INFORMATICA
INFORMATION SECURITY & RISK MANAGEMENT

67 Yonge St. #502
Toronto, ON. M5E 1J8
Tel: (416) 431-9012
InformationSecurityCanada.com

Informatica Corporation Case Study #1:

Information security analysis and remediation following insider breach

The Business Problem

Informatica was retained by the client - a non-profit organization – to investigate a security breach with the potential to publicly undermine the organization's work, alienate its partners and invite embarrassing media coverage. The challenges included the following questions:

1. What is the extent of the damage?
2. How exactly did the breach take place?
3. Are further breaches possible?
4. How can they be prevented?

The Approach

To answer these questions, Informatica experts used the FlexSecure security assessment methodology to plan and execute the following steps:

1. Conduct an information security assessment to determine the exposure, risk and security posture of the organization at the current point in time:
    a. Conduct key person interviews and passive data collection
    b. Use tools and technology to identify controls and gaps in security
    c. Manually validate and investigate vulnerabilities
2. Analyze employee access, procedures, habits and evidence to determine the "how"
3. Verify the exploitability and urgency of findings
4. Produce a confidential detailed management report and presentation outlining the findings, exposure to risk and additional threats.
    a. The report and management presentation included a technical report intended for the IT staff in charge of remediation and technical implementations.
    b. Threats were addressed individually and the strategy was laid out clearly to ensure an effective implementation.

As with many other engagements, a standards-based assessment was included to provide an independent expert view of the situation and render a statement of opinion to the board of directors.

Findings

As a result of the analysis, Informatica found the following problems:

1. The organization and its clients are at severe risk of financial liability and public embarrassment
2. Security controls do not match the sensitivity and importance of data.
3. Unauthorized copies of commercial and downloaded software are in use on servers and workstations.
4. The organization has weak security policies and unenforceable agreements.
5. There is little to no employee awareness and accountability regarding information security.
6. Financial records and confidential corporate information are accessible by unauthorized staff

Recommendations

Reports included recommendations for effective, rapid and sustainable remediation in the following four areas:

1. Administrative Security (15 recommendations) – example: Implement a clean desk, clear screen policy as a common sense approach to protect sensitive information
2. Technical Security (12 recommendations) – example: Adopt data encryption as a key element of the security strategy to preserve the confidentiality of data
3. Physical Security (7 recommendations) – example: Review all entrance locking mechanisms (the office's door lock remained stuck, potentially allowing entry to unauthorized parties over an entire week-end).
4. Supplementary suggestions (multiple recommendations) – example: Secure access to telephony system, encrypt off-site data and address security at satellite offices.

Case Study Summary

Informatica's deliverables following a two-week engagement were designed to effectively address all of the above concerns and produce a workable plan that could be implemented with existing or local resources. These deliverables included:

1. Auditor's Statement of Opinion
2. Management Presentation
3. Detailed Management Report
4. Detailed Technical Report

Informatica's effective security analysis and remediation framework applies to urgent cases as well as situations that require the introduction of 'best practices' to support industry compliance requirements, protective legislation and service level agreements. Informatica's certified security experts use best-of-breed IT security tools and assist with the implementation of effective solutions. Informatica provides world-class risk assessments and staff security awareness training to support an effective information protection program.