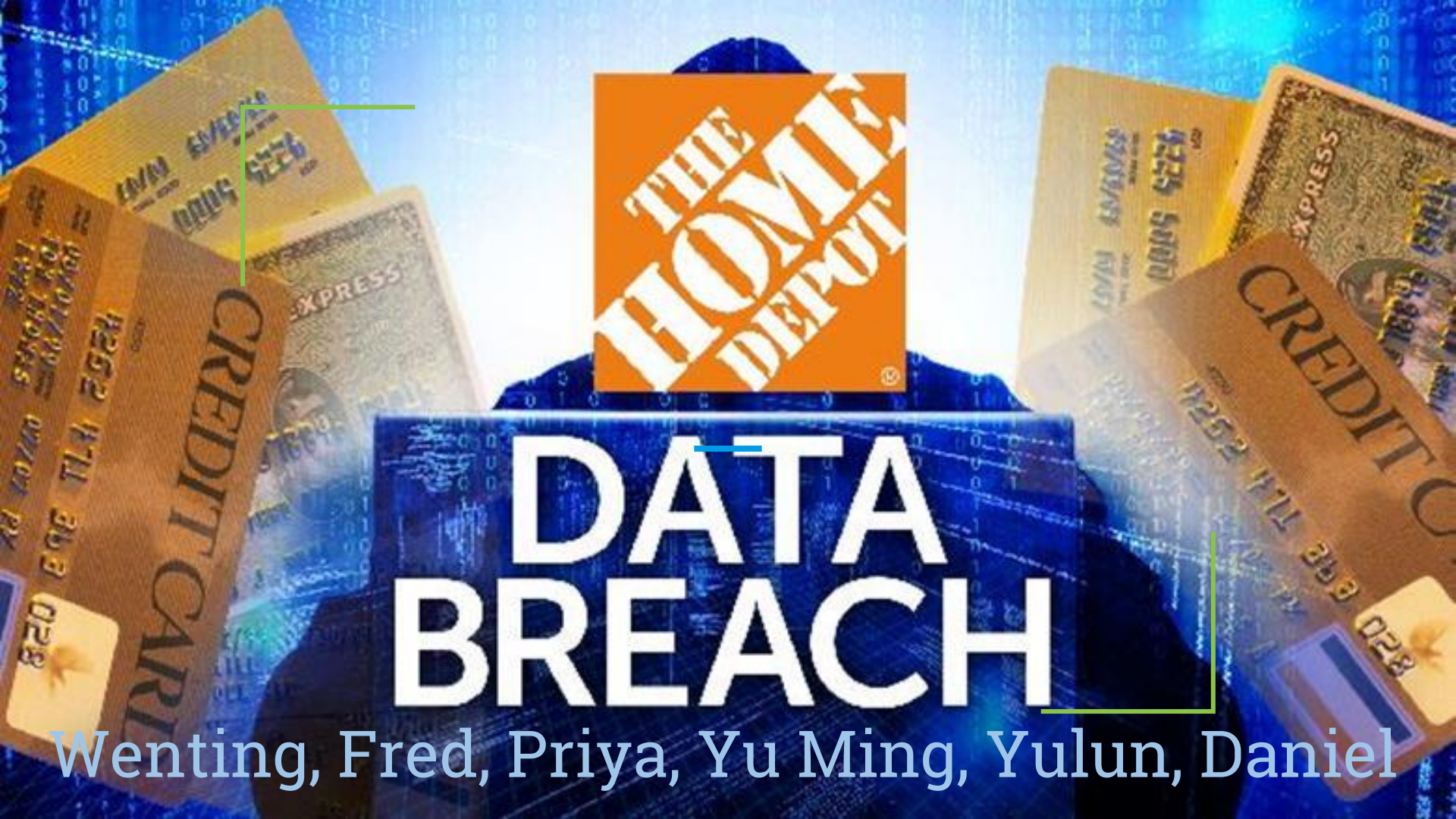
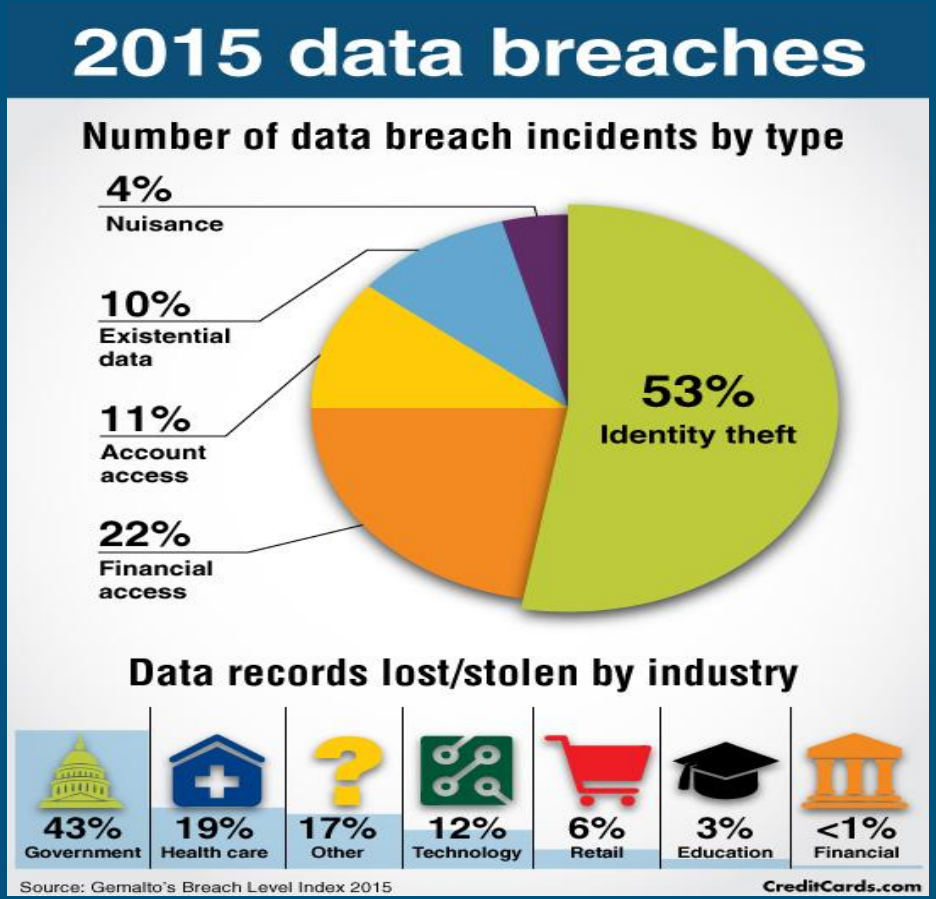
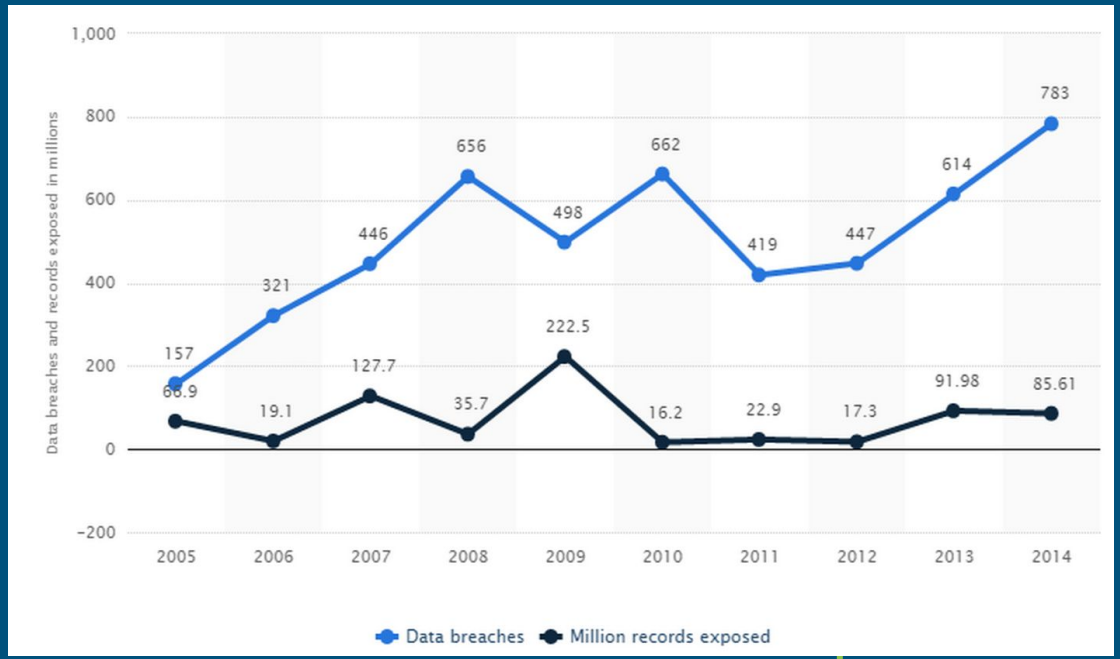


Wenting, Fred, Priya, Yu Ming, Yulun, Daniel



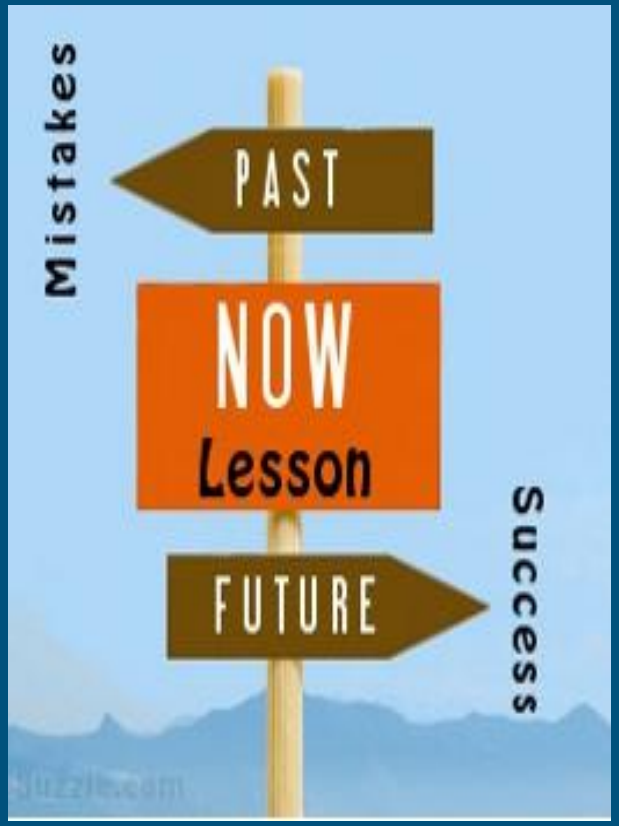
Top Causes of Data Security Incidents

- Phishing, hacking or malware
- Employee action or mistake
- External theft
- Vendor
- Internal theft
- Lost or improper disposal of data



A **data breach** is a security incident in which sensitive, protected or confidential **data** is copied, transmitted, viewed, stolen or used by an individual unauthorized to do

Figure 2 – Timeline of large retail data breaches after the Target breach



Are you Serious?

What Happened?

- Customer’s Personally Identifiable Information was compromised

Why They Did It?

- Financial Incentive

How Did This Happen?

- Outsourcing & Lack of IT knowledge

Customer Personally Identifiable Information

Impact Levels

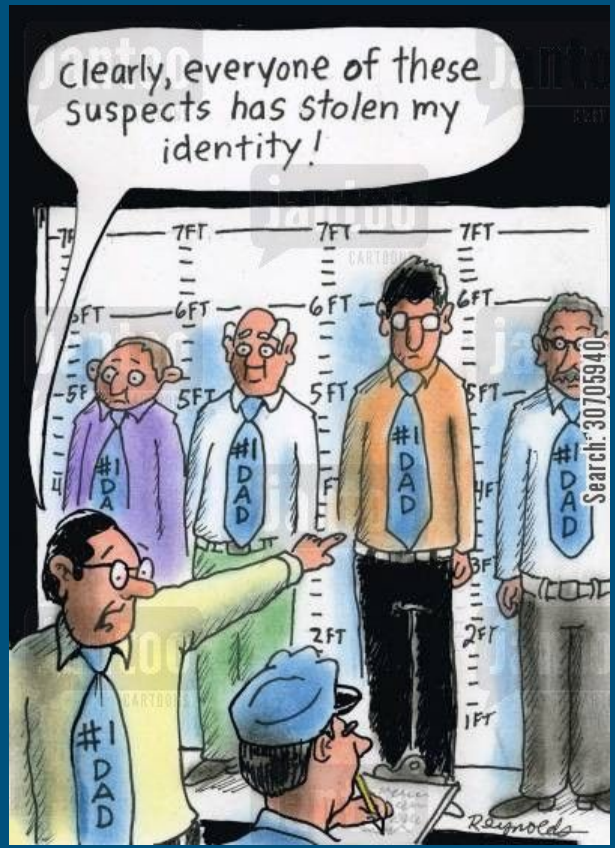
Low: Facebook

Medium: Temple #

High: Credit Card & Pin

SafeGuards

Policies
Procedures
Training



Financial Incentive

Sales Cycle

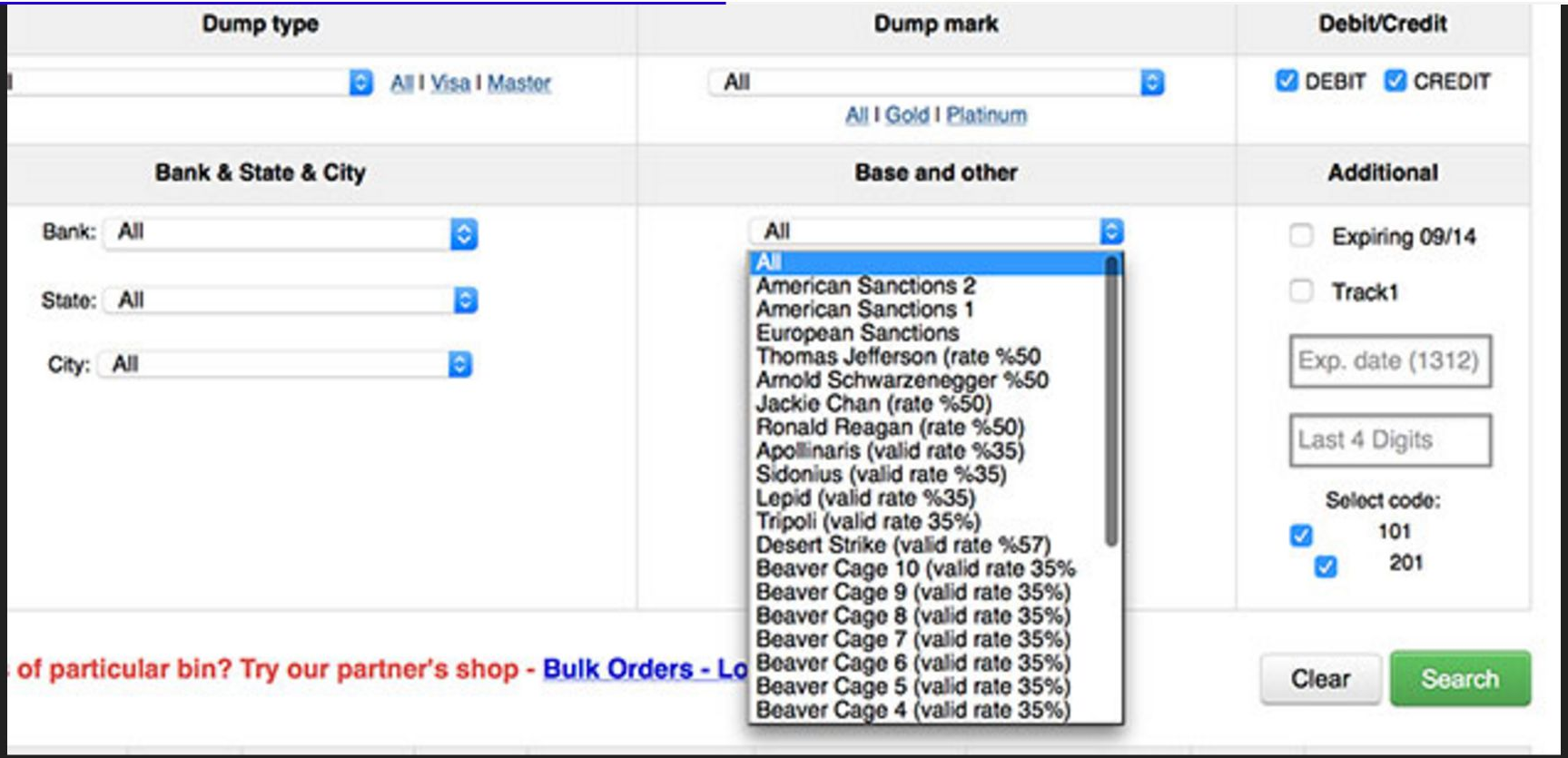
The “Darknet” Business Environment

Carders

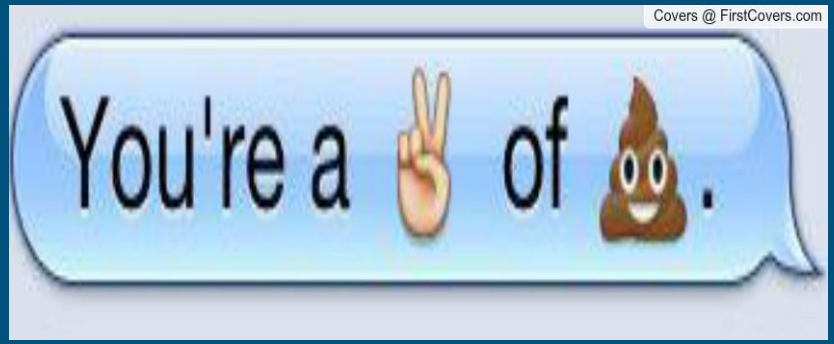
Gift Cards - Home Depot???

Dummy Addresses

I’m Fast as Fast Can Be, Never Catch Me



Negligence & Incompetence



Internal & External

POS System - Point Of Sale or Piece of S**T?

Zero-Day Vulnerability

Memory Scraping Malware

Impact to the business

We can measure the effect of the data breach in three ways:

1) Impact on stakeholders
2) Impact on reputation
3) Impact on the finances of Home Depot

Impact to the business (Stakeholders)

Stakeholders affected by data breach

Employees

Investors

Consumers

Impact on the employees

- Disruption in normal business operation
- Communication between management focused on data breach
- Dealing with disgruntled customers face-to-face.

Impact on the investors

- The company’s stock decreased after the announcement of the data breach.
- Although, Home Depot had recorded a 21% increase in earnings-per-share for Q3.
- Investors were not affected by data breach in the long-term.

Impact on the consumers

Customer data that was stolen included:

- Credit Card #
- City
- State
- ZIP

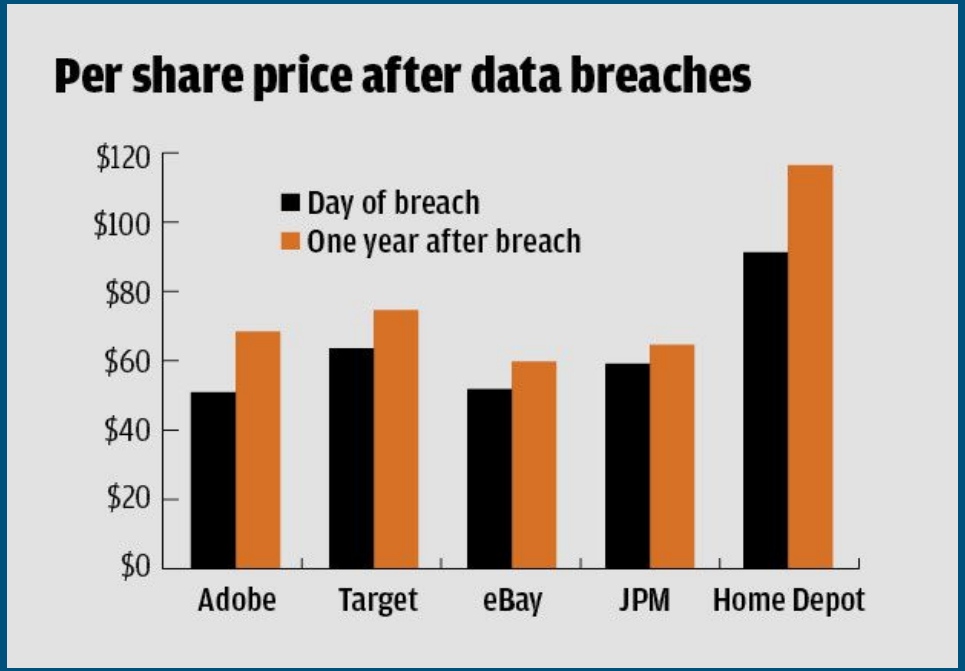
The customer had to go through the process of receiving compensation of their stolen information that had been used to illegally purchase goods by the thieves.

Impact to the business (Reputation)

How do we monetize the loss of Home Depot's reputation?

- A report by Ponemon Research estimated a 3% "high churn rate" following the breach.
  - This is less that the typical 6% for data breaches in other industries including retail.
- Why the low rate of attrition from Home Depot?
  - Strong US housing market (materials needed by contractors)
  - Trusted American brand
  - Lack of competition (Lowes, only true competitor)

Impact on the business (Reputation)



"Does a data breach really affect your firm's reputation?"

By Doug Drinkwater

Impact on the business (Financial Losses)

Based on the calculation of Forbes:

- Home Depot is set to lose $10 billion by the end of the decade.

In 2014, they had included a $28 million pre-tax expense for the data breach investigation.

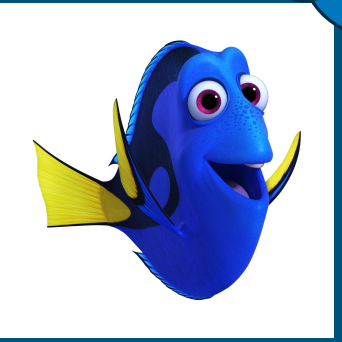
- $28 million only represents 0.01% of Home Depot’s sales revenue for 2014.

Most recently, the losses were expected to be around $62 million.

Root Causes

- Theft of payment cards
- Stolen third party vendor credentials
- RAM scraping malware
- Unsegregated payment network
- Zero Day vulnerability of Windows XP
- Advantage of POS which are vulnerable and never fixed
- Improper access management for vendors
- No Monitoring
- No vulnerability assessments
- Symantec Network Endpoint Solution not activated

Hi..I am Dory!
Third party

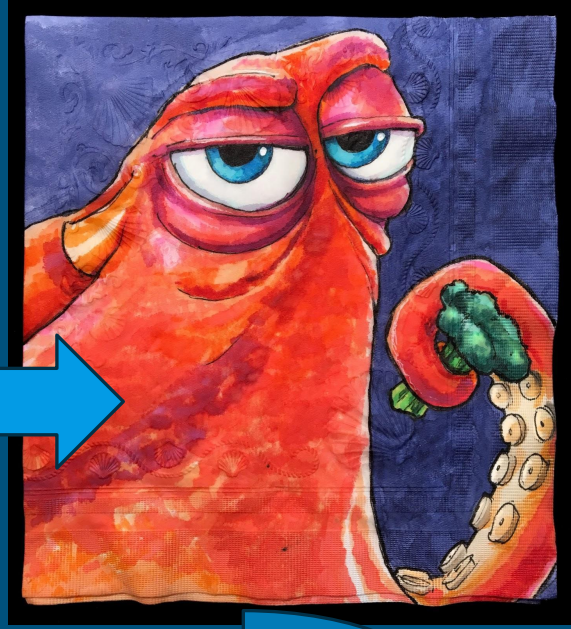


HI I am Hank!
And I have your credentials now Ms Third Party

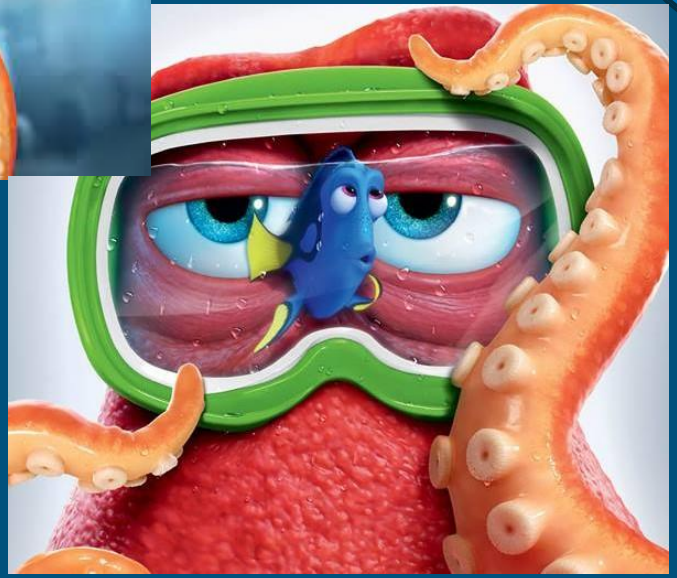
Now I will target all vulnerable POS

Card, Transactions

Scraping



Devil Server



Lalalal!
I am scraping for last 5 months
Seriously!
No security update
No monitoring
Poor access management

RAM SCRAPING MALWARE

- Malware installed at point-of-sale terminal preciously 7500 POS
- Attack on RAM to collect card details and email address
- RAM connects the card, the terminal, and the computer servers
- Uses software of connect to RAM and copy data
- Exploit the RAM which lacks up-to-date security system patches
- Brief period when transaction is taking place and card details are in clear text

Missing controls

- Employee security awareness training
- Third party access control
  a. Stolen credential from third parties vendors
  b. Acquired elevated right to gain direct access to home depot's Network and install malware
- P2P encryption
- Not frequently updated anti-virus software
- Old operating system
- Failure to maintain an adequate firewall
- Failure to use up- to-date antivirus software on its point-of-sale terminals
- Failure to restrict access to cardholder data on its network
- Vulnerability management program

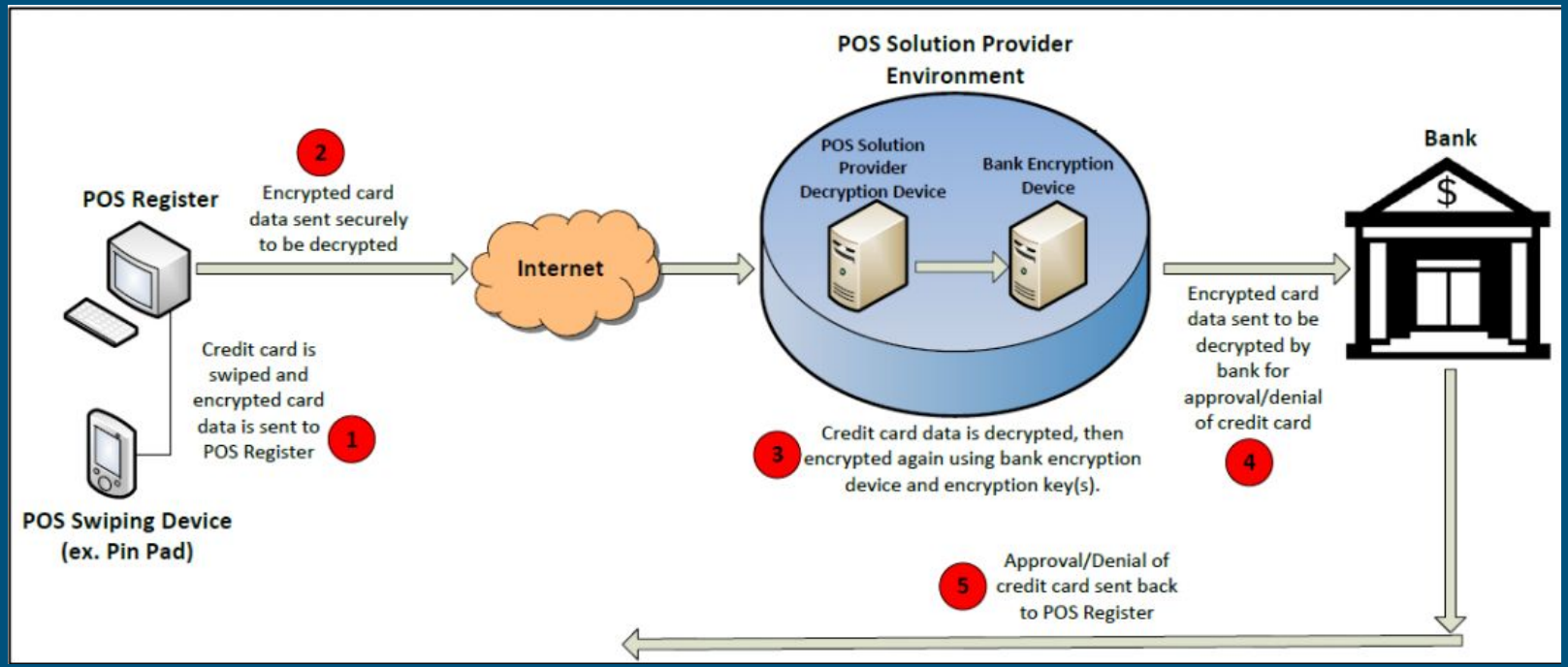
Reasons why controls are missing

- ALL these failures were due to
  - Unawareness of Cyber security by senior management
  - No lessons learned from small data breaches
    - Small data breach - Stores at Dallas, Columbia, Maryland
    - Ignorance of VISA warning letter
    - Ignorance of security consultant’s warning
  - Intention to cut corners to save money

Recommendations

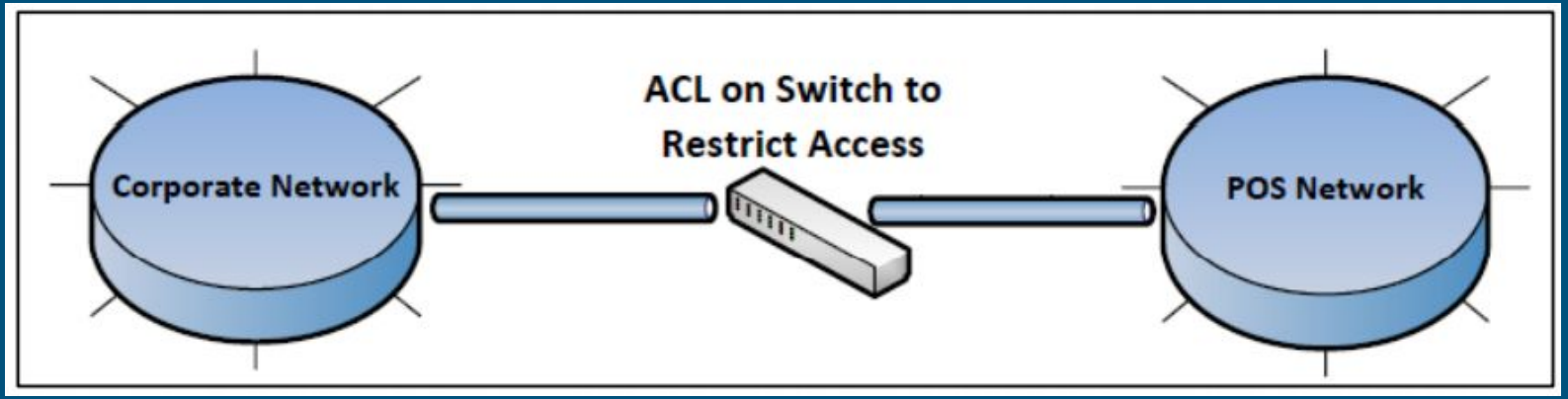
- P2P encryption-encrypts card data at the point of swipe, all the way to the bank for approval/denial of the transaction
- Network Segregation
- Managing third party vendor credentials

P2P encryption



POS Network Segregation

- POS network should be properly segregated from the rest of the corporate network.
- ACL denies all traffic between the two environment
- Network segregation allows to configure firewall rules (necessary connections only)



Managing Third Party Vendor Credentials

- Minimize access needed to perform their tasks and should be denied access to internal resources
- Manage the identities and access
- Have their own account
- Auditing

Questions

References

GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

Bloomberg Businessweek: *The Amazon.com of Stolen Credit Cards Made So Easy*

http://www.bloomberg.com/news/articles/2014-09-04/the-amazon-dot-com-of-stolen-credit-cards-makes-it-all-so-easy

http://www.creditcards.com/credit-card-news/Infographic-data-breaches.php

http://blog.gemalto.com/security/2016/03/03/2015-data-breaches-by-the-numbers/

http://www.steptoe.com/assets/attachments/4898.pdf

http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html

http://www.propertycasualty360.com/2016/04/12/what-are-the-leading-causes-of-data-security-breac?page=2&slreturn=1478566822

References

https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

http://www.forbes.com/sites/greatspeculations/2015/03/30/home-depot-will-the-impact-of-the-data-breach-be-significant/#4e2beeab69ab

http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/

https://www.giac.org/paper/gsec/36253/case-study-home-depot-data-breach/143349