Audit of Wireless Networking Security in Government, Phase 2

Released: March 2010
1st Follow-up: April 2011
2nd Follow-up: October 2011 Discussed by the Public Accounts Committee: May 2010 Transcript

Self-assessment conducted by the BC Institute of Technology

Recommendations

RECOMMENDATIONS ADDRESSED IN PREVIOUS FOLLOW-UP REPORT(S):	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**
Recommendation 2: BCIT's management reviews 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**
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**

Outstanding recommendations

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.	**Fully or substantially implemented**

Actions taken, results and/or actions planned

BCIT has completed the documentation, review, approval and publication of the Information Security Policy - Policy 3502 (http://www.bcit.ca/files/pdf/policies/3502.pdf). The policy speaks to this issue throughout the policy, and specifically in section 5.8.2. The specific guidelines and procedures that accompany the policy have both been developed and are currently in the approval process. The procedures and guidelines for accessing confidential and secure information include the use of the secured and encrypted SSID (Eduroam) and/or the use of a secured and approved VPN tunnel. Use of the BCIT VPN tunnel requires an explicit set of actions that include the individual requiring access to have Management approval, and the logging of the individuals AD identity in order for them sign on and use the VPN using that approved ID and password.

Audit of Wireless Networking Security in Government, Phase 2

Released: March 2010
1st Follow-up: April 2011
2nd Follow-up: October 2011 Discussed by the Public Accounts Committee: May 2010 Transcript

Self-assessment conducted by the Ministry of Labour, Citizens' Services and Open Government

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

Recommendations

RECOMMENDATIONS ADDRESSED IN PREVIOUS FOLLOW-UP REPORT(S):	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**
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**
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**

Outstanding recommendations

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 completed a proof of concept for basic Network Access Control. A Findings and Recommendation document was reviewed by Shared Services BC Executives and the document is now being revised based on the feedback, which will also align the document with the Transformation and Technology Initiatives.

Recommendations (Cont.)

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.

Audit of Wireless Networking Security in Government, Phase 2

Released: March 2010
1st Follow-up: April 2011
2nd Follow-up: October 2011 Discussed by the Public Accounts Committee: May 2010 Transcript

Self-assessment conducted by Simon Fraser University

All recommendations have now been dealt with, except Recommendation 3, which has been waiting for SFU's new IT governance framework to mature sufficiently. The policies, standards, and procedures implied by Recommendation 3 will come before the committee during the Fall 2011 semester.

Recommendations

RECOMMENDATIONS ADDRESSED IN PREVIOUS FOLLOW-UP REPORT(S):	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**
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**
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**
Recommendation 5: Enforce periodic change of password.	**Alternative action taken**
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**
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**

Outstanding recommendations

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.	**Partially implemented**

Actions taken, results and/or actions planned

A senior SFU committee, the IT Strategies committee, has met six times since its creation last year, and has discussed the new governance framework, developed an overall strategic plan for IT, formalized funding and approval processes for major IT projects, and approved several urgent projects. Wireless security policies and procedures will be brought to the committee for discussion and approval during the Fall 2011 semester.

Recommendation 7: Conduct review to limit the use of ad hoc and peer-to-peer networking.	**Alternative action taken**

Actions taken, results and/or actions planned

Most staff computers in administrative departments, and a growing number of them in academic departments, are "managed" desktops. Users do not have administrator access to them, the ability to act as a peer-to-peer server is disabled, and the software image on the machine is designed, enforced, and maintained by SFU IT Services.