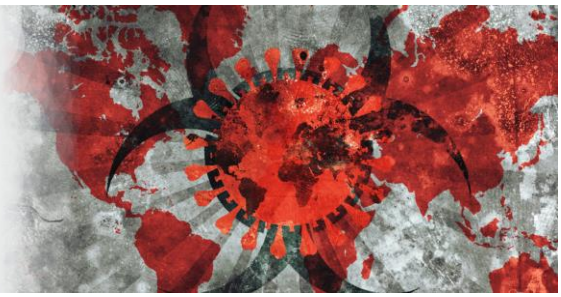
THOMPSON HINE



COVID-19 Update

March 2020

Review Teleworking Cybersecurity Policies and Practices

Key Notes:

- The increase in teleworking during the COVID-19 crisis creates unique data and infrastructure security challenges that organizations must address.
- New teleworking arrangements or increased volume of telework could also require changes to HIPAA documentation.

In response to concerns about COVID-19, many organizations are requiring their employees, contractors and other business partners to telework and use remote access technologies to perform their daily work or furnish services. While this may be unavoidable given the current health crisis, permitting access to an organization's internal resources from external networks can create risks for the organization's information technology (IT) environment. In fact, the U.S. Department of Homeland Security (DHS) recently issued a Cyber Awareness Alert warning organizations "to adopt a heightened state of cybersecurity" as teleworking increases.

Security Best Practices

When authorizing telework, an organization needs to consider the physical, technical and administrative security of all its remote access solutions and IT assets, including internal and third-party devices, remote access networks and servers, and the internal resources being accessed. DHS and other federal agencies have indicated that organizations should prioritize the following areas to mitigate information security risks in the telework context.

Unsecured networks. Organizations usually lack the ability to secure the external networks used by teleworking employees and vendors, such as broadband and cellular networks, which makes them more susceptible to compromise through eavesdropping and "man-in-the-middle" attacks. According to the National Institute of Standards and Technology (NIST), "[r]isk from use of unsecured networks can be mitigated, but not eliminated, by using encryption technologies to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints." The DHS Cyber Awareness Alert highlights the importance of using virtual private network (VPN) technologies to offer a secure communication tunnel between a teleworker's device and an organization's IT resources. Yet, according to DHS, "[a]s organizations use VPNs for telework, more vulnerabilities are being found and targeted by malicious cyber actors." In response, DHS recommends the following actions:

- Update VPNs, network infrastructure devices and all applicable IT devices with the latest software patches and security configurations.
- Alert employees to potential phishing attempts.
- Ensure IT security personnel are prepared to increase cybersecurity activities, including log review, attack detection, and incident response and recovery.
- Implement multi-factor authentication on all VPN connections to increase security.
- Require that IT security personnel test VPN limitations to prepare for mass usage.

In addition, the organization should remind employees of their data incident notification and response procedures and be on heightened alert to respond to an actual or reasonably suspected security incident as the number of teleworkers continues to increase.

Infected devices. An organization needs to be concerned with devices used for teleworking that are later brought into, and connected directly with, the organization's IT environment. According to NIST, "[a]n attacker with physical access to a client device may install malware on the device to gather data from it and from networks and systems that it connects to." In other words, if a device is infected with malware during its use for teleworking, once the device is connected to the organization's internal environment, the enterprise risk for malware infection increases significantly. To mitigate these threats, an organization should strongly consider employing antivirus and antimalware technologies, using network access control solutions to test the security of a device prior to allowing it to connect to an internal network, and using a separate network for all external client devices.

Physical security. An organization can implement security tools to restrict and monitor employees and guests and their IT assets and infrastructure on its premises. But employees and other third parties who are teleworking use their devices from a broad range of locations outside the organization's control, such as homes, hotels and coffee shops. These devices, whether laptops or phones, are susceptible to being lost or stolen. NIST states that organizations "should assume" that telework-related devices may be stolen by criminals seeking to exploit the data on them or use the devices to gain access to the organization's network. "The primary mitigation strategies for device loss or theft," according to NIST, "are to encrypt the client device's storage or just the sensitive data itself so that it cannot be recovered from the device by unauthorized parties, or to not store sensitive data on client devices."

Remote Access Policy

To avoid legal risk and minimize security concerns, an organization should formally adopt a written telework policy that, among other things:

- designates an internal point of contact for its oversight, management and implementation,
- establishes employee and vendor expectations and responsibilities,
- identifies IT equipment permitted in the telework context,
- incorporates other corporate policies and procedures (e.g., IT acceptable use policy), and
- outlines disciplinary actions for policy violations.

In addition, the policy should address how broadly internal resources are granted to individuals working remotely. According to NIST, "[o]rganizations should ensure that any internal resources they choose to make available through remote access are hardened appropriately against external threats and that access to the resources is limited to the minimum necessary through firewalling and other access control mechanisms." Moreover, when establishing telework and remote access policies, an organization needs to specify which employees must, at all times, have access to its IT infrastructure to perform critical security functions, which is especially important during times of emergency and business continuity.

HIPAA Security

An organization also needs to consider its potential obligations under the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). If an employee working remotely will have access to protected health information, which may occur if the organization is a covered entity or if the employee is working on behalf of the organization's health plan, the organization should revisit and update its HIPAA security risk analysis and policy. It should document any new risks presented by the teleworking arrangement, as well as any steps taken or new policies developed to mitigate those risks. If no changes are needed, the organization should nevertheless document that it performed the analysis.

FOR MORE INFORMATION

For more information, please contact:

Deborah S. Brenneman
513.352.6638
Debbie.Brenneman@ThompsonHine.com

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com

Kim Wilcoxon
513.352.6524
Kim.Wilcoxon@ThompsonHine.com

Julia Ann Love
216.566.5686
Julia.Love@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

or any member of Thompson Hine's Privacy & Cybersecurity, Employee Benefits & Executive Compensation or Labor & Employment practice group.

Additional Resources

We have assembled a firmwide multidisciplinary task force to address clients' business and legal concerns and needs related to the COVID-19 pandemic. Please see our COVID-19 Task Force page for additional information and resources.