CYBER UPDATE

NPIA, INC.
Insurance & Program Administration

White House Issues Ransomware Prevention Guidance to Businesses

In a recent letter addressed to corporate executives and business leaders, the White House emphasized that bolstering the nation's resilience against cyberattacks is a main priority for President Joe Biden's administration. Specifically, as ransomware attacks continue to rise in both cost and frequency throughout the country, the federal government is urging businesses to take this evolving cyber threat seriously.

These attacks—which entail a cybercriminal deploying malicious software to compromise a business's network or sensitive data and demand a large payment be made before restoring this technology or information—have quickly become a growing concern across industry lines. In fact, the latest research provides that ransomware attacks have increased by nearly 150% in the past year alone, with the median ransom payment demand totaling $178,000 and the average overall loss from such an attack exceeding $1 million.

While the White House has begun working with both domestic and international partners on various strategies to prevent ransomware attacks, the Biden administration is also encouraging businesses to play their part in minimizing this rising cyber concern. Rather than viewing ransomware attacks as a minor cyber risk, the federal government is instructing businesses to view these attacks as a significant exposure—one with the potential to wreak havoc on their key operations.

As such, the Biden administration is recommending that businesses convene with their senior leadership teams to review their ransomware exposures and implement these top cybersecurity measures:

- **Utilize the federal government's best practices.** Businesses should be sure to incorporate the best practices outlined in the Biden administration's Executive Order on Improving the Nation's Cybersecurity. This includes the following practices:
    - Implementing multifactor authentication on all workplace technology
    - Leveraging endpoint detection and response tools to identify and deter suspicious network activity
    - Encrypting sensitive data to make it less accessible to cybercriminals
    - Developing a trusted and skilled workplace cybersecurity team
- **Conduct frequent data backups.** In addition to the federal government's best practices, businesses should also prioritize securely backing up all sensitive data, images and other important files on a regular basis. Conducting such backups can help businesses remain operational and continue to access crucial data in the event that any workplace technology is compromised in a ransomware attack. Data backups should remain offline (not connected to key business networks) and be routinely tested.

- **Maintain updated security software.** To help safeguard workplace technology from ransomware threats, businesses should equip their systems and devices with adequate security software—such as antivirus programs, firmware protections and firewalls. Further, this software must be regularly updated to remain effective. That being said, businesses should also consider utilizing centralized patch management systems to keep security software on a consistent update schedule.

- **Ensure an effective incident response plan.** All businesses should have cyber incident response plans in place. These plans outline proper response protocols and offer steps for minimizing potential damages during cyberattacks. Businesses should make sure to include several ransomware attack scenarios within their response plans and routinely test these scenarios with their cybersecurity teams. Based on test results, businesses should revise their response plans accordingly.

- **Review workplace cybersecurity protocols.** Apart from testing their response plans, businesses should also regularly assess whether their existing workplace cybersecurity policies, procedures and software are sufficient in protecting against current risks—such as ransomware threats. In particular, businesses should consider using a third-party penetration tester to review their ransomware defense tactics and overall cybersecurity capabilities. Businesses should work with their trusted cybersecurity teams and IT experts to make workplace adjustments as needed (e.g., updating policies or purchasing new security software).

- **Keep critical networks separated.** In order to keep ransomware attacks from fully disrupting their operations, businesses should attempt to segment their various workplace networks (e.g., sales, production and corporate) from one another rather than having a unified network. Access to each network should be restricted to those who use them to conduct their job tasks. Networks should only allow internet access as needed. That way, businesses can avoid becoming completely compromised by single-network ransomware attacks and continue performing critical functions.

For additional risk management guidance and insurance solutions, contact us today.