Presented To:	Audit Committee
Presented:	Tuesday, Jun 17, 2014
Report Date	Wednesday, Jun 11, 2014
Type:	Managers' Reports

Request for Decision

Audit Review - Heartbleed Vulnerability Assessment

Signed By

Auditor General
Brian Bigger
Auditor General
Digitally Signed Jun 11, 14

Recommendation

THAT the City of Greater Sudbury receive this update on the results of the Auditor General's review to determine if there were any concerns related to the Heartbleed Vulnerability.

SUMMARY

Background
• This threat was identified during the week and resulted in almost immediate lock down of Canada Revenue Agency site.

Scope
• The Office of the Auditor General has not performed a comprehensive threat analysis of all locations of CGS and this report is based on online tests performed and information provided by IT.

Objectives
To assess the risk and mitigation strategies arising from discovery of threats to information technology resources of CGS from “Heartbleed” virus and vulnerabilities of SSL (Secure Socket Layer). This vulnerability allows attackers to intercept secure communications and steal sensitive information such as login credentials and personal data.

• Determine whether the City IT Department’s response to the Heartbleed threat appeared appropriate in the circumstances.
• Conduct independent tests (Symantec), to support staff assurances that risks to the City, if any, were minimal.

Methodology
• We interviewed the City’s IT Department staff regarding their response to the Heartbleed Vulnerability. Attendees:
• Jim Dolson, Manager of Network and Operations Support
• Clayton Schiewek, System Specialist
• Curtis Schiewek, Senior Programmer Analyst
• Brian Bigger, Auditor General, City of Greater Sudbury
• Vasu Balakrishnan, Senior Auditor, City of Greater Sudbury

Risks / Opportunities We Evaluated

• The City's IT Department assessment of, and response to OpenSSL Heartbleed Vulnerability

Elements Not Operating Effectively
• None observed through our follow up.

Elements Operating Effectively
• The Auditor General's Office performed a vulnerability test for OpenSSL Heartbleed vulnerability assessment from Symantec site on the following sites of the City of Greater Sudbury:
a) www. greatersudbury.ca
b) www.gsuinc.ca
c) www.gsps.ca/en/
d) www.sudburylibraries.ca/en/
e) www.sdhu.com/

The test results were as follows:

Site Address and site Test result Other vulnerabilities
www. greatersudbury.ca – City of Greater Sudbury Server is not vulnerable to Heartbleed attack.

- None

www.gsuinc.ca – GSU Inc. Server is not vulnerable to Heartbleed attack.

- None

www.gsps.ca/en/ -Greater/Grand Sudbury Police Encountered an issue scanning this site for the Heartbleed Vulnerability.

- Wrong certificate installed. The domain name does not match the certificate common name or SAN.

www.sudburylibraries.ca/en/ -Sudbury libraries Encountered an issue scanning this site for the Heartbleed Vulnerability.

- Wrong certificate installed. The domain name does not match the certificate common name or SAN.

www.sdhu.com/ - Sudbury and District Health Unit Server is not vulnerable to Heartbleed attack.
2 Errors.

- Wrong certificate installed. The domain name does not match the certificate common name or SAN.
- The certificate has expired. This site is not secure.

• In the two instances where an issue was encountered during scanning for sites of Sudbury libraries and GSPS, risk from failure of tests and the likely impact needs to be assessed by the information technology department, based on the type of information transmitted between potential users. A copy of the report has been shared with IT.

Among other information provided by IT during a meeting, the following was noted:

1. One of the two servers that rely on SSL is used internally by CGS employees with no remote access,
2. The other server that was used for non critical applications as storing bus routes etc was briefly exposed to this threat during the period 17th Dec., 2013 to 7th April, 2014, when the vulnerable SSL1 was patched.
3. City employees use Windows NetMotion Mobility XE client to remotely access City IT resources. This software is not susceptible to the Heartbleed vulnerability.
4. Information Technology department plans to force all employees to change their passwords in a phased manner - 50 users at a time during the week from 14 April, 2014.
5. A plan to assess risk exposures arising from exchange of information between various stakeholders and

other locations of CGS such as Pioneer Manor is proposed to be initiated with remedial responses, if required.

Based on the information provided during the meeting, it appears no remote payment transactions are being performed by these other locations of CGS.

Management Response

We cant comment with respect to the health unit or GSU, however GSPS and the Library sites show up as a false positive simply because there is no SSL needed or active on those sites. The scanning tool is returning a false positive because it is specifically looking for SSL certificates. None exist nor are they required with any non SSL sites. If the nature of those specific sites were to change in the future and security was required, SSL and certificates would be implemented at that time.

Conclusion

The City IT Department's response to the Heartbleed threat appeared appropriate in the circumstances.

Independent tests supported staff assurances that risks to the City, if any, were minimal.

We thank Staff for their cooperation and assistance in the completion of this review.

Vasu Balakrishnan, CPA, CA, CIA, CISA
Senior Auditor
vasu.balakrishnan@greatersudbury.ca

Brian Bigger, CPA, CGA, CRMA
Auditor General
brian.bigger@greatersudbury.ca