# Potential Security Risks Due To Dumpster Findings Report

By Joseph Subrath

February 23, 2025

Section 1: Dumpster Findings

The corporation, Alexander Rocco Corporation, has potential security risks due to items found inside of a dumpster outside of the company. The entity responsible for filling those dumpsters with items is called Alika’s Cleaning Company. The Alexander Rocco Corporation uses Alika’s Cleaning Company for janitorial services. The following items were found inside of the dumpster.

A) A company phone directory.

B) A Windows Server 2008 training kit.

C) 23 outdated Oracle magazines.

D) Notes that appear to be programs written in HTML, containing links to a SQL Server database.

E) 15 company memos from key employees.

F) Food wrappers.

G) An empty bottle of expensive vodka.

H) Torn copies of several resumes.

I) An unopened box of buisness cards.

J) An old pair of women’s running shoes.

Section 2: Relevance Of Items

**Item 1.A: Company Phone Directory**

The company phone directory is a directory that contains the names and phone numbers of employees. This gives a list of targets by name to try and contact, to try and gain critical information about the company, as well as a method of contacting them. This could also give an attacker a list of names and phone numbers to use to try an impersonate employees.

**Item 1.B: A Windows Server 2008 Training Kit.**

The Windows Server 2008 server kit can indicate that the Alexander Rocco Corporation potentially uses a client-server network model. This could also indicate that the network operating system being used to manage resources is Windows Server 2008. In information security, there are 5 fundamental security principles, diversity, limiting, layering, simplicity, and obscurity. The main principle that seems to be violated by finding the Windows Server 2008 server kit, would be obscurity. Security by obscurity is obscuring to the outside, what is on the inside. This makes attacks much more difficult. By revealing the version of network operating system being used by the corporation, an attacker can use this information to find the vulnerabilities of the system in order to attack it. Along with this, because the server has such an important job in managing resources, this is a big security risk.

**Item 1.C: 23 Outdated Oracle magazines**

Oracle is a company that offers many products and services. Some examples of products would be the Oracle cloud infrastructure, cloud applications, and Oracle hardware and engineered systems. Similar to the risk of discovering item 1.B, finding these magazines may violate the principle of security by obscurity. These magazines could indicate that the Alexander Rocco Corporation uses Oracle, or used Oracle for key services. That means Oracle could potentially have critical information about the Alexander Rocco Corporation that could compromise security. Therefore, what the attacker would need to do is find and exploit vulnerabilities in Oracle, and try to get access to the information Oracle has on the Alexander Rocco Corporation.

**Item 1.D: Notes That Appear To Be Programs Written In HTML, Containing Links To A SQL Server Database.**

The finding of item 1.D, notes that appear to be programs written in HTML, containing links to a SQL server database, could possibly allow for an injection attack, particularly an SQL injection. A Standard Query Language injection targets SQL severs, introducing malicious code into them. A lot of data can be exploited from this, like getting all users email addresses.

**Item 1.E: 15 Company Memos From Key Employees**

Finding memos, especially from key employees can be very important to an attacker, depending on the type of attack they would use against the Alexander Rocco Corporation. The memos can be used to gather little bits of information an attacker can use, for an attacker who is trying to build up enough information to impersonate an employee. Along with this, these are memos from key employees, which are the prime type of employees to impersonate to get meaningful results when impersonating an employee.

**Items 1.F and 1.G: Food Wrappers and An Empty Bottle Of Expensive Vodka**

These two items could indicate that these are two items that people like to consume. Therefore, it can be used against them in a social engineering attack. Along with a social engineering attack, if combined with other information gathered from employees by items in the dumpster, it can be used in a spear phishing attack against employees, who if they like the items they are being targeted with, and are convinced about the offer’s legitimacy because of their personal information being mentioned, they could fall for a scam offer and give away valuable information to an attacker that may be used in another attack, like an impersonation attack.

**Item 1.H: Torn Copies Of Several Resumes**

Torn copies of several resumes could be pieced together in order to be readable. These resumes could give vital background information about employees, possibly key employees, allowing more information to be built up in an impersonation attack.

**Item 1.I: An Unopened Box Of Buisness Cards**

An unopened box of buisness cards could be used to gain vital information needed to perform an impersonation attack, gain more data on an employee being targeted for an attack, or can be used itself in performing an impersonation attack.

**Item 1.J: An Old Pair Of Women’s Running Shoes**

An old pair of women’s running shoes could indicate that the pair of shoes were worn down because of how much the owner used it, showing that she most likely likes the pair of shoes. Therefore, these shoes could be used in a phishing or spear phishing attack against employees of Alexander Rocco Corporation, advertising a false offer from the company who made the worn out shoes, which could get an employee or employees to give sensitive personal information.

Overall, all of the items found in the dumpster are relevant to a security breach in some way. Items like memos from key employees, old resumes, food wrappers, an empty bottle of expensive vodka, an unopened box of buisness cards, a company phone directory, and an old pair of women’s running shoes, could be used together to gather information on employees. These items can be used to gather general information about employees, or if enough pieces of information are gathered together overall from these attacks on key employees, an attack such as an impersonation attack can occur which may cause extensive damage to the Alexander Rocco Corporation. Other items like outdated Oracle magazines, a Windows Server 2008 server kit, and notes that appear to be programs written in HTML, containing links to a SQL Server database, could give attackers enough information to attack the infrastructure of the Alexander Rocco Corporation in an effective way.

Section 3: Recommendations

Some recommendations that I have for the Alexander Rocco Corporation management to prevent sensitive information being so easily accessible like this again in the future would be, firstly, create new policies that ensure that employees dispose of certain items in a responsible way. For example, items with sensitive information, like old resumes and memos, should be shredded first before being thrown away. Another recommendation that could be made is for the Alexander Rocco Corporation to require that Alika’s Cleaning Company lock the dumpster outside of Alexander Rocco Corporation only being unlocked by an employee the day of trash pickup, this way the garbage bin is unlocked for the minimum amount of time required for trash pickup.