
Reliability & Security
Workshop
WECC
March 17–18, 2026
San Diego, California

Insider Threat with OT/SCADA Environments

Protecting Critical Infrastructure From Within

Brandon Storment
WECC Auditor

Electric Reliability & Security for the West

March 18, 2026

Agenda

- What insider threats are and why it matters
- Risks specific to energy systems
- Real-life examples
- Mitigating insider threats + everyday steps to stay safe
- What to do if something goes wrong
- Key things to remember and Q&A

What is an Insider Threat?

- Insider: anyone with a “key” to the kingdom
  - Employees, contractors, partners
- Insider threat: when someone with a key accidently or intentionally causes a problem

Understanding Insider Threats in the Energy Sector

- Insider threats matter profoundly to the energy sector because the industry is designated as uniquely critical infrastructure
- Control of physical infrastructure (OT/ICS/SCADA systems)
- High consequences of disruption
- Complex workforce and supply chain
- Blended cyber-physical and geopolitical risks

Non-malicious Insider Threats

- Non-malicious (also known as the unintentional, accidental, or negligent) insider threat
  - Stem from human error, carelessness, lack of awareness, or being tricked by external attackers
    - Accidental — These involve genuine mistakes with no disregard for rules — human error
    - Negligent (or careless) — These involve insiders that know or should know the security policies but choose to ignore or bypass them for convenience, creating avoidable risk

Malicious Insider Threats

- Malicious insider
  - A person (current or former employee, contractor, partner) who deliberately misuses access to harm the organization
    - Theft of sensitive data for personal gain or espionage
    - Sabotage of systems or data
    - Collaborating with external attackers to compromise the organization
- Per CISA (U.S. Cybersecurity and Infrastructure Security Agency) — “Malicious insiders take actions to harm and organization for personal benefit or to act on a personal grievance”

Compromised Insider Threats

- Compromised insider
  - Legitimate users whose accounts/devices have been hijacked by external attackers
    - Credential theft
      - Phishing
      - Malware
      - Credential theft
      - Social engineering
    - Unauthorized access to sensitive data using stolen credentials
- This is one of the most challenging modern cybersecurity problems since it exploits trust from the inside out

Types of Insider Threats

Type	Intent	Common Cause	% of Incidents	Typical Examples
Malicious	Deliberate harm	Revenge, greed, espionage	~13–25%	Data theft for sale, sabotaging systems
Unintentional	None (accidental/negligent)	Human error, carelessness, being tricked	~75–87%	Phishing, missent emails, poor habits
Accidental	Zero disregard	Honest mistake	Varies	Wrong email recipient, accidental delete
Negligent	Knows better but ignores	Convenience, burnout, multitasking	~50–60%	Bypassing VPN, ignoring updates
Compromised	Victim of attack	Phishing, credential stuffing, social engineering	Significant portion	Account hijacked -> attacker acts inside

Types of Insider Threats

Type	Intent	% of Incidents	Avg. Cost per incident	Common Examples	Detection Difficulty
Malicious	Deliberate harm	~13–25%	Highest ($715K–%5M)	Data theft for sale, sabotage, espionage	Very high (knows the systems)
Negligent	Careless/no intent	~75–87%	Lower but high volume	Mis-sending files, ignoring policies	Moderate
Compromised	Victim (tricked)	~20% (credential theft)	High (~$679–$779K)	Phishing -> account hijack	High (blends in)

Why Do Insider Threats Happen?

- Most are accidental:
  - Lack of training (“I didn’t know that was risky”)
  - Being too busy or taking shortcuts
  - Unintentional insider threat
- Some are careless:
  - Thinking “It won’t happen to me”
  - Wanting to get the job done faster
- Very rare intentional cases:
  - Someone angry or upset with the company
  - Financial problems or being offered money

Real Life Example — Stuxnet (2010)

- System was air-gapped
- Person gaining employment/access
- Person gained access to the exact centrifuge setup/configuration -> allowing for developers to tailor the worm precisely
- Person physically delivers the malware via USB flash drive or infected laptop
- Nuclear facility equipment slowly damaged over months
- Screens showed “normal” while machines broke

What was the failure here and how do we address it?

Real Life Example — Colonial Pipeline (2021)

- Financially motivated
- Ransomware incident that disrupted fuel supplies
- Fuel pipeline shut down -> gas shortages
- Breach stemmed from poor management of insider credentials and access controls
- Initial access via compromised VPN account belonging to a former employee that hadn’t been deactivated after they left (stolen password)
- The “insider issue” — inadequate offboarding process, weak password hygiene, and not enforcing MFA

What was the failure here and how do we address it?

Real Life Example — Ukraine Power Outage (2015)

- Breach relied on unwitting insiders and social engineering
- Started with spear-phishing in early 2015
- Hackers stole login details via fake emails.
- Remotely turned off power to 225,000 homes.

What was the failure and how do we address it?

Real Life Example — Saudi Aramco (2012)

- Potentially a geopolitical malicious insider
- Malware widespread deployment and persistence
- 30,000 office computers wiped clean
- Likely started with one wrong click

What was the failure and how do we address it?

Real Life Example — CrowdStrike (2024–2025)

2024

- Trusted insider turned accidental threat
- Accidental error in the development and the deployment life cycle

2025

- Employee shared internal screenshots with a hacking group
- CrowdStrike detected the issue
- Proceeded to contain the issue
- Fired the suspicious insider

How Does an Entity Detect Insider Threats?

- Trust but verify
- Monitoring:
  - Tools that notice unusual login times or places (e.g., someone logging in at 3 a.m. from another country)
  - Alerts for big file downloads or unusual changes to settings
  - Cameras and badges that track who goes where
  - Automatic checks on emails and USB use

Simple Ways We All Can Help

- Treat unexpected emails like junk mail — don’t open or click on links
- Only use company issued and approved USBs (no personal ones)
- Lock computer when stepping away
- Strong passwords + two-factor login

What An Entity Should Be Doing

- Separating office and control networks
- Segregating duties
- Tools watching for unusual activity
- Regular training and tests
- Extra checks for contractors/partners and supply chain

If Something Goes Wrong — What Happens Next?

1. Safety first — protect people
2. Follow emergency steps
3. Report quickly
4. Investigate to learn, not blame
5. Lessons learned for next time

Key Things to Remember

- Most risks are accidents — like losing your keys
- Simple habits stop most problems
- You are the strongest lock your company has
- Speaking up helps everyone

Resources and Support

- Regular training sessions
- Anonymous reporting line
- IT help desk
- Quick guides in break rooms
- Talk to your supervisor any time

ELECTRIC RELIABILITY & SECURITY FOR THE WEST

ENGAGE WITH WECC


WECC
www.wecc.org | 801-582-0353
155 N 400 W, Salt Lake City, Utah 84103, USA