McDonald Hopkins Attorney **Insight.** Business **Foresight**®

Businesses urged to take action to protect against the growing threat of ransomware

Alexander Misakian, Dominic A. Paluzzi, James J. Giszczak | Friday, June 4, 2021

In light of a growing number of large scale ransomware incidents that have severely impacted large business operations in the United States, the White House released a memorandum on June 2 providing guidance for corporate executives and business leaders to take certain actions to protect against the threat of ransomware. Private companies are encouraged to:

1. **Implement best practices from President Joe Biden’s Executive Order.** President Biden’s Executive Order recommends the following best practices:
    - **Employ a skilled, empowered security team** – Able to respond appropriately to constantly evolving threats and vulnerabilities, and empowered to approach and guide the business to adopt necessary policies and technologies.
    - **Adopt encryption technologies** – Protects sensitive information while it is in transit or while it is at rest in your system or in an email account and prevents a bad actor from viewing it even if stolen.
    - **Utilize endpoint detection & response software** – Identifies cyber threats and intrusions in real time, allowing your team to immediately respond to an incident.
    - **Adopt multifactor authentication** – Prevents a bad actor from accessing your network or account using only compromised credentials. Even complex passwords alone are routinely compromised.

2. **Back up data offline, and regularly test backups.** In the last few years, threat actors have not only been encrypting systems but seeking out and encrypting or destroying backups as well. The best

defense for this situation is to consistently back up your systems and store those backups in an offline location. Crucially, your team should regularly test those backups to ensure that they are good and able to be used for restoration after a cybersecurity incident.

3. **Update and patch systems promptly.** Many recent cybersecurity incidents have been the result of a system or software vulnerability that had a patch or update available. Continue to adopt updates or patches to protect against existing weaknesses that make your business susceptible to attack.

4. **Test your incident response plan.** To quote Benjamin Franklin, "by failing to prepare, you are preparing to fail." Businesses without an incident response plan fare much worse and amass greater costs than those that do. Your incident response plan should not be a dead document, but should be constantly evolving and regularly practiced in different scenarios with your incident response team. McDonald Hopkins can help your team draft and adopt an incident response plan, and provide tabletop exercises that will guide you through your plan.
5. **Check your security team's work.** We recommend that your company engages an independent third party provider to test your systems and identify any vulnerabilities that could make your network susceptible to attack.

6. **Segment your networks.** By keeping your networks separate, you will isolate any system compromise and limit the amount of damage in the event of a cybersecurity incident. Critically, by minimizing and segmenting your data, you will also limit sensitive or personal information exposed during an incident.

The McDonald Hopkins incident response team has seen a surge in ransomware incidents in recent weeks, and urge all clients and businesses to immediately take action in the form of the recommendations above. Each of the above actions will significantly reduce costs related to a data security incident, and will limit downtime for business operations following an incident .

If you need assistance implementing any of the above recommendations, drafting or testing your incident response plan, or responding to a cybersecurity incident, the McDonald Hopkins Data Privacy and Cybersecurity team is available 24/7 to help.

Alexander Misakian

Dominic A. Paluzzi

James J. Giszczak