

When Ransomware Strikes: 7 Steps You Can Take

Now to Prepare

Ransomware is still on the rise. These operational tips can help lessen the blow if you're hit.

If you walked into work tomorrow to find your company had been hit by ransomware, would you know what to do? Who would you call? How would you find their phone numbers if your computer was locked up? How would you notify customers?

There are many aspects to preparing for ransomware, including technical tips such as maintaining a current, offline backup of your data. This article isn't about those technical steps. It's about the practical, operational measures you can take now to prepare yourself and your company for the moments after an incident occurs. What's your emergency plan? Who would you want on your team? How would you communicate?

Few of us are good at preparing for the unexpected, but planning ahead will make life a lot easier if disaster strikes. And when it comes to ransomware, there's a good possibility it will. After the WannaCry attack in May, which infected some **300,000 computers** in the first few days, the head of the FBI's Cyber Division called ransomware "a **prevalent, increasing threat**," and said attacks are likely to rise in future. **Other reports** also predict an increase.

With that in mind, here are seven steps you can take now to prepare yourself and your company for the moments after ransomware strikes. Some of these can be applied broadly to other critical incidents, while some are ransomware-specific.

1. Plan your initial response. Your team members may not be used to dealing with stressful situations, so make sure they know what to do. This includes where they'll gather to discuss the problem, where press inquiries should be directed, and what to tell customers and staff. Most of the time, this means planning the who, what, when, and how. Once you have this plan, share it with your team ahead of time, and...

2. Store your response plan in multiple locations. If your plan for incident response is stored on your PC and you're locked out, you can't even get started on your recovery. Ransomware can affect your desktop, your servers, or both. Store copies of your plan in multiple locations, including at least three separate cloud services. And set a calendar alert to remind yourself to update them periodically.

3. Pick your team now. Who needs to be in the room in the moments after an incident occurs? Your CEO and CIO are a given, but you may also want your heads of PR, legal, HR, and other department chiefs. Draw up a list now and make sure everyone knows they're on it. Also, get their contact details for off-work hours, and share them with the rest of your team.

4. Have a communications plan in place. You may find yourself locked out of your primary, preferred method of communication, so know which channels you'll fall back on. Email might not be an option, so prepare to use other means. If your smartphones are still working, collaboration apps can be a good way to communicate as a group — just make sure everyone has the app installed. But ransomware can [also strike mobile devices](#), so as with all aspects of preparedness, have a backup. Storing phone numbers and personal email addresses in multiple locations is a good place to start.

5. Decide now who'll take charge. There's a lot to do in the moments after an attack, including directing employees and contacting law enforcement, customers, and partners. Someone will need to oversee and manage the recovery effort and be ready to answer questions as they arise. It could be your CIO, COO, head of security, or someone else — but it's best to have a clear, single owner. Decide now who that will be, so the responsibility doesn't suddenly get dropped in their lap that morning.

6. Have a discussion now about how you'll respond. Whether you decide to pay the ransom will likely depend on the severity and nature of the incident, but it's better to begin this conversation now than in the heat of the moment. The FBI has said it [doesn't condone payment](#) because it wants to discourage future attacks, but it also recognizes that every business will need to make its own decision. It can't hurt to start talking about this now, so your team is at least familiar with the trade-offs when a decision has to be made.

7. Know your appetite for risk. You can't plan for everything, so figure out how much you risk you can tolerate — and how much potential harm you can deal with — and then make a trade-off. For example, some companies will do a disaster recovery exercise every month, to be sure they're always prepared. But that's a big time commitment, and others will opt for once a quarter. It all depends how much "insurance" you want built into the system. These are tough calls, but they need to be made deliberately and in advance.

If you're lucky, you'll never have to face a ransomware incident, but luck isn't how you run a business. Your technical teams will have put in a lot of work guarding against attacks and mitigating damage. But responding operationally, informing customers, and keeping the company moving forward falls to management. It's often hard to imagine a situation you've never been in, but try to picture that morning when your phone rings and you learn your company has been hit. Think about all the things you'll wish you'd have done — and start doing them now.

https://www.darkreading.com/author-bio.asp?author_id=4842

Profile of Patrick Hill

Atlassian SRE Solutions Lead News & Commentary Posts: 1

Patrick Hill is SRE Solutions Lead at Atlassian, a provider of team collaboration and productivity software that helps teams organize, discuss, and complete shared work. Teams at more than 100,000 organizations use Atlassian products including JIRA, Confluence, HipChat, Trello, and Bitbucket. Based in Austin, Texas, Hill helps build teams and processes to ensure consistently high performance and availability of Atlassian's internal and external cloud services.

<https://www.darkreading.com/endpoint/when-ransomware-strikes-7-steps-you-can-take-now-to-prepare-/a/d-id/1330313?>

11/6/2017

03:30 PM



Patrick Hill