CYBERSECURITY LAW ALERT
March 3, 2026

By: Steven J. Kuperschmid, Esq.
Nicole E. Osborne, Esq.
Tyla R. Phillip, Esq.

RMF
RUSKINMOSCOUFALTISCHEK P.C.
Smart Counsel. Straight Talk.

Practical Cybersecurity Measures Amid Heightened Global Risk

Recent geopolitical developments, including escalating global tensions, have increased the risk of cyber threat activity directed at U.S. businesses and institutions. Cyber threat actors, whether they are foreign state-sponsored or domestic criminals, exploit uncertainty and often take time to “study” an organization before they plan an attack. Most often, threat actors are looking for organizations that handle sensitive and valuable data which may include, but are not limited to, professional services firms, financial institutions, healthcare providers, and middle-market companies. This alert outlines practical steps that organizations should consider taking to reduce risk and strengthen their cybersecurity posture.

The first practical way to increase your organization’s cybersecurity is to improve your company’s access controls for both in-person and remote work. This may include implementing multi-factor authentication (MFA) wherever available, particularly for email logins, remote access to servers, cloud services, and financial systems where any sensitive data may be held. A good way to gauge if your organization has some unwanted cyber visitors is investigating unexpected MFA prompts. Companies should also require employees to use unique and strong passwords that are distinct from any other password used by the employee. Another small but highly impactful tip is requiring all employees to change their passwords at least once a quarter, if not more frequently.

Where employees are permitted to work from home, companies must also take important safeguards to protect information accessible to employees remotely. Simple ways to boost cybersecurity for remote workers include requiring a VPN or similar protections and prohibiting the use of public Wi-Fi without appropriate safeguards. Laptops and mobile devices should also be encrypted and protected with strong authentication measures.

Second is educating employees of how threat actors gain access to the system by gaining their trust, usually by a phishing attempt or social engineering. Organizations should remind employees to be extra cautions of emails that: (1) create a sense of urgency or pressure to respond; (2) request login credentials, wire transfers, or other sensitive information; (3) contain unexpected attachments or links; or (4) appear to come from executives, vendors, or clients but contain subtle inconsistencies. It is important that employees are adequately trained to be able to identify and promptly report any suspicious communications sent to them. Businesses should be engaging in regular testing of their employees through the use of mock, but realistic, phishing attempt emails, especially in light of an increase in sophistication and accuracy due to the use of Artificial Intelligence by threat actors.

Third, ensure timely patching and updates. Many successful attacks exploit known vulnerabilities for which patches already exist. To ensure compliance, companies should conduct an internal audit to ensure their network is secure. This may entail confirming that operating systems, servers, applications, and network devices are fully up to date, and applying security patches promptly, particularly for internet-facing systems and remote access tools.

Any internal audit should also remove or isolate unsupported software and legacy systems where possible. For example, backups should be stored in isolated environments away from the primary network. Restoration procedures should also be tested frequently to ensure backups are accessible to keep your business running in case of an emergency.

Fourth is protecting sensitive data in every communication. While this goes without saying, it is nonetheless important to use encryption for data at rest and in transit. Emails that contain highly confidential or sensitive information should also be sent via encrypted email for an added layer of protection. Companies should also only permit employees to access data necessary to perform their roles. This is particularly important as social engineering attempts are often geared at those with the most access, so by limiting the number of employees who have access, you limit the pool of ideal candidates to threat actors.

Fifth is ensuring your business partners are also protected. Many cyber incidents originate through vendors or service providers. Companies should ensure they are adequately vetting any external or third-party vendor they share data with, in any capacity. It is important to ensure that these vendors are also investing in maintaining cybersecurity safeguards. Any contracts with external companies or vendors should appropriately address data protection and incident notification obligations.

Finally, every organization should have a clear plan for responding to cybersecurity incidents. While no company hopes to be involved in a cybersecurity incident, the response is much smoother when there is a clear and accessible plan to look to for next steps. This plan should be memorialized and should identify key personnel within your organization and any external assistance your company may need with respect to a technical response, legal review, and any reporting requirements. Education and training are also key components to incident response. Organizations should ensure decision-makers understand escalation procedures and consider tabletop exercises to test readiness before an actual incident occurs. In the event of any incident, organizations should always contact their own outside counsel first, in an attempt to maintain privilege over the breach investigation.

Periods of global instability often heighten cyber risk, as they tend to create opportunities for malicious actors to exploit uncertainty and gaps in preparedness. The measures outlined above are practical to implement for most organizations and with proper guidance, they can drastically improve your company’s cybersecurity posture. If you need assistance with cybersecurity preparedness, incident response, regulatory considerations, or want to memorialize an incident response plan for your company, please contact:

Nicole E. Osborne, Esq.	**Steven J. Kuperschmid, Esq.**	**Tyla R. Phillip, Esq.**
516.663.6687	**516.663.6686**	**516.663.6503**
nosborne@rmfpc.com	**skuperschmid@rmfpc.com**	**tphillip@rmfpc.com**