eBOOK

Are You Exposed?

The Rise of the Contractor & His Impact on Security

SailPoint

The Snowden debacle has shed light on government contractors with high-level security access and just how much damage they can do if they so choose. But it's not just the National Security Agency (NSA) who is at risk of an insider attack from a contractor, as evidenced by the onslaught of high-profile data breaches such as Target, AT&T and DuPont, just to name a few. Even the Korean Credit Bureau (KCB) disclosed that a temporary contractor who had access to its systems was able to steal customer details including names, social security numbers, credit card numbers and expiration dates. Clearly, security issues like these are widespread.

Today's corporations, from manufacturing to IT to home healthcare to security, rely more heavily upon third-party consultants to complete specific assignments and keep labor costs down. According to an analysis from CareerBuilder, nearly 3 million people are employed in temporary contract jobs today, and that number will continue to rise into the foreseeable future. And while these arrangements provide businesses with a competitive edge and the flexibility to expand and contract their workforce as needed, there are associated risks that, if not handled properly, can outweigh the benefits. Businesses must be smart about protecting against the potential risks that contractors bring into the virtual workplace, especially as compliance regulations increasingly expect that contractors are subject to the same IT controls and safeguards as every other employee.

The Risks of Contractors

A breach by a third-party service provider has direct ramifications on data security, as well as on the overall brand – and subsequently the bottom-line, as evidenced by Target's $10 million settlement. While the responsibility for a third-party contractor can be a grey area – especially if contracted through a service provider or vendor – an organization is always responsible for managing and monitoring who has access to their systems. For instance, under the Florida Information Protection Act of 2014 (FIPA), if a third-party service provider has a breach, the healthcare provider, not the third-party organization, is responsible for notifying patients.

The benefits of a contractor may be outweighed by the potential security risks if not handled appropriately.

This responsibility makes it imperative for organizations to pay attention to contractors. But the reality is, it's no easy task. Here are a few critical challenges posed by contractors:

1 **Untracked Staff**
Contractors often bypass HR when entering an organization and as such are not tracked through HR or any centralized system. In the event that there is a breach or data is compromised, HR is unable to take any action because they have no awareness or the details of the third party.

2 **Ineffective Onboarding and Exit**
The revolving door of temporary staff puts pressure on IT systems. There is a significant onboarding process, requiring one or two more offline processes than is typical for an employee entering through HR. For example, the hiring business line will send IT an email informing an executive to grant a contractor access. These ad hoc requests build up and IT has no visibility into when and how many they will receive, which makes it difficult for project planning and budgeting. Without an agreed-upon process in place, IT has no power to drive efficiencies.

3 **Lingering Post-Contract Access**
Contractors have access to systems and sensitive data that continues after they are terminated because there is no formal process for severing access. Adding to this risk is the fact that contractors move around from organization to organization, sometimes are working multiple contracts at once. If they jump to a competitor, lingering access could be potentially catastrophic. Permanent employees are less likely to do damage to their employer since they have a vested interest in the company, where contractors might think it's permissible to share confidential data.

4 **Access Outside the Network**
As part of the clean up when a contractor leaves, it is no longer okay to simply turn off network access. As more and more companies look to SaaS apps to reduce costs, mission-critical data is now being kept outside the network. It is more imperative than ever that IT has full visibility into who has access to what – whether it's on-premises or in the cloud – to ensure they have the full picture and turn off all critical access points.

5 **Lack of an Authoritative Source for Contractors**
One of the biggest challenges organizations face with managing contractors is that there is no single person who owns the "approved contractors" list. To combat this, IT should partner with finance to manage the list and monitor for any lingering unauthorized access. Alternatively, IT can merge disparate authoritative sources across employees and contractors to get a single view of the user base and apply common controls to both types of internal users.

What makes this area of data security such a challenge is finding the right balance between limiting risk and opening up access to sensitive applications and data that a contractor needs to perform his/her job. Unfortunately, there's no silver bullet solution to this problem, but if companies take a layered approach that includes awareness and education, as well as preventive and detective controls, they will be much more secure. First and foremost, companies need to be explicit about their policies in this area and clearly define what is considered illegal usage of proprietary data.

At the same time, companies need to proactively monitor and manage contractors' access privileges, with the goal of limiting access to only what is required to perform a given job. Identity management plays a critical role in helping companies ensure that contractors' access privileges are appropriate and conform to policy. These benefits can include:

Centralized Visibility

Continuously and actively review what information contractors have access to in order to make sure it's appropriate for the work they are doing. This is achieved by implementing a system that allows for centralized visibility into which contractors have access to what within the infrastructure.

A Risk-Based Approach

Since contractors pose a higher security risk to the network because they don't have the same relationship as a long-term employee, create an identity risk model to better understand where the hot spots are. Details like whether this contractor is working with a competitor are critical.

Termination of Access Tied to the Contract End Date

Close the loop once the consultant leaves. Put an automated process in place to terminate all access just like you would to an employee. During the onboarding process for new contractors, capture the length and nature of the contract so that access expires automatically. This is often easier said than done, because organizations rarely have a centralized process for contractors. One "work around" for that is to assign an accounts payable person, who pays close attention to when a contractor should no longer get paid, as an access reviewer.

Aggressive Cleanup of Contractor Access

Upon termination of a contract, simply severing network access isn't enough. It is also critical to ensure that the organization cleans up the access environment at the individual application and entitlement level that the contractor was given. Oftentimes an organization will continuously reuse certain contractors that can quickly rack up a number of access points over the years as IT turns on and off their overall network access if they don't delve into the application and entitlement details. Because of this, contractor access should be certified every 90 days.

As the economy continues to get stronger and businesses benefit from contingent workers, the issue of unmonitored access for third-party workers will only escalate. Organizations that implement good identity management strategies that incorporate contractors as part of their overall governance strategies can protect themselves from past, present and future threats. Those that don't heed this advice put themselves and their business at incredible risk.