Lockton Cyber & Technology Practice

Revocation of Access

April 2020

KEY CONSIDERATIONS WHEN TERMINATING EMPLOYMENT RELATIONSHIPS

As protection measures against COVID-19 remain in place in the U.S., companies in many sectors are struggling to keep operating. The lockdown is impacting revenues sharply and management is having to make very difficult decisions to keep the business afloat. Some see no other option than making staff redundant.

We at Lockton understand this is not a decision that is taken lightly but may be necessary in some cases. There are some precautionary measures we would like to recommend to protect an organization's sensitive information and data when terminating employees' contracts.

The risk is real, particularly when a large number of employees are working remotely. There are many examples of disgruntled employees accessing an organization's information and disseminating files in retaliation for being laid off. Employees who voluntarily resign are not exempt from such behavior either.

Information that is compromised may be subject to local privacy laws triggering additional issues for the employer. The concerns may extend to organizational intellectual property or other digital assets. Quite aside from the commercial ramifications of the possible compromise of intellectual property, from a cyber security perspective, the risks are clear. Threats of cyber extortion and data breaches are very real and must be managed appropriately.

Updated processes and effective security controls reduce the risk of terminated employees damaging or sabotaging systems or attempting to disrupt operations.

Former employees' access to an organization's network must be terminated effectively. An aspect often overlooked is the immediate need to communicate termination to the business's critical partners and vendors. This issue is rarely addressed, causing potential liability issues where the flow of critical information continues to take place from a third party to the former employee. Worse still, there may be instances where your employee has access to a business partner's system.

The process must be a coordinated effort within the organization, including HR, supervisors, IT and any other key decision makers involved with employee practices.

When termination is inevitable, issues surrounding an employee's access to information should be addressed as soon as possible to determine any immediate revocation of access (even while the individual remains employed), as well as the ultimate revocation of all access.

This mitigates the risk of critical files, work products, systems, private information, intellectual property or any other valued information being damaged, sabotaged or disrupted by the employee even before they leave employment.

Within certain businesses, this will be an automated process, generating electronic requests for revocation of access on a set date and time. In other cases, this will be a manual process of communication throughout the organization, providing alerts and requesting that certain actions be taken at certain times. The exact process will be based on maturity levels of an organization's systems.

The revocation of access must be documented. The goal ought to be to revoke access in a manner that makes good business sense, operationally, commercially and legally.

It goes without saying that your organization will need to be compliant with all other legal and regulatory processes, including, in the United States, the HIPAA Security Rule:

> "164.308(a)(3)(ii)(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section."

A few key items to incorporate into your business's termination process pertaining to access control management include:

1. While disabling the employee's access to all systems, such as Active Directory and any remote access credentials, don't delete it. You may need or want to reenable it later for future use.
2. Compile a list of all locations where the employee stored data, including cloud storage platforms.
3. Compile a list of all partners and vendors the employee had access to and inform those entities of the employee's departure from the organization.
4. Ensure the employee's telephone is not forwarded to any external numbers, such as their cell phone.
5. Change their voicemail password.
6. Revoke access to your corporate Content Management Systems (CMS), such as Dropbox accounts.
7. Secure and disable all SaaS accounts.

The Lockton Cyber & Technology Practice educates our clients about the latest privacy and cyber threats and latest regulatory requirements as they evolve globally.

LOCKTON®