



# Information Security Challenges in Energy Industry

---

WHITE PAPER

**Author: Neeraja Murthy**

---

The increased risk of cyber-attacks has meant that companies in the energy industry are placing a renewed focus on reviewing and enhancing their existing information security measures. Additionally certain trends in the energy industry have increased the security risk profile of the industry's information systems. While companies are reviewing the information security strategies and mechanisms, a number of government/regulatory agencies are also in the process of defining security regulations with which companies need to comply.

This white paper presents the information security challenges faced by industries in the energy sector and then recommends the steps which organizations need to take in order to meet these challenges and to comply with the regulatory norms.

**Table of Contents**

**INTRODUCTION ..... 3**

**INFORMATION SECURITY THREATS AND VULNERABILITIES ..... 4**

**SECURITY OF THE SCADA NETWORKS ..... 4**

**INFORMATION SECURITY STRATEGY ..... 5**

**STEP 1: SECURITY RISK ASSESSMENTS ..... 5**

**STEP 2: SECURITY POLICY AND PROCESS DEFINITIONS ..... 5**

**STEP 3: SECURITY FRAMEWORKS/  
IDENTITY MANAGEMENT SOLUTIONS ..... 6**

**STEP 4: NETWORK ARCHITECTURE REVIEWS  
AND IMPLEMENTATIONS ..... 6**

**CONCLUSION ..... 6**

**ABOUT THE AUTHOR ..... 6**

**ABOUT WIPRO TECHNOLOGIES ..... 7**

**WIPRO IN ENERGY & UTILITIES PRACTICE ..... 7**

## Introduction

Traditionally, legacy and other energy industry applications have been stand-alone systems accessible to a limited number of users mostly within the corporate itself. In addition, SCADA systems have typically resided on networks, which are inaccessible from the corporate networks. This isolation approach had resulted in a limited access to the systems and applications. Security for these applications was built for this scenario which assured the degree of security that was deemed necessary.

Like other industries, companies in the utility industry have fragmented security implementations across the organization with no integrated information security mechanisms, processes or systems in place to implement or manage information security. The task of ascertaining the level of security and the need for enhancement is therefore a difficult one.

## **Information Security Threats and Vulnerabilities - Security in an Open Environment**

Deregulation is breaking the industry into smaller independent units, driving the need for increased networking. The new environment of de-regulation and increased competition means that companies need to open up their information systems for sharing of information with multiple parties such as suppliers, vendors, customers etc. Examples include Internet-based billing presentment and payment systems, energy trading systems etc.

This will involve an integration of disparate application and infrastructure systems belonging to multiple organizations as well as providing online access to a large user base over the Internet. Systems which were previously closed and in many cases, proprietary, now need to be inter-connected for information exchange. Many of these systems which were designed to work as stand-alone systems with a minimal amount of security are now connected to the Internet making them vulnerable to cyber-attacks. The traditional approach of building security mechanisms within the applications has resulted in multiple duplicated user and access data stores and poses a significant challenge for integration.

### **Security of the SCADA Networks**

SCADA networks were initially designed to maximize functionality and focused on performance, reliability, flexibility and safety. As a result SCADA systems have weak security mechanisms.

As the energy industry becomes more automated and electronically connected, there is an increased connectivity of the SCADA systems to the rest of the world. The need for remote access computing means that business applications such as energy trading, customer service systems, maintenance scheduling etc, which are likely to be exposed to the Internet, require deriving/sharing their information from the SCADA systems. Existing control systems, which were originally designed for use with proprietary, standalone communications networks, were later connected to the Internet, but without adding the technology needed to make them secure. Therefore the traditional assumptions of SCADA networks being inaccessible from corporate networks and thereby secure from the vulnerabilities of the corporate networks no longer hold good.

### **Mergers & Acquisitions**

The increasing number of mergers and acquisitions in the de-regulated utility industry means that companies need to have the ability to rapidly integrate security data and processes between disparate systems. Since most organizations have a fragmented security infrastructure without an integrated one-view of their employees, partners and customers, the security infrastructure is typically not geared to meet a large fundamental change in the user base.

### **Security Management costs**

Organizations including those in the utilities industry are increasingly looking at doing more with less. The current fragmented security systems of most organizations means that the expenditures of staff, time and money for performing day-to-day security management such as user and resource provisioning, password resets etc. are significant. The absence of a streamlined process for security administration and management means that a significant amount of the IT budget needs to be spent on these activities rather than on other technology initiatives. With the increased competition in the de-regulated environment the Identity Management Systems have to be designed to reduce operational costs while focusing on providing exemplary customer service.

### **Regulatory Compliance**

Recent events have resulted in an increased number of regulatory agencies/government bodies issuing new security regulations with which companies need to comply. One such example is the proposal for 'Security Standards for Electric Market Participants' by the FERC.

The absence of streamlined, coordinated administration and audit methodologies means that organisations find it difficult to identify their current levels of compliance and to define a roadmap for achieving compliance with such regulations.

## **Information Security Strategy**

In order to meet the challenges facing them, utility companies will have to focus on a holistic approach to achieving enterprise security. An integrated corporate-wide initiative is critical in identifying and implementing a highly secure, integrated, flexible and robust security architecture.

### **Step 1: Security Assessments**

A current state analysis of the security measures is the first step to implementing a successful enterprise security system. In addition to reviewing the technical controls, organizations will have to review their security processes and practices to identify the current state of information security and define the roadmap for the enterprise security architecture. Organizations will have to conduct a thorough 'as-is' analysis, security risk assessments, data classifications exercises and enterprise systems architecture reviews to identify the current security levels, security gaps, vulnerabilities and threats. Based on the findings of the security assessments, companies should identify the necessary security initiatives.

### **Step 2: Security Policy and Process Definitions**

Where these are not already available, companies must define corporate wide security policies and processes, incident response, business continuity programs and security guidelines. Although regulations and standards are still emerging, these must be an important input into the security policies definition. A large number of companies already have a set of security policies and guidelines in place; however, measures to ensure the strict compliance of the information security systems to these policies are typically not in place. Companies must define policies for periodic audits of the systems for compliance. Security policies must also be reviewed to ensure that they address the new threat scenario.

### **Step 3: Security Frameworks/ Identity Management Solutions**

Development of robust security architecture is the first step towards building an effective protection mechanism in any organization. Energy companies will need to define an integrated security framework to meet the challenges in the new open and de-regulated environment. Companies will need to focus on defining integrated security frameworks and identity management mechanisms for access to applications/systems across the organization. An integrated framework providing consolidated directories, single sign-on and authorization, user provisioning and auditing should be deployed to successfully achieve regulatory compliance and cut down operating costs of security management.

A unified integrated security infrastructure will also ensure rapid integration with security infrastructure of other merged/acquired companies. A robust security architecture will also be a major contributor to the enhanced security of the corporate and SCADA network.

### **Step 4: Network Architecture reviews and implementations**

Based on the new threat scenarios, companies will have to review their network architecture design, type of traffic flows in and out of the organization as well as within the organization and appropriately enhance their perimeter defenses. It becomes imperative for companies to undertake network architecture design enhancements including firewall, intrusion detection systems, virus protection systems, VPN and server hardening to ensure that they provide adequate protection to the organization's information security systems.

## **Conclusion**

A number of recent events have raised the risk profiles of corporate information systems making them more vulnerable. Energy companies are therefore forced to renew their focus on information security to provide enhanced security in a cost-effective manner. By following a holistic approach to enterprise security detailed above, organizations can mitigate these risks, reduce operating costs and meet regulatory compliance deadlines.

Additionally, the increasingly competitive deregulated environment has also meant that companies need to focus on operational efficiencies and cost-savings. The increasing number of mergers and acquisitions requires that the security infrastructure be scalable and flexible to support the unpredictable business environment. The streamlining of security management processes and technologies and the creating of robust security frameworks should therefore receive renewed attention.

## **About the Author**

Neeraja Murthy is currently working as a Senior Security Consultant with Wipro's Enterprise Security Services group. She has vast experience in the areas of application security frameworks and solutions. She has worked extensively on security consulting projects involving requirements study, solutions design, development and product evaluation. She has initiated and managed a number of security projects in different security technology areas including extranet access management, directory services, authentication and authorization frameworks and user provisioning solutions.



## About Wipro Technologies

Wipro is the first PCMM Level 5 and SEI CMMi Level 5 certified IT Services Company globally. Wipro provides comprehensive IT solutions and services (including Systems Integration, IS Outsourcing, Package Implementation, Software Application Development and Maintenance) and Research & Development services (hardware and software design, development and implementation) to corporations globally. Wipro's unique value proposition is further delivered through the pioneering Offshore Outsourcing Model and stringent quality processes of SEI and Six Sigma.

## Wipro in Energy & Utilities Practice

Wipro has a focused energy & utilities practice with 1000 consultants and works with clients across USA and Europe in both regulated and de-regulated markets. The key areas of focus in this space are customer service systems (including billing, metering and invoicing), work and asset management systems, network operations systems, corporate management, finance and payroll systems. Our services span across consulting, implementation, development, support and maintenance services for the IT needs of the energy, network-based, regulated utilities and energy markets. Our client base includes a range of entities, including investor owned utilities, public power utilities, regional transmission companies and independent system operators.

---

For more white papers logon to <http://www.wipro.com/insights/>

© Copyright 2003. Wipro Technologies. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Wipro Technologies. Specifications subject to change without notice. All other trademarks mentioned herein are the property of their respective owners. Specifications subject to change without notice..

### Worldwide HQ

Wipro Technologies,  
Sarjapur Road,  
Bangalore-560 035,  
India.  
Tel: +91-80-844 0011.

### U.S.A.

Wipro Technologies  
1300, Crittenden Lane,  
Mountain View, CA 94043.  
Tel: (650) 316 3555.

### U.K.

Wipro Technologies  
137 Euston Road,  
London, NW1 2 AA.  
Tel: +44 (20) 7387 0606.

### France

Wipro Technologies  
17, Square Edouard,  
VII, 75009 Paris.  
Tel: +33 (01) 5343 9058.

### Germany

Wipro Technologies  
Am Wehr 5,  
Oberliederbach,  
Frankfurt 65835.  
Tel: +49 (69) 3005 9408.

### Japan

Wipro Technologies  
# 911A, Landmark Tower,  
2-1-1 Minatomirai 2-chome,  
Nishi-ku, Yokohama 220 8109.  
Tel: +81 (04) 5650 3950.

### U.A.E.

Wipro Limited  
Office No. 124,  
Building 1, First Floor,  
Dubai Internet City,  
P.O. Box 500119, Dubai.  
Tel: +97 (14) 3913480.

[www.wipro.com](http://www.wipro.com)

eMail: [info@wipro.com](mailto:info@wipro.com)

**Wipro Technologies**

*Innovative Solutions, Quality Leadership*