

AT&T Consulting

Security Services for Mergers and Acquisitions

Introduction

Without question, 2009 has been an eventful year for the economy. The corporate downsizing and mergers now commonplace in the current market are a cause for not only concern about the health of our economy, but also concerns relating to the security of personal and financial data.

With companies being sold and mergers taking place, and on such tight deadlines, mistakes regarding the confidentiality and privacy of the data could be made. This presents an increasing risk for the security of personally identifiable information entrusted to these firms.

The goal of a typical Merger and Acquisition (M&A) transaction is to be able to benefit from the combined strengths and create a larger economic value. While doing so, overlooking information security risks can be detrimental to the business. Some of threats that mergers and acquisitions face include:

- Insider Threat
- Phishing Attacks
- Identity Theft
- Social Engineering
- Denial of Service
- Corporate Espionage
- Misuse of Information
- Theft, Fraud

Security in the M&A Process

Information Security needs to be an integral part of the M&A process. The changing security, risk, and threat profile requires that a security strategy be defined and executed during M&A. This Security Strategy brings together the relevant people, processes and technology to address the security challenges as a merged business.

Key aspects of information security that should be considered include the following:

- Aligning the Information Security Program Policies to reflect the new business
- Identity and Access Management
- Intellectual Property Protection
- Data Security
- Business Continuity
- Compliance Management and Governance

Solution

AT&T Consulting provides a variety of services that can help address the security risks and challenges that organizations face during and post M&A.

Security Strategy Development

An effective information security strategy is the key to meeting the challenges and risks that are posed by M&A. By treating security as an asset, it is possible to create a landscape where business practices and applications can be shared and integrated post merger based on a model of trust and accountability while maintaining the security objectives of the organization.

This can have the net effect of accelerating the M&A process and helping meet business mandates for consolidated applications, IT systems, and other assets.

To achieve this, it is critical for merging organization's to review their information security policies and combine them to align with the post merger organizations business goals. Once policies are aligned, a gap analysis should be performed, assessing the merged organization against the new policy and standards. A roadmap can then be generated showing the procedural and technological changes that will be needed.



Third Party Risk Assessment

For a successful M&A, it is crucial to identify key information assets. A risk assessment process is necessary to understand what you are trying to protect, and hence its value. Accurate information asset definitions will assist in the selection of controls to defend that data. The overarching goal is to protect organizational information assets, contribute to the security of interdependent critical infrastructures, and thus help protect the company's intellectual property.

A third party risk assessment should not only be performed based on due diligence but can also facilitate integration of the two security organizations, and assessing the potential impact of information security risks on competitiveness, financial loss, and legal liability.

Architectural Review

With a merging network, an architecture review is crucial in order to evaluate the security of the organization's network perimeter, and understanding how remote access and connectivity is secured. The network architecture review analyzes the organizations physical and logical network topology with a detailed examination of three critical areas:

- Network device configuration
- Management and monitoring capability
- Location and configuration of critical network services

Penetration Testing and Vulnerability Assessment

A vulnerability assessment service gives you the security posture of your network for a single snapshot in time. Due to the changes in infrastructure resulting from the M&A process, you may need to perform this security snapshot again in order to remediate any new vulnerabilities and to formulate your security agenda going forward.

Application Security

When companies come together, so must their application infrastructures. Securing and integrating applications, however, can open up a wide variety of security risks. The application security review can help identify security vulnerabilities by reviewing and probing an application's security controls.

Business Continuity

When it comes to business continuity, taking a proactive planning approach is essential especially during a merger/acquisition. Disruption of business from any type of event could lead to lost information,



revenue, customer confidence, and market share. AT&T Consulting can help the organization plan to achieve a state of business continuity, where critical business processes, systems and networks are available to support your availability objectives.

Compliance Management and Governance

The regulations that may become applicable after M&A might change the compliance framework and it is important to understand the applicable regulations to be able to tailor the controls to meet the changing regulatory landscape. Compliance driven efforts can be consolidated during the overall integration of the two business operations to achieve the required efficiency while maintain compliance. AT&T Consulting can work with your organization to develop a sustainable compliance management program that ensures ongoing regulatory compliance while keeping the process streamlined and cost effective.

Key Benefits

AT&T Consulting takes a holistic approach to the Merger and Acquisition security assessment, addressing elements of people, technology, and processes. We combine in-depth knowledge and use of Information Security Standards of Good Practice (SOGP), applicable regulatory requirements and our experience in information security management practices within the industry.

Security Solutions: Expertise from a Trusted Provider

AT&T provides a unique and world-class portfolio of assessment, compliance and related security services. Our stability, experience and expertise, and commitment to open standards have established us as a strategic and Trusted Advisor with our customers. With AT&T you can expect high quality solutions, a global network of proven technology, and a cost-effective program-based approach to meet your security and compliance needs.

For more information contact your AT&T Representative or visit us at www.att.com/consulting.

