Wireless Networking Security: Phase 3 (*Summary Report*)

Camosun College

Released: December 2011
1st Follow-up: March 2012
Discussed by the Public Accounts Committee: this report has not yet been discussed

Self-assessment conducted by Camosun College

Camosun College is continuing to follow up on the recommendations as part of a wider focus on security of systems and enterprise data. Completion of most of the recommendations is expected to be accomplished during 2012.

Recommendations

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
MAINTAIN EFFECTIVE MANAGEMENT OF WIRELESS SECURITY	
Recommendation 1: Finalize and formally adopt the Information and Network Security Policy, and support the policy with detailed standards on wireless networking security and specific procedures or guidelines to manage wireless networking resources.	**Partially implemented**
Actions taken, results and/or actions planned Policies have been developed and are now in the process of institutional review prior to final approval and publication. Standards, procedures and guidelines being updated.	
Recommendation 2: Update communication of IT security policies, guidelines, procedures and standards to wireless device users; work to make people aware of the risks of using unsecured wireless networking; and communicate this message more visibly (e.g. by posting notices in Wi-Fi areas, by running a warning page on the log-on screen).	**No action taken**
Actions taken, results and/or actions planned Natural follow up to Recommendation 1. When materials are approved and published, this recommendation will be completed.	
Recommendation 3: Formalize the IT security function by detailing the responsibilities in the Senior Network and Security Administrator job description; and ensure that senior IT management provides strong oversight and monitoring of the IT security function.	**Fully or substantially implemented**
Actions taken, results and/or actions planned IT security is defined as part of the role of the current Senior Network Administrator job description, which is current. The Director ITS is the senior technology position at the college and has oversight of the security function.	

Recommendations (Cont.)

Recommendation 4: Periodically update the job descriptions for key IT positions to ensure proper accountability for the associated roles and responsibilities.

Partially implemented

Actions taken, results and/or actions planned

Inventory of all ITS job descriptions has been done and key positions are in the process of review by the college.

Recommendation 5: Establish a formal training program for key IT staff to ensure that their knowledge in IT is kept up-to-date and they are able to properly maintain and install the network.

Alternative action taken

Actions taken, results and/or actions planned

The college and ITS does not have the financial capacity to implement this recommendation. Funding exists for targetted training and selected professional development opportunities.

Recommendation 6: Formally document the network infrastructure, with details showing how the network is integrated with the wired and wireless networks; and have senior IT management formally approve the network infrastructure diagram and update it periodically.

Partially implemented

Actions taken, results and/or actions planned

Documentation on network infrastructure is being completed by new network resources.

SECURE WIRELESS INFRASTRUCTURE

Recommendation 7: Change certain wireless connecting practices to higher level security settings.

No action taken

Actions taken, results and/or actions planned

The college requires a public wireless connection capability and feels this is a low risk.

Recommendation 8: Require all staff who have higher level access rights to systems, applications and data to use only secured wireless methods, such as Eduroam.

Partially implemented

Actions taken, results and/or actions planned

Eduroam is now fully functioning and will be the recommended wireless access for all staff.

Recommendation 9: Follow best practice to properly segment the IT network in order to mitigate the risk of the whole network being exposed should security be compromised.

Partially implemented

Actions taken, results and/or actions planned

Logistically challenging and the college feels that this is a relatively low risk.

Recommendations (Cont.)

Recommendation 10: Follow recognized best practices relating to password security, requiring the:

- regular changing of passwords;
- creation of effective passwords; and
- enforced change of passwords for key personnel.

No action taken

Actions taken, results and/or actions planned

Mandate for implementation of this recommendation still pending. Expected action for summer 2012.

MONITOR WIRELESS SECURITY

Recommendation 11: Implement secure back-up procedures for activity logs in case the original logs are accidentally or intentionally deleted or altered.

Fully or substantially implemented

Actions taken, results and/or actions planned

Done.

Recommendation 12: Establish formal policies and procedures for monitoring network activities. The policies should cover, at a minimum: types of monitoring; frequency of monitoring; designated authorized individuals; documentation requirements; retention of logs; and reporting.

Partially implemented

Actions taken, results and/or actions planned

Review and further development of documented procedures under way. Tools developed to regularly scan logs for anomalous activities.

Recommendation 13: Perform regular scanning to validate the functionality of the wireless controller to ensure it is functioning in accordance to expected functionality.

Fully or substantially implemented

Actions taken, results and/or actions planned

Done. Regular scanning continues.

Recommendation 14: Formulate action plans to deal with: unauthorized access devices; security/privacy breaches; and intrusive or malicious activities against the college network either through wired or wireless network.

Partially implemented

Actions taken, results and/or actions planned

Action plans are developed. Documentation and publication to come.

Recommendation 15: Ask the vendor to provide a list of criteria for use in determining whether the monitoring devices are programmed adequately with sufficient logic to detect malicious activities.

No action taken

Actions taken, results and/or actions planned

College is uncertain of the viability and practicality of this recommendation.

Wireless Networking Security: Phase 3 (*Summary Report*)
University of British Columbia

Released: December 2011
1st Follow-up: March 2012
Discussed by the Public Accounts Committee: this report has not yet been discussed

Self-assessment conducted by the University of British Columbia

The University of British Columbia would like to thank the Auditor General office for working with us to identify improvements to the management and security of our wireless LAN. We have made progress in all areas with two recommendations being fully or substantially implemented and expect to be able to fully or substantially complete the remaining items within the next year.

Recommendations

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
MAINTAIN EFFECTIVE MANAGEMENT OF WIRELESS SECURITY	
Recommendation 1: Expand WLAN policies to cover the minimum areas listed in best practice guides, in order to ensure the enforcement of undisputed direction for WLAN security and infrastructure.	**Partially implemented**
Actions taken, results and/or actions planned UBC committed to performing a gap analysis against the points listed in the audit to identify which ones would be applicable for our institution and then implement the changes. To-date we have completed the gap analysis and are initiating the process of drafting changes to Policy #130.	
Recommendation 2: Require that the Information Network Security Policy be supported by detailed formal documentation of standards on wireless security networking and by specific procedures and guidelines to manage wireless networking resources.	**Partially implemented**
Actions taken, results and/or actions planned We are consolidating our technical, product, process and reference standards into detailed formal documentation and are approximately 50% complete.	

Recommendations (Cont.)

Recommendation 3: Have senior IT management periodically review, update and approve key policies and guidelines.	**Partially implemented**

Actions taken, results and/or actions planned

The university has undertaken a new Information Security Management programme that has reviewed and substantially re-written the UBC Information Security Manual, which forms the main body of policy #106, UBC's primary security policy; the remaining two policies will be reviewed under the context of that programme, as a part of our overall information security governance on a regular basis. Reviews are to be conducted on an annual or bi-annual basis depending upon the policy.

Recommendation 4: Require that all job description documents for key IT personnel show evidence of having been formally approved, and when, by Human Resources and senior IT personnel.	**Fully or substantially implemented**

Actions taken, results and/or actions planned

Unfortunately, due to a change in our position management system, some of the older job descriptions were not transferred from the previous system to the new one, causing the discrepancies identified in this audit; however, all job descriptions in UBC IT have since been reviewed, within the context of a new IT career framework that was developed jointly with the central HR department, and all UBC IT job descriptions have been updated. Additionally, as part of the new Performance Development processes, managers review their employees JD's and makes notes on changes and justify those changes for the official records. Any significant changes are updated in the Position Management system and are then sent to HR to receive their formal approval.

MONITOR WIRELESS SECURITY

Recommendation 5: Implement secure back-up procedures for activity logs in case the original logs are accidentally or intentionally deleted or altered.	**Fully or substantially implemented**

Actions taken, results and/or actions planned

We have acquired and deployed a SIEM solution and are now capturing the activity logs thereby providing the back-up required.

Recommendation 6: Perform regular scanning to validate the functionality of the wireless controller to ensure it is functioning in accordance to expected functionality.	**Partially implemented**

Actions taken, results and/or actions planned

We previously had an informal practice of war-walking, whereby we validate the effectiveness of our automated rogue AP detection via the WCS. As a result of this recommendation we have formalised this process so that the results of that war-walking exercise are documented, tracked, correlated and reported to management on a regular basis. To carry out this activity we have hired an individual and are in the process of providing training to carry out the activity.

Recommendation 7: Ask the vendor to provide a list of criteria for use in determining whether the monitoring devices are programmed adequately with sufficient logic to detect malicious activities.	**Partially implemented**

Actions taken, results and/or actions planned

The Cisco WCS is a state of the art WLAN management system that detects rogue APs in real-time. We are working with the vendor on defining the necessary criteria.