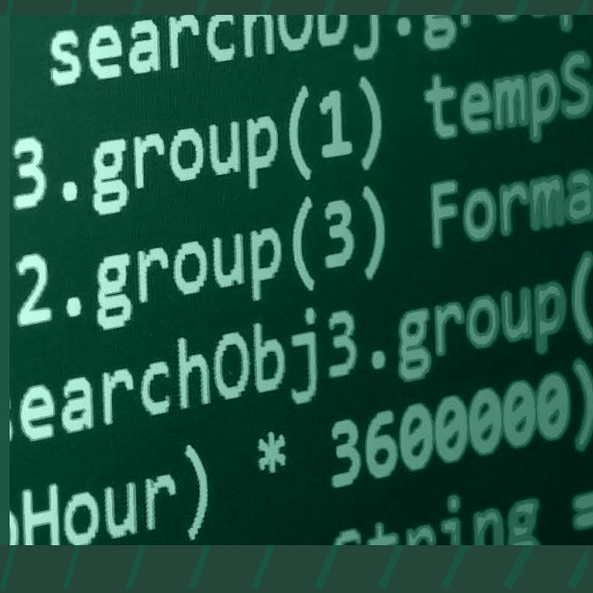
DELL Technologies

5 Recommendations for Surviving a Ransomware Attack



1 Maintain a comprehensive incident response plan

- Focus on minimizing the impact of an attack
- Practice, test, and update often
- Have an incident response team ready ahead of time
- Consider cyber insurance as a part of your overall resilience strategy
- Include plans to work with law enforcement

2 Have a clear communication strategy in place

- Create communication templates in advance
- Ensure timely and clear communications inside the organization
- Be prepared to communicate externally, if applicable
- Adhere to applicable notification regulations

3 Ensure robust data protection

- Safeguard critical data in an isolated, immutable, air-gapped data vault
- Prioritize recovery by service / infrastructure
- Practice recoverability
- Pair capabilities like clean room to your recovery time objective
- Ensure the integrity of recoverable data

4 Don't assume an immediate return to normalcy

- Paying ransom should be a last resort
- Ensure compliance to legal and regulatory requirementsbefore paying
- No guarantee that the hacker will return your data even if ransom is paid

5 Emphasize training and education

- Conduct attack simulations
- Monitor and test employees' security hygiene practices
- Use tools like phishing tests and email security training

It’s no longer a question of “if”—but “when.”

Enterprises must plan as if an attack is inevitable, despite their best defenses.To discuss what to do when disaster strikes, Dell subject matter experts Jim Shook, Global Director of Cybersecurity and Compliance Practice, and Steven Granat, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, sat down with Brian White, Senior Consultant, Product Marketing, for Dell Data Protection.

> You need to bring the right people in and conduct a drill and simulate actions so when an attack does happen, everybody immediately knows what they’re doing.”
>
> ***Steven Granat**, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, Dell Technologies*

Maintain a comprehensive incident response plan

When an attack occurs, all key stakeholders – pretty much everyone in the organization and third parties like suppliers as well – must know what to do. A written incident response plan should outline a clear sequence of action, Shook advises. A comprehensive plan will address technological, process, and communication steps from immediate action all the way through recovery. Make sure to maintain a written paper document as well, as digital modes of communication might be non-operational. “You need a plan that you can literally go to the shelf and pull down,” Granat says.

Have a clear communications strategy

Most organizations will need to communicate to key stakeholders, and in many cases will need to comply with regulatory requirements. Create different templates for both internal and external communications with systematic instructions for whom to notify in what sequence—and when. Plan for phone and email systems being down.

Implement a robust data protection strategy

A key goal of making it through a ransomware attack is to restore the data and recover as painlessly as possible, while also avoiding paying the ransom. A strong data protection strategy is a key part of achieving those goals, but will need to comprise both technology and processes. “Use immutable data and cyber vaults to store enough data that you can trust or at least as validation points that will enable you to recover systems,” Shook advises. Ensuring that the data is protected is the first step; you must also have the people and processes in place to recover it. Third party experts can assist, but they should be brought in at the planning stage.

Don’t assume an immediate return to normalcy – even if you pay ransom

Payment of a ransom, which should only be considered as a last resort, does not guarantee the switch will be turned back on right away. Remember that you’re negotiating with a criminal, and even if you do get the decoder keys, you need a strategy in place for newly recovered data. To start with, you must test decrypted data and rebuild all systems methodically. Repeating meticulous attention to what-if events before an attack even takes place will go a long way to achieving resilience. “Understanding the different applications and dependencies in your tech infrastructure is critical to an efficient return to steady state. ‘Do I have a viable recovery source and a recoverable target?’ ‘Do I have data that’s free from compromise?’ These are important considerations to think about,” Granat says.

In the recovery phase, you also need to ensure the adversary has actually left your systems. “You need to make sure that the fire is out in your house and also find out what started that fire in the first place because without these two critical pieces of information, you’re leaving yourself vulnerable for future attacks,” Shook says.

Training and practice are critical

An important part of cyber resilience is comprehensive training, that ranges from ensuring that employees practice strong cybersecurity hygiene all the way to routinely practicing the recovery plan. “You need to bring the right people in and conduct a drill and simulate actions so when an attack does happen, everybody immediately knows what they’re doing,” Shook says.

Ransomware may be inevitable in today’s threat landscape, but through planning and execution you can minimize the operational, financial, and reputational impact. The goal is to get back to normal as quickly and painlessly as possible.

Learn how to address some of today's top cybersecurity challenges at **dell.com/cybersecuritymonth**

DELL Technologies