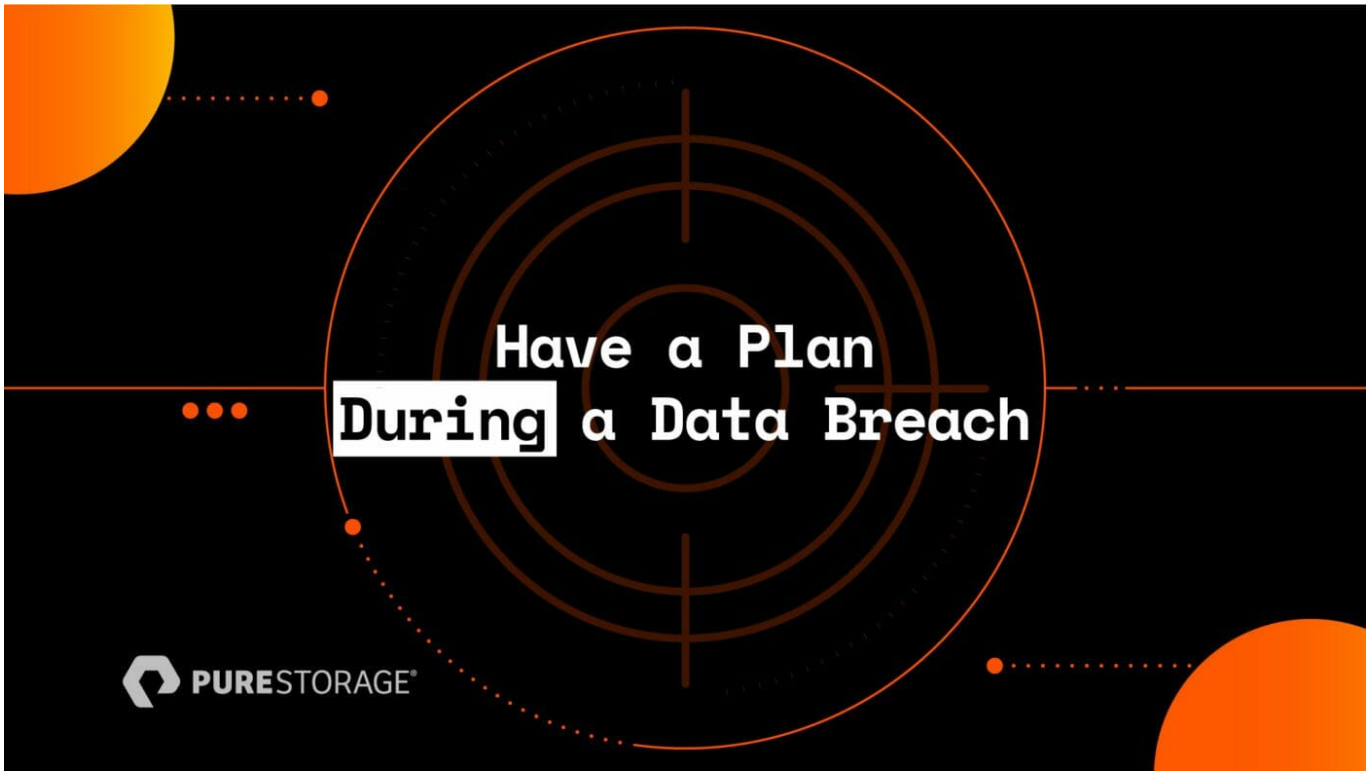
A 5-Point Plan for the “During” of a Data Breach



In this article, I’ll cover what to do **during a ransomware attack** and discuss what critical decisions you’ll be faced with, whom you should reach out to first, and other key steps to take to minimize damage.

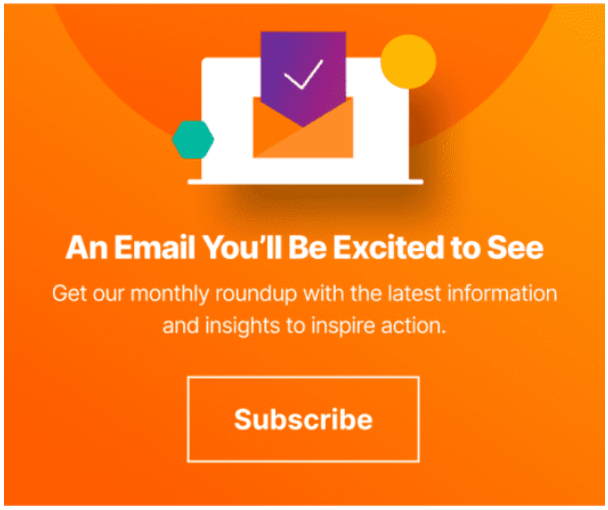
What’s Happening During a Ransomware Attack?

In a previous article, I walked you through what could be happening before an attack. Now, let’s look at what happens when the alarm bells have sounded and you’re suffering an attack or a breach. So, what exactly is going on at this phase?

- After launching a campaign or “dwelling” in your environment, attackers have launched their campaign. Sensitive files may be exfiltrated for use in a secondary attack if the encryption campaign is unsuccessful or in an attempt to make more money.
- Attackers may use exploit toolkits to gain elevated access (i.e., admin access) to your environment.
- Once in your environment, attackers will identify key systems, including critical infrastructures like Active Directory, DNS, backup, and primary storage systems.
- Attackers may change credentials to lock you out of systems.
- Attackers may target backups first for deletion or corruption. They might also encrypt front-end backup servers to render catalogs useless.
- Then, attackers could target and encrypt primary user data files on host systems.

6 Key Aspects of Response and Recovery During Ransomware

Knowing what ransomware attackers or hackers are up to is the first step. Now it's time to swing into action. Your exact disaster recovery plan will depend on your business and the breach, but this guide from the FTC is a great place to start. There are also security breach notification laws in the United States you'll need to adhere to. If you haven't prepared for these things yet, check out this guide to help you kick off some crucial conversations with your CISO.



Here are six steps to take during an attack to help minimize damage and speed up recovery.

1. Contain the attack and lock down your environment.

At the first sign of a breach, isolate impacted systems on the network by disconnecting them completely or quarantining them in a private network enclave. This will help stop the spread and minimize damage.

Never fully shut down systems or turn off the power—doing so greatly reduces or eliminates the ability to forensically analyze those devices later. Update credentials and passwords on clean machines. If any information was posted on your site, remove it and contact search engines to clear the cache

2. Execute your backup communications plan if email systems are down and mobilize your emergency response team.

In my article "5 Questions to Ask Your CISO," question #4 is "If we are under attack, how will we communicate?" You should have already nailed down a well-defined communications plan, and now is the time to use it. Inform leaders and internal stakeholders about the attack, whether it's via mobile phone or an alternate email address. Get IT and security teams, senior leaders, and outside security consultants on the horn ASAP—we'll cover more on that below.

Next, you need to mobilize your emergency response team.

Your emergency response team should have been assembled with some key players. Depending on your company, this could include forensics experts, legal counsel, InfoSec, IT, investor relations, corporate communications, and management. Everyone on the team should have clear marching orders, as should others involved in recovery. In our "Hacker's Guide to Ransomware Mitigation and Recovery" e-book,

former hacker Hector Monsegur notes that this is especially important, “otherwise, network and systems administrators are left using their own judgment to neutralize the threat, which in my experience is usually ineffective or even disastrous,” he says.

3. Launch your external communications plan.

Get in touch with critical partners and authorities. Engage external tech partners to help (that includes your storage provider and any other vendors). If you’re working with the media, regulators, and legal teams after an attack, it’s helpful to maintain an updated list of contacts within local offices of law enforcement authorities such as the FBI in the United States. Contact your cyber insurance providers who can explain coverages and limitations. Contact local authorities and the FBI, if necessary, and be sure to mention any compliance obligations and potential penalties.

You’ll also want to launch your plan to notify affected customers and businesses. You might have drafted a notice and letter that help you frame up the information you’re obligated to share, recommendations for those affected, and a clear statement of what you plan to do next.

4. Begin the forensic process.

Monsegur says, “Assuming that you have all the proper network monitoring tools in place, such as SEIMs and logs, a well-trained staff looking for anomalies and events will be able to identify an attack in action.” Security and access logs can help you identify the source of an attack fast. These logs can also provide the required proof of compliance to regulatory agencies, so you’ll want to make sure they’re adequately protected and secure from deletion.

Triage impacted devices and prioritize them for forensic review. Your security team should determine what type of attack was launched and the breadth to which it’s impacting your environment. The sooner this happens, the sooner your team can apply patches and also restore a clean backup. Once you have that, you can begin the restoration process into a staged environment.

Tip: “Prepare your environment for investigations down the line with your vendors or law enforcement,” advises Monsegur. “If you’ve brought in a company to do an investigation, make sure there’s a handoff between them and law enforcement.”

5. Move to your staged recovery environment.

It’s time to begin your actual physical recovery. As part of your disaster recovery plan, you’ll want to have a recovery environment that has been staged and tested and is ready to go, giving you a “prebuilt” way to get back online right after an event. This includes having a line of sight to new hardware and systems, as there’s no guarantee you’ll be able to use your existing kit or hardware, which could be taken by authorities or investigators as evidence or might need to be quarantined.

Having clean hardware, like the clean storage environment shipped to you next business day with Pure Storage’s new Ransomware Recovery SLA in Evergreen//One, can get you quickly back on track, not just a temporary fix.

With SafeModeTM snapshots, you’ll also be able to start recovering right away with immutable backups of your data. During an event, this feature is particularly important because attackers won’t be able to hinder your ability to get back online quickly.

Stay Ready: Adopt STaaS with a provider that has a recovery SLA

This, of course, needs to happen *before* the data breach but greatly affects the *during* as it will help you recover much more quickly. With data storage as a service (STaaS), you can have the flexibility and cost-effectiveness you need to make the most of your data storage, which translates directly to operational agility and the mitigation of IT risk.

Pure's Evergreen//One™ combines the agility and flexibility of public cloud storage with the security and performance of an all-flash infrastructure. This SLA-driven storage service will improve how you store, mobilize, and protect your data.

The ransomware recovery SLA is key, as it ensures you're back up and running without damaging your business. Our new ransomware recovery SLA mitigates the impact of a ransomware event and protects your data with speed, simplicity, and security at scale.

Our new recovery SLA offers:

- Next business day shipping of recovery array(s) (48-hours to AsiaPacific)
- Expedited shipping (varies by region)
- 48 hours to complete your recovery plan
- 8 TiB/hour data transfer rate
- Onsite professional services from time of array arrival to through RMA of infected array

Be Ready for Recovery with Pure

Knowing the challenges you'll face first and the immediate steps you can take during ransomware attacks can help minimize loss, cost, and risk. Pure Storage® can help you take swift action at the "during" stage by:

- Providing always-on, data at rest encryption, with no performance overhead or management required
- Eliminating the ability for protected data to be modified or deleted, thus ensuring recoverability

***Revisit part one in this series for the "before" of an attack*, and stay tuned for part three, where I'll go into the actions you can take after an attack.**

Like this article and want to read more? **Sign up for our monthly Perspectives email today. And we promise not to spam you, just inform and inspire you!**

Post Likes 2

Color orange–gradient

Color orange–gradient

Color orange–gradient

Color orange–gradient

Color orange–gradient