Wireless Networking Security: Phase 3
(Summary Report – Results of Completed Projects) Camosun College

As at: August 1, 2012
Released: 2 December 2011
1st Follow-up: March 2012

Self-assessment conducted by Camosun College IT Services

Comments:

Progress continues to be made on the majority of the recommendations. College has just completed a full external security audit, including a wireless component. Recommendations from that review will be the next priority in the security project portfolio.

Camosun College has completed the majority of work recommended in this audit and recommends that the AG close this audit file.

Recommendations

RECOMMENDATIONS ADDRESSED IN PREVIOUS FOLLOW-UP REPORT(S):	SELF-ASSESSED STATUS
Maintain Effective Management of Wireless Security	
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**
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**
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**
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**

Recommendations (Cont.)

Outstanding 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.	**Fully or substantially implemented**
Actions taken, results and/or actions planned Policies and procedures developed and awaiting adoption by governance group in fall 2012	
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).	**Partially implemented**
Actions taken, results and/or actions planned Communication will occur after governance has endorsed & adopted policy & procedures.	
Recommendation 4: Periodically update the job descriptions for key IT positions to ensure proper accountability for the associated roles and responsibilities.	**Fully or substantially implemented**
Actions taken, results and/or actions planned Done.	
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.	**Fully or substantially implemented**
Actions taken, results and/or actions planned Documentation complete and approved by Director, IT Services	
Recommendation 7: Change certain wireless connecting practices to higher level security settings.	**No action taken**
Actions taken, results and/or actions planned College requires public wireless connections and no further action will be taken.	

Recommendations (Cont.)

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.	**Fully or substantially implemented**
Actions taken, results and/or actions planned Eduroam is the standard for staff and recommended for student use	
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 no further action is planned	
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 from Governance committee expected in Fall 2012	
Monitor Wireless Security	
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 In process of development	
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 Documentation and publication still in progress	
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 No further action is anticipated.	

Wireless Networking Security: Phase 3
(Summary Report – Results of Completed Projects) University of British Columbia

As at: August, 2012
Released: 2 December 2011
1st Follow-up: March 2012

Self-assessment conducted by the University of British Columbia

Comments:

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 with four recommendations being fully or substantially implemented and expect to be able to fully or substantially complete the remaining recommendations by the end of the calendar year.

Recommendations

RECOMMENDATIONS ADDRESSED IN PREVIOUS FOLLOW-UP REPORT(S):	SELF-ASSESSED STATUS
Maintain Effective Management of Wireless Security	
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**
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**

Outstanding 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**

Recommendations (Cont.)

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.

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

Actions taken, results and/or actions planned

The university currently has Policies #104 and #106 under review via a dedicated committee. That review will also set out terms for the periodic reviews. Policy #130 is being updated to address issues identified in the report and will also have a set review period as part of that update.

Monitor Wireless Security

Recommendation 6: 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

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 provided 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 have contacted the vendor but have had difficulty obtaining a clear response as to whether or not they will provide the criteria.