



Case Study



Client Profile

Since 1993, DynMcDermott Petroleum Operations Company (DM) has served as the Prime Contractor for the Department of Energy (DoE) Strategic Petroleum Reserve (SPR) Project. The SPR is an emergency supply of crude oil stored in huge underground salt caverns along the coastline of the Gulf of Mexico in Louisiana and Texas. Authorized by Congress in 1975, the SPR is today the nation's energy "insurance policy," the largest stockpile of crude oil in the world. In its capacity as the Management and Operations contractor, DM is responsible for the safe and efficient operation of all SPR sites as well as the New Orleans Project Management office. Primary emphasis is placed on conducting all operations in an environmentally safe, highly secure and responsible manner. As a result, security of the data, business systems and Supervisory Control And Data Acquisition (SCADA) and Distributed Control Systems (DCS); real time controls that make up the SPR's critical infrastructure, is paramount to ongoing operations as well as national security.

Executive Summary

To ensure the security, reliability and availability of DoE SPR systems, DynMcDermott regularly conducts vulnerability assessment of the business, cyber, physical and control system assets to determine risk of accidental breach as well as targeted systems attack. These zero knowledge penetration attempts and collaborative assessments include:

- Externally-Accessible Assets
- Internally Accessible Assets
- Energy Management Systems (DCS)
- Network Infrastructure (Servers, Routers, Databases)
- Remote Access
- Wireless DCS Control Systems
- Social Engineering and Physical Audit
- Network Architecture Analysis

DM well understands the grave outcome of a possible take over of command and control systems in the plant environment, or potential breach of these systems by exploiting vulnerabilities within information systems that connect to plant operations.

Solution

A comprehensive assessment requires a multi-disciplined and multi-tasking set of activities that need to be executed and managed in a coordinated manner. Since there is no such thing as 100% secure, and not



everything is worth protecting at all cost, an asset focused approach is paramount to satisfying audit **and** hardening objectives. The DYONYX network vulnerability assessment methodology incorporates a risk management process, consistent with the NIST¹ Enterprise Risk Management Framework, which addresses the need to reconcile identified risk events with the risk profile of the organization. The provisions of the Delivery and Support domain of CobiT (Control Objectives for related Technology) developed by the IT Governance Institute) have also been incorporated as applicable².

This methodology incorporates both a bottom-up and top-down business security analysis set of tasks. That is, from a bottom-up perspective, cyber and physical vulnerabilities that are discovered in the hardware and network infrastructures and penetration testing are mapped to the underlying business processes through the impacted application systems and databases. This bottom-up approach and the linkages to the underlying business processes, along with our detailed design level security process and hacker mentality abilities provides the framework for assessing the business risks associated with each identified vulnerability. From a top-down perspective, the policy and procedural provisions detailed in the Control Objectives of the Ensure Systems Security process of CobiT are utilized as the template for assessment of the security practices. This approach provides multiple paths in identifying security vulnerabilities, correlating the same with the underlying systems and databases, and assessing benefits and risks. To many it often comes as a surprise to learn that securing a network, critical application system or database involves more than just superb technical security skills. Securing any one of these assets also requires deep psychological understanding of the hacker's mentality and motivation as well. Reducing or eliminating the psychological *motivation* or *stimulation triggers* for an attack is sometimes as important as striving to eliminate the actual *opportunity* for an attack. DYONYX has worked with DM on several DoE SPR risk management projects over the past two years.

Control System Specific Risk Assessment

Successful attacks can originate from Internet paths through the corporate network to the DCS network and on to the DCS application systems. Alternatively, attacks can originate from within the DCS network from either upstream (DCS applications) or downstream (RTUs) paths. What is an appropriate configuration for one installation may not be cost effective for another. Flexibility and the employment of an integrated and coordinated set of layers are keys in the design of a security approach. In terms of the corporate network exposures, the following discussion applies:

Firewalls, properly configured, can protect passwords, IP addresses, files and more. However, without a hardened operating system, hackers can directly penetrate private internal networks or create a Denial of Service (DoS) Condition, rendering the firewall useless.

Proxy servers are critical to re-create TCP/IP packets before passing them on to, or from, application layer resources such as HTTP and SMTP. However, the employment of proxy servers will not eliminate the threat of application layer attacks.

¹ National Institute of Standards and Technology (www.nist.gov)



Operating systems can be compromised, even with proper patching, to allow network entry as soon as the network is activated. Further, in place operating system upgrades are less efficient and secure than design-level migration to new and improved operating systems.

Application layer attacks; i.e., buffer overruns, worms, Trojan Horse programs and malicious Active-X code, can incapacitate anti-virus software and bypass the firewall as if it wasn't even there.

While policies and procedures are included not in the design review, they do constitute the foundation of security policy infrastructures. Implementing effective policies and procedures can reduce legal liabilities and ensure subsequent prosecution of violations. Unfortunately, developing, documenting and enforcing effective security policies are some of the most difficult measures to manage. Only a conscious, ongoing, proactive network security program can have any realistic success over the long term.

As stated in the SPR Request for Proposal, the DYONYX team will use the NIST 800-30 methodology for assessing the risk of IT systems (as illustrated in **Figure 1**).

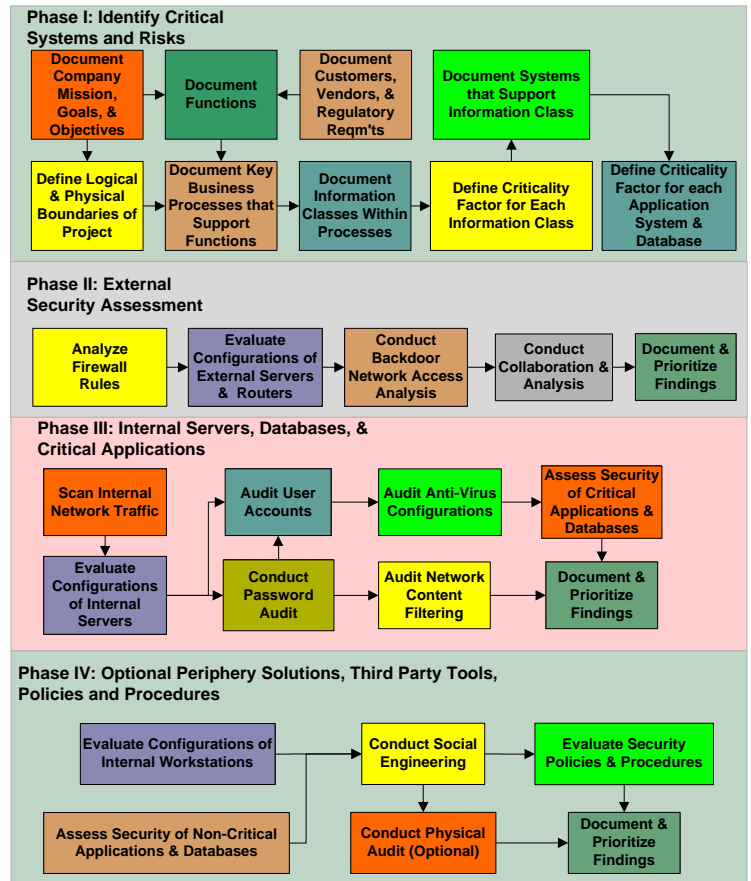


Figure 1 - NIST 800-30 Methodology