THE
NATIONAL LAW REVIEW

Cyber Risks in the Workplace: Managing Insider Threats

Tuesday, October 10, 2017

Article By Moriah Daugherty
Lindsay Buchanan Burke
Covington & Burling LLPInside Privacy

Communications, Media & Internet
Labor & Employment
All Federal

Today, one of the most critical risks a company can face is the cyber risks associated with its own employees or contractors. Companies are confronting an increasingly complex series of cybersecurity challenges with employees in the workplace, including employees failing to comply with established cybersecurity policies, accidentally downloading an attachment containing malware or providing their credentials in response to a phishing scam, or intentionally stealing company information for the benefit of themselves or the company's competitors by simply copying information to their email or a thumb drive and leaving the company. Contractors or consultants with access to company systems can pose these same challenges. To guard against these risks, companies can implement various policies and procedures to address an employee's tenure, from pre-hiring to post-employment, and can implement many of these same precautions with respect to contractors, consultants, or any other third parties with access to company systems.

Before hiring employees or contractors, companies can ensure they have in place policies and procedures to protect themselves. Particularly important policies include: acceptable use of electronic devices and systems; mobile device; data collection and retention; notice and consents for monitoring and collection of information on company systems; and background check policies that permit pre-employment and ongoing vetting of all employees. Companies should enact enhanced screening and background checks for new hires who will have access to the company's "crown jewels" and systems that can connect to or access the same, and should require third parties that provide contractors to demonstrate that they are doing the same.

When drafting policies, companies should ensure all important stakeholders are coordinated—including Human Resources, Information Technology, and Legal—and that all employee-related policies are aligned with other company policies, particularly the incident response plan, data security, and cybersecurity policies.

When onboarding employees, companies should use procedures including training, policy review, and key acknowledgements and consents to establish a culture of awareness and compliance. It is particularly important for companies to complete the following tasks during employee onboarding: apprise new employees of the company's expectations regarding protection of confidential information and critical infrastructure (including ensuring that no new employee has brought any confidential information from another company with them); provide a briefing of policies governing employee access to information and those that could implicate employees' privacy; notify employees that they have no expectation privacy if using personal devices for business purposes; and obtain employee consent to any applicable monitoring. Employees should be asked to execute a non-disclosure agreement and other documents that protect the company's information, and the executed copies of these documents should be safely stored in the company's personnel file or human resources system.

Companies can and should also implement parallel procedures for outside directors, vendors, contractors, and third parties with access to company networks and systems.

After employees begin work, companies should regularly assess indicators of any potential issues, including any unusual systems accessed by employees; what documents and information employees are downloading, printing, or emailing; when employees are performing actions on company systems; and any

efforts by employees to exceed access privileges or records of failed log-in attempts. Conducting real-time monitoring of employees has significant privacy implications, particularly outside the United States. As a result, a company will typically want to notify employees of the monitoring and obtain prior consent or acknowledgement that an employee's use of the system constitutes consent to the interception of their communications and the results of such monitoring may be disclosed to others, including law enforcement.

Companies should conduct regular, required training with employees concerning cyber risks, including the risks associated with phishing attacks and fraudulent email solicitations. In addition, companies should make sure that compliance with security policies is included as a metric in performance evaluations for employees, particularly those employees with access to business critical information.

These same procedures should be in place for contractors, consultants, or any other third parties who have access to company systems and information. If necessary, companies should review the contracts they have in place with vendors or staffing agencies to ensure that proper procedures and consents are in place.

If a company believes an employee is potentially disgruntled or an insider threat, the employee's manager should coordinate with other departments—including Legal, Human Resources, and Information Technology—to obtain additional information and plan a course of action. Investigations can include forensic computer or network searches, preservation of affected systems, and interviews with employees. While developing the facts, a company should consider when or how to suspend or revoke a suspected insider threat's access or take additional action against the insider—though beware that taking action against a suspected employee is likely to implicate employment laws in the United States or elsewhere.

When off-boarding employees, companies should take steps to protect themselves. It is imperative for companies to develop policies and procedures for off-boarding employees that are directed at minimizing risks of data leakage. Exit interviews should be conducted wherever possible; they will allow companies to spot potential problems or identify red flags.

When an employee resigns, a company should decide whether to institute a protocol to remove or limit the employee's access to confidential information even before an employee's last day at work. HR should work with IT to audit the employee's most recent network access and email activity to ensure the employee has not harvested any confidential information.

When the company is preparing to terminate an employee, the company should implement a protocol to protect company confidential information, including reducing employee's access to networks and systems before or simultaneously with notifying the employee of the impending dismissal. The same should be done when a contract with a consultant, vendor, or contractor is nearing its end.

All employees who leave the company and all contractors whose contracts end should be reminded of ongoing obligations to protect the confidential information of the company and should be asked to return all company information, documents, and electronic equipment before their last day at work.

Employees can present a significant threat to a company's business critical information, as can contractors or consultants with access to company systems. Companies should ensure that relevant departments within the company, such as the legal, human resources, and information technology departments, are coordinating to take steps to protect the company against such threats, including those set forth above.

Source URL: https://www.natlawreview.com/article/cyber-risks-workplace-managing-insider-threats