AT&T Security Consulting – Mobility Security Risk Assessment Services

Assess Mobility Security Risks and Help Secure your Mobile Ecosystem

Mobility is transforming the way we conduct business and driving increased productivity for the enterprise, it also adds important security considerations that require mindful planning. Mobile devices and smart phones extend the wired information infrastructure, increasing the overall risk to organization networks and information assets. The balance between information protection and information access becomes more complex as the proliferation of mobile devices increases. To cope with the challenges introduced with the adoption of mobility in an organization, enterprise level mobility security standards must be adopted to support and promote a secure mobile ecosystem.

Evolving Security Needs of a Mobile Enterprise

• Managing and limiting access to sensitive information assets available to mobile devices
• Guarding the sensitive data that is stored on the device
• Securing lost or stolen devices
• Protecting against Malware – Viruses, worms, trojans and spyware
• Safeguarding against Direct Attack – Attacking device interfaces, browser exploits, etc.
• Defending against Data Communication Interception – Sniffing data as it is transmitted and received
• Securing against Identity Theft – Accessing resources with a user’s identity or credentials

Elements of Mobility Security

As the traditional enterprise boundaries begin to fade, it is paramount that mobile devices and the sensitive information they contain be managed and protected. As a result, security perimeters must also expand beyond the internal network to these numerous critical endpoints.

Mobile Device Management

Mobile device management within organizations becomes more complex and important as both the number of devices and the amount of sensitive data stored on the devices increases. A lost or stolen device may compromise the critical data stored on it, unless there are processes and tools in place to protect it.

Mobile Device Asset Discovery and Inventory

The first step in securing the mobile organization network is the identification of the current inventory of mobile devices and OS clients that exist within your infrastructure. Next, you must integrate the mobile devices that have been identified in this process into your existing asset inventory database. Consider the following as you develop or update your mobile device asset inventory:

• How will you identify the mobile assets?
• What are the related assets to this mobile device, for example, additional memory cards?
• How do you identify the asset owner and the business purpose of each device?

Benefits

• Supports the standardization of mobile eligibility, device types and service provisioning
• Supports a consistent level of end point security to help reduce risk
• Enables alignment with security and business objectives to maintain the integrity and confidentiality of your mobile ecosystem
• Incorporates best practices and strategies to safeguard organizational information exposed through mobile devices
• Promotes better alliance with your organization lines by being prepared
• Accelerates application deployment

Features

• Tier I – Mobility Security Risk Assessment
• Tier II – Mobility Security Risk Assessment and Mobile Application Security in depth review
Mobile Device Security Policy
Organizations need to identify and develop mobile security policies to be deployed which will provide adequate protection. The level of protection has to be aligned with the level of risk that the organization is willing to accept. These policies should ensure that the many regulatory or compliance concerns that might be applicable are addressed. The mobile security policy should be integrated within your overall information security policy framework. Key elements to address in the mobile device security policy are:

- Physical security of the device
- Address lost or stolen devices
- Acceptable uses of the device
- Encryption
- Password protection
- Storage
- Backup
- Access control
- Authentication
- Monitoring

Like every other security policy, an organization must regularly review its mobile device security policy, particularly after the acquisition of new mobile devices, configuration changes and in the wake of security incidents involving mobile devices.

Mobile Application Security
Mobile applications extend traditional network boundaries and introduce new avenues of attack. They often provide access to sensitive business and personal information. They are constantly challenging and extending their reach. Organizations need to ensure that a secure coding process is followed while building mobile applications and should include security testing as part of the Software Development Life Cycle (SDLC) process.

Security Awareness
Creating awareness programs to educate employees on the importance of protecting the organization’s confidential and sensitive information (including electronic information) and their own personal information helps staff better understand and reduce risks for mobile devices.

The introduction of modern mobile devices and smartphones to a corporate network environment brings with it new risks. Because of the increasing complexity and capabilities of mobile devices and smartphones, the security of these devices becomes critical in maintaining the confidentiality, integrity and availability of your systems and data.

In our experience, the rate at which mobile technologies are advancing surpasses the speed at which enterprises are able to adapt their procedures and processes to deal with new risks and challenges. This may jeopardize the organization’s security posture. There are a number of security considerations which are often not considered for mobile devices and smartphones, including but not limited to:

- Mobile device management and monitoring
- Device level attacks

Key Benefits
AT&T Consulting provides security services for your organization’s infrastructure that custom fit your requirements. We combine our vendor neutral in-depth knowledge of networking technologies, together with industry standards, applicable regulatory requirements, and business and technology requirements, in order to deliver information security services to your organization.

- Zones of trust, network segmentation and access control
- Patch application and management

Service Offering
AT&T Security Consulting offers Security and Risk Assessment services and provides a third party validation of the security framework that you have in place to adapt to the changing mobile infrastructure. This assessment covers the following areas of mobility security:

- Device inventory and controls
- Mobile device management
- Mobile device security
- Application controls
- Data controls
- Network level controls and protections

Our service helps you conduct a thorough security analysis of your current mobility ecosystem. The review assesses the effectiveness of your mobility infrastructure as it relates to data protection, application security, infrastructure protection, physical security and overall security governance and compliance.
Service Description

<table>
<thead>
<tr>
<th>Mobility Security Risk Assessment</th>
<th>Mobility Security Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tier I</strong></td>
<td><strong>Tier II</strong></td>
</tr>
<tr>
<td>- Security Configuration Review</td>
<td>- Security Configuration Review</td>
</tr>
<tr>
<td>• Mobile Application Security Review</td>
<td>• Mobile Application Security Review</td>
</tr>
<tr>
<td>- Review of application security requirements for third party apps</td>
<td>- Mobile Application Security Policy Review</td>
</tr>
<tr>
<td><strong>Deliverables</strong></td>
<td><strong>Deliverables</strong></td>
</tr>
<tr>
<td>• Mobility Security Risk Assessment Executive Summary Report</td>
<td>• Mobility Security Risk Assessment Executive Summary Report</td>
</tr>
<tr>
<td>• Templatized Policies and End User Agreements</td>
<td>• Templatized Policies and End User Agreements</td>
</tr>
<tr>
<td>• Best practice guidelines on security configuration for mobile device management</td>
<td>• Best practice guidelines on security configuration for mobile device management</td>
</tr>
<tr>
<td>• Device management process guidelines</td>
<td>• Device management process guidelines</td>
</tr>
<tr>
<td>• Application Development Gap Analysis</td>
<td>• Application Security Assessment Report</td>
</tr>
<tr>
<td>• Application Development Gap Analysis</td>
<td>• Application Security Assessment Report</td>
</tr>
</tbody>
</table>

**Security Solutions: Expertise from a Trusted Provider**

AT&T provides a unique and world-class portfolio of compliance and related security services. Our experience, expertise and commitment to open standards have established us as a strategic and trusted advisor.

By leveraging AT&T, you can expect best-in-breed 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, visit us at www.att.com/consulting/security, email us at mss@att.com or call 1-877-954-7771.