



**Internal Audit Department**  
350 South 5th Street, Suite 302  
Minneapolis, MN 55415-1316  
(612) 673-2056

*Audit Team on the Engagement:*  
Jacob Claeys, CGAP, CICA  
Magdy Mossaad, MBA, CIA, CMA, CFE, CPA  
Protiviti

- Mike Thor
- David Lubin
- Benny Sharp
- Marc Doyle
- Paul Slye

---

# External Penetration Assessment

**Published by Order of the Audit Committee  
on  
April 25, 2012**

Report # 2012-02

This External Penetration Assessment included a review of security data that the Minnesota Data Practices Act legally classifies as not public. To protect City resources and comply with the Act, we withheld specific security-related details from this publicly released report. We communicated all pertinent details to management in a separate, not public document.



**Date:** April 25, 2012

**To:** Otto Doll, Information Technology (IT)

**Cc:** Beth Cousins, IT  
Jayne Khalifa, City Coordinator's Office  
Deb Parker, IT  
Bert Sletten, IT

**Re:** External Penetration Assessment Report # 2012-02

### **Background**

The City of Minneapolis (The City) processes and retains information on behalf of citizens, employees and other stakeholders that is classified as not public data by the Minnesota Government Data Practices Act. The City has legal requirements under state and federal law to safeguard the not public data it retains. Effective information security relies on the combination of robust technical configurations, automated and/or manual processes and proper accountability to ensure the confidentiality, integrity and availability of corporate systems and data.

The Internal Audit Department (IA) engaged Protiviti Inc. (Protiviti)<sup>1</sup> to conduct a network penetration assessment of the City's external infrastructure (internet accessible). The City's external technology infrastructure is composed of a variety of computing platforms, operating systems, applications, services, and network devices that support critical applications and store critical business information.

Project objectives focused on evaluating controls in place to mitigate threats and risks that may compromise the internet-facing information technology environment that supports City's business operations.

This report is intended solely for the use of management and leadership of the City and is not to be used or relied upon by others for any purpose whatsoever. This report and the related findings and recommendations detailed herein provide management with information about the condition or risks and internal controls at a point in time. Future changes in environmental factors and actions by personnel may adversely impact or enhance these risks and controls in ways that this report did not and cannot anticipate. For all responses where management is not choosing to follow these recommendations, the City is accepting the associated risk.

This report presents the results of the External Penetration Assessment that was performed for the City during November and December 2011. The scope of the review was limited to specific target systems which were agreed upon during project scoping. This summary report is designed for the reader to understand the level of security assessed, to identify security deficiencies and areas of strength and weakness, and to develop a course of action to correct vulnerabilities and mitigate associated risks.

Vulnerability testing is an uncertain process which is based upon past experiences, currently available information, and known threats. It should be understood that all information systems, which by their nature are dependent on their human operators, are vulnerable to some degree. Therefore, while IA believes to have identified detectable vulnerabilities on the systems analyzed, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures. This report

---

<sup>1</sup> Any reference to IA throughout this report refers to the work performed by Protiviti.



identifies known vulnerabilities that were detected during the test period; new devices, configuration changes and new/future vulnerabilities were not tested. While the matters presented herein are the result of our review, had additional procedures been performed, other matters may have been identified that would have been reported.

Additionally, this report contains information concerning potential vulnerabilities of the City and methods for exploiting them. This External Penetration Assessment included a review of security data that the Minnesota Data Practices Act legally classifies as not public. To protect City resources and comply with the Act, IA withheld specific security-related details from this publicly released report. IA communicated all pertinent details to management in a separate, not public document.

### **Objectives and Scope**

The primary objective of the assessment was to identify and evaluate the security posture and potential risk exposures associated with the City's external network environment. Emphasis was placed on evaluating information that was publically available and attempting to escalate any achieved access to see if access to internal City resources could be accessed. Fieldwork was conducted from November 14, 2011 through December 20, 2011.

The scope of the assessment included the following:

- External Network Penetration Testing – Performed testing against City Internet-facing (external) assets in an attempt to identify weaknesses that could be exploited by a user who did not have physical access to City office locations and/or internal network.

### **Summary of Conclusions**




The City has many good aspects to its external network security posture. The security measures in place are apparent as the review identified relatively few vulnerabilities. The number of open ports and unnecessary services is kept at a minimum. The majority of services were found to be running up to date versions. Attempts to perform cross-site scripting attacks were stopped by strong input filtering on externally facing web applications. Checks for common vulnerabilities due to improperly configured systems and services produced only low results. No high risk level vulnerabilities were observed; however, during the review several opportunities for improvement in the external environment were also observed.

IA has provided recommendations in this report to the management of the City's IT department.

## Criticality Rating Definitions






IA has assigned one of the following risk levels to the observations made during this assessment. Each risk level indicates the impact and likelihood of observed vulnerabilities in the City's Control environment. This assessment can be used by management as a tool to determine how quickly attention should be given to each observation provided within this report. Risk levels assignments are subjective and based on the scope of work completed for this assessment only.

The risk levels assigned by IA are described below:

Risk Level	Significance
 <b>High</b>	Observed vulnerabilities assigned a high risk level are considered to present an imminent and significant threat and should be addressed as soon as possible.
 <b>Medium</b>	Observed vulnerabilities assigned a medium risk level do not pose an immediate threat, but could likely cause a noticeable impact. These should be addressed in a timely manner once high level risks have been addressed.
 <b>Low</b>	Observed vulnerabilities assigned a low risk level are considered to present threats that are unlikely to occur and would have a smaller impact. These should receive the lowest priority when being addressed.

## Summary of Observed Vulnerabilities

The table below provides a summary of the observations identified during the 2011 external penetration assessment.

Ref.	Observed Vulnerabilities	Criticality
<b>1. External Network Penetration Testing</b>		
<b>1.1</b>	<b>Missing updates and patches</b> An update is needed to some services. <i>IT Management agrees and will implement solutions to address this issue by December 31, 2012.</i>	 Medium
<b>1.2</b>	<b>Improper Output Sanitization</b> Data is not completely sanitized. <i>IT Management agrees and will implement solutions to address this issue by December 31, 2012.</i>	 Medium
<b>1.3</b>	<b>External FTP</b> One external host has an FTP service enabled. This service does not use secure authentication mechanisms. <i>IT Management agrees and will implement solutions to address this issue by December 31, 2012.</i>	 Medium
<b>1.4</b>	<b>Web Platform Configuration</b> Two hosts have configuration issues with the web platform software. <i>IT Management agrees and will implement solutions to address this issue by December 31, 2012.</i>	 Low
<b>1.5</b>	<b>Insecure SSL Configuration</b> SSL configuration issues were identified on some hosts. <i>IT Management agrees and will implement solutions to address this issue by December 31, 2013.</i>	 Low

Abbreviations /Definitions	
<b>The City</b>	City of Minneapolis
<b>Cross-Site Scripting</b>	Modifying the response from a web server through the request to include malicious content executed by the client browser.
<b>FTP</b>	File Transfer Protocol – A common service for transferring files between hosts
<b>Host</b>	A computer connected to a network.
<b>IA</b>	Internal Audit Department
<b>IT</b>	Information Technology Department
<b>Open Ports</b>	In TCP/IP networking, each host has ports for services to communicate on. An open port has a service communicating on a specific port.
<b>SSL</b>	Secure Sockets Layer – Protocols employed by web servers to secure communication by encryption and certificate authentication.