Home Depot and Target Case Study
Gerald Rigdon - 2023

Case Study Questions:

1. What is the Home Depot case?

Per (Krebs, 2014), malware known as "Kaptoxa", which was a variant of "BlockPOS" used in the Target security breach, was placed on Home Depot Point-of-Sale or POS terminals. The malware was designed to read the data from cards that were swiped at infected POS terminals. Subsequent analysis revealed the malware was deployed via access to the Home Depot network using a third-party vendor's logon credentials and designed to escape detection from anti-malware tools by masquerading as a component of the anti-malware software package itself. The stolen data from millions of Home Depot customers was ultimately offloaded to a server which was also compromised, and used File Transfer Protocol, or FTP, to send the data to a final destination. Once in the possession of cyber criminals the stolen information was then sold on the black market and used by other criminals to purchase items illegally using stolen credit card numbers. Further investigations revealed the criminal network was linked to anti-American propaganda originating outside of the United States.

A retrospective analysis (*Cyber Aware Case Study,* n.d.) disclosed the following timeline, which resulted in the loss of fifty-six million credit and debit accounts and fifty-three million customer email addresses:

- April 2014 – Hackers gained access from a third-party vendor's logon credentials and took advantage of a Microsoft Windows vulnerability.
- June 2014 – Custom malware was deployed on POS terminals.
- September 2014 – Stolen credit card numbers and email addresses were offered for sale on the illegal market.

2. What are the vulnerabilities, threats, and resulting risks that both Target and Home Depot may have faced?

In both cases:

- The POS terminals were vulnerable to malware deployment.
- Third party accounts had inadequate access controls.

- Networks providing access to third parties were not properly isolated from networks containing customer transactions.
- Monitoring systems were insufficient.

In 2013 and 2014 most POS terminals were designed to read data such as owner of credit card, type of card, credit card number, expiration date, etc., from cards designed with magnetic stripes which were easily read (Hawkins, 2015). Although new and more secure technology is now commonly used, both companies could have made better use of the malware detection mechanisms available at the time. Moreover, given the costly data breach of the Target corporation a year earlier, Home Depot failed to learn from that security breach. At the time of the Home Depot incident, Windows XP was used on the POS terminals even though more hardened Windows Embedded POSReady had been available since 2009 (Hawkins, 2015).

While third party accounts may be necessary, obviously both companies demonstrated poor management of these credentials. Moreover, having two-factor authentication may have prevented both breaches given it was the initial access into the network that allowed the malware to be deployed on the POS systems. Even assuming the hackers were able to overcome two-factor authentication, proper segregation of the POS system network with separate access control would have added another layer of protection. Since proper risk assessment includes both prevention and incident response, a proper monitoring system should have caught the breach even though all prevention measures had been overcome. Yet, per the aforementioned timeline (*Cyber Aware Case Study,* n.d.), several months elapsed before there was an awareness that a breach had occurred.

As a result, (*Case Study: Home Depot Data Breach Cost $179 Million*, 2021), the initial assessment of financial loss for Home Depot was estimated at 179 million without counting legal fees. Over the long term, such breaches represent a threat and risk to the business itself beyond the initial financial setback. Reputation damage can have future repercussions which may lead to eventual corporate demise due to eroding confidence in the customer base.

3. What are the benefits of quantitative risk assessment over qualitative risk assessment? What are the disadvantages of quantitative risk assessment compared with qualitative assessment? How does this connect to the Home Depot case?

According to (Volkin, 2021), the risk management lifecycle includes following seven main processes that are complementary to each other, two of which are listed below:

1. Perform **qualitative risk analysis** and select the risk that needs detailed analysis.

2. Perform **quantitative risk analysis** on the selected risk.

As indicated, these processes include both qualitative and quantitative risk assessment emphasizing the necessity of both. As implied from their intuitive definitions, qualitative analysis is more subjective, concern, and scenario driven, and quantitative assessment is more objective with the use of numbers for measurable values.

Quantitative Benefits (Volkin, 2021):

- Objectivity in the assessment
- Powerful selling tool to management
- Direct projection of cost/benefit
- Flexibility to meet the needs of specific situations
- Flexibility to fit the needs of specific industries
- Much less prone to arouse disagreements during management review
- Analysis is often derived from some irrefutable facts

From this list one can conclude that numbers are powerful and help remove emotional content. Yet, such concise and detached calculations are often difficult to make and constrained by time, complexity, ability to collect data, and reliability of the data. Hence, making a final decision based on numerical representations alone assumes such can adequately capture all the necessary inputs upon which important decisions can be made.

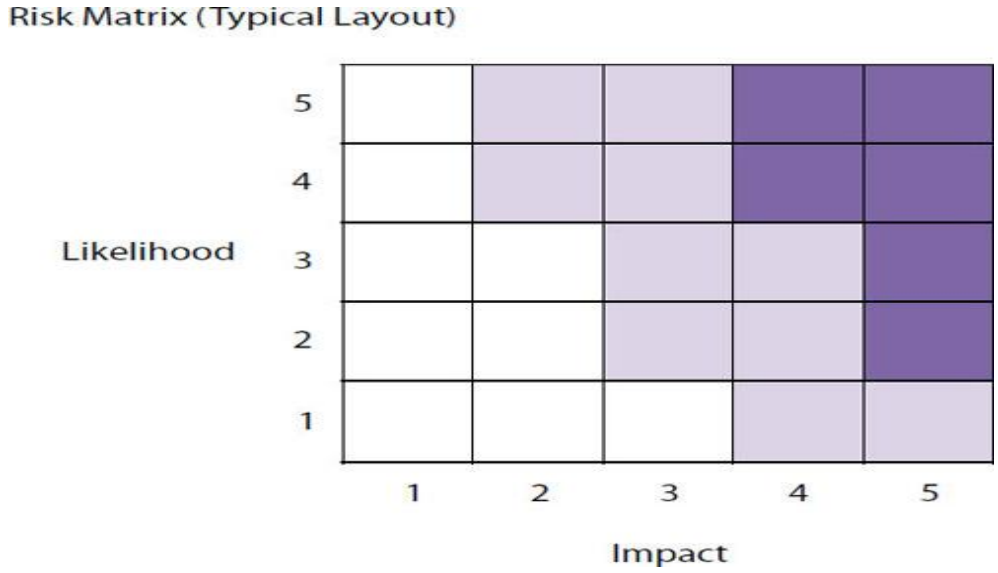
For Home Depot, the most important starting point was to have a risk management process in place where both qualitative and quantitative assessments were considered. Following a process provides a comprehensive approach where both hard data and subjective considerations are used in a complementary way to secure the computing environment.

4. How can identification of risk help Home Depot with organizational decision making?

According to the study from (*Cyber Risk Opportunities Case Study*, n.d.), risk scores were collected from thirteen internal experts across a company after completing a survey with 145 questions. After identifying the top five risks, senior decision makers prioritized a risk mitigation plan in order to close the

gaps on the identified risks. This included a cyber risk scorecard to track progress and monthly check-in meetings. This proactive approach alerted the company to new developments in the cybersecurity landscape and a way to measure the change in risk over time.

In the case of Home Depot, an initiative-taking risk assessment and identification of risks would have produced a risk matrix (Graves, 2000) shown below, where, for example, an Impact of 5 and a Likelihood of 3 would have produced a result in the unacceptable region. Such numbers are conceivable considering the preceding, recent Target security breach. When performing this assessment on the vulnerability of the POS terminal or the network access of third party vendors, the Target incident would have been an important input that revealed a very high impact and a likely probability given this industry precedence.



As a result, this risk assessment would have been immensely valuable to organizational decision making. Home Depot would have needed to pursue risk mitigations to reduce the likelihood of occurrence. In applying the learning from the Target incident, it would have been apparent that cost-effective measures could have been taken. Adding just two measures; two-factor authentication for third parties and a separate authentication process for POS network access would have meant implementing best practices that could have moved the likelihood scale to very unlikely. The key takeaway from risk assessment identification is that important business decisions can be made to implement mitigations where the residual risk falls in acceptable regions.

Further demonstrating the success that follows proper risk identification (Ivan, 2023) Identity and Access Management Systems allowed one business to "automate the monitoring of system vulnerabilities and secure access for 220,000 company users and outsiders while also establishing 40 additional workflows" and an airline to "monitor and manage the workforce privileges of

CIP identities using vaulting and password rotation policies which led to secure access for 1000 privileged identities and 10,000 devices." These examples reveal that Home Depot likewise could have been a success story had they followed a sound risk management process.

5. Which of the three (3) risk assessment techniques (quantitative, qualitative, hybrid) could have helped with early identification of data breach risks at affected stores?

Let us first take a more detailed look at both quantitative and qualitative risk assessments.

Quantitative method consisting of the following steps (Liu, 2023):

- Step 1: Inventory Assets and Identify Asset Value (AV).
- Step 2: Calculate Exposure Factor (EF).
- Step 3: Calculate Single Loss Expectancy SLE as follows:
    - SLE = AV x EF
- Step 4: Identify Annualized Rate of Occurrence (ARO).
- Step 5: Calculate Annualized Loss Expectancy (ALE) as follows:
    - ALE = SLE x ARO
- Step 6: Cost Benefit Analysis of Countermeasures as follows:
    - CBAC = ALE before Countermeasures – ALE after Countermeasure – Annualized Cost of Countermeasure

Qualitative method (Graves, 2000) as follows:

- Impact – rating risk using a basic one-dimensional scale.
    - very low/low/medium/high/very high
- Likelihood – a conventional approach to capture the extent to which risk effects are likely to occur.
    - very unlikely/low likelihood/ likely/ highly likely/near certain

Strictly speaking, the qualitative approach is probably the most effective in identifying data breaches early on because it forces one to ask the right questions. In order to evaluate the likelihood for a specific scenario within their computing environment, one would have to perform a threat modeling exercise

to understand the vulnerabilities and their likelihood. However, it is possible to perform the steps per (Liu, 2023) while using nonnumerical measures. So, in agreement with (Volkin, 2021) both assessments should be used in an effective risk management process which may be satisfied by a hybrid approach.

For example, answering the following questions from (Liu, 2023) qualitatively would have given a much richer perspective on the cost vs the benefits:

- What is this asset worth to us?
- How much of this asset could we lose in an incident?
- How many times per year can this incident happen?

Therefore, assuming Home Depot had followed either a qualitative method or a hybrid approach based on subjective scaling, they would have needed to assess the likelihood and impact of security breaches in the context of a cost benefit analysis. The results of such an analysis should have identified significant risk, especially considering the Target event and the comparable business and network models of both companies.

References:

Case Study: Home Depot Data Breach Cost $179 Million (2021, August). archtitan.com. https://www.arctitan.com/blog/case-study-data-breach-cost-home-depot-179-million/

Cyber Risk Opportunities Case Study. (n.d.) cyberriskopportunities.com. https://www.cyberriskopportunities.com/case-study-cyber-risk-managed-program/

Cyber Aware Case Study (n.d.). dni.gov. https://www.dni.gov/ncsc/e-Learning_CyberAware/pdf/Cyber_Aware_CaseStudy_HomeDepot.pdf

Graves, R. (2000) *Qualitative Risk Assessment*. pmi.org. https://www.pmi.org/learning/library/qualitative-risk-assessment-cheaper-faster-3188

Hawkins, B. (2015, October). *Case Study: The Home Depot Data Breach.* sans.org. https://www.sans.org/white-papers/36367/

Ivan, F. (2023, February*). Real-Life Case Studies: How Businesses Improved Security and Efficiency with Identity and Access Management Solutions*. techtheleaad.com. https://techthelead.com/real-life-case-studies-how-businesses-improved-security-and-efficiency-with-identity-and-access-management-solutions/

Krebs, B. (2014, September). *Home Depot Hit By Same Malware As Target*. krebsonsecurity.com. https://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/

Liu, M. (2023, September). *Risk Control Overview of Risk Management Tools and Techniques.* marymount.edu.

Volkin, E. (2021, April). *Risk Assessment and Analysis Methods: Qualitative and Quantitative*. isaca.org. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods