ITAM FORUM

IT Asset Management's important role in any Ransomware response plan

By Elise Cocks
IT Asset and License Management – Director
Freddie Mac

This article first appeared in Issue 1 (April 2022) of ITAM Insights, the ITAM Forum's membership magazine.

itamf.org

What is Ransomware?

According to the FBI, Ransomware is a type of malicious software, known as malware, that prevents you from accessing your computer files, systems, or networks and demands a ransom to be paid for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

Common attack vectors include:

- Email campaigns known as "phishing" where a malicious file or link embedded in an email deploys malware when clicked
- Remote Desktop Protocol (RDP) vulnerabilities: cyber criminals obtain user credentials to access company systems and deploy malware internally
- Software vulnerabilities: cyber criminals leverage weaknesses in common software to gain access to internal systems to deploy malware internally

Many companies have already been impacted by Ransomware. News-worthy headlines show that large companies, small companies, and government entities have all fallen prey. During 2021, Accenture, CompuCom, Kia Motors, the National Basketball Association (NBA), the University of Miami, and many local and national U.S.A. government agencies were impacted by Ransomware.

How can Ransomware affect your company?

If affected, your company is at risk of temporary or total data loss, which can render your company unable to communicate internally, provide its services, or conduct business. Cyber criminals also threaten to release data to the public, which can cause reputational damage or loss of intellectual property.

What can be done to lower the risk of Ransomware?

To minimize the risk of Ransomware, teams across IT, Information Security, Data Governance and Enterprise Crisis Operations should team together to align on the following best practices:

- Backup data, systems, and configurations
- Enable multi-factor authentication to applications and systems
- Keep applications and systems updated and patched
- Maintain an up-to-date information security solution, including vulnerability detection and management, penetration testing, and staff training of information security best practices
- An incident response and business continuity plan that's actively exercised

How can IT Asset Management play a role in a Ransomware response?

Chances are, your company has an overarching incident response plan and business continuity plan in place to respond to an emergency, but how can ITAM contribute to responding to a Ransomware attack?

ITAM practitioners have the data at their fingertips to know which users have which assets and can quickly help incident response efforts to identify the scope of a potential attack. ITAM teams are uniquely poised to ensure that end users can gain access to functioning endpoints in the event of a Ransomware attack that renders endpoints unusable, and they can and do it in a way that minimizes risk through proper asset tracking and by maximizing cost by leveraging the right assets. ITAM also has access to which users have which software or files installed, who has access to download licenses and software packages, and can coordinate blocking access to infected files.

"A recommendation for how many computers to have on hand specifically for a Ransomware event is 10% of your end-user population."

A function of the ITAM program includes the responsibility for sourcing equipment and tracking its use. For this reason, an ITAM plan to respond to a Ransomware attack is critical in determining how to get a Ransomware-impacted workforce up and running if corporate devices are impacted.

You probably already have a well-developed plan for replacing end-user endpoints. It happens daily when an end user has an issue with their hardware, and it may happen on a large scale to address OS migrations, like, for example, upgrading your users from Win7 to Win10. Maybe you rely on a third party to ship imaged devices to your users; maybe you image your own devices onsite; and maybe you have a hybrid of the two. A response plan should be based around how you manage endpoint distribution today and identify opportunities for future improvement.

Regardless of whether you image your own endpoints or work through a third party, you need to know how many endpoints you have on the shelf ready to be deployed, and how many you have in the wings ready for the imaging process. You're likely managing that inventory to the number of devices needed to meet expected new user onboarding and as-needed replacements. Now you need to consider how many more you need to have on hand so that you have the surplus you'll need to start a mass migration process if many users are affected.

A recommendation for how many computers to have on hand specifically for a Ransomware event is 10% of your end-user population. This gives you a head start to build computers for replacement and receive enough back from those you replaced so they can be wiped and reimaged to hand out to additional impacted users.

When it's determined that an attack has occurred, your company's incident management response should kick in to identify and triage the impact. Once your partner teams have restored the services impacted by the Ransomware attack – which could be any combination of services from Active Directory to Storage – ITAM is ready to jump in and replace endpoints if needed.

In a likely scenario, software or a file contained on the endpoint is the Ransomware trigger. The computer gold image likely needs to be rebuilt and updated to remove the software that had been the Ransomware trigger to ensure new machines don't fall victim again. The imaging team would be alerted by the incident response team and a new image prepared.

Once the new image is ready, any computers that had been on the shelf need to be reimaged so you can

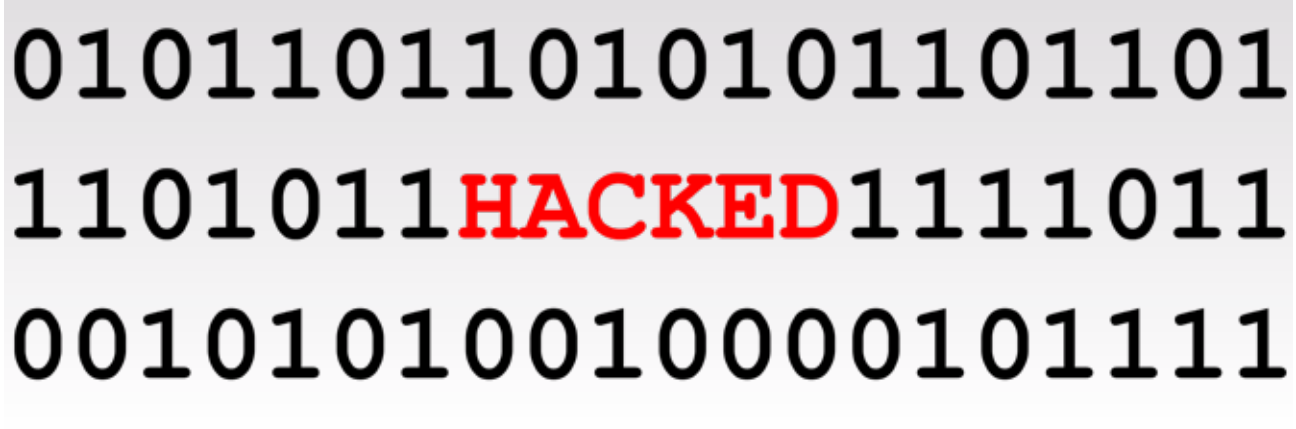

Image by Gerd Altmann from Pixabay

start swapping users onto unaffected machines. Your standard migration efforts kick in where you may do a combination of hosting onsite classroom migrations for users to come in and return their old computer and receive a new one, and ship computers to remote users with a return label in the box for the user to ship the affected equipment back. Every computer that gets returned gets reimaged and turned around to the next user until all users are operational with a safe computer.

Conscript staff from partner teams and other departments to staff up the effort to image endpoints, host classrooms to swap endpoints in bulk, and ship endpoints to remote users, working in shifts if necessary. Emergency processes shouldn't cut corners; make sure tickets are entered to assign equipment to the right user to maintain the integrity of the ITAM data.

If you're managing your imaging and inventory with a third party, work out the plan for how much reserve stock is needed, SLAs to migrate an affected user base if the worst-case scenario is that all end users in your company are impacted, and how to manage shipping to remote vs onsite users.

Based on the number of impacted endpoints, the amount of stock you have on hand to replace them, and the rate at which you can replace those endpoints, make sure you have a formula for how quickly ITAM can contribute to the Ransomware response plan.

What improvements can ITAM adopt to automate or otherwise speed up the process?

The less dependency you have on your physical onsite network, the less dependency you have on physically replacing the physical endpoints. The ability to conduct a remote wipe and remote reimage could eliminate the need for physical replacements, creating a self-service, in-place solution.

Exceptions to this automation will be whether your endpoint fleet has different technical specs or if you are in the middle of an OS migrations. Not all computers may be able to run the specs of the current image, and that subset may need hands-on attention.

Other solutions that eliminate reliance on the corporate physical endpoint are Virtual Desktop Infrastructure or Desktop as a Service Solution in which end users can securely access virtual desktops from any computer they have at home.

In conclusion

IT Asset Management should play an important role in any company's incident response and Ransomware Response plan. An ITAM practitioner should be well versed in the likely scenarios that Ransomware can present itself and should look for ways to contribute to a response. Knowing your partner teams in software distribution, Information Security, end-user group policies, and the technology and security stack is helpful in efforts to predict likely attack vectors and find ways to respond to and protect against the threat.

In a likely scenario where a Ransomware attack locks users out of their endpoints, knowing how much stock to have on hand in the event of having to replace endpoints and having a well-defined process to manage endpoint replacement in an emergency are key. Ensuring strong endpoint imaging processes, including how to quickly update the gold image and reimage devices are paramount. Finally, ITAM should have an eye to the future for how to reduce the dependency of replacing the physical device through implementation of a cloud-enabled wipe and reimage as the preferred solution.

Supporting material: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

Elise Cocks
Director – IT Asset Management,
Freddie Mac

Elise Cocks is IT Asset and License Management – Director with Freddie Mac. She has more than eight years of ITAM experience and manages a team she has grown in both size and responsibility. She enjoys solving complex challenges across IT and business areas to make ITAM processes and data more consumable and better controlled.