Cyber Resiliency Case Study
Retailer: A

This case study is an anonymized description of a successful cyber attack on a large U.S. retailer. Cyber attackers exploited critical vulnerabilities in the retailer's computer system to inflict costly damage to the organization's operations. The details provided in this case study were taken from public reports, and the recommended cyber resiliency techniques are based on this public information as opposed to insider information or firsthand knowledge of the systems.

What Happened

In 2013, Retailer A was the victim of a data breach suspected of being the work of the same group of Eastern European thieves who orchestrated a cyberattack on another retailer earlier the same year. These criminals compromised 40 million credit and debit card accounts during the attack on Retailer A. The attack continued in January 2014 when personal information — including names, phone numbers, email, and mailing addresses — was stolen from as many as 70 million customers. As many as 110 million of the retailer's customers were compromised during these two incidents.

How the Attack Happened

The cyber criminals used a specific form of malware that was dedicated to grabbing sensitive data out of hardened POS terminals. They exploited a third-party vendor's weak security that allowed them to compromise Retailer A's network.

Retailer A gave network access to a third-party vendor whose weak security allowed the attackers to obtain credentials which in turn provided them a foothold in Retailer A's network. Retailer A's more sensitive systems were not isolated, and the attackers were able to move from less sensitive areas of Retailer A's network to areas storing consumer data. While Retailer A's anti-intrusion software provided multiple automated warnings that hackers were installing malware and even warned about the routes these hackers would use to exfiltrate data from Retailer A's network, they succeeded in carrying out their attack against Retailer A.

The Impact

The impact of the breach described here was far reaching, to the retailer and their customers.

- 46% decline in 2013 fourth quarter profits from previous year
- $61 million in total breach-related expenses
- Fines of up to $90 per instance of compromised cardholder data ($3.6 billion total) for violating industry security standards

- Additional revenue loss from payment card counterfeit fraud claims stemming from the cards whose information was sold on the black market and used for fraudulent purchases
- $100 million expense to switch Retailer-branded debit and credit cards to the more secure chip-and-PIN card technology. This switch includes installing new payment terminals
- Decline in consumer trust —after consistently claiming a place within Brand Index's top 10 brands

Combatting Threats through Cyber Resiliency

This attack demonstrates the vital importance of protecting critical assets and infrastructure. A compromised system led to the theft of customer information and a violation of customer trust. While traditional defenses (i.e., firewalls, DMZs, intrusion detection systems) are designed to keep attackers out; cyber resiliency techniques focus on limiting direct and collateral damage while continuing critical mission or business operations in the face of an attack. The use of the proper cyber resiliency techniques can minimize the damage during the attack and limit the impact of a breach. The cyber resiliency techniques discussed in each row of the following table are listed in alphabetical order.

Attack Vectors	Cyber Resiliency Techniques	Benefit Potential
Excessive privileges to third-party vendors with network access and insecure wireless communications.	**Analytic monitoring:** Gather and analyze data on an ongoing basis to identify potential vulnerabilities and adversary activities, and assess damage.	Analytic Monitoring can identify changes to critical systems and other indications of adversary activity such as data streams going to unapproved locations or unauthorized streams of encrypted traffic.
	Privilege Restriction: Apply least privilege to restrict privileges given to third-parties to the absolute minimum necessary.	Applying Privilege Restriction controls the privileges associated with individuals' or a group's (e.g., vendors) access credentials to only those necessary.
	Realignment: Align cyber resources with core aspects of business functions, thus reducing the attack surface.	Using the Realignment technique, identifies non-essential business functions (e.g., those provided by third party vendors). Realignment can identify any data that is not needed and eliminate it from storage, temporally minimize access (e.g., vendors only need access during a narrow window for maintenance.) and identify data or resources that require elevated (e.g., multifactor) authentication.
Critical functions not isolated. Too much connectivity allowed attackers to move from the edge of the corporate network and exploit the systems responsible for processing consumer data.	**Coordinated Defense:** Use multiple, distinct mechanisms (defense-in-depth) to protect critical functions.	Coordinated Defense can provide additional security for critical corporate systems by requiring the adversaries to circumvent multiple defenses.
	Segmentation: Separate systems responsible for critical functions so these systems are not accessible via the vendor portal.	Properly segmenting the external access points (e.g., vendor portal and non-corporately owned devices) can protect the internal corporate network and point-of-sale (POS) systems from unnecessary

Attack Vectors	Cyber Resiliency Techniques	Benefit Potential
		access. Coordinated Defense used with Segmentation can limit and expose attacks earlier in their lifecycle.
Lack of coordinated response. In some cases the cyber security responsibilities were split across several executive roles. A lack of clear and comprehensive policies and procedures, and insufficient training resulted in retailers not responding to warnings, or attackers being able to avoid triggering warnings.	**Adaptive Response:** Define procedures and adopt technology that allows for quick response to the incident indicators.	Indicators for various malware were publicized around the time of the incidents. Adaptive Response can add policies, procedures, and technology to respond to these indicators.
	Coordinated Defense: Assign cyber security responsibilities; implement incident investigation and handling procedures; monitor public security channels for new threat indicators.	Coordinated Defense can help build a coordinated, top-down cyber security management chain. In addition, it can coordinate training with real word, practical exercise attack scenarios. The combination of Adaptive Response and Coordinated Defense can increase the probability that alerts from anti-intrusion software will be effectively used to limit the attack.
Presence of malware. Malware was present on the corporate system and used to collect and export credit card information. Even in cases where antivirus was used, the antivirus was unable to detect the malware.	**Non-persistence:** Generate and retain resources as needed for a limited time.	With Non-persistence, software in critical components can be replaced with known good copies either as part of an ongoing process or as part of a response to an attack. This impedes the adversary's ability to obtain a foothold in the defender's environment without requiring the defenders to detect the attack.
	Substantiated Integrity: ascertain whether critical services, information stores, information streams and components have been corrupted.	Substantiated Integrity provides a mechanism to identify when critical components have been corrupted and must be replaced or addressed.