FEDInsider

4 Ways the Energy Sector is Building Better Security Practices

Energy Sector Leaders Discuss Security & Governance

Over the course of 2020, we have seen companies in nearly every sector embrace remote work to help keep their personnel safe during the global pandemic. This is true even in places like the energy sector where teleworking and remote workforces were not always readily accepted. In a sector like energy and utilities, social distancing may be the new way of doing business, but companies still need to operate within the compliancy bounds of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) framework.

Several innovative companies are finding ways where NERC CIP and remote work can come together. Workers are able to do their jobs remotely, and their companies stay compliant with the highly restrictive NERC CIP standards. Industry leaders from some of those firms recently got together on a FedInsider virtual event to discuss how they are maintaining a necessary level of daily governance while also supporting a remote workforce. The following are four key elements to their success.

1. Modernizing & reducing/eliminating as many manual processes as possible

As technology evolves, it often offers new and convenient ways to store and present data. However, sometimes there is a lot of resistance to replacing tried and true methods such as Microsoft Excel spreadsheets or paper hard copies. The key is to try to get away from those processes, even if doing so is initially painful.

"Like many maturing programs, we managed through a number of spreadsheets and manual processes," said IAM Program Manager Sue Glynn at American Transmission Company. "Originally, compliance was mostly managed by our corporate security team. As the bulk of our regulated access was physical access, it required a badge that was issued by corporate security."

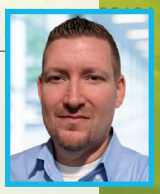
Glynn went on to say that it would take anywhere from five to ten minutes to open some of their more complex spreadsheets, much less begin to work with them. Additionally, managers would spend several weeks every quarter auditing access permissions instead of focusing on their primary roles. While Excel is a great tool, there comes a point where something more streamlined is better for identity management and compliance procedures. Additionally, Excel documents are not always audit approved due to weaker security than other access management tools.

Because of all of that, Glynn said they had to simply commit to removing the manual processes from their system and began to look for technology partners who could assist with that effort.

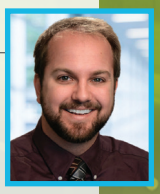
Featuring:

- **Sue Glynn**
  IAM Program Manager, American Transmission Company

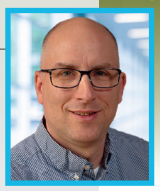
- **Mike Ellie**
  IAM Analyst, American Transmission Company



- **Jeff Haima**
  Senior Cybersecurity Analyst, American Transmission Company



- **John Peters**
  Senior Enterprise Infrastructure Specialist, Sacramento Municipal Utility District (SMUD)



- **Andrew Brorsen**
  Founder & Senior Partner, Cirrus Cybersecurity Group

2. Security Reports Will Likely Spike after Automation, and that is Good

Whenever automation is brought into an organization, especially a utility that is constantly monitoring its security posture, there is likely going to be a huge spike in reports. While this situation can be alarming, and make it seem like the company is falling out of compliance, Jeff Haima, the Senior Cybersecurity Analyst at American Transmission Company says that there is no need to panic. In fact, the spike is actually good news.

"This sounds counterintuitive, but the spike proves that your program is working," said Haima, "What you've just done is taken a flashlight and looked around in all the dark corners of your organization and found some things that you didn't even know existed."

For Haima, the automation spotlighted some vulnerabilities that had gone undetected before. With the strict compliance

standards of NERC CIP, discovering every potentially unknown compliance issue can mean the difference between a passed or failed audit, so he was grateful. Haima added that as those newly found vulnerabilities are fixed, the number of alerts will slowly drop back to normal once again.

3. You have to Improve Visibility to Resolve Data Set Problems

Turnover is inevitable within any workforce, and the energy sector is no different. Each time an employee resigns or is terminated, there is a potential risk of their access not being properly and immediately revoked. Visibility helps keep human resources and systems compliance teams on the same page to ensure that any access is removed as soon as the employee in question is no longer with the company.

"If someone leaves the organization and the manager doesn't terminate that person in a timely fashion, then you've got a risk for a potential violation," said John Peters, Senior Enterprise Infrastructure Specialist for the Sacramento Municipal Utility District. "If you improve your visibility, then you can set up policies to always catch that sort of thing."

Visibility into your data is also critical when dealing with a remote workforce. Good visibility can support things like computer forensics, Peters said. That way you always know who touched different systems, or who might be affected by a malicious program or intrusion.

4. Automate Employee Onboarding Using Role-based Datasets

Onboarding new employees can be stressful and time consuming. In the past, it could be done in person with a human resources officer collecting and assigning all the access and permissions a new employee requires to perform their assigned job duties. But it is not always easy to do remotely, and even if you can, you are still reinventing the wheel every single time.

A better method, according to Mike Ellie, an IAM Analyst with American Transmission Company, is to assign roles to employees based on their job title or code. Then when a new employee comes onboard, you simply assign them everything they need in terms of access based on that new job or title.

"We're really knocking out a good, you know 50% to 60% of access needs today based on who you are, and what we know about you," Ellie said. "In some cases, the manager does not really need to do anything at all, although they can always add more access a couple of weeks into the person's employment if needed."

As an organization continues to develop and automate roles, and the managers become more familiar with that process, it can really speed up the onboarding process. That is something that Ellie says can save a lot of time for any organization, but it works especially well within utilities, which tend to have more complex access rules and procedures.

Compliance Does Not Equal Security

Achieving 100% compliance with the NERC CIP standards does not equate to a Utility being 100% secure from malicious actors or human error. All companies charged with "protecting the grid" must also have a strong security program with continual assessment of their defense-in-depth capabilities.

Reducing risk from either non-compliance or a security event can be achieved with the combination of strong processes and controls supported by leading security solutions from SailPoint and SecZetta.

Identity Security is the New Perimeter for Utilities

Complementing a strong compliance program to address common gaps with NERC CIP compliance is a strong security program. Proper investment and integration of SailPoint and SecZetta facilitate improved controls over common issues which lead to increased risk and deficiency fines from NERC CIP Audits including:

- Timely removal of access for employees and contractors who are no longer authorized to NERC CIP-designated access (physical or cyber) such as from termination, job change, or transfers.
- Verification of the resource identity, timely completion of mandatory NERC CIP-designated training courses, and confirmation background checks completed and passed prior to assigning authorized resources to NERC CIP-designated access.
- Support the Audit with required documentation and the maintenance of the policies, processes, and controls to minimize the effort and impact on both internal and costly external resources.
- Routine compliance-related activities such as Third-party Employment Verification, Access Certifications, and Exception Management.

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

Carahsoft
1493 Sunset Hills Road
Reston, VA 20190
Contact: Maggie Manfredi

(703) 230-7488
Maggie.Manfredi@Carahsoft.com
Carahsoft.com/vendors/SailPoint
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

SailPoint
11120 Four Points Drive
Austin, TX 78726
Contact: Cathy Cromley

(703) 517-4419
Cathy.Cromley@SailPoint.com
Sailpoint.com/identity-for/government
Facebook.com/SailPoint
Linkedin.com/company/SailPoint-Technologies
@SailPoint