Securing NERC Data: On-Premises vs. Hybrid Cloud

Suchismita Chatterjee

Cyber Security Product Specialist| M.S.-University of North Texas

Abstract

The increasing reliance on digital infrastructure in the energy sector has intensified the need to secure sensitive data, particularly in environments governed by the North American Electric Reliability Corporation (NERC) standards. This paper examines the comparative effectiveness of on-premises and hybrid cloud solutions in securing NERC Bulk Electric System Cybersecurity Information (BCSI). It explores critical factors such as compliance adherence, data sovereignty, scalability, and operational resilience. While on-premises systems offer robust control over data and infrastructure, hybrid cloud models provide flexibility and cost-efficiency, albeit with additional challenges in maintaining consistent security protocols across platforms. Through a detailed analysis of case studies and security frameworks, the paper highlights best practices for selecting and implementing secure infrastructure. The findings aim to guide energy sector stakeholders in making informed decisions that balance innovation with stringent regulatory compliance.

Keywords: NERC compliance, cybersecurity, Bulk Electric System Cybersecurity Information (BCSI), on-premises security, hybrid cloud, data sovereignty, operational resilience, cloud scalability, energy sector, regulatory compliance.

1. Introduction

The energy sector is a cornerstone of national infrastructure, making its cybersecurity requirements critical. NERC standards enforce strict regulations to protect Bulk Electric System Cybersecurity Information (BCSI), ensuring the reliability and security of the grid. As organizations strive to modernize their IT environments, they face a pivotal decision: whether to maintain an on-premises infrastructure or adopt a hybrid cloud model. This decision impacts not only their operational agility but also their ability to meet NERC compliance requirements.[5][4]

This paper explores the trade-offs between on-premises and hybrid cloud solutions in securing NERC data. By analyzing the strengths, weaknesses, and implementation considerations of each approach, the paper aims to provide actionable insights for energy sector stakeholders navigating this complex landscape.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are a set of mandatory cybersecurity standards designed to protect the critical infrastructure of the North American electric utility industry. These standards aim to secure the operational technology (OT) used in generating, transmitting, and distributing electric power. With the increasing reliance on data and digital technologies in the energy sector, ensuring the security of NERC data is paramount.[7][6]

The NERC CIP standards are pivotal for maintaining the reliability and security of the North American bulk power system. Since their introduction in 2006, the standards have evolved to address emerging threats, technologies, and best practices. There are 15 CIP standards that cover various aspects of cybersecurity, specifying minimum controls and processes for power generation and transmission companies to ensure the reliability and security of the North American power grid.

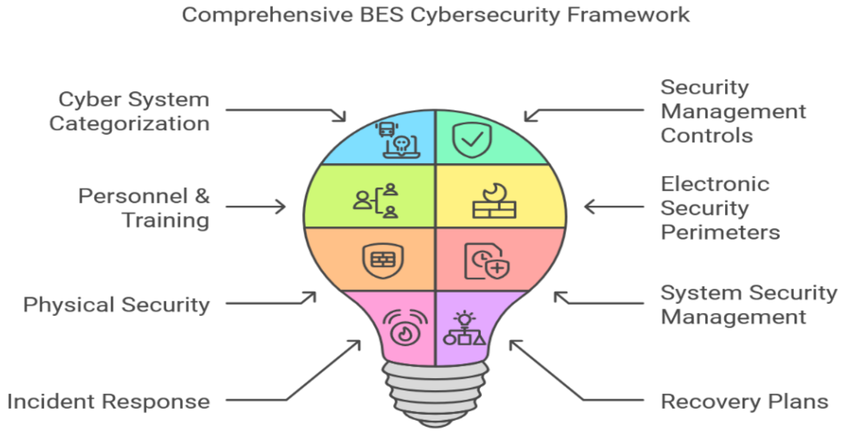
The core objective of NERC CIP is to safeguard Bulk Electric System (BES) Cyber System Information (BCSI) and "critical assets" from unauthorized access and security risks. Critical assets are defined as facilities, systems, and equipment that, if compromised, could impact the reliability or operability of the BES.[4]

NERC CIP standards require the implementation of cybersecurity hygiene practices, such as patch management, robust authentication, and measures to prevent malicious code. They also address issues like the use of removable media, transient assets, and supply chain security, recognizing the significance of these areas in maintaining a secure environment.

Here's a concise summary of the 12 critical infrastructure protection requirements outlined in NERC CIP:

- CIP-002-5.1a BES Cyber System Categorization: Identify and categorize BES cyber assets to apply appropriate cybersecurity requirements based on their potential impact on the BES.
- CIP-003-8 Security Management Controls: Establish consistent security management controls with clear responsibility and accountability to protect BES Cyber Systems.
- CIP-004-6 Personnel & Training: Enforce personnel risk assessments, training, and security awareness to minimize the risk of compromise from individuals accessing BES Cyber Systems.
- CIP-005-7 Electronic Security Perimeter(s): Manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP).
- CIP-006-6 Physical Security of BES Cyber Systems: Manage physical access to BES Cyber Systems by specifying a physical security plan.
- CIP-007-6 System Security Management: Manage system security by specifying technical, operational, and procedural requirements.
- CIP-008-6 Incident Reporting and Response Planning: Specify incident response requirements to mitigate the risk of cybersecurity incidents.
- CIP-009-6 Recovery Plans for BES Cyber Systems: Specify recovery plan requirements to support the continued stability and reliability of the BES.
- CIP-010-4 Configuration Change Management and Vulnerability Assessments: Specify configuration change management and vulnerability assessment requirements to prevent unauthorized changes.
- CIP-011-2 Information Protection: Specify information protection requirements to prevent unauthorized access to BES Cyber System Information.
- CIP-012-1 Communications Between Control Centers: Protect the confidentiality and integrity of data transmitted between control centers.
- CIP-013-2 Supply Chain Risk Management: Implement security controls for supply chain risk management of BES Cyber Systems.

Figure 1: Comprehensive BES Cybersecurity Framework


Comprehensive BES Cybersecurity Framework
Cyber System Categorization
Security Management Controls
Personnel & Training
Electronic Security Perimeters
Physical Security
System Security Management
Incident Response
Recovery Plans

1.1 On-Premises Data Centers

On-premises data centers are facilities owned and operated by an organization, where IT infrastructure and data are stored within the organization’s physical premises. This approach provides direct control over security measures and data access but also presents unique security challenges that must be addressed to ensure the protection of critical NERC data.[3]

Securing on-premises data centers involves several key strategies and best practices. Controlling physical access to the data center is fundamental. Organizations should implement multi-layered access control systems, such as biometric locks, access cards, and surveillance systems. Conducting background checks for employees and contractors is also essential to enhance physical security. Network security is another critical aspect, requiring robust protection of both the network perimeter and internal network segments to prevent unauthorized access and lateral movement within the network. This includes the deployment of firewalls, intrusion detection systems, and effective network segmentation.

Data protection is vital for securing NERC data at rest and in transit. Implementing encryption, data loss prevention (DLP) technologies, and secure backup and recovery mechanisms are critical components for safeguarding sensitive information. Vulnerability management is equally important, involving regular security assessments, vulnerability scanning, and timely patching to identify and address security weaknesses in on-premises systems and applications.[10]

Addressing personnel security is essential to mitigate the risks of human error and insider threats. Organizations should adopt strong authentication mechanisms, such as multi-factor authentication (MFA), and invest in security awareness training for employees. Additionally, layered security defenses play a crucial role in protecting data centers from evolving threats. By implementing multiple layers of security, organizations ensure that an attacker must breach several barriers to access sensitive data, aligning with the principles of the "Zero Trust" framework.

By integrating these measures, organizations can create a resilient and secure environment for on-premises data centers, effectively safeguarding critical NERC data against a wide array of threats.

1.2 Hybrid Cloud Environments

Hybrid cloud environments, which combine on-premises infrastructure with cloud services, offer the benefits of flexibility and scalability while maintaining some level of control over critical data. However, securing these environments, particularly for NERC data, requires addressing unique challenges and implementing tailored best practices.[11]

The complexity of managing security across both on-premises and cloud environments necessitates effective coordination and integration of security tools and policies. Ensuring visibility and control over data and resources throughout the hybrid environment is vital for security monitoring and incident response. This includes the ability to thoroughly inspect security environments and promptly identify emerging vulnerabilities. Protecting sensitive NERC data in the cloud while adhering to compliance requirements is a top priority, as is understanding the shared responsibility model for cloud security. Organizations must secure their data and applications, while cloud providers handle the security of the underlying infrastructure.

To address these challenges, organizations should adopt unified security solutions that provide comprehensive visibility and control across both on-premises and cloud environments. A zero-trust architecture, which involves continuous verification of users and devices, is instrumental in minimizing the attack surface and limiting potential damage. Robust encryption of data at rest and in transit across the hybrid environment is crucial for protecting sensitive information. Centralized monitoring tools and processes are essential for detecting and responding to threats effectively.

Regular security audits and vulnerability assessments are critical for identifying and mitigating security gaps. Automating security processes, such as vulnerability scanning and patch management, can enhance efficiency and reduce the risk of human error. A comprehensive disaster recovery plan that accounts for both on-premises and cloud environments ensures business continuity in case of disruptions. Secure network connections between on-premises and cloud systems should be established using Virtual Private Network (VPN) tunnels or dedicated private connections, and network topology should be carefully reviewed. Secrets management practices, such as rotating credentials and certificates, help prevent data leaks.[15][5]

Additionally, ensuring secure communication between cloud and on-premises environments requires implementing robust encryption and authentication mechanisms for data in transit. For legacy OT devices that may lack modern security features, organizations should employ network segmentation, access controls, and regular vulnerability assessments to mitigate risks effectively.

By implementing these best practices, organizations can establish a robust security posture in hybrid cloud environments, protecting critical NERC data and maintaining compliance with regulatory standards.[2][5]

2. Comparing On-Premises and Hybrid Cloud Security for NERC Data

Securing NERC data is critical for maintaining the reliability of the North American power grid. Both on-premises and hybrid cloud environments present unique security advantages and challenges. A comparative analysis of these two approaches can help organizations determine the most suitable strategy for their needs.

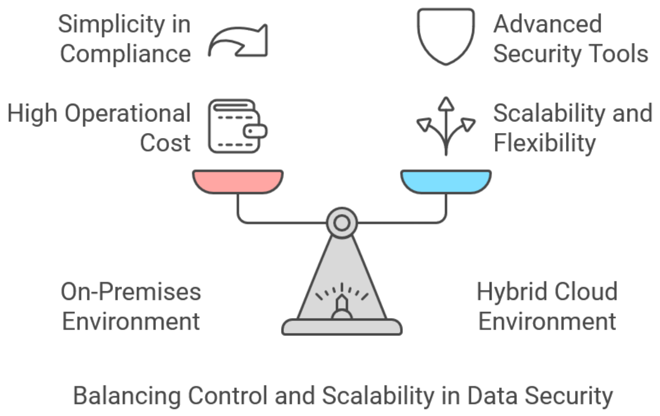
- **Control and Ownership**
  - On-Premises: Organizations have full control over the physical infrastructure, data storage, and security configurations. This direct control simplifies compliance with NERC standards but requires significant investment in resources and expertise.
  - Hybrid Cloud: While on-premises components maintain some control, cloud providers manage the underlying infrastructure. Organizations must work within the shared responsibility model, balancing their security obligations with those of the cloud provider.
- **Scalability and Flexibility**
  - On-Premises: Scaling resources in response to demand is limited by the capacity of the existing infrastructure, often requiring costly upgrades.
  - Hybrid Cloud: Offers dynamic scalability and flexibility, enabling organizations to adapt to fluctuating workloads while still retaining control over critical on-premises data.
- **Physical Security**
  - On-Premises: Physical security is entirely the organization's responsibility. This requires implementing measures such as multi-factor access controls, surveillance, and employee background checks.
  - Hybrid Cloud: While physical security for cloud infrastructure is managed by the provider, organizations remain responsible for securing their on-premises components.
- **Cybersecurity and Network Security**
  - On-Premises: Network security is centralized, which simplifies oversight but can create single points of failure. Organizations manage firewalls, intrusion detection systems, and segmentation to protect the network.
  - Hybrid Cloud: Extends security challenges across multiple environments. A unified security strategy, leveraging encryption, zero-trust principles, and centralized monitoring, is critical to prevent vulnerabilities from cloud-to-on-premises interactions.
- **Data Protection and Compliance**
  - On-Premises: Data resides entirely within the organization’s environment, simplifying compliance with NERC CIP standards but requiring robust encryption, backup solutions, and access controls.
  - Hybrid Cloud: Ensuring data security and compliance requires implementing encryption, secure data transfer mechanisms, and adhering to cloud provider compliance certifications.

- **Resource Allocation**
  - On-Premises: Security is resource-intensive, requiring dedicated staff for maintenance, monitoring, and incident response.
  - Hybrid Cloud: Allows organizations to leverage cloud providers' expertise and resources, reducing the internal burden but requiring careful management of hybrid security strategies.
- **Threat Detection and Incident Response**
  - On-Premises: Relies on in-house tools and personnel to detect and respond to threats. Incident response times may vary based on resource availability and expertise.
  - Hybrid Cloud: Offers access to advanced tools, such as AI-driven threat detection and managed security services. Centralized monitoring solutions can help bridge on-premises and cloud environments for faster responses.
- **Cost Implications**
  - On-Premises: High initial investment for infrastructure and ongoing operational costs for maintenance, upgrades, and security measures.
  - Hybrid Cloud: Lower upfront costs with flexible pay-as-you-go models, but managing hybrid environments can introduce hidden costs in integration and monitoring.

Table 1: Comparison of On-Premises vs Hybrid Cloud

Feature	On-Premises	Hybrid Cloud
Control	Full control over data and infrastructure.	Shared responsibility model with cloud provider, partial control over cloud infrastructure.
Cost	High upfront investment in hardware and infrastructure, ongoing maintenance costs.	Pay-as-you-go model for cloud services, potentially lower upfront costs but variable ongoing expenses.
Scalability	Limited scalability; requires significant investment and effort to expand infrastructure.	Highly scalable; can easily adjust resources as needed without major upfront costs.
Compliance	Full responsibility for meeting compliance requirements, including NERC CIP standards.	Shared responsibility for compliance; organization ensures data and app security while the cloud provider manages infrastructure.
Operational Efficiency	Can be less efficient due to manual processes and in-house maintenance.	Can be more efficient with automation, cloud services, and external security tools.
Security	Direct control over security measures, but requires dedicated resources for management.	Relies on a combination of on-premises and cloud security controls, requiring integration of both security strategies.
Data Residency	Data remains entirely within the organization's physical premises, making it easier to meet compliance.	Data may be stored in geographically diverse cloud locations, potentially introducing compliance complexity.
Performance	Can offer high performance with dedicated resources and no network latency issues.	Performance can be affected by network latency and cloud service availability, though cloud resources may scale to meet demand.

Figure 2: Balancing Control and Scalability in Data Security



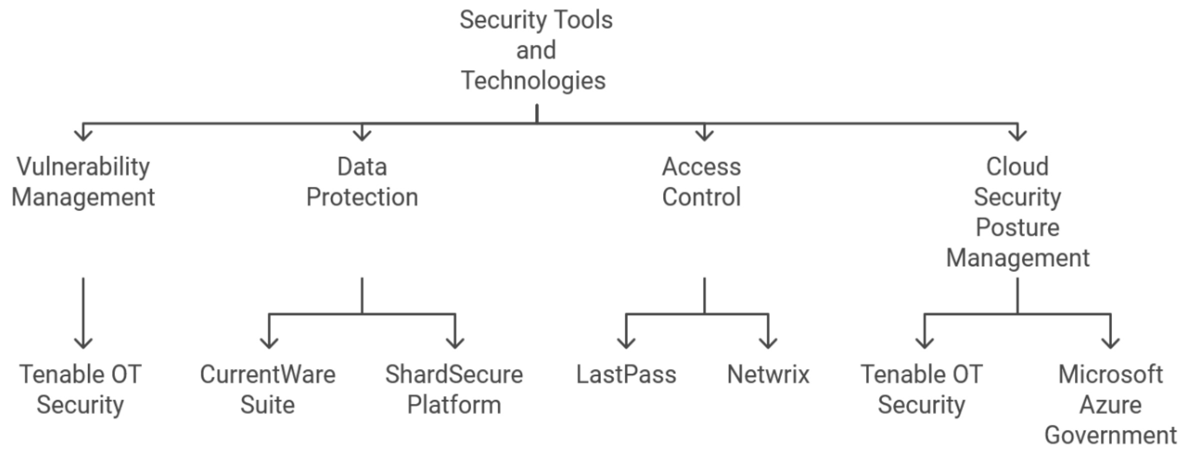
3. Security Tools and Technologies for Protecting NERC Data

To effectively secure NERC data in both on-premises and hybrid cloud environments, organizations can utilize various security tools and technologies. These tools can be categorized based on their core functions, providing essential protection for critical data.

- Tenable OT Security: This tool offers comprehensive vulnerability management capabilities for both on-premises and hybrid cloud environments. It helps identify and remediate vulnerabilities in operational technology (OT), ensuring the security of critical infrastructure.
- CurrentWare Suite: This suite provides data loss prevention (DLP) and endpoint security features designed for on-premises environments. It enables organizations to monitor and control data access, preventing unauthorized data exfiltration or leakage.
- ShardSecure Platform: ShardSecure offers robust data encryption and ransomware protection, particularly suited for hybrid and multi-cloud environments. This platform helps protect sensitive data while enabling flexible cloud storage solutions.
- LastPass: A popular solution for secure credential storage and role-based access control, LastPass helps organizations manage authentication and user privileges in both on-premises and hybrid cloud environments.
- Netwrix: This tool enhances visibility into access events and aids in the detection of anomalies within on-premises systems. It helps organizations monitor and enforce proper access controls, ensuring only authorized users can access critical data.
- Tenable OT Security: In addition to its vulnerability management features, Tenable OT Security also provides cloud security posture management capabilities for hybrid environments, enabling organizations to secure cloud resources while maintaining control over their on-premises systems.
- Microsoft Azure Government: This platform offers a FedRAMP High-authorized cloud environment with enhanced security features tailored for protecting NERC data. It provides a secure, compliant infrastructure for organizations working with sensitive data in the cloud.
- Cloud-based security tools such as Security Information and Event Management (SIEM) systems and next-generation antivirus (NGAV) solutions often provide cost-effective alternatives to on-premises solutions. By leveraging the scalability and flexibility of cloud services, these tools can offer advanced security features at a lower cost. The ability to scale security operations in response to emerging threats further enhances the efficiency of cloud-based solutions.

Incorporating these tools into a comprehensive security strategy helps organizations safeguard NERC data, ensuring both on-premises and hybrid cloud environments remain secure and compliant with regulatory standards.

Figure 3: Security Tools and Technologies



4. Factors to Consider

When comparing on-premises and hybrid cloud approaches for securing NERC data, several key factors should be considered. First, the cost of on-premises solutions typically involves high upfront capital expenditures (CAPEX) for hardware, software, and infrastructure. In contrast, hybrid cloud solutions can offer significant cost savings by utilizing the pay-as-you-go model of cloud services, which reduces the need for extensive on-premises infrastructure. Regarding scalability, on-premises solutions have limited capacity, requiring substantial investment to expand resources, while hybrid cloud solutions provide greater scalability, enabling organizations to easily adjust cloud resources as needed. Both approaches require organizations to meet NERC CIP compliance requirements, although hybrid cloud solutions may involve shared responsibility with the cloud provider. In terms of operational efficiency, on-premises solutions can be less efficient due to the need for manual processes and ongoing maintenance, whereas hybrid cloud solutions enhance operational efficiency through automation and the use of cloud services. These factors are essential for organizations to evaluate when deciding between on-premises and hybrid cloud strategies for securing NERC data.

In addition to cost, scalability, compliance, and operational efficiency, several other factors are important when evaluating on-premises versus hybrid cloud solutions for securing NERC data. One such factor is security. On-premises solutions provide organizations with direct control over their security measures, enabling them to implement and customize protections based on their specific needs. However, this also places the burden of managing and maintaining security on the organization. In contrast, hybrid cloud environments offer a combination of on-premises and cloud security controls, leveraging cloud provider security measures and enabling organizations to focus on critical aspects of their infrastructure.[17][14]

Data residency is another key consideration. On-premises solutions ensure that data remains within the organization’s physical control, which can be essential for meeting regulatory and compliance requirements. Hybrid cloud solutions, on the other hand, may involve data being stored in geographically diverse locations, raising concerns around jurisdictional and compliance issues.

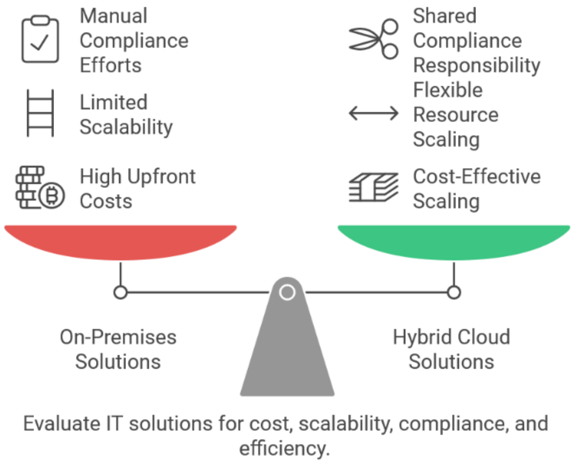
Performance is also a critical factor. On-premises solutions often deliver high performance with dedicated resources, which is essential for organizations with high-throughput requirements. However, performance in hybrid cloud environments can be influenced by network latency and cloud service availability, which could impact the speed and reliability of accessing NERC data.

Finally, disaster recovery and business continuity are vital elements to consider. On-premises environments typically require organizations to build and maintain their own disaster recovery strategies, which can be resource-intensive. Hybrid cloud solutions can offer built-in disaster recovery features provided by cloud service providers, allowing for faster recovery times and more efficient continuity planning.[2][3]
These additional factors further highlight the importance of a comprehensive evaluation when choosing the best approach for securing NERC data. Depending on the organization's priorities—whether it's control, performance, security, or disaster recovery—both on-premises and hybrid cloud solutions offer distinct advantages and challenges.

Table 2: Factors to consider in On-Premises and Hybrid Cloud Approaches for Securing NERC Data

Factor	On-Premises	Hybrid Cloud
Cost	High upfront capital expenditures for hardware, software, and infrastructure.	Pay-as-you-go model reduces the need for extensive on-premises infrastructure, offering cost savings.
Scalability	Limited scalability; requires significant investment to expand resources.	Highly scalable; can easily adjust cloud resources as needed.
Compliance	Full responsibility for meeting NERC CIP compliance requirements.	Shared responsibility for compliance with the cloud provider.
Operational Efficiency	Can be less efficient due to manual processes and ongoing maintenance.	Improved efficiency through automation and use of cloud services.
Security	Direct control over all security measures; fully customizable but resource-intensive to maintain.	Combines on-premises and cloud security controls; leverages provider’s built-in protections.
Data Residency	Data remains within the organization’s physical control, ensuring full ownership.	Data may be stored in geographically diverse locations, raising potential jurisdictional concerns.
Performance	High performance with dedicated resources; ideal for high-throughput needs.	Performance can be affected by network latency and cloud service availability.
Disaster Recovery	Requires building and maintaining dedicated disaster recovery solutions on-premises.	Offers built-in disaster recovery features and faster recovery through cloud providers.
Flexibility	Limited to the organization’s infrastructure and capabilities.	Offers flexibility to adopt new technologies and integrate services seamlessly.
Resource Management	Requires dedicated IT teams for management and maintenance.	Frees up internal resources by outsourcing infrastructure management to cloud providers.
Innovation	Slower adoption of innovative technologies due to infrastructure constraints.	Faster access to advanced technologies and tools provided by the cloud.

Figure 4: Factors to consider


Manual Compliance Efforts
Limited Scalability
High Upfront Costs
Shared Compliance Responsibility
Flexible Resource Scaling
Cost-Effective Scaling
On-Premises Solutions
Hybrid Cloud Solutions
Evaluate IT solutions for cost, scalability, compliance, and efficiency.

5. Conclusion

Choosing between on-premises and hybrid cloud for securing NERC data depends on various factors, including the organization's specific needs, risk tolerance, budget, and compliance requirements. On-premises solutions offer greater control and potentially higher security but require significant upfront investment and can be less scalable. Hybrid cloud solutions provide flexibility, scalability, and cost-effectiveness but require careful planning and management to ensure data security and compliance.

Organizations should carefully evaluate the advantages and disadvantages of each approach, considering factors such as the sensitivity of NERC data, compliance requirements, budget constraints, scalability needs, in-house expertise, and risk tolerance. Conducting a thorough risk assessment and developing a tailored security strategy based on these factors is crucial.

Ultimately, the best approach is to develop a comprehensive security strategy that aligns with the organization's overall business objectives and risk management framework. The evolving threat landscape and the critical role of the energy sector in modern society underscore the importance of securing NERC data to maintain a reliable and secure power grid.

6. References

1. Brown, Nick, et al. "A highly scalable Met Office NERC Cloud model." arXiv preprint arXiv:2009.12849 (2020).
2. Brown, Nick, et al. "A directive based hybrid met office nerc cloud model." Proceedings of the Second Workshop on Accelerator Programming using Directives. 2015.
3. Brown, Nick. "Exploring the acceleration of the Met Office NERC cloud model using FPGAs." High Performance Computing: ISC High Performance 2019 International Workshops, Frankfurt, Germany, June 16-20, 2019, Revised Selected Papers 34. Springer International Publishing, 2019.
4. Christensen, Dane, et al. "Risk assessment at the edge: Applying NERC CIP to aggregated grid-edge resources." The Electricity Journal 32.2 (2019): 50-57.
5. Kingdon, Andrew, Jeremy RA Giles, and Jonathan P. Lowndes. "Future of technology in NERC data models and informatics: outputs from InformaTEC." Geological Society, London, Special Publications 408.1 (2017): 245-253.
6. Zhang, Song, Xiaochuan Luo, and Eugene Litvinov. "Serverless computing for cloud-based power grid emergency generation dispatch." International Journal of Electrical Power & Energy Systems 124 (2021): 106366.

7. Anderson, Dave, et al. "GridCloud: infrastructure for cloud-based wide area monitoring of bulk electric power grids." IEEE Transactions on Smart Grid 10.2 (2018): 2170-2179.
8. Luo, Xiaochuan, Song Zhang, and Eugene Litvinov. "Practical design and implementation of cloud computing for power system planning studies." IEEE Transactions on Smart Grid 10.2 (2018): 2301-2311.
9. Groom, Steve, et al. "The NERC Earth Observation Data Acquisition and Analysis Service (NEODAAS)–a new partnership for supporting the UK academic community." Proceedings of the Remote Sensing Society Conference Reading, UK. 2006.
10. Weaver, Gabriel A., et al. "Toward a cyber-physical topology language: Applications to NERC CIP audit." Proceedings of the first ACM workshop on Smart energy grid security. 2013.
11. Cissé, Moh. "Third-party risk management: Strategy to mitigate 'on-premise'and 'cloud'cyber security risks." Cyber Security: A Peer-Reviewed Journal 3.2 (2019): 103-115.
12. El Alloussi, Hassan, Laila Fetjah, and Abdelhak Chaichaa. "Securing Card data on the Cloud." International Journal on Advances in Security Volume 9, Number 1 & 2, 2016 (2016).
13. Akinade, Sarat Kehinde. "Database as a service: Security and privacy issues, and appropriate controls." (2020).
14. Zhang, Song, et al. "Big data analytics platform and its application to frequency excursion analysis." 2018 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2018.
15. Akinbi, Olushola Alexander. An Adaptive Security Framework for Evaluating and Assessing Security Implementations in PaaS Cloud Models. Diss. Edge Hill University, 2015.
16. Hurd, Carl M., and Michael V. McCarty. A survey of security tools for the industrial control system environment. No. INL/EXT-17-42229. Idaho National Lab.(INL), Idaho Falls, ID (United States), 2017.
17. Popović, Nemanja D., Dragan S. Popović, and Ivan Seskar. "A novel cloud-based advanced distribution management system solution." IEEE Transactions on Industrial Informatics 14.8 (2017): 3469-3476.
18. Ismail, U. Framework for Security Transparency in Cloud Computing. Diss. University of East London, 2020.