Summary of Security Assessment Findings (SAMPLE)

Assessment Date: 1/12/2011

Client: SAMPLE

SAMPLE COMPANY'S IT network has been determined to have an overall security categorization of **Moderate to High**. Risk assessment includes network, security, public access to folders, wireless security, database access and network access.

Summary of System Security Risks

Network Security		
Risk	**Findings**	**Risk Level** (Low, Moderate, High)
Company Email	Over 350 GB of mail data with 34+ mailboxes over 2GB each overburdens an Exchange server that is already overloaded	**Moderate**
Anti-virus	Numerous devices do not have current versions of anti-virus protection. Devices could be compromised leading to unauthorized network access and "lost" client data	
Open Ports	Several ports (10+) are currently open to the Internet for no apparent purpose; several of these types of ports are known targets for Trojans. At first glance, they do not appear to designated for specific applications or authorized third party access.	**Moderate**
Network Printers	N/A	**N/A**
Password Complexity	Acceptable domain password complexity	**Low**
Assessor Comments & Recommendations	Overburdened servers can lead to performance latency, and ultimately, corrupted data. Interception of unencrypted client confidential files via open network ports are a favorite vehicle for the broadcasting of Trojan viruses using your server as a proxy.	

Public Access to Folders		
Risks	**Findings**	**Risk Level** (Low, Moderate, High)
Shared Folders	"Acceptable" security on shared folders, but data filing system could user better organization.	**Low**
Guest Ports	N/A	**N/A**
Passwords	Acceptable domain password complexity	**Low**
Assessor Comments & Recommendations	A disorganized data filing system makes it more difficult for IT to quickly implement changes (i.e., change permissions) and recover files.	

Wireless Security		
Risks	**Findings**	**Risk Level** (Low , Moderate, High)
Wireless Encryption	Currently using WEP encryption. WPA 2 is recommended.	**High**
Encryption Identification	Good security keys on WAPs (w ireless access points)	**Low**
Coverage	Acceptable: At least three w ireless access points are available from anyw here in the office	**None**
Assessor Comments & Recommendations	Hackers (or other malicious users, typically disgruntled employees) can easily gain full access to the system, from your hallw ay, w ith WEP encryption. We recommend sw itching w ireless encryption to WPA2 immediately. Outdated encryption schemes makes the netw ork vulnerable to new viruses.	

Database Access		
Risks	**Findings**	**Risk Level** (Low , Moderate, High)
Database Access	Standard security and domain authentication is acceptable	**Low**
Other	Database server is overtaxed and can cause slow ness in application performance	**Low**
Assessor Comments & Recommendations	Overburdened server requires optimization of database or an upgrade to higher-capacity hardw are (server).	

Network Access		
Risks	**Findings**	**Risk Level** (Low , Moderate, High)
Unwarranted Access	Over half of the instances of Java and Adobe do not have the latest security patches installed	**High**
Assessor Comments & Recommendations	We highly-recommend patching the highly-visible vulnerabilities ASAP to protect from intruders. Storing non-core, security risk-prone softw are together w ith core-business applications (i.e., Juris) opens the door for additional security risks, primarily unauthorized access.	

Recommended Course of Action – immediately move to WPA2 encryption algorithms for wireless access; hackers in the outside hall (or disgruntled employees) can gain network access in less than five minutes with tools that can be downloaded from the Internet at no charge. Update anti-virus on all devices, including those not attached to the network, e.g. – laptops not in the office.