Tinker, Tailor, Who's the Spy?

How to Safeguard Your Company from the Insider Hack

BY JULIE M. ENGBLOOM

The headlines are full of data breach attacks — millions of credit card numbers stolen, healthcare information hacked — all of it feeding the thriving cyber-crime economy. More often than not, the bad actors lurk outside the borders of the U.S. and are rarely held accountable. These external-based attacks come in various forms, including social engineering plots using increasingly sophisticated forms of subterfuge that can fool the most experienced of employees. These types of breaches garner the bulk of the media and public's attention.

Under the radar, at least from the public's perspective, are those breaches that originate from inside the company. The target is proprietary information. The insider hack is more difficult to detect and mitigate, and is often more economically crippling to the company than traditional forms of hacking.

A company's intellectual and proprietary information is often its most valuable asset. While insider threats are not as common as external breaches, they often are more expensive to the company. External attacks typically, though not always, target customer information, while insider threats target a company's intellectual property. Most troubling, insiders are trusted personnel who often have full access to the company's most critical assets: intellectual property, trade secrets and other forms of highly sensitive information.

An internal threat can originate from all levels within an organization, from CEOs, to interns, to third-party vendors. Companies must, of course, take measures to protect the perimeter of their physical and virtual footprint from outside intruders. In addition, companies must take steps to protect the perimeter from the inside out. When addressing the insider risk, pairing technological protocols, along with comprehensive employee policies, can mitigate the threat. And while all of these tools require an investment of time and money up front, the cost savings in the long run can be significant.

1. Information Technology Protocols. The first level of defense is to create roadblocks for deliberate (or inadvertent) attempts to move sensitive and/or valuable information off-site without permission. Businesses need to identify their most prized possessions (pricing strategies, technical/engineering specs, financial data, acquisition tactics, etc.) and then take steps to shelter them. For example, managing user access rights will limit the number of employees with easy access to certain types of information based on that individual's role within the company. This type of role-based, hierarchical access approach can be coupled with logging mechanisms and other IT protocols that will both deter misuse and detect it if it occurs. In addition, review your company's firewall protocols. Oftentimes, a company's firewall works to prevent malicious attacks from coming in. Verify that your company's firewall restricts and tracks outgoing data too.

2. Personnel Protocols. It is difficult to identify employees or vendors that pose a risk. A trusted employee may experience financial problems that could make them vulnerable to undue influence in the form of a bribe. A disgruntled employee passed over for a promotion may decide to exact revenge. Identifying an insider threat is not easy. Companies must establish confidentiality policies and engage in frequent communication regarding those policies to increase awareness around safeguarding confidential information. Doing so demonstrates the importance the company places on its proprietary assets and also demonstrates its seriousness with respect to addressing a breach, should it occur. Managers and staff must be trained about access, nondisclosure and confidentiality. Finally, review the company's employee handbook section on confidentiality and think about adopting an Acceptable Use of Technology policy.

The insider hack is more difficult to detect and mitigate, and is often more economically crippling to the company than traditional forms of hacking.

Companies must employ both technological and policy-related tools to ensure that data and system integrity are protected against both external and internal threats. Both before and after a breach occurs, counsel (in-house or external) can play a vital role in preparing a breach plan, developing suitable employee policies and procedures, working with law enforcement if appropriate, and navigating the post-breach landscape of notification and litigation, should it occur. ■

Julie M. Engbloom is a shareholder at Lane Powell where she co-chairs the Privacy and Data Security and Business Crisis Management and Emergency Remedies Practice Groups. She is a litigator who represents clients in a wide range of matters including breach of contract and fiduciary delinquencies, internal investigations, banking and financial litigation, and privacy and data security breach response and data breach-related litigation. Julie can be reached at 503.778.2183 or engbloomj@lanepowell.com.