become compromised. Various industry studies have shown that unpatched computers are the root cause for up to 60% of security breaches. By efficiently maintaining its infrastructure at a current level of software, an organization can significantly reduce their risks of compromise.

In South Dakota, we have been through multiple iterations of software patching solutions for desktops and portable computers. The problems with our previous solutions included:

- Not all software manufacturers prioritized keeping their product current;
- The timeliness of delivering patches was unpredictable;
- Successful installation of the updates was not being verified;
- Validating update compatibility with endpoint software was difficult or not completed;
- Reports were minimal and uninformative;
- Resources were scarce to confirm updates were consistently and effectively installed.

In our 2018 – 2020 Cybersecurity Strategic Plan, *Protection* Objective 1.2 is defined below:

OBJECTIVE 2		
1.2	Technology	Make the best use of technology to provide protection, identification, monitoring, detection, alerting, and reporting capabilities.

Our tactical step supporting this objective was to:

> *Improve upon a secure technology infrastructure by maintaining standard software levels using an effective patching process.*

Maintaining current software versions sounds like a simple goal, but it has significant enterprise implications. The wide variety of devices that belong to an organization elevates the overall complexity of the update process. Creating this process at no additional costs to the state was a significant accomplishment! We undertook a remarkable, transformational effort using a combination of existing tools and staff to build a sustainable service that will contribute to our mission of protecting confidential government assets long into the future.

SD: Patch Management

Concept

By no means is South Dakota measured as a large state, other than perhaps by geography, open spaces, and pheasants. The Executive Branch has a fluctuating number of approximately 9,500 desktop and laptop computers wholly managed by a technology support team of 51 individuals. That ratio of 186 computers for every support staff person is high for any industry.

In order to work effectively, we must work smarter, not harder. There is a famous quote by Adam Stone:

> *"Anything that you do more than twice has to be automated."*

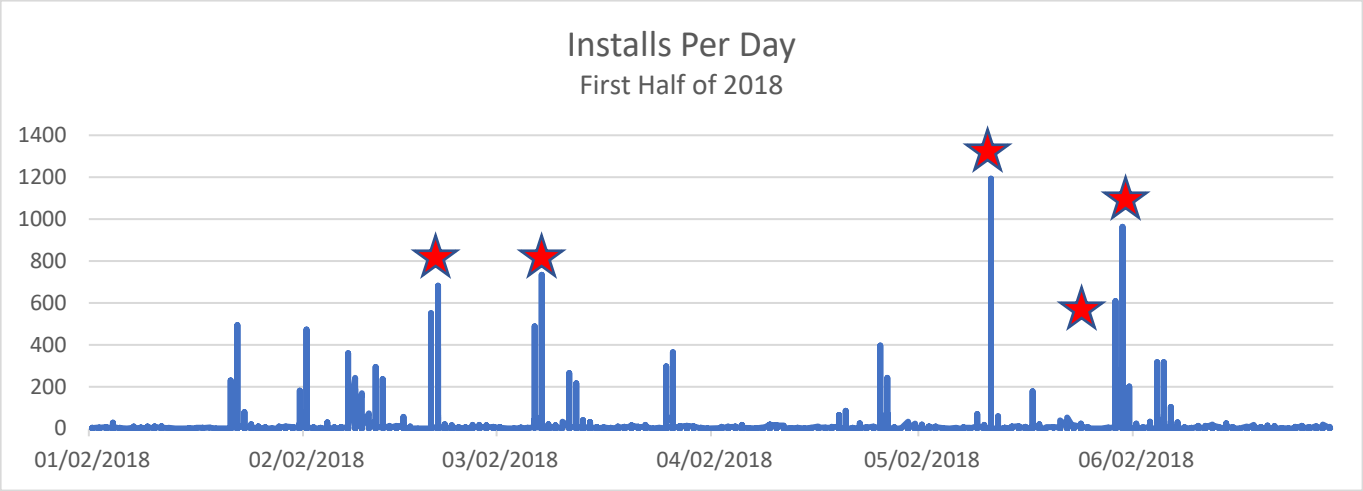
We needed a dependable, reliable, and timely method to deliver software updates to our endpoint devices. Here is a set of problems we faced:

- Every organization has a variety of software from several developers, including Microsoft, Adobe, Oracle, Esri, Google, HP, custom-developed, et al. Most software vendors do a poor job at enabling an enterprise-wide update of their software. This industry gap puts the responsibility on the customer to develop a sustainable solution.
- The quicker you can deliver a software patch, the greater the reduction of the organization's risk posture. The longer it takes to update devices, the higher a chance of the cyber threat actor seizing the opportunity of the vulnerability.
- Every time a new patch is released, determining the compatibility with existing software is a significant concern. There is nothing more frustrating to clients than having features or devices not functioning after attempts to improve them. Experiences like this will make clients reluctant to participate. Sustaining computer functionality after updates is paramount to the patching and update process.
- Delivering patches consistently to our internal network clients is challenging enough, but our remote workforce is much tougher. This issue has three components to it:
    - Building an accurate inventory to understand how many devices you are managing and identifying the current software versions is the foundation to this process.
    - Confirming that the updates can be delivered to the device.
    - Once delivered, ensuring that the patch is successfully applied. As this final step often involves rebooting or logging off the computer, clients fearful of losing their work are reluctant to do. Devising a method to ensure the patches are successfully installed was a critical step.
- Measuring the degree of effort for the patching efforts helps define the value of the process. The number of patches applied, timeline to implementation, number of computers impacted, etc. are all key performance indicators to help explain the breadth of the service. This capability had not existed in a measurable manner for us.
- Nobody wants to take responsibility for managing a volatile process where you can directly impact the usability of a client's machine. Previously, the patch responsibility was distributed amongst geographically based teams throughout the state. Team members were reluctant to send out updates unless the updates were addressing actively exploited vulnerabilities.

SD: Patch Management

- *Everybody is responsible hence nobody is accountable* was the attitude. Success varied as to updates being reliably delivered.

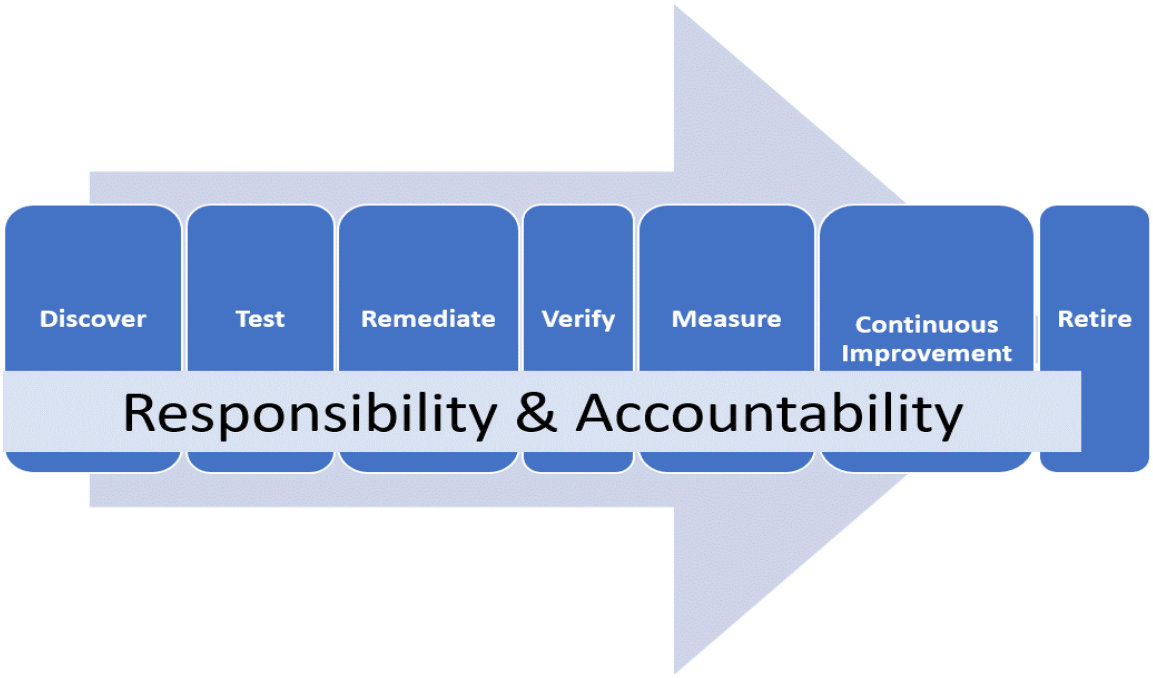
As shown in the graph below, only five patches were installed over 600 times between January and June 2018. Of these, only one patch was installed over 1,000 times.



In this same timeframe there were 1,642 vulnerabilities released with 620 of those rated Critical, High, or Important. We only delivered 58 of those patches for an abysmal 3.5% rate. Additionally, the 58 patches were only installed a total of 12,177 times. That's an average of 202 workstation installs per patch out of a total of 9,500+ workstations.

Significance

We developed a seven-step methodology to reduce our risk.

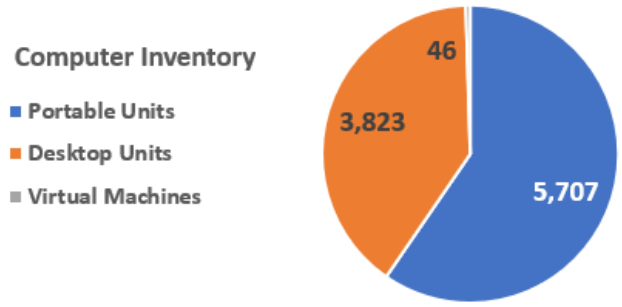


SD: Patch Management

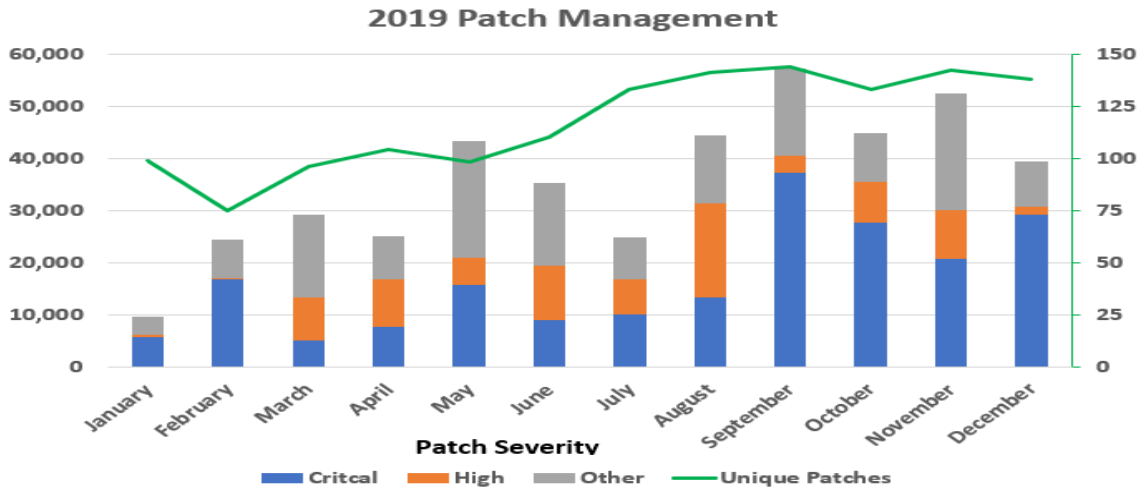
Responsibility & Accountability

The first step was the assignment of two full-time employees dedicated to the patching services. They were given the task of supporting, maintaining and optimizing the patching process. A small but very effective team dedicated to the daunting responsibility ensures that the service is managed through its' lifecycle.

1. **Discover**
   You cannot support what you cannot see. Therefore, the first step to building a successful patching process involved consistently identifying the inventory of software and hardware installed on the infrastructure. This indicated our environment included 9,576 computers and 1,665 printers. We then performed a software scanning assessment to determine the current software and OS versions.



2. **Test**
   Building on the information gathered from the first step, potential patches are evaluated. Patches are prioritized for evaluation based on their severity (Critical, High, Medium, Low). Furthermore, as testing proceeds, we find it useful to monitor multiple independent online sources for any reported issues as other organizations are testing patches and updates.
3. **Remediate**
   Upon approval, the patch definitions are moved to a scheduled process for release. Using existing tools, patches are deployed every Friday, consolidating the rollout window to the weekend when most employees are away from their computers. This gives our endpoints plenty of time to check in and apply updates with less inconvenience to the client. This solution patches computers regardless if they are on the inside of our network or are remote workers.



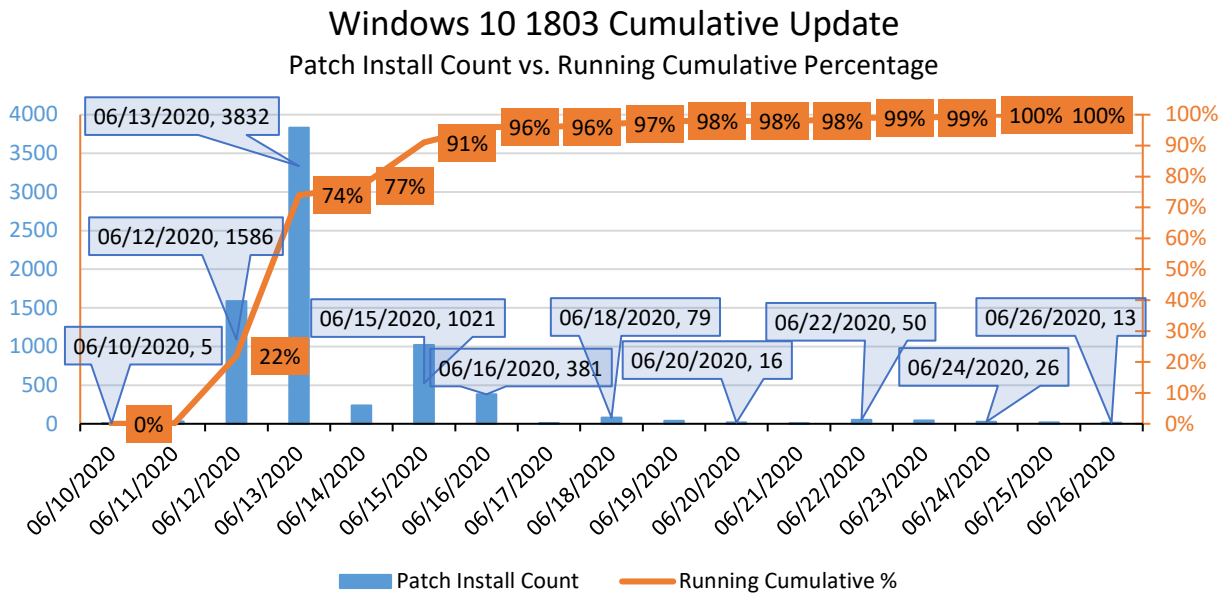
The above graph demonstrates our success across many factors. Total unique manufacturer patches vary from 75 to over 140 per month. Installing Critical and High Patches on a regular basis is prioritized. Finally, the total number of times devices were 'touched' approached 60,000 in the busiest month. That is an average of 6+ updates per device!

4. **Verify**

   We utilize multiple tools to verify successful vulnerability remediation. In addition to the information identified in the Discover Step 1, we run a network scanner against the same infrastructure weekly. If we were medical professionals, this would be our "second opinion". This has the added benefit of discovering vulnerabilities that weren't identified in Step 1. In these cases, we will implement our own patch or return to Step 3.

5. **Measure**

   Measuring our performance is paramount to the success of our patching efforts. The team was tasked with finding a way for generating meaningful reports. We accomplished this using Microsoft's Power BI to build dashboards. We can access the meaningful patching data elements and generate valuable reports for publication. The last major update to the Measure step came by including deployment statistics over the lifetime of a patch. With this data, we can make comparisons with other patches to make predictions and follow trends in the effectiveness of our patching process. This graph shows the entire patching lifecycle from Inventory on June 10 through 100% patch installation 14 days later. 90% of devices were updated within 4 days of patch release (June 12 – June 15)!

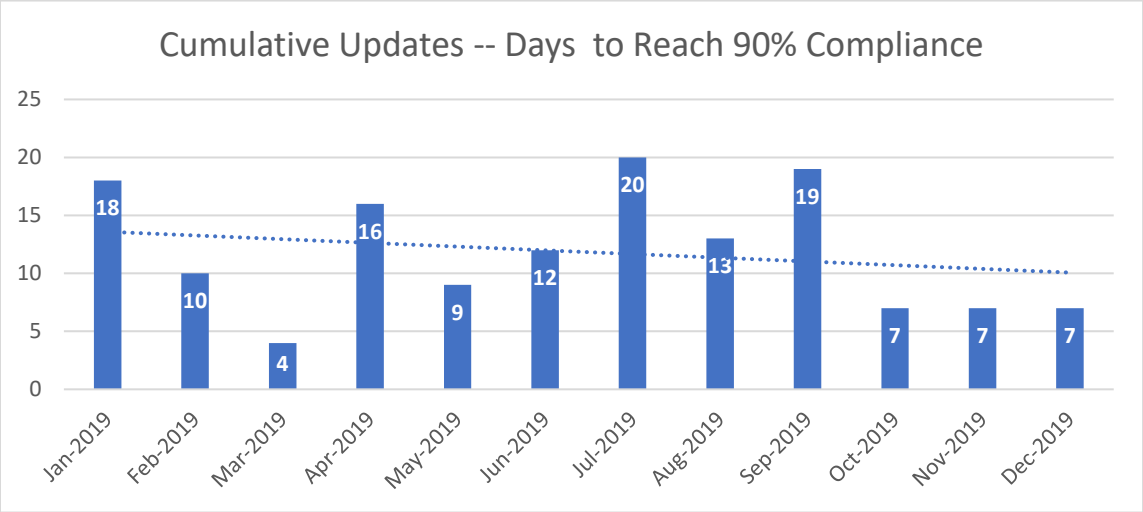


6. **Continuous Improvement**

An effective patching process requires you to revisit updates to ensure they are being successfully installed. We do this by searching for vulnerable software that should have already been remediated. It becomes a problem if the number of affected computers isn't decreasing after a deployed patch. Common issues are the patch not working, the computer not having

enough disk space or not connected to the network in some manner. If you're not making periodic re-evaluations, you will overlook these compounding issues.

This graph shows the number of days it took to reach our 90% compliance within 10 days goal for the year. The patch deployment time through regular efficiency tunings allowed us to reach that goal. Industry reports indicate it takes an average of 22 days to develop a functional exploit from a discovered vulnerability. Our patch process consistently takes less than 10 days, keeping us far ahead of the average exploit time.



7. Retire

When a patch is no longer needed, we move it to our 'do not scan' area. This eliminates the need to repeat a scan. There are typically two ways a patch gets retired: it's been replaced by a newer patch, or the patch is no longer applicable to our environment.

Impact

The outcomes of cybersecurity can be measured in multiple ways using a host of statistics and risk management controls. There are only a few though that can demonstrate the true success of your program. Those include the number of breaches, ransomware and other incidents, virus infections, financial loss, lost data, etc.

In South Dakota, those metrics are ZERO from 2018 through today. Our Patch Management program for our end devices has not allowed any compromises. None. That is a remarkable accomplishment! We are very confident that the Patch Management processes established meet our Strategic Plan objective, are sustainable and will continue to give us thorough end-device protection in the years to come. Software patching is only one piece of our IT infrastructure defenses, but it is a vital piece of that protection.