South Texas Electrical Power (STEP)

By

Amjad Alqahtani, Ricardo Figueroa

IS-6343-001: Cyber Risk Management, May 7, 2025

Dr. Gregory White

Table of Contents

Executive Summary

The South Texas Electrical Power (STEP) is a private utility organization that supplies electricity to six small towns in South Texas. Despite being a leader in harnessing solar and natural gas power generation and engaging in R&D efforts for EV charging infrastructure, STEP faces significant cybersecurity challenges due to inadequate security policies, limited IT staff, and outdated or insecure practices. These issues could be of severe negative impact to the company if not adequately addressed, in the wake of the cybersecurity threat proliferation that have attacked several critical infrastructure globally. This report highlights the most important cybersecurity threats, evaluates the risks, and provides a prioritized roadmap for enhancing STEP's cybersecurity posture.

1. Introduction

In today's world, where digital change is driving innovation and operational efficiency, the evolution of cybersecurity threats has emerged as a defining challenge for organizations across all sectors. As technologies evolve, so do the tactics and motivations of malicious actors seeking to exploit vulnerabilities for financial, political, or strategic gain. The energy sector, being critical to national infrastructure, has become an increasingly attractive target for cybercriminals and nation-state attackers alike. Utility companies like South Texas Electrical Power (STEP) are particularly at risk since they are highly dependent on operational technology (OT), legacy systems, and growing remote access capabilities. Additionally, insufficient resources and limited cybersecurity expertise can create exploitable vulnerabilities that compromise service continuity, safety, and customer trust. With STEP going into emerging technology such as electric car charging and solar power, it will have to modernize its attitude to cybersecurity so it can match or stay ahead of the rapidly evolving threat landscape. This report provides a balanced assessment of STEP's current stance on cybersecurity, identify imminent threats and risk, and propose a comprehensive and phased range of recommendations on how to bolster defenses.

2. Cybersecurity Threat Landscape

The current cybersecurity threat landscape is increasingly complex and multifaceted, shaped by evolving attack methods and vulnerabilities across diverse digital environments. Effective defense strategies must combine technical solutions, policy enforcement, and human-centric security awareness to address these dynamic and interrelated risks.

2.1. Key Threats

Vishing and phishing attacks stand out as an even greater risk for STEP due to a clear lack of comprehensive cybersecurity training among employees. These socially engineered attacks exploit human vulnerabilities rather than system flaws (Jones et al., 2020). Employees might inadvertently click malicious links, download infected attachments, or share login information over the phone. Without continued awareness campaigns and practice phishing simulations, compromise through email spoofing or fake calls are high threats, which gives the attackers possible points of entry into STEP's internal networks and sensitive operations.

Ransomware is similarly and arguably disastrous, especially since the organization relies on shared access systems and there is no adequate network segmentation. If one system is compromised, the malware will easily traverse the whole network, shutting out users and encrypting files throughout departments (Akibis et al., 2024). The interconnected nature of systems, from power generation, administration, and customer service means even a localized intrusion could cause widespread operational shutdown. Lack of real-time backups or independent network boundaries can amplify the impact and recovery time.

STEP also needs to consider malicious and accidental insider threats, which are potentially significant. Granting employees administrator privileges with insufficient screening or ongoing training creates a lethal exposure (Haimed et al., 2023). Disgruntled staff or even well-intentioned employees unaware of best practices knowledge can inadvertently or intentionally compromise systems. The absence of access auditing and role-based access controls aggravates the risk, making tracking or monitoring illicit actions difficult. Developing stringent procedures and continuous behavior monitoring is required to mitigate this insider threat vector.

STEP's shared facilities, which include the server rooms and administrative sections, have weak physical security controls with limited to pretty much non-existent controls against unauthorized access. Without proper entry processes, surveillance mechanisms, or biometric authentication controls, attackers might physically gain access to secured areas. Once inside, they can hack servers, install malicious devices, or obtain information from insecure endpoints (Jones et al., 2020). Having external contractors or shared facility users only makes matters worse, necessitating physical security policy and infrastructure reviews.

Credential theft is also a potential issue, especially because using the same passwords for all important systems in STEP is so widespread. This greatly increases the threat of privilege escalation, where once an attacker gains access to one account, they can laterally move across the network with minimal challenges (Jones et al., 2020; Mansfield-Devine, 2021). Lack of multi-factor authentication (MFA) and poor password practices also weaken the defensive posture. Enforcing on identity and access management (IAM) practices is essential to remedy this attack.

Worse still, the organization is exposed to social engineering attacks like tailgating and pretexting due to human error since these are not addressed properly. This gap renders staff unfit to identify and respond to deceitful tactics utilized by attackers to bypass physical and virtual barriers (Jones et al., 2020). The staff are the first defense line, and without knowledge on such tactics, STEP's security position is compromised.

From a technical view, the company is vulnerable to Denial of Service (DoS) Attacks, a substantial threat to its operations. By overwhelming networks with unnecessary traffic, such attacks can disrupt access to critical services like customer portals, billing systems, and remote plant controls (Singh & Gupta, 2022). This impact is exacerbated by the company’s limited incident response capabilities and monitoring tools, whose latency in detection and mitigation may worsen the situation. Furthermore, the absence of proper firewall rules and outdated intrusion prevention systems leave the network vulnerable to volumetric and application-layer DoS attacks.

Remote access gateways in form of VPNs, and software like TeamViewer present STEP's expanding attack surface. The secure setup of VPNs is optional rather than forced, thereby creating inconsistency in protection, while poor endpoint management compromises it (Mansfield-Devine, 2021). Remote exploitation is highly likely on systems accessed through personal or unmanaged devices. Without centralized control and security enforcement, attackers could leverage exposed access points to infiltrate the network and exfiltrate sensitive data.

Finally, intellectual property theft is also a critical concern, with STEP's R&D facility being a significant threat. R&D offers minimal protection for proprietary innovation, especially in EV charging technologies. Standalone Linux systems with no centralized monitoring, supplemented by unsecured wireless networks, create a fertile environment for exploitation (Chen et al., 2023). With weak access controls and encryption, it would be simple for attackers to intercept or steal precious research, at the expense of competitive advantage and long-term innovation efforts.

2.2. Attack Vectors

Email continues to be a leading cyber threat vector, and when it comes to STEP, the infrequency of awareness training makes its employees extremely vulnerable to phishing and malware attacks, which threat actors can take advantage of through social engineering. Unencrypted wireless LANs at some STEP locations put the company even further at risk. Guest and research segments without proper encryption or isolation enable attackers to hijack or inject malicious data on the network. Remote access tools such as TeamViewer, coupled with the optional rather than mandatory use of VPNs, introduce additional vulnerabilities (Chen et al., 2023; Mansfield-Devine, 2021). Such applications may become portals to unauthorized access, especially if endpoints are left unsecured and without robust monitoring or enforcing multi-factor authentication.

The use of shared and weak passwords on multiple platforms significantly compromises STEP's security against brute-force and credential-stuffing attacks. Once a single set of credentials is compromised, attackers can move laterally within the network, escalating access, and maximize the damage potential (Mansfield-Devine, 2021). In addition, the organization's inability to regularly manage software patches and endpoint security leaves room for exploitation (Akibis et al., 2024). Unpatched systems remain vulnerable to common bugs and security vulnerabilities, which may be used by insiders and outsiders to breach security or subvert operations.

Finally, insider abuse or error remains a major risk factor. Granting distributed admin rights without strict control or accountability guarantees that even well-meaning employees can unwittingly leave the organization open to attack. Meanwhile, malicious insiders can exploit the absence of controls to act undetected, compromising systems or leaking confidential information.

3. Organizational Risks

Priority	Risk	Description
1	OT System Compromise	Disruption of energy generation with high impact on service delivery.
2	Ransomware	Limited segmentation and poor endpoint security pose major risks.
3	Social Engineering Attacks	Untrained employees are vulnerable.

4	Insider Threats	Inadequate admin access control and oversight.
5	Data Breaches	Especially from R&D due to Linux isolation and open Wi-Fi.
6	Physical Security	Shared server rooms and badge access inconsistencies.
7	Weak Off-boarding	Delayed account revocation and asset recovery.

4. Recommended Cybersecurity Controls (Phased Approach)

A phased cybersecurity approach prioritizes strong access control, basic security hygiene, and early threat detection in the initial stages. As maturity increases, it shifts toward integrated monitoring, user training, and adaptive, behavior-driven controls. This strategic layering enhances an organization's ability to proactively detect, respond to, and recover from threats.

4.1. Near-Term (0–3 Months)

In the immediate term, STEP will have to adopt VPN use for all remote access to ensure secure encrypted paths between employees and internal systems. The use of unique, complex passwords has to be mandated for every system, as opposed to the current use of shared credentials, considerably reducing the susceptibility to credential attacks (Grobler et al., 2020). All staff must receive fundamental security awareness training, especially on subjects like phishing, vishing, and tailgating to build social engineering resistance (Jones et al., 2020). Additionally, an Intrusion Detection and Prevention System (IDS/IPS) can be utilized for real-time detection and response to unauthorized access (Kizza, 2024). finally, endpoint security should be increased by implementing enterprise-level Endpoint Detection and Response (EDR) solutions to identify and neutralize malware and malicious activity on devices.

4.2. Mid-Term (3–9 Months)

In the medium term, STEP needs to implement Role-Based Access Control (RBAC) to provide users with only the access necessary to perform their job functions. Security policies like password management, access control, and incident response need to be established and enforced (Khan, 2024). Regular vulnerability scanning and penetration testing should be conducted to actively identify and remedy security vulnerabilities. STEP's network also needs to be separated into sections like OT, R&D, business operations, and guest access to prevent attackers from lateral movement. Finally, Multi-Factor Authentication (MFA) should be applied to add another layer of protection for accessing critical systems.

4.3. Long-Term (9–18 Months)

In the long run, STEP should deploy a Zero Trust Architecture that assumes breach and verifies every access request. Adopting a Security Information and Event Management (SIEM) solution to centralize log collection and analysis for proactive detection of threats is also effective (González-Granadillo et al., 2021). The Business Continuity and Disaster Recovery procedures need to be documented and tested regularly for organizational resiliency. Simulation attacks involving Red-team and Blue-team cyber security training can also be employed to assess defense systems.

Finally, a Third-Party Risk Management Program must be established to oversee and reduce the risk of exposure from external vendors and partners.

5. Policies, Plans, and Programs to Implement

A strong cybersecurity framework requires coordinated policies, plans, and programs that address technical risks (like malware propagation and perimeter breaches), strengthen human factors (through better password hygiene and employee engagement), and build sector-specific protections for critical infrastructures. Organizations must design and implement comprehensive policies, plans, and programs to address technical, human, and organizational challenges.

5.1. Security Policies

STEP should have a strong Password Management Policy requiring secure password generation, frequent rotation, and blocking of reuse across systems. This will further protect from brute-force and credential-stuffing attacks. There should be an Acceptable Use Policy indicating what constitutes proper use of corporate hardware, networks, and software to minimize abuse and insider threat (Kizza, 2024). The Remote Work Policy should include provisions for securing connections and equipment when working remotely, like mandated use of VPN and encrypted storage. Lastly, the Access Control Policy should contain an explanation of how access is granted, monitored, and removed from systems, so users have no more access than they require to get their job done.

5.2. Security Plans

STEP should have a comprehensive Incident Response Plan that documents detailed procedures, roles, and responsibilities for detection, response, and recovery from security incidents. The plan should detail precise containment, eradication, and post-incident activities to enhance the organization's defenses (Grobler et al., 2020). There should be a Backup and Recovery Plan to ensure that all critical data is regularly backed up and that recovery steps are tested and functional. Backups should be safely stored, with at least one copy stored offline or offsite to prevent the risk of ransomware attacks and improve recovery time (Akibis et al., 2024; Chen et al., 2023). In addition, a Disaster Recovery Plan must be created outlining how STEP will restore its business after a major disruption, like a cyber-attack, natural disaster, or hardware failure. The plan must also include predetermined recovery time objectives (RTOs) and recovery point objectives (RPOs) so downtime and data loss are minimized.

5.3. Programs

Besides the core training and operations efforts, STEP should apply several advanced cybersecurity competences to strengthen its infrastructure and follow industry best practices further. Centralized Authentication and Access Control should be established, following NIST SP 800-171 guidelines (Sell & Dupuis, 2023). This will offer secure, role-based access management and help impose least privilege principles on systems.

Network Time Synchronization must be enabled on all systems and log infrastructure to ensure accurate and uniform timestamps. This is important for log correlation and forensic investigation to succeed. Network Perimeter Protection must be reinforced with Unified Threat Management (UTM) firewalls (Lekkala & Gurijala, 2024). These should also have intrusion prevention systems (IPS), web filtering, email security, and advanced threat intelligence capabilities.

Endpoint Configuration Management must be performed using tools such as Microsoft 365 Intune to provide centralized visibility, device compliance scanning, and security policy enforcement on employee devices. Vulnerability Testing must be a routine, achieved through regular internal and external testing on a scheduled basis to reveal and remedy exploitable system vulnerabilities (Lekkala & Gurijala, 2024). Data Classification and Labeling should also be implemented to discover and classify sensitive information, enabling the development of information barriers and data loss prevention (DLP) controls.

Security Monitoring through a Security Information and Event Management (SIEM) system for real-time analysis of events and alerts must be prioritized to enhance threat detection and incident response. System Hardening processes must be initiated to apply baseline security configurations to all systems, reducing attack surfaces by disabling unnecessary services and ports (Sell & Dupuis, 2023). Finally, Application Whitelisting should be implemented so that only trusted software is permitted to operate within the network, preventing the introduction and execution of unauthorized or malicious software.

Above all, STEP must implement a Security Awareness Training Program to provide employees with ongoing training on common cyber threats, safe computing practices, and how to identify and report suspicious activity. Onboarding training, periodic renewal training, and phishing tests should be included in the program to assess and reinforce learning (Reeves et al., 2021). A Security Operations Program should also be deployed to oversee day-to-day security activities like log monitoring, patching, and fulltime system and network monitoring for vulnerability or anomaly. Finally, an Audit and Compliance Program must be established to ensure STEP observes internal policies and any applicable industry regulations (Reeves et al., 2021). This program would perform regular internal audits, prepare for external assessments, and assist in maintaining a culture of accountability and continual enhancement in cybersecurity practices.

6. Conclusion

The South Texas Electrical Power (STEP) operates in an increasingly exposed cyber environment, where its activities like hybrid energy systems, remote access, and advanced R&D have numerous exposure avenues. This report identified significant risks such as ransomware, phishing, insider risk, and poor access control, as well as leading operational technology and sensitive data risks. To address these, a sequence of phased security controls was proposed, such as secure authentication, use of VPN, network segregation, and eco-friendly practices such as Zero Trust and SIEM. Tactical measures such as disaster recovery, incident response, and training of personnel have to be deployed to implement security into operations beginning from lower levels. By adopting the recommended policies and cutting-edge security software, STEP can not only secure its assets, but also pioneer cyber resiliency in the energy sector.

7. Next Steps

- Review and adopt near-term controls immediately.
- Assign a dedicated security role or outsource security operations.
- Begin policy drafting and security training programs.

Prepared by: Rick and Amjad Alqahtani
Contact Information: **ricardo.figueroa@my.utsa.edu**, Amjad.alqahtani@my.utsa.edu

References

Akibis, M., Pereira, J., Clark, D., Mitchell, V., & Alvarez, H. (2024). Measuring ransomware propagation patterns via network Traffic Analysis: an Automated approach. Research Square (Research Square). https://doi.org/10.21203/rs.3.rs-5180048/v1

Chen, J., Sun, S., Xia, C., Shi, D., & Chen, G. (2023). Modeling and analyzing malware propagation Over wireless networks based on hypergraphs. IEEE Transactions on Network Science and Engineering, 1–12. https://doi.org/10.1109/tnse.2023.3273184

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759. https://doi.org/10.3390/s21144759

Grobler, M., Chamikara, M. a. P., Abbott, J., Jeong, J. J., Nepal, S., & Paris, C. (2020). The importance of social identity on password formulations. Personal and Ubiquitous Computing, 25(5), 813–827. https://doi.org/10.1007/s00779-020-01477-1

Haimed, I. B., Albahar, M., & Alzubaidi, A. (2023). Exploiting misconfiguration vulnerabilities in Microsoft's Azure Active directory for privilege escalation attacks. Future Internet, 15(7), 226. https://doi.org/10.3390/fi15070226

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Namin, A. S. (2020). How social engineers use persuasion principles during vishing attacks. Information and Computer Security, 29(2), 314–331. https://doi.org/10.1108/ics-07-2020-0113

Khan, J. A. (2024). Role-Based access Control (RBAC) and Attribute-Based Access Control (ABAC). In Advances in information security, privacy, and ethics book series (pp. 113–126). https://doi.org/10.4018/979-8-3693-1431-9.ch005

Kizza, J. M. (2024). System Intrusion Detection and Prevention. In Texts in computer science (pp. 295–323). https://doi.org/10.1007/978-3-031-47549-8_13

Lekkala, S., & Gurijala, P. (2024). Establishing robust perimeter defenses. In Apress eBooks (pp. 133–142). https://doi.org/10.1007/979-8-8688-0823-4_13

Mansfield-Devine, S. (2021). Who's that knocking at the door? The problem of credential abuse. Network Security, 2021(2), 6–15. https://doi.org/10.1016/s1353-4858(21)00018-0

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle Cyber fatigue. SAGE Open, 11(1). https://doi.org/10.1177/21582440211000049

Sell, M., & Dupuis, M. (2023). Designing an industrial cybersecurity program for an operational technology group. Information Technology Education Conference, 125–130. https://doi.org/10.1145/3585059.3611438

Singh, A., & Gupta, B. B. (2022). Distributed Denial-of-Service (DDOS) attacks and defense mechanisms in various Web-Enabled computing platforms. International Journal on Semantic Web and Information Systems, 18(1), 1–43. https://doi.org/10.4018/ijswis.297143