



### Project Objectives

- » Assess the overall organizational security posture
- » Determine the next best steps to improve their security posture and position ChemCo to achieve their organizational objectives including securing their Intellectual Property.

### Key Project

#### Activities/Deliverables

- » Identified deficiencies in the Control environment that left the organization subject to significant legal, reputation, and financial loss via an IT Controls Audit
- » Identified deficiencies in the network architecture and key systems that reduced the security, reliability, and availability of key business systems via Vulnerability Assessment and Penetration Testing
- » Identified deficiencies in the design and security of a key Extranet application that left the organization susceptible to malicious activity by key customers and suppliers via an Application assessment.
- » Jointly developed a Security Road Map to optimize ChemCo's security posture and ensure IT's contribution to organizational success

## CASE STUDY

# Security Risk Assessment & IT Controls Audit

When major multi-national chemical corporation, ("ChemCo") was looking to bolster their security by acquiring additional enterprise security solutions for a layered defense, they called upon Pivot Point Security to assess their current security posture and recommend the most effective solutions given their current circumstances.

### NEXT BEST STEP

ChemCo had long ago addressed their basic security concerns in the forms of VPN, firewalls and antivirus solutions in order to maintain the security baseline required in an enterprise environment. With continued growth in their international locations and a very large and diverse network spanning over 50 countries, ChemCo was looking to take the next step to further strengthen their security. By purchasing and implementing additional layers of information technology security, primarily in the form of network intrusion detection systems/intrusion prevention systems (IDS/IPS) ChemCo sought to improve the overall security of their intellectual property.

ChemCo turned to Pivot Point Security for a recommendation on the most effective IDS solution to fit their organization's needs. Realizing that information security solutions are not a "one size fits all" proposition, Pivot Point began the interaction with some key questions:

- » Have you recently assessed your Information Technology control objectives?
- » What Internal or Regulatory compliance issues are ChemCo subject to ?
- » Does IT's Strategic Plan dovetail with that of the organization?
- » What systems, data, applications, events represent the greatest risk to ChemCo ?

Like many other enterprises, most of the answers were "Not sure." Pivot Point recommended that ChemCo take the next step, and perform a baseline Security Assessment prior to moving ahead with the planned purchase of a NIDS solution. This would help provide guidance on how to best invest in the next step to bolster their overall security, be it via an IDS, training, or other services and solutions. ChemCo agreed to the Security Assessment (including a

Rapid Risk Assessment) supported by a substantive set of testing to confirm these risks pose a real threat to the security of ChemCo.

### RISK ASSESSMENT

The Rapid Risk Assessment phase of the project was conducted with key personnel from various functional areas within the organization (e.g., Research, Human Resources, Information Technology, Executive Management, etc.) Using a pared down version of \*OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation-SM, a risk-based strategic assessment and planning technique for security), the group was able to identify those IT related events (e.g., malicious access to core Intellectual Property, failure to comply with Sarbanes Oxley, disaster at Corporate Headquarters, non-availability of key Extranet application) that represented the most significant risks to ChemCo. This assessment provided a basis for downstream activities including the Controls Audit, Penetration Testing, and resulting in an IT "Road Map" construction.

### CONTROLS ASSESSMENT

Pivot Point's control assessments leveraged COBIT—Control Objectives for Information Technology framework, an internationally accepted reference framework for Information Technology security and control practices. Leveraging the Risk Assessment output, Pivot Point conducted a very targeted Controls Assessment.

#### Key Findings included:

- » Policies and Procedures were not developed to address key risk areas, (e.g. no Data Classification procedures had been put in place to ensure that key Intellectual Property was protected appropriately.)
- » Insufficient monitoring (system auditing, vulnerability assessments, patch management) on critical business systems including their ERP and key

\*Operationally Critical Threat Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.



Extranet application.

- » Disaster Recovery and Business Continuity (e.g. no processes were in place to verify the integrity of the backups) were insufficient.
- » Insufficient Segregation of Duties (e.g., Network Admins could alter security logs after taking malicious action).

Following the IT controls assessment, Pivot Point Security compiled and delivered a report to ChemCo management and security personnel detailing our findings, including control deficiencies discovered and recommendations to help mitigate risks associated with the known deficiencies. Executive Management expressed, "the value of the IT Controls audit to the strategic business goals of their company was extremely clear".

#### VULNERABILITY ASSESSMENT

After the IT controls assessment was completed, a Vulnerability Assessment (VA) was performed on critical network segments and systems. Using a combination of open source and commercial VA tools, the Pivot Point VA specialists collected vulnerability information about the networks and systems. Analyzing the data, many types of common operating system vulnerabilities were identified. Through the combination of controls assessment (ChemCo's processes, policies and personnel controls) and risk assessment (identified vulnerabilities flagged by the Pivot Point team's VA tools), Pivot Point helped ChemCo identify key vulnerabilities and provided detailed recommendations on how to best mitigate them and more importantly, preclude them from recurring.

#### PENETRATION TESTING

The final phase of the assessment, Penetration Testing (PT) is a method of evaluating the security of a computer system or network by simulating an attack by a malicious individual. Pivot Point PT specialists (with specialties in network, application and operating systems security) attempted to exploit the vulnerabilities identified during the Vulnerability Assessment from both an external and internal posture.

Focusing on the most significant risk points identified during the Vulnerability Assessment, the Pivot Point Security PT specialists attempted to gain access to key systems. The PT report identified that key systems on the client's corporate Intranets and Extranets were successfully compromised. Pivot Point delivered a detailed report covering the tools and methodologies used to exploit the systems and an assessment of the overall impact of the exploit on ChemCo's operations.

#### RECOMMENDATIONS

From the information gathered in each phase of the Pivot Point Security audit, a detailed executive summary was provided to ChemCo's management. The executive summary provides management perspective on where their security posture ranks in relation to their peers. A separate technical report geared to IT was also delivered which included numerous detailed recommendations mitigating the vulnerabilities identified.

Lastly, working in concert with ChemCo's CIO, Pivot Point worked to refine their IT Strategic Plan into a multi-year roadmap. The plan defined and prioritized the next best steps to address key organizational risks. This resulted in ChemCo developing a plan that meets their organizational strategic objectives, including criteria for IDS/IPS vendor and measures to further secure the sensitive data on their systems.

When the Pivot Point team conducted a follow up with ChemCo, they also discovered that the upper management was able to better grasp the overall impact/significance of IT security and the IT Control environment as it related to ChemCo's business objectives. The CIO leveraged the roadmap to garner additional executive-level support and funding for the IDS/IPS solution, end-user security training and future independent audits based on this greater understanding.



#### ABOUT PIVOT POINT SECURITY:

Achieving, and more importantly maintaining, a "reasonable & appropriate" security posture in today's environment requires a new approach. We approach IT Security as a business issue and focus on IT Governance, appropriate balance of key elements (people, process, & systems) and objectives (risk, cost, usability, and performance), strong control environments, and ongoing monitoring capabilities. Those safeguards are the hallmarks of today's best security architectures and the strength of Pivot Point Security.

Pivot Point Security is the premiere provider of information security auditing, penetration testing, enterprise security management, vulnerability assessment and mitigation services and solutions in the NY / NJ / PA metro area.

Clients (small business through international corporations) benefit from our Internal Control oriented approach to Information Security and our assistance with complex issues including Sarbanes Oxley, HIPAA, and SAS-94.