Remote Access Policy Audit

Johnson & Associates

December 1, 2015

Group Members

- Christopher Brewer
- Mauchel Barthelemy
- Nicholas Gikonyo
- Victoria A. Johnson

BACKGROUND

Johnson & Associates is a privately held law firm located in Center City Philadelphia that provides legal services to clients. Due to the important nature of the work, remote access using technologies such as Virtual Private Network (VPN) and Citrix is provided to the company information systems and data to certain employees and vendors to perform their work. Not all employees and vendors are entitled to this. Secure remote access is provided in an effort to help increase workers productivity and provide excellent services to clients.

Security is a serious matter at J&A. Poorly secured remote access augment the risk of exposing critical private and confidential company, employee and client data, which in turn could cause financial loss and other harmful business impacts. This is the primary reason the company's IT Strategy Committee, Board of Directors and IT Department have adopted necessary measures to protecting the sensitive information and produce an audit of the company's Remote Access Policy.

SCOPE AND OBJECTIVES

This audit document serves to clarify the purpose and objectives of the remote policy and to comply with industry laws and regulations. The Federal Government requires that all firms across the United States, regardless the natures of business, to design audit plans pertaining to Cyber Security. Therefore, J&A must plan and execute the audit to collect sufficient, appropriate evidence in order to provide a reasonable basis for our findings and guidelines/rules from the audit objectives. This document addresses J&A's practices in place as of 12/01/2015.

The following are J&A's audit objectives:
- Provide an assessment of the remote access control framework
- Evaluate user and device authentication, application controls and data controls
- Ensure adequate logging, monitoring and notification
- Ensure compliance with IT Security Policy.
- Identify potential areas that need improvement

CONTROL OBJECTIVES, CONTROL ACTIVITIES AND EVIDENCE

Control Objectives	Control Activities	Collection Method	Evidence
Ensure only approved users have remote access	Remote access request procedures are followed and documented	a. Get list of VPN users and cross check with access request forms b. Interview some approving managers to validate they provided authorization	-Employee and vendor list -Remote access request forms -Manager statements -Company hierarchical chart
	Terminated users have no remote access	a. Get list of terminated users in the last year b. Check logs to ensure none has connected since termination date c. Verify account is disabled/deleted in active directory d. Get list of permissions revoked in the last year and reason(s) provided	-Termination request forms -Active directory screenshots -Log search screenshots
	Business needs are evaluated and documented periodically and on job/role change	a. Get list of recent job changes b. Check if access request form are reviewed accordingly c. Get list of permissions modified in the last year and reason(s) provided	-Modified remote access request forms -List of job changes
Ensure only authorized devices can access corporate network remotely	Remote device provisioning procedures are followed and documented	a. Get list of all authorized devices b. Verify device provisioning forms were completed c. Interview approving manager to validate authorization	-List of authorized devices -Device request forms -Helpdesk tickets
	Unauthorized devices have no remote access	a. check firewall device access control list b. check firewall logs for devices connected in last year c. Configure and test an unauthorized device	-Firewall logs
Ensure remote devices have latest updates and antivirus definitions	Authorized devices must be up to date	a. Generate report from antivirus server b. Generate report from update services server c. Verify host integrity check is performed on connection	-Reports from servers -Device software inventory report

Control Objectives	Control Activities	Collection Method	Evidence
		d. Generate report showing devices denied access due to updates and/or antivirus	
Ensure adequate controls to protect unauthorized access to data remotely	Test and verify data and application controls	a. review remote connection profiles b. review remote application permissions c. run report on users denied access to application remotely	-Remote application and data profiles -Application logs -Firewall logs
Verify lost/stolen devices are reported to the company as required	Check that reporting procedures are followed	a. get list of devices reported lost or stolen in the last year b. check firewall access control list for devices reported lost in the list c. run report on authorized devices that have not connected in 30 days c. review firewall logs for devices	-Lost device list -Firewall logs
Ensure adequate logging and monitoring of all remote user actions and notifications	Acceptable logging level is enabled on all devices	a. check application logging level for VPN users b. check firewall logging level c. collect notifications sent to admins for anomalies detected d. check logs are secured, unmodified and backed up e. test notification(s)	-Firewall configuration -Emails with notifications -Tickets/documents showing action(s) on notification
Ensure strong acceptable encryption is used	Remote users use 128-bit key or larger	a. run firewall report for encryption technology used in the last 60 days b. run report to show devices denied access in the last year due to inadequate encryption c. test device with inadequate encryption	-Firewall logs

Collection Methods and Required Documentation

To complete our objective, we will take representative sample of remote users and vendors and gather evidence.

1. Physical Evidence:
   a. Review completed “Remote Access Request Forms”
   b. Review documentation of permission, roles and access control lists.
   c. Test a sample of users’ and vendors’ authorization and access control
   d. Test authentication methods for a sample of users and vendors
   e. Test unauthorized devices
   f. Test terminated employees and vendors access
   g. Review past audit reports
   h. Review internal IT reports

2. Testimonial Evidence
   a. Interview IT staff
   b. Interview IT management
   c. Interview managers providing approvals
   d. Interview remote users and vendors (phone and in-person)

3. Documentary Evidence
   a. Review firewall logs
   b. Review application profiles and logs
   c. Review network access logs
   d. Review reports and audit logs
   e. Review related policies, e.g. password policy, and procedures
   f. Review remote users’ authorized devices with IT staff

Samples of forms, reports, configurations and logs were copied and collected as part of evidence to support our findings in the report. All information is strictly confidential.