International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Anticipation of Key Challenges of Implementing Emerging Automation Tools for Vulnerability Management and Risk Assessment in a NERC Environment

Suchismita Chatterjee

DevSecOps Consultant | M.S. University of North Texas

Abstract:
The North American Electric Reliability Corporation (NERC) plays a vital role in safeguarding the North American power grid. This organization is responsible for developing and enforcing reliability standards, conducting risk assessments, and ensuring the secure operation of the Bulk Electric System (BES).
To address the increasing threat of cyberattacks and physical security breaches, NERC established the Critical Infrastructure Protection (CIP) reliability standards. These standards provide a framework for protecting critical infrastructure, including power plants, transmission lines, and control systems, from potential disruptions. Entities responsible for maintaining the reliability of the power grid face numerous challenges in complying with NERC CIP standards. These challenges include an ever-evolving threat landscape, complex technical requirements, and the need for continuous improvement.
Emerging automation tools offer a promising solution to these challenges by streamlining compliance, enhancing security, and mitigating risks. However, implementing these tools in NERC environments presents unique challenges that must be carefully considered. This paper anticipates the key challenges of implementing emerging automation tools for vulnerability management and risk assessment in NERC environments. Challenges include production sensitivity, cost/feature mismatch, labour mismatch, safety concerns, customized mitigation, and prioritization of vulnerabilities for vulnerability management. Challenges for risk assessment include complex systems integration, viability of integrating automation, and it's monitoring and adaptation, ongoing training and standardization, vendor risk assessments, and data breach notification. Despite these challenges, automation tools offer significant benefits, including improved security, reduced risk, increased efficiency, cost savings, and enhanced system performance. The report also provides an overview of emerging automation tools, relevant NERC CIP requirements, the impact of automation on existing security processes, potential risks and vulnerabilities, and best practices for successful implementation. The question is are we there yet to anticipate a fully commissioned automated system for NERC environment and evaluating the feasibility of minimalizing the human interference—How much caution is enough to mitigate attack and its key challenges.

Keywords: NERC CIP, Automation Tools, Vulnerability Management, Risk Assessment, Cybersecurity, Critical Infrastructure Protection, Power Grid, Reliability Standards, Best Practices, Emerging Threats

1. Introduction

The North American Electric Reliability Corporation (NERC) serves as a critical body for ensuring the reliability and security of the North American power grid. To mitigate risks associated with cyberattacks, physical threats, and other vulnerabilities, NERC's Critical Infrastructure Protection (CIP) standards provide a robust framework for safeguarding critical infrastructure. However, as the complexity and scale of threats continue to evolve, traditional approaches to vulnerability management and risk assessment are often insufficient to address these challenges effectively.

Emerging automation tools have the potential to revolutionize these processes by enhancing efficiency, accuracy, and responsiveness in identifying and mitigating vulnerabilities. These tools can streamline compliance efforts, reduce human error, and enable real-time risk assessments, ensuring that organizations maintain robust security postures. Despite their advantages, implementing these advanced solutions in a NERC-regulated environment poses significant challenges. These challenges include integrating automation within legacy systems, meeting strict regulatory requirements, and managing potential operational disruptions. This paper explores the key challenges associated with implementing emerging automation tools for vulnerability management and risk assessment within the NERC environment.

By anticipating these challenges, organizations can develop effective strategies to harness the benefits of automation while maintaining compliance and ensuring the continued reliability and security of critical infrastructure.

Critical Infrastructure Protection (CIP) standards play a pivotal role in safeguarding essential systems and services that underpin society's daily operations. In the context of the North American Electric Reliability Corporation (NERC), these standards are designed to protect the Bulk Electric System (BES) from an array of threats, including cyberattacks, physical security breaches, and natural disasters. The importance of CIP standards lies in their structured approach to identifying, mitigating, and managing vulnerabilities and risks, ensuring the reliability and resilience of critical infrastructure.

- Proactive Risk Management: CIP standards provide a systematic framework for identifying vulnerabilities in critical systems, assessing associated risks, and implementing mitigation strategies. By requiring organizations to adopt proactive measures, such as regular vulnerability assessments, risk analysis, and incident response planning, these standards minimize the likelihood of disruptive events and their potential impact on the power grid.[1]
- Enhanced Cybersecurity Posture: As cyber threats targeting critical infrastructure become increasingly sophisticated, CIP standards serve as a cornerstone for robust cybersecurity. They mandate the implementation of advanced security measures, such as access controls, network segmentation, and encryption, to protect sensitive data and systems. This ensures that the BES remains resilient against evolving cyber threats.[5]
- Regulatory Compliance and Accountability: NERC CIP standards establish clear requirements and guidelines for organizations, promoting accountability and ensuring consistent security practices across the industry. Compliance audits and enforcement mechanisms encourage entities to prioritize security and continuously improve their defense mechanisms.[11]
- Resilience Against Physical Threats: In addition to cyber risks, CIP standards address physical security by requiring organizations to protect critical facilities and infrastructure from unauthorized access, vandalism, and natural disasters. This dual focus ensures a holistic approach to safeguarding the BES.[2]

- Continuous Improvement and Adaptability: The dynamic nature of threats to critical infrastructure necessitates ongoing adaptation. CIP standards are designed to evolve with emerging challenges, encouraging entities to adopt innovative technologies and practices. This adaptability ensures that organizations remain prepared for future risks.
- Protection of Public Safety and Economic Stability: A secure and reliable power grid is essential for public safety, economic stability, and national security. CIP standards help mitigate the risks of large-scale outages, which could have cascading effects on industries, communities, and governments.[6]

As the complexity and frequency of threats to critical infrastructure grow, traditional manual methods for vulnerability management and risk assessment often fall short of meeting the speed and scale required to ensure security. Emerging automation tools are revolutionizing how organizations identify, prioritize, and mitigate vulnerabilities, providing a robust solution for enhancing these processes within NERC-regulated environments.

- Improved Speed and Efficiency: Automation tools can rapidly scan and assess vast IT and OT infrastructures, identifying vulnerabilities in real time. Unlike manual processes, which can be time-consuming and prone to delays, these tools enable continuous monitoring, ensuring that risks are detected and addressed promptly.[15]
- Real-Time Risk Assessment: Automation technologies leverage real-time data collection and advanced analytics to assess risks dynamically. This capability allows organizations to prioritize vulnerabilities based on their potential impact, focusing resources on addressing the most critical threats.[4]
- Consistency and Accuracy: Human error is a common challenge in vulnerability management. Automated tools minimize the risk of oversight by standardizing processes and performing repetitive tasks with high precision. This ensures consistent and reliable assessments across complex systems.[8]
- Integration with Threat Intelligence: Modern automation tools often integrate with threat intelligence platforms, enabling organizations to stay ahead of emerging threats. By correlating vulnerability data with external threat intelligence, these tools enhance situational awareness and improve the organization's ability to respond to new risks.
- Enhanced Compliance with NERC CIP Standards: Automation tools streamline compliance efforts by automating the documentation, reporting, and auditing processes required by NERC CIP standards. They can generate detailed reports, track remediation efforts, and maintain audit trails, reducing the burden of manual compliance tasks while ensuring adherence to regulatory requirements.[13]
- Predictive Analytics and Machine Learning: Many emerging tools incorporate advanced technologies such as machine learning and predictive analytics. These capabilities enable the tools to identify patterns, predict potential vulnerabilities, and recommend proactive measures, moving beyond reactive risk management to a preventive approach.[2]
- Scalability and Adaptability: Automation tools are designed to scale with the organization, making them suitable for managing both small and large infrastructures. Their flexibility allows them to adapt to diverse environments, including legacy systems and hybrid networks common in NERC-regulated entities.[12]
- Cost-Effectiveness: By reducing the time and resources required for manual vulnerability assessments and compliance tasks, automation tools can lower operational costs while increasing the overall efficiency of security teams.[15]

Table 1. Emerging automation tools are available for vulnerability management

Tool	Description	Key Features	Limitations
Intruder	A comprehensive vulnerability scanning tool designed for continuous monitoring.	Continuous vulnerability scanning, attack surface monitoring, vulnerability prioritization.	May not be suitable for organizations with limited security expertise.
Astra Pentest	A platform that offers a combination of automated and manual penetration testing.	Comprehensive vulnerability scanning, detailed reporting, integration with other security tools.	Can be expensive for smaller organizations.
Prevalent	A tool that focuses on third-party vendor risk assessments.	Automates vendor risk assessments, provides risk scoring, integrates with vendor management systems.	May require significant customization to meet specific needs.
Nucleus	A platform that helps organizations manage compliance with multiple frameworks.	Automates compliance assessments, provides real-time monitoring, offers remediation guidance.	Can be complex to implement and configure.
Arctic Wolf	A managed detection and response service that provides 24/7 security monitoring.	Continuous security monitoring, threat detection and response, vulnerability management.	Can be costly for smaller organizations.
IBM Security QRadar EDR	A comprehensive threat intelligence platform that helps organizations identify and respond to threats.	Real-time threat detection, advanced analytics, integration with other security tools.	Can be complex to deploy and manage.
Qualys VMDR	A cloud-based vulnerability management solution that offers robust reporting and prioritization features.	Automated vulnerability scanning, risk scoring, remediation tracking.	Requires internet connectivity for full functionality.
InsightVM (Nexpose)	A tool that provides real-time end-to-end visibility into vulnerabilities.	Continuous vulnerability scanning, asset discovery, remediation planning.	Can be resource-intensive.

FireCompass	A continuous and automated red teaming and attack surface management platform.	Real-time vulnerability management, AI-powered analytics, integrated workflows.	May require specialized expertise to fully utilize its capabilities.

1. Overview of NERC CIP Standards

The North American Electric Reliability Corporation (NERC) plays a central role in safeguarding the Bulk Electric System (BES) across North America, ensuring its reliable and secure operation. The Critical Infrastructure Protection (CIP) standards are a cornerstone of NERC's mission, providing a structured framework to protect critical infrastructure from cyber and physical threats. [1,4]

NERC's primary mission is to develop and enforce standards that ensure the reliability and security of the BES. Within this mission, the CIP standards are designed to protect critical infrastructure by:

- Identifying and categorizing critical cyber assets essential for BES reliability.
- Establishing mandatory security controls and processes for asset protection.
- Providing a compliance framework to guide entities in securing their operations.

The CIP framework is built on a series of standards (e.g., CIP-002 through CIP-013), each addressing specific aspects of cybersecurity, such as asset identification, access management, incident response, and supply chain risk management. Collectively, these standards offer a comprehensive approach to mitigating risks and ensuring resilience.[6]

The evolving threat landscape and the stringent requirements of compliance create a multifaceted challenge for organizations operating within NERC-regulated environments. Cyber threats targeting critical infrastructure are becoming increasingly sophisticated, often leveraging advanced techniques to bypass traditional security controls. This escalation in threat complexity requires organizations to adopt proactive and innovative approaches to safeguard their systems. Additionally, the rapid pace of technological advancements, including the widespread adoption of IoT devices and smart grid technologies, introduces new vulnerabilities that complicate the security landscape further.

Compliance with NERC CIP standards, while essential, can also be resource-intensive and demanding. Organizations must dedicate significant time and effort to meet the rigorous requirements of vulnerability assessments, patch management, and incident response protocols. The continuous need to maintain up-to-date compliance documentation and prepare for periodic audits adds another layer of complexity. Furthermore, many entities face resource constraints, with limited budgets and skilled personnel to implement and sustain the necessary security measures. [7,18]

These challenges are compounded by the dynamic nature of the regulatory environment, where updates to CIP standards require organizations to adapt their security practices swiftly. Balancing the need to comply with evolving standards while addressing emerging threats remains a significant hurdle for ensuring the resilience and reliability of critical infrastructure.

NERC CIP standards encompass various technical requirements that can be challenging to implement. Organizations need to address physical security, cybersecurity, and incident response planning. Specific NERC CIP requirements relevant to automation tools include:

CIP Standard	Description	Relevance to Automation
CIP-002-5.1a	Requires entities to categorize BES Cyber Systems as high, medium, or low impact.	Automation tools can help with the categorization process by automatically identifying and classifying assets based on their criticality and potential impact on the BES.[1]
CIP-003-7	Requires the development and implementation of a cybersecurity program.	Automation tools can support the implementation and management of cybersecurity programs by automating tasks such as policy enforcement, vulnerability scanning, and security awareness training.[7]
CIP-005-6	Requires the establishment of an Electronic Security Perimeter (ESP) to protect critical cyber assets.	Automation tools can help monitor and enforce the ESP by automatically detecting and blocking unauthorized access attempts and alerting security personnel to potential breaches.[6]
CIP-007-6	Requires the implementation of System Security Management controls, including access controls, security patch management, and malicious code detection.	Automation tools can automate many of the tasks associated with System Security Management, such as user access management, patch deployment, and malware scanning.[3]
CIP-008-5	Requires the development and implementation of an incident response plan.	Automation tools can assist in incident response by automating tasks such as threat detection, alert correlation, and incident reporting.[7]
CIP-009-6	Requires the development and implementation of recovery plans for BES Cyber Systems.	Automation tools can support recovery efforts by automating tasks such as system backups, data restoration, and failover procedures.[2]
CIP-010-5	Requires the implementation of Configuration Change Management and Vulnerability Assessments[16]. This standard requires entities to conduct vulnerability assessments, including paper vulnerability assessments (PVA)	Automation tools can automate vulnerability scanning, configuration assessment, and change management processes, helping organizations comply with CIP-010-5 requirements.[4]

	annually and active vulnerability assessments (AVA) every three years.	
CIP-013-1	Requires the development and implementation of supply chain cybersecurity risk management plans.	Automation tools can support supply chain risk management by automating vendor risk assessments, monitoring vendor security posture, and enforcing security requirements in vendor contracts.[5]

2. Key Challenges of Implementing Automation Tools in NERC Environments

Implementing automation tools in NERC-regulated environments for vulnerability management and risk assessment offers significant benefits, but it also presents several critical challenges. These challenges stem from the unique characteristics of operational technology (OT) environments and the stringent requirements of the Critical Infrastructure Protection (CIP) standards.

For vulnerability management, one of the primary challenges is the sensitivity of production environments. NERC environments manage critical infrastructure, and disruptions caused by traditional vulnerability scanning methods can jeopardize the stability of the power grid. Active scanning, in particular, poses risks of interfering with operations, making it essential to adopt solutions specifically designed for OT environments [1,4,7]. Additionally, there is often a mismatch between the cost and features of many automation tools. High-end solutions may include functionalities unnecessary for smaller entities, leading to increased costs and operational complexity. Organizations must carefully assess their specific needs and choose tools that align with their operational scale and requirements.

Another significant challenge lies in labour and expertise. While automation tools can reduce the manual workload associated with vulnerability management, they require skilled personnel to configure, manage, and operate effectively. Organizations often need to invest in ongoing training to bridge this gap. Safety concerns also come into play when applying patches in OT environments. Incorrectly implemented patches can disrupt critical systems, compromise safety, or affect operational reliability, highlighting the need for careful configuration and validation of automated processes. Moreover, automation tools must be adaptable to organizational-specific contexts, as not all identified vulnerabilities pose an immediate risk. This requires tools to support customized mitigation strategies and prevent unnecessary remediation efforts. Effective prioritization of vulnerabilities is also crucial, as organizations must focus resources on addressing the most critical risks that could impact the Bulk Electric System (BES). [1,11]

For risk assessment, integrating automation tools into the complex systems of NERC environments is particularly challenging. Utilities often operate diverse infrastructures with interconnected components, including legacy systems and modern OT devices. Ensuring seamless integration across these systems requires significant technical expertise and robust interoperability capabilities. Furthermore, automation tools must keep pace with the constantly evolving regulatory landscape and threat environment. Tools need the ability to dynamically monitor compliance with NERC CIP standards and adapt to new requirements or emerging risks. [4,10]

Ongoing training and standardization across the organization are also essential for the effective use of au-

tomation tools. Personnel must be equipped with the knowledge and skills to utilize these tools optimally, and standardized internal processes are critical to maintaining compliance and operational consistency. Vendor risk assessments further complicate the implementation of automation tools, as NERC CIP standards require thorough evaluations of third-party vendors to mitigate supply chain risks. Ensuring vendors adhere to security best practices and establishing clear breach notification requirements in contracts are vital to maintaining the integrity of the BES.

Despite the potential benefits, these challenges highlight the need for a careful and strategic approach to implementing automation tools in NERC environments. Organizations must balance the capabilities of automation with the unique demands of their operational contexts to enhance both security and compliance effectively.

3. Benefits and Risks of Automation

While implementing automation tools in NERC environments presents challenges, the potential benefits are significant. These benefits include:

- Improved Security: Automation tools can help organizations identify and address vulnerabilities more efficiently, leading to a stronger security posture and a reduced risk of cyberattacks.[3]
- Reduced Risk: By automating risk assessments and compliance monitoring, organizations can proactively identify and mitigate potential risks to the BES, minimizing the likelihood of disruptions and outages.[4]
- Increased Efficiency: Automation can streamline various security processes, freeing up personnel to focus on more strategic tasks and improving overall operational efficiency.[5]
- Cost Savings: By automating repetitive tasks and reducing manual effort, organizations can potentially realize cost savings in the long run. Automation can also help avoid costly penalties associated with non-compliance.
- Enhanced System Performance: Automation can contribute to improved system performance by enabling proactive control and more efficient operations and maintenance.[3]

While automation tools offer numerous benefits, it is essential to be aware of the potential risks and vulnerabilities associated with their use. One of the key risks is the potential for unauthorized access to automation tools or the systems they manage. Without robust access controls and authentication mechanisms, unauthorized users may gain access to critical systems or manipulate security configurations, putting the integrity of the system at risk Another challenge lies in configuration management. Misconfigured automation tools can create security gaps or lead to unintended consequences. Organizations must implement strong configuration management practices to ensure that these tools are properly set up, maintained, and aligned with security protocols to avoid vulnerabilities.

Open-source software components are often integrated into automation tools, and while these components can provide flexibility and cost benefits, they also present potential security risks. Open-source software may contain vulnerabilities that attackers can exploit, so organizations must thoroughly evaluate the security of these components and apply appropriate risk mitigation strategies.

Reducing the attack surface is another critical step in minimizing cyber risks. This can be achieved by removing non-essential features, reducing privilege levels, and ensuring that patches and updates are applied promptly. By limiting the potential avenues for attack, organizations can make it more difficult for malicious actors to exploit vulnerabilities in the automation tools. Access control and isolation are fundamental to securing automation tools. By controlling access to these tools and isolating them from

both the internet and internal networks, organizations can prevent unauthorized access and reduce the impact of potential security breaches. Finally, continuous monitoring and log analysis are essential for identifying and responding to security threats. By regularly monitoring automation tools and analysing security logs, organizations can detect suspicious activity early and take necessary action to mitigate risks before they escalate.

4. Implementation and Best Practices

The figure below (Figure 1) illustrates a step-by-step approach for implementing automation tools in NERC environments, providing a visual workflow to guide the process.

- Identify Needs and Objectives: The first step is to understand the specific needs of the organization, including what challenges they are facing in managing vulnerabilities and risks. This step sets clear objectives for the automation process and aligns the implementation with organizational goals.
- Conduct Risk Assessment: This step involves evaluating the potential risks and vulnerabilities present in the current environment. By identifying areas of weakness, organizations can prioritize their mitigation efforts and ensure that automation tools address the most pressing security challenges.
- Select Automation Tools: Based on the results of the risk assessment, the next step is to select the appropriate automation tools. This involves evaluating various tools that can help with vulnerability management, risk assessment, and compliance monitoring while ensuring compatibility with the NERC environment.
- Develop Implementation Plan: After selecting the tools, a detailed implementation plan is developed. This plan outlines how the tools will be integrated into existing systems, the required resources, and the timeline for deployment. It ensures that the process is structured and that any potential obstacles are anticipated.
- Implement Automation Tools: This phase involves deploying the selected automation tools within the NERC environment. Proper configuration and integration with existing infrastructure are critical to ensure smooth functionality.
- Train Personnel: Once the tools are implemented, it is important to train personnel on their use. This ensures that staff are equipped with the knowledge to operate the tools effectively and to maintain security across the environment.
- Continuous Improvement: The final step emphasizes the need for continuous improvement. Automation tools must be regularly monitored and updated to keep pace with evolving threats and compliance requirements. This ensures that the tools remain effective in protecting the infrastructure.

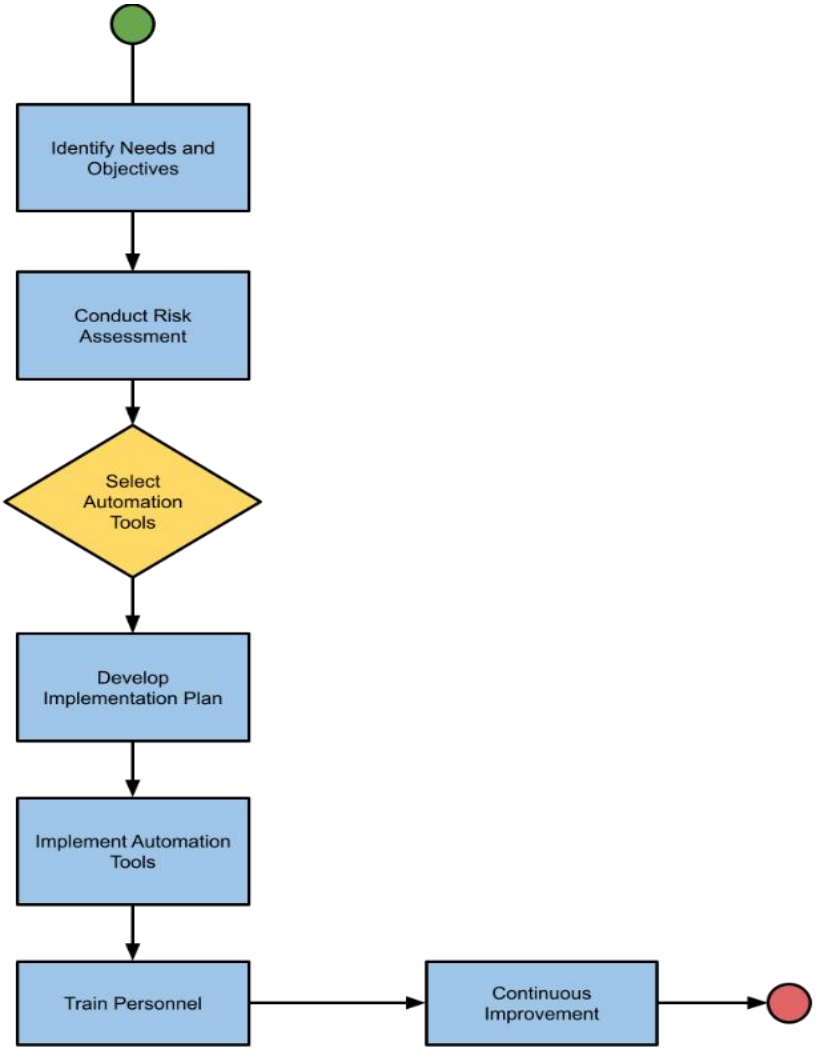

Figure 1. Implementing Automation Tools in NERC Environments: A Step-by-Step Approach

To successfully implement automation tools in NERC environments and maximize their benefits while mitigating risks, organizations should adopt several best practices. First, conducting a comprehensive risk assessment is crucial to identify potential vulnerabilities and prioritize mitigation efforts. This helps organizations focus on addressing the most pressing risks first, ensuring a more effective security posture. [3,6]

Cultivating a culture of security within the organization is also essential. Promoting the importance of cybersecurity at all levels, coupled with regular security awareness training, fosters a proactive approach to security across the workforce. Ongoing training is vital, ensuring personnel remain up to date on the latest threats, security best practices, and proper use of automation tools. [5,12]

Automating repetitive tasks wherever possible is another critical step. Automation helps reduce human error and enhances operational efficiency, making processes more reliable and consistent. To complement this, conducting regular incident response drills is important to ensure that personnel are well-prepared to handle security incidents swiftly and effectively.[10]

Engaging third-party experts can also support the successful implementation and management of automation tools. Their expertise can assist in the selection, deployment, and ongoing maintenance of

these tools, ensuring that they are configured and optimized for the specific needs of NERC environments.[10]

Continuous improvement is key to maintaining an effective automation strategy. Regularly evaluating the performance and effectiveness of automation tools ensures that they remain aligned with organizational needs and evolving security threats. Continuous monitoring of these tools and the systems they manage allows for the early detection of anomalies and potential security breaches, providing opportunities for rapid response.

Role-based access control (RBAC) should be implemented to ensure that only authorized personnel have access to sensitive systems and data, reducing the risk of unauthorized access. Additionally, conducting regular security audits helps assess the effectiveness of security controls and identify areas for improvement, while incident response plans must be regularly tested to ensure their readiness in the face of real threats.[8]

Organizations should also consider obtaining cyber insurance as a financial safeguard against the potential impact of cyberattacks. Participating in cyber threat intelligence-sharing initiatives helps stay informed about the latest threats and vulnerabilities, enabling better preparedness.[16]

Encrypting sensitive data is crucial to protecting it from unauthorized access, ensuring confidentiality even in the event of a breach. Implementing risk scoring tools can help automate vulnerability prioritization, allowing organizations to focus remediation efforts on the most critical vulnerabilities. Furthermore, ensuring seamless integration of automation tools with existing systems, such as security information and event management (SIEM) systems, avoids data silos and enhances the overall security infrastructure. Finally, organizations should prioritize software integrity and authentication by assessing software upgrades, testing new software before installation, and verifying the authenticity of patches to prevent malicious code from being introduced. [17] Establishing patch management processes, either through vendor contracts or internal systems, ensures that updates are deployed promptly, with patches thoroughly tested to avoid compatibility issues or unintended consequences. These best practices form the foundation of a robust and secure automation strategy in NERC environments, ensuring both efficiency and resilience.

5. Conclusion

Implementing emerging automation tools for vulnerability management and risk assessment in NERC environments presents both challenges and opportunities. While challenges such as production sensitivity, cost/feature mismatch, and the need for ongoing training must be addressed, the potential benefits of automation are significant. These benefits include improved security, reduced risk, increased efficiency, and cost savings.

By carefully considering the challenges, understanding the relevant NERC CIP requirements, selecting appropriate automation tools, and following best practices, organizations can successfully implement automation and strengthen the security and reliability of the North American power grid. Continuous monitoring and adaptation are essential to ensure that automation tools remain effective in the face of evolving threats and changing regulatory requirements.

Ultimately, the successful implementation of automation tools can contribute to a more resilient and secure BES, safeguarding critical infrastructure and ensuring the reliable delivery of electricity to millions of people.

6. References

1. Upadhyay, Darshana, and Srinivas Sample. "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations." Computers & Security 89 (2020): 101666.
2. Fortunato, Sebastian Salvatore. Risk Management in ICS/SCADA Systems to Enhance Security within the Energy Sector. MS thesis. Utica College, 2020.
3. Qassim, Qais Saif, et al. "A review of security assessment methodologies in industrial control systems." Information & Computer Security 27.1 (2019): 47-61.
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. Glenn, Colleen, Dane Sterbentz, and Aaron Wright. Cyber threat and vulnerability analysis of the US electric sector. No. INL/EXT-16-40692. Idaho National Lab.(INL), Idaho Falls, ID (United States), 2016.
6. Duffey IV, H. Thomas J. Exploring the Impact of NERC CIP Regulatory Compliance on Risk and Security for Bulk Electric System Grid Cyber-Attacks: A Qualitative Phenomenological Study. Diss. Northcentral University, 2018.
7. Ney, Valerie A. Energy Sector Cybersecurity Supply Chain Risk Management: Evaluating the Political and Regulatory Compliance Challenges and Developing the Supply Chain High-Risk Evaluation Framework (SCHEF). MS thesis. Utica College, 2021.
8. Peterson, John, Michael Haney, and R. A. Borrelli. "An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants." Nuclear Engineering and Design 346 (2019): 75-84.
9. Fortunato, Sebastian Salvatore. *Risk Management in ICS/SCADA Systems to Enhance Security within the Energy Sector*. MS thesis. Utica College, 2020.
10. Proctor, Matt, and Terry Smith. "Lessons learned from NERC CIP applied to the industrial world." *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*. IEEE, 2017.
11. Dolezilek, David, and Laura Hussey. "Requirements or recommendations? Sorting out NERC CIP, NIST, and DOE cybersecurity." *2011 64th Annual Conference for Protective Relay Engineers*. IEEE, 2011.
12. Zafirovic-Vukotic, Mira, et al. "Secure Scada network supporting NERC CIP." *2009 IEEE Power & Energy Society General Meeting*. IEEE, 2009.
13. Mertz, Mike. "NERC CIP compliance: We've identified our critical assets, now what?"." *2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*. IEEE, 2008.
14. Reynolds, Chuck, and Alex Henthorn-Iwane. "Automating the NERC CIP Compliance-Test Lab to Meet CIP Standards." *ITEA Journal of Test & Evaluation* 34.4 (2013).
15. Kalibjian, J. "Implementing NERC CIP compliance with automated tools." (2007).
16. Christensen, D., Martin, M., Gantumur, E., & Mendrick, B. (2019). Risk assessment at the edge: Applying NERC CIP to aggregated grid-edge resources. *The Electricity Journal*, *32*(2), 50-57.
17. Dolezilek, D., & Hussey, L. (2011, April). Requirements or recommendations? Sorting out NERC CIP, NIST, and DOE cybersecurity. In *2011 64th Annual Conference for Protective Relay Engineers* (pp. 328-333). IEEE.

18. Duffey IV, H. T. J. (2018). *Exploring the Impact of NERC CIP Regulatory Compliance on Risk and Security for Bulk Electric System Grid Cyber-Attacks: A Qualitative Phenomenological Study* (Doctoral dissertation, Northcentral University).