

NERC CIP AND IDENTITY MANAGEMENT

Many enterprises are currently preparing themselves for NERC CIP compliance. In large enterprises, the overhead to prepare, report and maintain CIP compliance is and will be onerous. Additionally, CIP requires physical and electronic security compliance. What most enterprises don't realize is that identity management is the solution they require to keep reporting costs down, integrate physical and logical security and help segregate the SCADA and IT networks.

CIP REPORTING AND "ATTESTATION REPORTS"

The main idea behind NERC CIP is to ensure that enterprises know who is on their critical infrastructure and quickly remove identities who no longer require access. In other industries like finance doing Sarbanes-Oxley compliance reporting, some senior managers had full-time people spending several days per quarter reviewing access records. This led to the development of electronic attestation reports generated by the identity management system. Today, large financial enterprises, in a few minutes, approve the reports and are able to delegate them to the people who are closest to the identities. The same thing should be done with CIP reports.

All critical infrastructure applications provisioning, changing and de-provisioning of identities is handled by the identity management system. Reports are easily generated to the appropriate managers on whatever time basis you decide: a week, month, quarter, half-year, etc. Managers can quickly scan the list, decide to select all identities on the list, then click on ones who have changed and then submit their approval. This is particularly important when you have contractors and third parties who are using your critical infrastructure systems. Often there is poor tracking of these identities leaving the enterprise or no longer requiring access.

PHYSICAL AND LOGICAL SECURITY INTEGRATION

Most critical infrastructure enterprises have security for SCADA, IT and Physical security managed by three separate departments. This results in the creation of security gaps where a potential malicious person can take advantage of the gaps.

For example, building master keys are often lost or not returned or a contractor, who has badge access to a secure area, still has their badge and active access after leaving the enterprise. A targeted attack using a combination of weaknesses in SCADA, IT and physical security is therefore possible.

Identity management can help ensure that all identities are quickly terminated when they leave the enterprise, that building master keys are recovered and check to ensure that an identity is still "active" when accessing a critical infrastructure point.

I CAN HELP

My name is Guy Huntington. I have led many Fortune 500 identity projects. At Toronto Hydro, I recently designed a identity management solution that integrates physical and logical security for all identity types who access the SCADA system, provides attestation reports, uses stronger authentication for critical areas and apps, etc. I also instigated a vulnerability assessment for SCADA, IT and physical security. If you're interested in learning how to lower your CIP compliance costs and strengthen your overall SCADA, IT and Physical security, then call me at 604-861-6804 or email me at guy@hvl.net.