O'HAGAN MEYER

RAPID RESPONSE & INCIDENT MANAGEMENT

Best Practices to Prevent & Respond to Ransomware Attacks

Ransomware and data theft extortion remain a harrowing and ever-threat. Ensuring that all steps are taken so that your business is not completely "locked down" with no functionality of your company's computer system is key to very continuity of the business. Further, protecting stored data or data in transit from theft and the threat of public disclosure is not only important from a liability risk standpoint, but also from a business reputation standpoint. Here are some "best practice" tips and strategies to not only prevent these issues from occurring, but to minimize and mitigate the impact in the event of a compromise.

Ongoing Employee Training: Your employees are your first line of defense to protect your business from cyber-attacks. At least annual cybersecurity training should be required for every member of your workforce. Completion of this training should be documented. Supplemental training and as-needed updates regarding specific cyber threats should be provided. Regular training will not only help your workforce identify common threats but ensure that your workforce appreciates the importance of cyber security. O'Hagan Meyer attorneys can assist in providing this training upon request.

Segmented and Offline Backups: Backups must be kept segmented and offline. Threat actors routinely attempt to find and delete or encrypt backup data. Having an offline or segmented backup will allow you to restore your data without making a ransom payment and will avoid extended period of downtime in the event of an attack. Backups should also be tested regularly, and you must verify that backups are not corrupted before restoration.

Segment Your Network and Limit Access: Network segmentation divides your network, and the applicable data, into smaller parts. Network segmentation isolates any network intrusion and limits the damage from any ransomware attack. Access should also be limited on an "as-needed" basis. If a particular user does not need access to part of your network to perform their job, then access to that part of the network should not be granted.

Patch Regularly: Vulnerabilities in software and firmware from outside sources are a constate area of concerns. Your organization should monitor for information regarding needed "patches" to eliminate those vulnerabilities and regularly apply patches and software updates. Applying patches and software updates will close security gaps and keep your system security.

O'HAGAN MEYER

RAPID RESPONSE & INCIDENT MANAGEMENT

Implement Multifactor Authentication: Multifactor authentication should be implemented for access to all information, systems, and devices. Passwords alone are not sufficient to protect your network. A second form of verification, such as a PIN or an authentication application should also be required.

Proper IT Security: Your organization should use available anti-virus software, firewall and endpoint protection to secure your network. These security solutions prevent unauthorized traffic, blocks viruses and malware and protects the various devices on the network. Use of each type of security solution listed is recommended.

Create and Use an Incident Response Plan: It is important to have a written incident response plan ("IRP") in place addressing how your organization will respond to a ransomware attack. The IRP should identify the key members of your organization, along with outside vendors, that will be involved in the incident response, and the various steps that will be part of the incident response. One of the first steps should be contacting your cyber insurance carrier. Your organization should regularly practice its incident response through tabletop exercises. Once you have determined that you are experiencing a ransomware attack, the IRP should be activated. Do not try to rush the response by not following the plan. Organizations often create larger problems by rushing their response, such as by restoring from corrupted backups or by contacting the threat actor without first researching the attack and developing a negotiation strategy. O'Hagan Meyer attorneys can assist in creating an IRP and with pre-breach practice.

Create a Business Continuity Plan: Along with your IRP, your business should create a business continuity plan to consider how your business will operate if you do not have access to your computer network and/or data. Following the onset of an attack, it can be weeks before full access is restored. To minimize damage, it is important that your business returns to full operation as soon as possible. Devising a business continuity strategy will allow your business to continue operations, and let you focus on investigating and remediating the attack.