Contractor Access:
Mitigating Security and Risk Issues

Contractors—a necessary evil?

Today's workforce is undergoing a transformation, expanding to include a growing number of contractors, partners and service providers. This type of outsourcing continues to be on the rise, despite high-profile security incidents. Although the 2013 Target breach grabbed a lot of headlines, it is not an outlier. Companies like Cogent Healthcare, Stanford Hospital, Beebe Healthcare and even the EPA have had breaches that were the result of "temporary" access.

So why is the trend continuing despite the evident risk? The truth is that businesses do not really have the luxury of asking, "can we afford the risk of a contractor?" Business operations and financial realities dictate the importance of contract help. So rather than reducing the number of outside hires, IT and security teams are being asked to find a way to mitigate the risk.

Contractors represent a unique challenge for business. Their contracts have a defined lifespan, so there is a need to ensure that they become productive, as soon as possible. A substantial roadblock to productivity is granting them access to necessary systems, which in many cases house sensitive information.

What causes contractor risk?

The truth is, contractors themselves are not the only source of risk. In fact, many businesses have unintentionally built risk into the process of provisioning identity and access across the organisation. Here are a few common drivers of incremental risk:

- **Over credentialing:** It is often difficult or time consuming to grant granular access to specific systems and much easier to give blanket access to all systems. That makes stolen credentials even more dangerous because of the extent of what may be done with them.
- **Human error:** The person requesting the access (the business sponsor) often is not the one who creates the access credentials. When there is a handoff, the party responsible for granting access could misunderstand what is required and magnify risk. Further, many systems rely on manual processes that introduce the possibility of human error.
- **Bypassing processes:** It is easy for the proper process to get circumvented, especially if it is time consuming. When time becomes an issue—whether because of other responsibilities or a large volume of credentials required—people take shortcuts. If the system allows for it, standard process will be ignored whenever expediency dictates.

MITIGATING THE RISK: CHANGE YOUR THINKING ABOUT IDENTITY AND ACCESS

Anytime you provision an identity and grant access to your systems, you are creating risk. But there are plenty of things you may do to make sure that the risk is managed. The key to doing so is a comprehensive approach to identity and access management across your organisation. Start with these basic principles:

1. *Minimise the number of different tools used for identity and access management (or centralise them if possible)*
2. *Eliminate loopholes so that the established process is the only way that access is granted (there should be no way around it)*
3. *Standardise the process for granting access for both contractors and employees*

NetIQ

The 2013 Target breach grabbed a lot of headlines, but companies like Cogent Healthcare, Stanford Hospital, Beebe Healthcare and even the EPA have had breaches that were the result of "temporary" access.

But the risk is not just from granting access—it is from not revoking it. Credentials generally remain active until turned off, and many organisations do not have a formal process to do so. As a result, not only might contractors have access to too many things, they may have it after they have left the organisation.

Another problem is that once the credentials have been applied, they may be used for any purpose. Usually this happens because the credentials are not tied to a specific function. So there is no "proper" usage standard against which to check.

Risk is not exclusively tied to breaches either. If processes may be bypassed, proving compliance becomes difficult or impossible. Further complicating matters, identity and access rights may not be centralised. If the process of granting access is different between multiple enterprise and cloud environments, then risk of inconsistent policy and human error is magnified.

Things to look for in an access solution

There is a range of solutions in the market that can help you minimise contractor access risk. Choosing the right one for your organisation may seem like a daunting task. Here are a few things that you should look for when evaluating solutions:

- **Ease of use:** If the system is easy for everyone to use, it is less likely to be circumvented:
  - Business sponsors (those who understand specifically what level of access is required) should be able to request access in an interface designed specifically for them.
  - Access requests should be easy to define and limit at a granular level.
  - Provisioning should happen with as little human intervention as possible and should happen immediately.
  - Access privileges should be very easy to turn off and they should be time bound.
- **Comprehensiveness:** The tool should work for all of the environments and systems you use in your organisation (cloud software platforms, network access, on-premises tools) and apply consistent rules to each of those disparate environments.
- **Reporting capabilities:** For visibility and governance purposes.
- **Identity-based activity tracking:** Provide identity-tracking capabilities, so that it is easy to see what is being done with credentials that have been issued.

Automating your identity, provisioning and approval processes are critical to giving non-standard employees appropriate access to the information they need in order to do their jobs. With powerful automated provisioning, delegated Active Directory administration and more, NetIQ can help. To learn more, visit the NetIQ Identity & Access Management solution page. **www.netiq.com**

Worldwide Headquarters

1233 West Loop South, Suite 810
Houston, Texas 77027 USA
Worldwide: +1 713.548.1700
U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com
http://community.netiq.com

For a complete list of our offices in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit **www.netiq.com/contacts.**

Follow us:

584-AP0005-001 07/14 DS