COMPLIANCE WEEK

Rewriting the cyber-compliance playbook: Strategies for new era of data theft, economic espionage

By Rod Rosenstein & Sumon Dantiki, CW Guest Columnists

Dynamic cyber-threats, evolving regulatory enforcement, and continuous technological advances portend that every company should expect investigative scrutiny of its technological risk management processes. Implementing technical measures is not enough. Compliance executives must design programs and implement protocols to proactively identify and manage the enterprise risk posed by data theft and economic espionage.

Organizations with valuable intellectual property, sensitive data, and novel technologies face an unprecedented technological risk landscape. Sophisticated hackers, often sponsored by foreign governments, can target any organization. The Cyberspace Solarium Commission warned that "our adversaries have developed new tools that hold data and essential information systems at risk [and] ... enable more sophisticated cyberattacks at greater scale, for lower cost, and by a host of capable adversaries."

While targeted company data breaches continue to make headlines, there is also a new trend of systemic cyber-campaigns with indiscriminate effects. The "WannaCry" ransomware attack launched by North Korea hit 100 countries and cost more than $8 billion. The "NotPetya" cyber-attack caused worldwide losses of $10 billion. In a recent case, the U.S. Department of Justice alleged that Iranian hackers stole 31 terabytes of documents and data from more than 315 universities in 22 countries, 30 American companies, and five American government agencies. In another matter, the Department charged Chinese agents for stealing intellectual property, data, and other valuable information from more than 45 technology companies and U.S. government agencies. One industry study noted simply: "Seemingly, no matter what defensive measures security professionals put in place, attackers are able to circumvent them."

Rod Rosenstein, a partner at King & Spalding and former Justice Department deputy attorney general (left); and Sumon Dantiki, a partner at King & Spalding.

In response, the regulatory framework surrounding data security is growing more complex. Federal agencies now consider cyber-security in regulatory approvals for everything from vehicles to medical devices and make cyber-security a significant factor in government contracts and procurement. And if a data breach occurs, state attorneys general, the Securities and Exchange Commission, the Federal Trade Commission, foreign data protection authorities, and others investigate the cause and penalize companies for failing to anticipate attacks and protect data.

This trend will only grow. The Department of Justice requested that any national data breach notification law in-

clude a requirement to "promptly" notify law enforcement. Similarly, the Department of Commerce recently proposed a rule authorizing national security reviews of a wide range of foreign communications equipment and services acquisitions, including providers of cloud services, software, and medical and video devices.

Companies need to shift their compliance mindset to address this new landscape and integrate technological defense into their operations by taking six steps:

» **Identify threats.** Establish processes to identify new cyber-threats; implement policies, training, and technical actions to mitigate threats; and develop effective mechanisms to assess compliance.
» **Address regulatory changes.** Review new regulatory and enforcement actions and respond with proactive internal assessments and necessary corrections.
» **Conduct ongoing due diligence.** Regularly assess and update vetting of suppliers, service providers, vendors, and customers that import risk.
» **Manage technological adoption.** Participate in procurement and deployment processes to spot risks and develop mitigation strategies as new technologies create new vulnerabilities.
» **Update resilience plans.** Craft resilience plans for data theft and other cyber-breaches with remedial measures that extend beyond strategies to continue operations.
» **Document compliance.** Document policies, procedures, and compliance measures, with an eye toward future inquiries. Enforcement authorities are not impressed by written policies and procedures; organizations need to demonstrate effective implementation and continuous improvement.

Organizations that adopt a "when, not if" approach to cyber-attacks will take proactive steps that defend against breaches and mitigate damage when they occur. Companies should expect investors, business partners, legislators, regulators, enforcement authorities, and other stakeholders to ask whether they have devoted appropriate attention to technological risk, and compliance professionals should be able to prove that they have anticipated attacks and prepared to address them. ■

Rod Rosenstein, a partner with King & Spalding, served in the U.S. Department of Justice for three decades, including as Deputy Attorney General and U.S. Attorney for Maryland. He helps clients resolve complex regulatory and litigation challenges, including government investigations, crisis management, internal investigations, national security, compliance, and monitoring.

Sumon Dantiki, a partner at King & Spalding, served in several senior roles at the U.S. Department of Justice, including as Senior Counselor to the Director of the FBI. A former federal prosecutor, Sumon helps clients prevent and address national security, cyber, and data privacy matters, as well as other critical risks.