5 White House Recommendations for Modern Data Protection Against Ransomware

Ransomware has hit the headlines in a big way over the past several weeks—causing widespread gas shortages, disrupting meat plant operations, exposing critical police files, and more. And this latest flurry of attacks is just the tip of the iceberg.

According to a report from Group-IB, ransomware attacks surged by 150% in 2020, with the average extortion amount doubling. The uptick in ransomware campaigns has only continued, impacting both the private and public sectors in growing numbers.

In response to these increasing cyber threats, the White House recently raised ransomware to the top of the national security agenda, issuing a bluntly worded warning for American businesses to take urgent security measures to protect against attacks.

The Rise of Ransomware on a Massive Scale

Unfortunately, ransomware attacks aren't just growing in frequency; they're also becoming far more costly and disruptive. In fact, according to Sophos' global survey, "The State of Ransomware 2021," the average

total cost of recovery from a ransomware attack increased from $761,106 in 2020 to $1.85 million in 2021—and these ransoms are continuing to increase. FBI Director Christopher Wray went so far as to compare the string of recent attacks to the challenge posed by the 9/11 terrorist attacks. So, what has changed?

Hackers used to gain access primarily through phishing emails that would deploy malware when an unsuspecting employee clicked on a link. The malware would encrypt company servers, and the decryption key would be offered in exchange for a five- or six-figure ransom. Typically, these threat actors didn't target company information, nor did they know which company they would ultimately target. It was about searching for opportunities to exploit a system.

But the game has shifted, becoming a dangerous threat to businesses' core operations. Today's attacks involve exfiltrating company information, understanding the financial picture, and identifying opportunities to exploit for maximum gain.

Threat actors are often sophisticated criminal organizations that seize sensitive company data and target backup systems before issuing a "pay up or else" ultimatum. The ransom now being demanded is also significantly higher—often tens of millions of dollars.

Ransomware Protection Is a National Security Priority

With ransomware now a national security priority, the US government has begun to implement a range of efforts to counteract attacks, such as developing new policies surrounding ransom payments and holding countries accountable for harboring cybercriminals.

Anne Neuberger, deputy national security adviser for cyber and emerging technology at the White House, believes the executive order will "set the goal, give it a timeline, and then establish the process to work out the details."

Yet, addressing the risk also requires a concerted effort, with businesses sharing the responsibility of thwarting attacks.

5 Steps to Reduce Ransomware Risks

The newly released White House memo outlines five steps that businesses can take now to bolster their defenses in response to the current ransomware threat.

1. Back up your data. Backing up data, system images, and configurations is a fundamental part of protecting yourself against ransomware. Unfortunately, today's sophisticated attacks head straight for backups—compromising everything before taking over production environments. In other words, standard backups aren't enough.

A multilayered defense with a modern approach to backup and restore is essential. Backup data and backup metadata must be protected in an immutable state. By backing up files through frequent snapshots that can't be deleted, encrypted, or modified, organizations gain peace of mind that their data is locked down from malicious attacks. That protected data must also be readily available in a time of need, requiring underlying infrastructure that delivers accessibility and speed. With this level of data protection and restore, businesses can avoid the major organizational, reputational, and financial impacts of a ransomware attack.

It's also essential to understand that there are two critical components associated with backing up data:

- **Proven recoverability:** Organizations must have proven recoverability that goes beyond immutability. While sophisticated attackers can't tamper with an immutable backup, they can delete it if they have the right credentials. A solution like Pure's SafeMode™ snapshots eliminates the ability for the attacker to delete your backups and is essential for recoverability.
- **Ability to recover quickly:** Along with having an immutable recovery point, you also need to be able to recover quickly. As we've seen with recent attacks, organizations have had to pay ransoms in an attempt to speed recovery times because their backup systems were so slow to restore. Therefore, backups and recoverability aren't enough. Speed, like the petabytes of restore per day that you can achieve with solutions like Pure FlashRecover™, Powered by Cohesity® and Rapid Restore are critical to getting key systems up and running faster.

2. Update and patch systems promptly. This includes having visibility into your IT estate and staying on top of the security of operating systems, applications, and firmware—and applying critical patches as needed. A centralized logging platform that logs details about all systems and a patch management system can be beneficial. A risk-based assessment strategy that supports your patch management program and an effective security analytics program to identify anomalies in your environment are also key.

A solution like Pure FlashBlade® gives you the ability to log all your systems via a platform like Splunk or Elastic. It provides the critical, high-speed analytics processing required to help identify attackers in your environment, hopefully before they launch their attack.

3. Create and test your incident response plan. Testing is a critical component of reducing ransomware risk. Along with creating an incident response plan, consider the infrastructure necessary to support it. Today's best plans are highly focused on prevention with the solutions in place to catch issues before they occur. Testing your response plan must include testing the supporting infrastructure, as well as all components of the process. Just table-topping and testing the process isn't enough as it won't identify the real gaps that likely exist in the restoration capabilities.

Failing over between sites is also a critical component of testing. Organizations should ensure their storage solutions have the ability to fail over seamlessly—and with little to no data loss. Solutions like Pure ActiveCluster™ offer a true zero RPO/RTO. This means true, instantaneous failover with no manual intervention. In addition, solutions like Pure ActiveDR™ offer a near-zero RTO/RPO with the click of a button. Such solutions can also aid in disaster recovery testing by allowing you to test failover capabilities and then fail back with no user intervention. This is a huge benefit, especially to large and/or geographically dispersed organizations.

4. Check your security team's work. You'll want to double down on testing your internal security and ability to ward off an attack. A third-party penetration testing service is well worth the investment. Then, prioritize and address any identified vulnerabilities. Bug bounties can also be a valuable option that allows you to get a more "real world" look into how vulnerable your organization is from the eyes of real, external attackers. Often, penetration testers take a fairly siloed approach to testing. They have a one-size-fits-all assessment methodology and tooling, which ultimately limits the outcomes that are available. Bug bounty programs, on the other hand, have no such guardrails and give full "creative freedom" to the attackers to find vulnerabilities that allow access into your environment.

5. Segment your networks. With cybercriminals more focused on disrupting operations than just stealing data, it has become vitally important to separate corporate business functions from manufacturing/production operations. Carefully filter and limit internet access to operational networks,

identify links between these networks, and develop workarounds or manual controls to ensure ICS networks can be isolated and continue operating if your corporate network is compromised.

Keep in mind that the whole premise of segmentation is to ensure a degree of recoverability by limiting an attacker's ability to destroy systems. Segmentation is both expensive and time-consuming. It requires continual care and feeding and resources to manage. SafeMode offers the same technical result, without the overhead and complexity of virtual networking. SafeMode also creates out-of-band, multifactor-authentication-protected backup snapshots that can't be deleted, even by an attacker who holds administrative credentials.

Along with these best practices, the executive order also recommends that businesses immediately implement the following common sense, security practices:

- Enable multifactor authentication.
- Deploy an endpoint detection and response system.
- Encrypt all data, at rest and in use.
- Develop or seek a skilled, empowered security team.

Corporate Boards Also Play a Role in Data Security Oversight

Along with the White House, the US Federal Trade Commission (FTC) has also sounded the alarm on increased security threats to data. Stressing the need for corporate boards to prioritize data security and ensure consumer and employee data is protected, the FTC encourages companies to:

- **Build a team of stakeholders from across your organization.** A sound data security program includes stakeholders from business, legal, and technology departments, including both high-level and operational experts.
- **Establish board-level oversight.** Cyber risks should be prioritized within the boardroom and not simply delegated to an audit committee. Board-level oversight can ensure cybersecurity threats, defenses, and responses have the attention of senior management and get the necessary resources.
- **Hold regular security briefings.** Cybersecurity is not a one-and-done project. It requires board members to be informed, engaged, and updated. With regular briefings, boards can effectively manage their oversight responsibility, as well as understand the security landscape and prioritize threats to the company.
- **Don't confuse legal compliance with security.** A common misconception is that compliance translates into good security. It doesn't. Because cybersecurity threats are rapidly evolving, boards should ensure that their security programs are aligned to their unique needs, priorities, technology, and data—and not just geared toward meeting compliance obligations and requirements.

It's All About Protection, Detection, and Rapid Recovery

No business wants to experience the disruption of a ransomware attack or pay a costly ransom. Perhaps, now more than ever, it's essential to build cyber resiliency with modern data protection that guards your data from becoming a target, provides early detection, and reduces downtime.

Pure places a unique and focused emphasis on the security of data with solutions like SafeMode, ActiveCluster, ActiveDR, Rapid Restore, and FlashRecover. We don't just help organizations meet the guidance outlined above—we help them exceed it considerably. While the White House guidance offers some very practical advice, it misses on the critical aspect of recovery.

How many backups exist or how fast they can be taken isn't all that important. When systems go down, what really matters is how fast you can bring your business back online. An appropriate data protection architecture with a data bunker for long-term retention and recoverability must be designed and implemented to enable a rapid restore that ensures both recoverability and speed.

During the last year, we learned that there's no such thing as business as usual. Today it's about planning for the unusual, the unexpected, and being alert to what can happen when we relax and assume it's someone else's job to watch the network. When it comes to security, everyone, at every level, has a role to play. And for this level of attention, having the right technology and partner is key.

Contact the team at Pure Storage® to learn how we're helping companies reduce their risk of ransomware attacks with a multilevel approach to ransomware mitigation, network security, and complete data recovery.