

Death by 1,000 Cuts

A Red Team case study

Customer Background

Sector: Retail

Revenues: In excess of \$100 Billion

Footprint: Global

Project Background

Duration: 8 weeks (max)

OccamSec Team Size: 4

Test Domains: Cyber and Physical

The Objective

How can we be destroyed by a cyber attack? This was the question posed by our client. Spoiler alert – it's challenging for a single cyber attack to bring down a giant organization. Our experience shows that direct attacks on technology—such as a hack that brings down a system, data theft, or a ransomware attack—can cause damage, but the impact is usually not enough to bring a large organization to its knees.

Instead, we've learned that technology often serves as a conduit to a larger outcome, and that's where the real damage occurs. A company that consistently fails its customers will suffer financially as those customers seek alternatives. This was the approach we took, and ultimately succeeded with, against one of the largest retailers in the world.

It Begins

The project began by talking to a number of stakeholders to determine what the impact of the attack would need to be (10% revenue drop), identify key business processes, and review any other relevant information. Over the course of 2 weeks information was analyzed, follow up conversations were held and several high impact scenarios identified. The conclusion was an attack known as "Death by 1,000 cuts".

Death by 1,000 cuts involved a multi pronged attack designed to erode customer confidence. Equipment across a range of stores (including refrigeration units and heating systems) could be disrupted, deliveries delayed, staff management systems compromised, internal communications accessed and the ability to send messages obtained, and key customer databases accessed and exfiltrated.

Since the engagement only had a finite amount of time the objective was to prove out that each target component could be breached. The customer database, HRMS, and comms systems were centralized. HVAC/Refrigeration and deliveries were standardized across all stores and distribution centers, so breaching a sample would be indicative that this could be executed at scale.

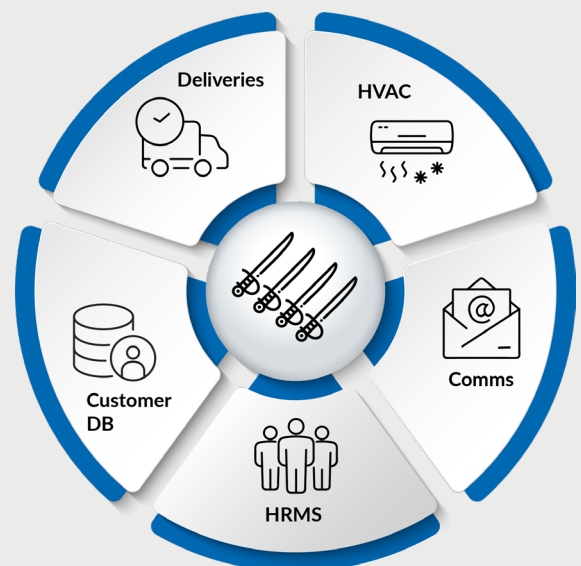


Fig 1: The target elements of death by 1,000 cuts

Attack Vectors

The team had 6 weeks to determine if the attack was viable, with that in mind three attack vectors were chosen:

- 1) The management room in a store;
- 2) An Internet facing application;
- 3) A vendor room.

The client concluded that the potential for a breach via any of these vectors posed a significant risk. However, they were confident that the combination of their technical controls and the security awareness training provided to their staff significantly lowered the likelihood of a successful breach.

Regarding their technical controls, we were not given specific figures on the client's security spending. However, according to Deloitte, the average tech budget in 2023 was 5.49% of revenue, with cybersecurity expenditure typically accounting for 6-14% of IT budgets (<https://www2.deloitte.com/us/en/insights/topics/leadership/maximizing-value-of-tech-investments.html>). For a company with \$100B in total revenue, this translates to an approximate security allocation of \$329M. Such an investment should provide sufficient protection to thwart any but the most well-funded nation-state attacks."

Initial Breach Attempts

Store Management Room

Store management rooms were located at the back of stores, behind a couple of swing doors. Various approaches were considered, the actual breach attempt unfolded as shown in fig 2:

1	On Superbowl sunday one of the team went to a store, disguised in a polo shirt and khakis, claiming to be from company tech support.
2	Based on information available online, he had a fake company ID, and some research provided the right names to reference. He arrived and asked to see the manager.
3	It was explained that there was a technical issue that needed to be fixed, and he had been sent to deal with it. They had some chit chat, then the manager gave him a desk and let him go to work.
4	A remote access tool was deployed on a system our team member brought with him. This provided a tunnel into the network. During this time the manager spoke openly to our team member about his job.
5	Our team member left the store after approximately one hour. The remote access tool remained active for the duration of the engagement and was not detected.

Fig 2: Store Breach

Network access from the management room provided full access to the internal network.

Application

One application was selected for testing. Despite various vectors being identified for possible exploitation, given the time frame, these were scheduled for testing at a later date.

Vendor Room

The vendor room area selected was accessible from the street, and turnstiles were in place, however it was easy to tailgate (walk in right behind someone) and gain access to the area. It was then simply a task of finding an empty room and attempting to install a remote access system. Network connectivity into the internal network was confirmed and the system deployed.

Since two remote access tools had been deployed, the decision was made to focus on the vendor room.

Trophy Achieved

In 12 days the project objectives were obtained with full access to the data analytics platform. Additionally the underlying Hadoop cluster was accessed with full privileges, giving the OccamSec team the ability to delete data, reconfigure the system, and any other administrator activity. No activity was detected, no alerts raised, all security controls were bypassed.

Fig 3 shows how this was achieved.

1	Obtained Valid Credentials	Access was obtained to the internal sharepoint. An extensive list of linux servers were identified along with engineer names. Documents were found authored by the engineers, one included details on internal repositories.
2	Accessed Public File Share	The repository was browsed and the packages available were analyzed. One package (named after a user) contained a private key and a server name. The server was accessed.
3	Escalated Privilege	By modifying a regular executing script on the server we were able to run commands as root. From there we determined that admins were using a "go" script to access other hosts. We examined this script, and found an ssh root key enabling access to other machines.
4	Cloudera Access	We accessed the host running cloudera. Examining scripts on this box revealed details on the MySQL instance being used for configuration information. The root password for MySQL was found in a backup script, we connected to MySQL and created and admin user, and accessed cloudera.
5	Full Access To All Data	We noticed that the data management portal was running over HTTP. Tcpdump was run on the servers we had compromised, and after a few hours we had DBA credentials. We used these to connect with full access to all data, and the trophy capture was complete.

Fig 3: Store Breach

This took time to achieve, since stealth was required the team could not run any intrusive tests and considerable time was spent analyzing SharePoint for data and reviewing scripts and configuration information we were able to obtain.

The Aftermath

Systemic Issues

The project identified a number of systemic issues which needed to be addressed. First, there is a lack of security awareness; for example, confidential data is being stored in accessible SharePoint files. However, while awareness training is a compliance requirement for many, we do not believe it provides any major value. Technical controls which remove the potential for human error have a far better chance of success: posters and a powerpoint session will not override basic human instincts.

Second, the security program was not built on high-impact business outcomes. As is often the case, the program was developed with little to no consideration of business impact—how does the organization generate revenue? What cyber attack impacts would cause the most harm? These questions had not been asked. Instead a standard defense in depth playbook was used, which is ok IF its deployed around impact. Looking to just secure everything, everywhere, and monitor everything is a recipe for disaster in most organizations.

Third, there was a lack of the realization that cyber security risk is constantly changing. An annual penetration test against specific applications may work, but given the cadence with which new vulnerabilities are discovered it is more likely that systems are exposed for long periods of time. Tied to this, it also needs to be understood that vulnerabilities can be chained together across both technical and non technical targets - the ability to access a supposedly secure area may not amount to much on its own, however that combined with poor control over network access points, a flat network structure, confidential information being stored in SharePoint files, and monitoring controls not based on actual attacks, is a recipe for disaster.

Tying these together is a misunderstanding of risk management, and possibly an over reliance on compliance requirements as the final word in security. It's often conveyed that attackers only need to succeed once for a major impact; this is a disservice to both attackers and defenders. One vulnerability alone is probably not going to destroy a business's revenue. A collection of them, with an attacker who is focused on that high impact outcome, presents a risk management issue that requires an holistic assessment of the organization - in terms of how it operates, not in regards to specific technical factors.

Return on Investment

Returning to the attack vectors section and the budget numbers, this project provides an accurate measure of the return on investment, since the trophy was considered - by the business - to have a material impact on revenue. Fig 4 shows the outcome.



Fig 4: Project ROI

Clearly, not every business generates \$100 billion in revenue. Yet, when executed with precision and focused on specific business impacts, red teaming can reveal critical vulnerabilities that must be addressed. Ready to ensure your security investments truly align with your business priorities? Contact us today to discover how we can tailor a security strategy that safeguards your bottom line.