NORMAN HANSON DETROY

Portland Office: (207) 774-7000
Lewiston Office: (207) 777-5200

Experienced. Efficient. Effective.

Ransomware: How to React When Prevention Fails

A variant of “Petya” is just the latest massive ransomware cyberattack currently crippling businesses and government offices across Europe and the United States. The particular focus on the Ukraine again points to Russia as the likely source, but the true identity of the actors is still unknown.

The increased sophistication and frequency of these threats are a timely reminder that a well-thought-out response plan can help minimize damage and preserve companies’ reputations. Here are key steps to consider when it’s too late for stress tests, policy reviews and software patches, and all other preventive measures have failed:

Immediate Action

1. **Implement**. Implement the company security incident response and business continuity plan, making sure that individuals in decision making authority chain are available and kept updated.
2. **Quarantine.** Isolate the infected computer or systems as soon as ransomware is detected to prevent it from attacking network or share drives.
3. **Secure Backup Data**. Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
4. **Secure Unencrypted Data**. Secure any partial portions of the ransomed data that might exist.
5. **Reset Passwords**. Change account and network passwords after the corrupted system has been isolated from the network. Remember to also change system passwords once the malware is removed from the system.
6. **Stop the Loading; Assess**. Registry values and files should be deleted to stop the program from loading. determine which stakeholders and interests could be implicated, and evaluate the prospects for quick remediation.
7. **Insurance**. Identify any potentially responsive insurance coverages for carrier notification.
8. **Report**. Contact law enforcement. In the United States, the recommended contact is the local Federal Bureau of Investigation (FBI) or U.S. Secret Service field office.

To Pay or Not to Pay.

The decision of whether or not to pay the ransom is a decision fraught with its own risks that require evaluation of all realistic options to protect shareholders, employees, and customers.

Generally speaking, our advice is not to pay the ransom, but victims will want to evaluate a number of factors, including the technical feasibility, timeliness, and cost of restarting systems from backup, the possibility of preventing sensitive company and customer data from being being further compromised, and the ability to tell customers that the company did attempt to protect their data by paying the ransom.

If you are a ransomware victim, you’ll want to also consider the following factors:

- First and foremost: Paying a ransom does not guarantee that you will regain access to your data. Many victims are never provided with decryption keys after paying a ransom for the simple reason that once the

payment has been received there's little incentive to release the keys.
- Others are subject to additional payment demands during the same ransomware event once they've shown themselves willing to pay.
- By paying, you may be making yourself more of a target for cyber criminals.
- Although many ransomware events appear to be state or quasi-state action that are designed more to disrupt than to extort money, payment nonetheless encourages this criminal activity.
- If you do decide to pay, consider acceptable payment methods (i.e., paying through bitcoin and not through credit cards). In no event should payment come from an existing financial institution or bitcoin account.

Prevention and avoidance are still the best way to avoid the risks and costs of a malware intrusion, but a response plan has to be part of every company's cyberattack response toolbox.