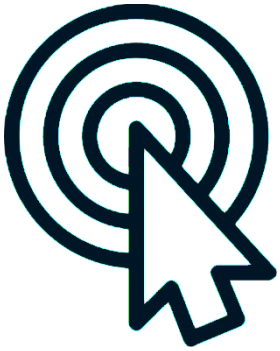
CASE STUDY

Target Corp. & Cybersecurity

What Could Target Have Done Differently?



THE SITUATION

On December 19, 2013, in the midst of the holiday shopping season, Target informed customers that they had been hacked, and that anyone who had shopped from November 27 to December 15 was at risk of having had their credit or debit card information stolen. This breach eventually cost Target over $28.5M in settlement costs and $202M in legal fees. How did it happen, and could it have been prevented?

THE ATTACK

On November 12, 2013, hackers were able to access Target's internal system via an HVAC vendor who had fallen victim to a phishing attack. They uploaded malware so that every time a credit card was swiped, they got the data before it was encrypted. Despite alerts from their internal IT security system, the malware went undetected for several weeks. Over this period of time, information from over **40 million credit and debit cards** was stolen, and up to **70 million customer records** were compromised. These records had personal identifiable information such as home addresses, email addresses, names, and more.

THE AFTERMATH

The FBI alerted Target on December 12, 2013 of a potential breach. They'd been monitoring the Dark Web and had noticed an increase in credit card credentials for sale that were associated with Target. If not for the FBIs dark web monitoring, the malware would've been allowed to continue to exist in Target's network.

Target spent 3 days verifying and investigating the claim, and then spent approximately 12 hours removing the malware from this system. Customers were at risk if they shopped up until December 15, 2013. The CEO was informed on December 15, and the Board on December 18.

On December 19, 2013 customers are informed about the 40 million credit cards. They won't be told about the 70 million personal records until January 10, 2014.

WHAT COULD TARGET HAVE DONE DIFFERENTLY?

There are at least 4 mistakes Target made that could've changed the outcome of this situation.

1. **Ignored System Warnings**
   Target had a cybersecurity system that alerted them to threats from the malware. Evidently there was difficulty with solution adoption of the cybersecurity system since it was human error, not technical error, that resulted in this system breakdown.

2. **Poorly Designed Network**
   The HVAC vendor should not have been able to access the payment systems in Target's internal network. The network design did not have enough separation and safeguards in place, and exposed Target to unnecessary risk, which ultimately cost them.

3. **Lack of a Business Continuity Plan**
   Even after being alerted by the FBI, it took Target 3 days to verify the attack and shut it down. It took them 3 days to tell their own CEO and a week to communicate to their Board. Throughout all of this they were able to operate their business but they left customers at risk. Target could've mitigated the damage if they'd had plans in place to properly respond to threats, and to responsibly continue their business without further exposing their customers to risk, and therefore undermining their trust in the company.

4. **Failure to Proactively Monitor the Dark Web**
   If Target had been proactively monitoring, they would've known when their credentials were compromised by the HVAC vendor if they'd appeared on the Dark Web. This could've potentially prevented the cyberattack completely, or alerted Target much earlier on. Without a Dark Web monitoring system, you don't know who could have access to your network, or how employees may be personally compromised.

"A practical solution to Protect, Detect, and Recover."
Dwight Stewart,
Managing Director
Results Matter Cloud Services Inc.

OUR SOLUTION

Target is fortunate that the FBI was monitoring the Dark Web for them. But smaller businesses are out of luck if they're not taking care of themselves. Our **Dark Web Monitoring Solution** means that you'll be alerted immediately when your compromised credentials are found online, giving you peace of mind and proactive protection.

We also help businesses construct and execute a **Practical Business Continuity (PBC) plan**. We provide image-based backups that can be stored both locally and in a secure cloud, so that with proper procedures in place businesses can be up and running without missing a beat. We understand that solution adoption is a large part of success which is why we make it an area of focus for our clients.

Results Matter Cloud Services Inc. is a managed services provider based in Calgary, serving clients starting in 1987 under the Computer Essentials brand and under the Results Matter brand in 1997. Results Matter Cloud Services are experts in business IT solutions and have extensive experience protecting clients no matter the industry they operate within. Solutions to business problems require tactics, technology and teams, and finding the right mix of each is their speciality.

Sources:

Cold Call Podcast. 21 Dec. 2016, https://hbr.org/podcast/2016/12/targets-expensive-cybersecurity-mistake. Accessed 6 Aug. 2019.

Abrams, Rachel. "Target to Pay $18.5 Million to 47 States in Security Breach Settlement." New York Times, 23 May 2017, https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

Settlement Administrator. "Commonly Asked Questions." Target Breach Settlement, 16 July 2019, https://targetbreachsettlement.com/mainpage/CommonlyAskedQuestions.aspx.

Results Matter Cloud Services | 9-2280 39 Ave NE, Calgary, AB T2E 6P7
T: 403-455-5969 | **E:** engage@rmcloud247.com | **W:** https://rmcloud247.com