Audit of Wireless Networking Security in Government, Phases 1 and 2

Released: March 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: May 2010 Transcript

Self-assessment conducted by the Ministry of Citizens' Services

Currently, three recommendations are fully or substantially implemented and two are partially implemented.

Recommendations

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 1: To support the government's IM/IT (information technology and management) policies relating to wireless network security, government establish adequate procedures to ensure ministry compliance with the policies as established by the Office of the Chief Information Officer.	Fully or substantially implemented

Actions taken, results and/or actions planned

Ministries are required to complete an annual Information Security Policy Compliance self assessment focused on evaluating their compliance with Information Security Policy.

Work has been conducted by the Office of the Chief Information Officer to validate configuration of wireless devices in locations where standard wireless services provided by SSBC were not being used. The result was that the non-standard wireless access points were deactivated as they could not meet the security standard.

SSBC is assessing the feasibility of implementing technology to provide additional control, visibility and reporting in order to support the government's IM/IT policies relating to wireless network security.

Recommendation 2: Shared Services BC regularly update the job descriptions of all key IT personnel to ensure the roles and responsibilities are clearly delineated.	Fully or substantially implemented

Actions taken, results and/or actions planned

Key job descriptions have been reviewed to ensure they meet current requirements. Annual reviews will be performed to ensure these job descriptions remain current.

Within Security Operations of Shared Services BC, job descriptions have not been updated since the most recent organizational restructuring, however, the roles and responsibilities regarding Security Operations have been unchanged. Those job descriptions remain accurate.

Though a series of organizational restructuring makes it challenging to keep job descriptions current, the roles and responsibilities remain unchanged in many cases. Shared Services BC reviews and updates job descriptions as needed.

Audit of Wireless Networking Security in Government, Phases 1 and 2

Released: March 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: May 2010 Transcript

Recommendations (cont.)

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 3: Government develop a network access control solution for monitoring and detecting, on a real time basis, unauthorized computing devices — particularly wireless — connected to the government network, including devices that are not configured properly.	Partially implemented
Actions taken, results and/or actions planned Shared Services BC has completed a proof of concept for basic Network Access Control, and a Findings and Recommendation document has been completed. The Findings and Recommendation document is being reviewed by Shared Services BC Executives.	
Recommendation 4: Shared Services BC implement mechanisms and procedures to scan and confirm that only properly configured and authorized wireless access devices are installed when connecting to the government network infrastructure.	Partially implemented
Actions taken, results and/or actions planned Fully addressing this recommendation is dependent on the implementation of Recommendation 3. Network Access Control will fulfill this requirement. This is also being addressed by the enhanced monitoring tools being implemented for the Payment Card Industry Data Security Standard.	
Recommendation 5: For monitoring purposes, Shared Services BC develop a process for establishing and updating an inventory list of authorized wireless access devices and that the list be verified periodically.	Fully or substantially implemented
Actions taken, results and/or actions planned Shared Services BC has established an inventory list of authorized wireless access devices for monitoring purposes and updates it on a regular basis for additions and removals.	

Audit of Wireless Networking Security in Government, Phases 1 and 2

Released: March 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: May 2010 Transcript

Self-assessment conducted by Simon Fraser University

Excellent progress has been made on instituting a more intentional governance structure for all aspects of information technology at SFU, with the formation of four senior committees and a number of lower-level standing and project steering committees. Some alternative actions have been taken to ensure we continue to provide a level of wireless security consistent with an open university environment where most machines using the wireless network are neither owned nor controlled by SFU.

Recommendations

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 1: Establish a formal IT committee with a strong mandate to oversee IT strategic direction, IT needs of the university community and, most importantly, the protection of the university's IT network.	Fully or substantially implemented

Actions taken, results and/or actions planned

The new IT governance committees are in the early stages of operation, with the first committee meetings held in June 2010. As planned, there are four governance committees: IT Strategies, Administrative IT, Research IT, and the Learning & Teaching Coordinating Committee. Initial activities have focussed on new approval processes and the articulation of high-level IT strategies.

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 2: Establish an IT Security Officer position that has exclusive duties and responsibilities relating to IT security and is accountable to independent senior management.	Fully or substantially implemented

Actions taken, results and/or actions planned

Our IT Security Officer has now begun meeting with the Internal Auditor, with the regularity and frequency of meetings to be determined by them. Internal Audit reports to the Vice-President, Legal Affairs, while IT Services reports jointly to the Vice-President, Administration and Finance, and to the Associate Vice-President, Academic.

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 3: Ensure that the Information Security Policy is supported with detailed wireless security standards and procedures to guide the implementation and maintenance of a robust wireless security network.	No action taken

Actions taken, results and/or actions planned

The new IT Governance committees have not yet discussed the need for or contents of either an Information Security Policy or wireless security standards and procedures.

Audit of Wireless Networking Security in Government, Phases 1 and 2

Released: March 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: May 2010 Transcript

Recommendations (cont.)

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 4: Establish policy and procedures to ensure that users are formally and regularly asked online to accept the policy for appropriate use of communication technology (including wireless) provided by the university.	Alternative action taken

Actions taken, results and/or actions planned

Students and other users are informed of the policy on appropriate use, on various web sites and in labs, and held accountable for following it.

The new IT Governance committees have not yet discussed how or whether formally accepting the existing policy on appropriate use will be required.

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 5: Enforce periodic change of password.	Alternative action taken

Actions taken, results and/or actions planned

SFU management, including the audit committee of the Board of Governors, maintains the position that frequent, mandatory password changes would not be beneficial.

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 6: Require staff with high-level access rights to systems, applications and data to access system resources using secured wireless methods only.	Alternative action taken

Actions taken, results and/or actions planned

This remains to be addressed, although we have no empirical evidence that this issue poses significant risk to SFU. Web pages and other communcations to staff continue to stress the general preference for using the secure wireless network, SFUNET-SECURE. This includes a link from the insecure wireless login page to instructions on connecting to the secure network.

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 7: Conduct review to limit the use of ad hoc and peer-to-peer networking.	No action taken

Actions taken, results and/or actions planned

Most of the devices that connect to SFU wireless are neither owned nor controlled by SFU, and so occasional uses of ad hoc and peer-to-peer networking occur, mostly on student-owned machines. We have no empirical evidence that this issue poses significant risk to SFU.

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 8: While monitoring wireless networking activities, ensure that log reviews are fully documented and include such information as the type of reports reviewed, the date of the review, and what action has taken place.	Alternative action taken

Actions taken, results and/or actions planned

Network monitoring & logging are part of our normal operations. While more audit reports of log reviews could certainly be assembled, this does not appear to add significant value to our wireless security, particularly in view of the automatic monitoring for certain types of unauthorized use that is performed currently by our Enterasys Dragon Security Command Console.

Audit of Wireless Networking Security in Government, Phases 1 and 2

Released: March 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: May 2010 Transcript

Self-assessment conducted by the BC Institute of Technology

Thank you for the opportunity to update our progress on the recommendations. Wireless networking security continues to be an important aspect at BCIT.

BCIT agreed with the three of the four recommendations. Of these three recommendations two of them are fully or substantially implemented and the third is expected to be in place by the end of 2011. For the fourth recommendation an alternative, already in place, was documented in the initial response.

Recommendations

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 1: BCIT ensure its policies address wireless network infrastructure in detail, and that the policies be supported by detailed wireless networking standards and specific procedures and guidelines for managing wireless network resources.	Fully or substantially implemented

Actions taken, results and/or actions planned

Initial Response: We agree with this recommendation. BCIT's policies are based on an international standard (ISO 17799:2005), and are intended to be independent of the network technology. Information specific to the security requirements and characteristics of each network zone is intended to be included in the "Procedures and Guidelines" associated with the policy. According to section "5.6 - Network Management" of Policy 3502 (Information Security Policy) last updated January 2009, each network zone, including the wireless zones, should have "….documentation covering its topology, configuration, and gateways to external networks and nodes…." and "…clear guidelines and…security characteristics". These are being documented as part of the "procedures and guidelines" associated with this policy, and are expected to be complete by June 2010.

Update: The guidelines associated with the information security policy have been updated to include detailed wireless networking standards and are expected to be published shortly. Wireless network zone documentation has been created that covers topology, configuration including defences and inter-zone relationships, zone usage and guidelines for devices within the zone.

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 2: BCIT's management review its policies to ensure that those relating to ad hoc and peer-to-peer networking, the enforcement of password security, and retention of activity logs generated by wireless systems follow recognized best practices.	Fully or substantially implemented

Actions taken, results and/or actions planned

Initial Response: We agree with this recommendation. All BCIT policies have a regular and predictive review schedule. BCIT's Information Security policy (Policy 3502) expressly addresses access control and password use requirements, as well as logging requirements for user activities. Specific details are being documented as part of the "procedures and guidelines" associated with this policy, and are expected to be complete by June 2010.

Update: The guidelines associated with the information security policy have been updated to include: ad hoc and peer-to-peer networking; enforcement of password security; and retention of activity logs generated by wireless systems. The guidelines are expected to be published shortly.

Audit of Wireless Networking Security in Government, Phases 1 and 2

Released: March 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: May 2010 Transcript

Recommendations (cont.)

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 3: Management require, in policy, staff with higher level access rights to systems, applications and data to log on using secured wireless methods only.	Partially implemented

Actions taken, results and/or actions planned

Initial Response: We agree with this recommendation. BCIT's priority however is to ensure end-to-end encryption. This ensures full protection and security regardless of where the user is accessing the application/data. As users are becoming more mobile and accessing systems remotely using network segments that are beyond the control of BCIT/ITS (for example, hot spots in airports, cafes, business centres in hotels, etc.), applying end-to-end level security and encryption will ensure that data is consistently protected regardless of where the user is accessing it. Additionally, BCIT has now implemented a secure VPN gateway for accessing data and systems from off campus. We will continue to promote the use of the secured Eduroam network for administrative users accessing applications and data wirelessly on campus, and will ensure that all "administrative" users accessing the wireless network on campus will be using Eduroam by default within 2 years.

Update: We have continued to promote the use of the secured Eduroam network for administrative users accessing applications and data wirelessly on campus. By the end of 2011 all "administrative" users accessing the wireless network on campus will be using Eduroam by default.

Recommendation 4: Job positions in IT network operations be supported by clearly defined responsibilities to ensure incompatible duties are not assigned to one individual. If segregation of duties is not possible or feasible because of resourcing limitations, we recommend that there be closer management oversight of the activities carried out by those in IT network operations.	Alternative action taken

Actions taken, results and/or actions planned

Initial Response: Policy 3501 (Acceptable Use of Information Technology) expressly states that "IT Administrators and other privileged users must protect the security of information and must not abuse their elevated privileges". BCIT IT Services operates under the ITIL framework and best practices for Change Control. This requires any system level change (software, infrastructure, etc.) be planned, reviewed, and approved by the Change Advisory Board (CAB) that has both Management and departmental technical resources allocated to this activity.

The CAB has the authority to approve or deny any updates, changes, additions to the IT environment.

Update: As stated in the initial response, system level changes require review and approval by the Change Advisory Board.