Home Depot Data Breach

Team 19

Team

Jake Joseph
jakejose@iu.edu

JJ Bogner
jjbogner@iu.edu

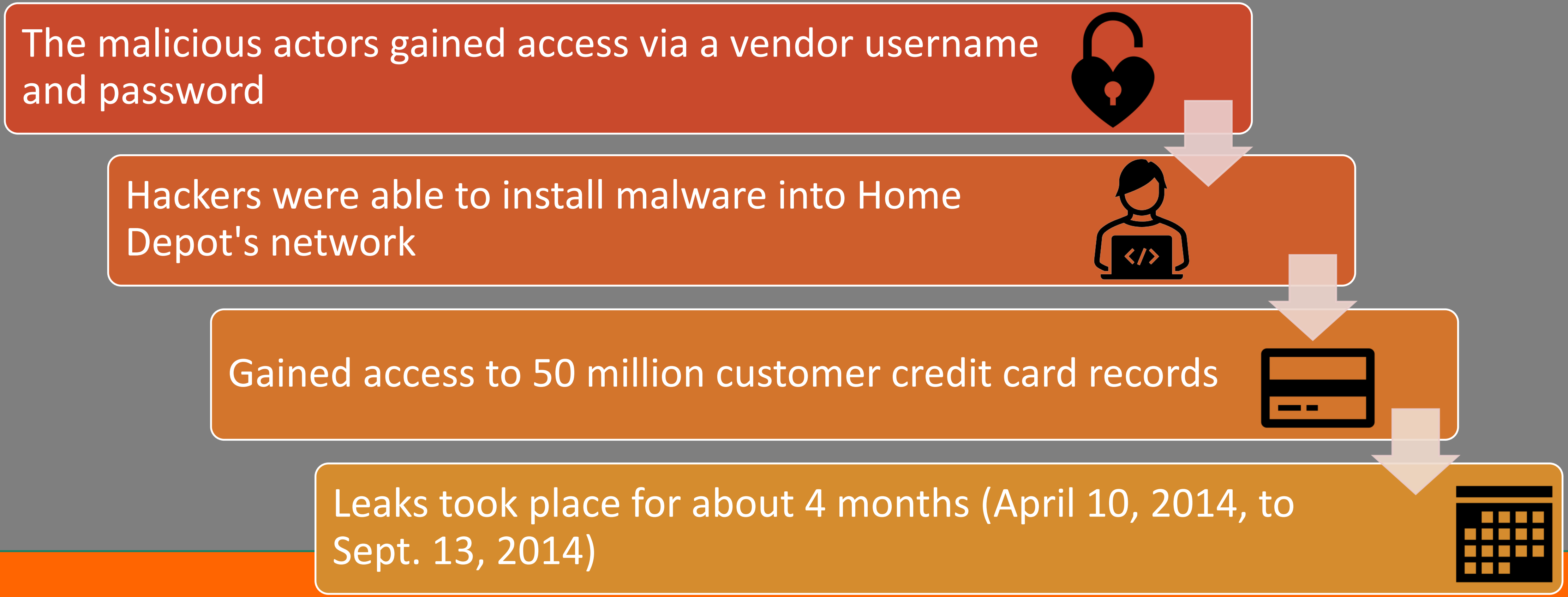
Priya Huddar
phuddar@iu.edu

Vivi Armacost
varmacos@iu.edu

Presentation Agenda

- Introduction
- Recommendations
- Timeline
- Risks & Mitigations
- Financials
- Conclusion

Incident Brief: Rundown of how Home Depot became victim to a breach, what was stolen, and how long it took place



The malicious actors gained access via a vendor username and password

Hackers were able to install malware into Home Depot's network

Gained access to 50 million customer credit card records

Leaks took place for about 4 months (April 10, 2014, to Sept. 13, 2014)

Incident Brief: Root cause of customer data incident and why it is important.

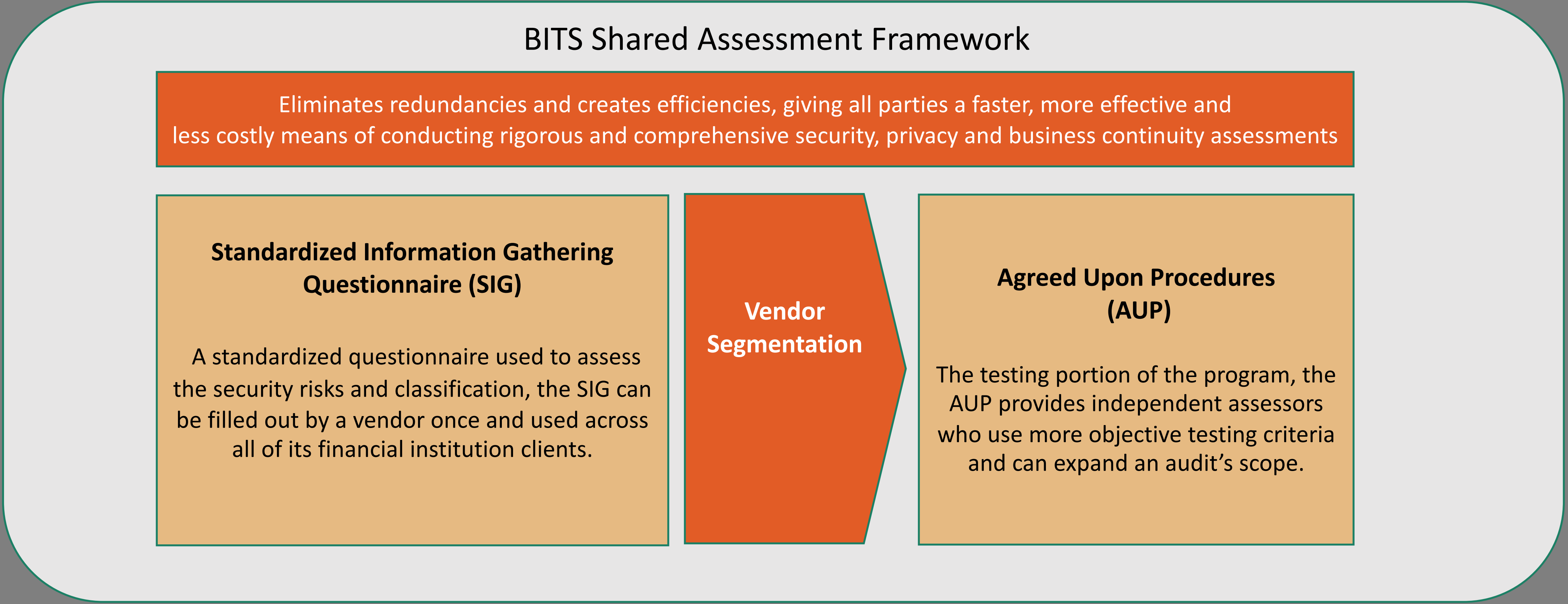
✓Much of the risk in this particular incident can be allocated to Home Depot’s vendor management

✓The vendor did not have proper controls and best practices in place to handle compromised credentials through a phishing attack

✓Faults of the vendor lead to a greater chance for breach of Home Depot’s systems

➢ How can Home Depot address flaws in its vendor management to prevent a similar attack?

The new Vendor Risk Management model will standardize information gathering, segmentation, negotiation, and auditing



BITS Shared Assessment Framework

Eliminates redundancies and creates efficiencies, giving all parties a faster, more effective and less costly means of conducting rigorous and comprehensive security, privacy and business continuity assessments

Standardized Information Gathering Questionnaire (SIG)

A standardized questionnaire used to assess the security risks and classification, the SIG can be filled out by a vendor once and used across all of its financial institution clients.

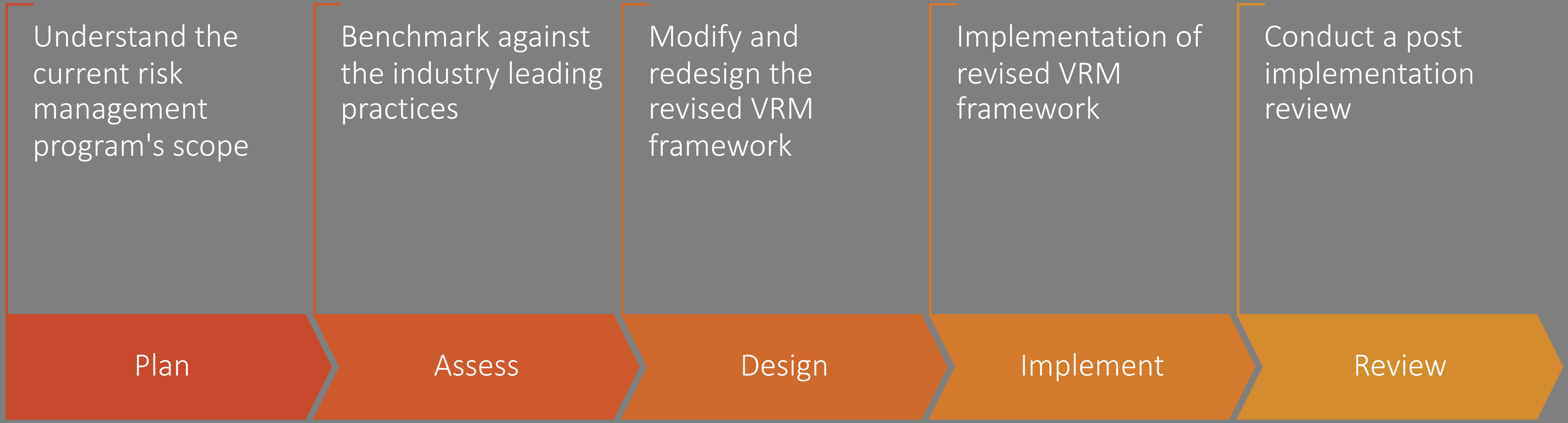
Vendor Segmentation

Agreed Upon Procedures (AUP)

The testing portion of the program, the AUP provides independent assessors who use more objective testing criteria and can expand an audit's scope.

A comprehensive VRM program will reduce IT risk by identifying vendor security practices and information responsibility

The implementation plan for a new vendor relationship business process will involve reviewing the current enterprise standards, identifying the weaknesses and updating processes with consistent iteration



Plan: Understand the current risk management program's scope

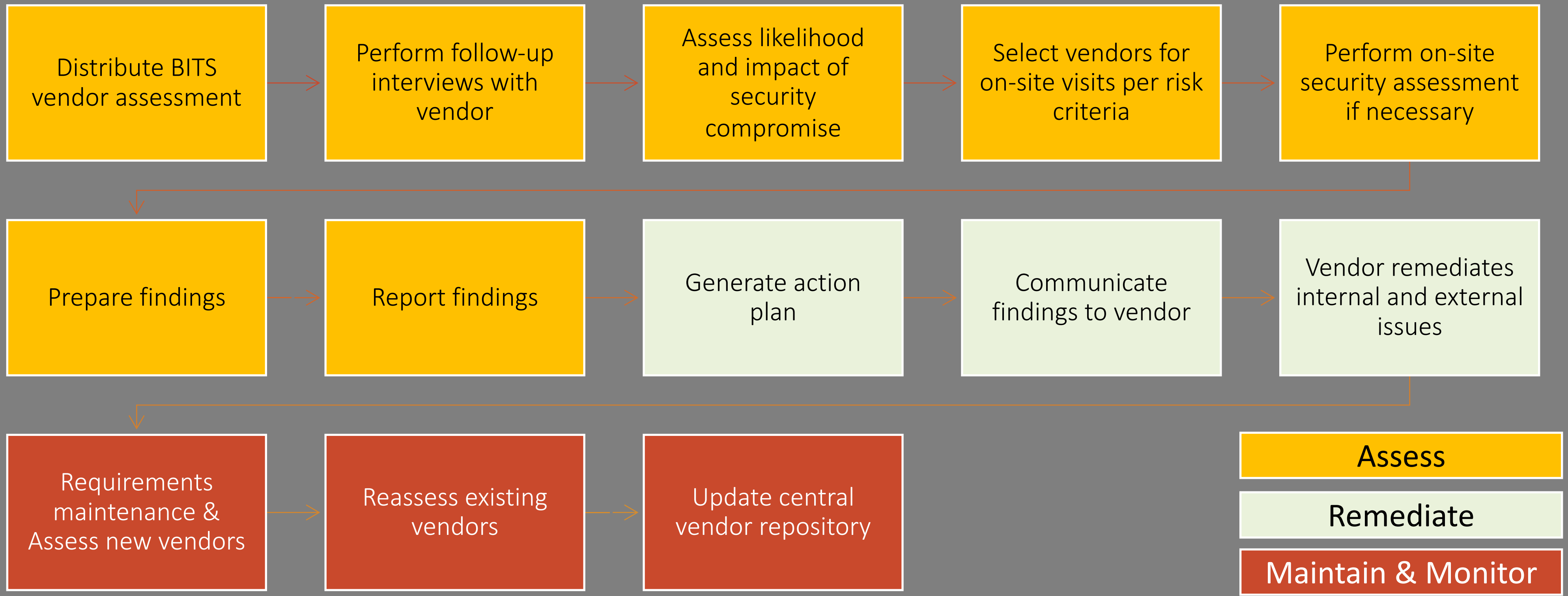
Assess: Benchmark against the industry leading practices

Design: Modify and redesign the revised VRM framework

Implement: Implementation of revised VRM framework

Review: Conduct a post implementation review

Post-breach vendor allocation will involve initial assessment as well as continuous monitoring and remediation within the reach of the vendor



Distribute BITS vendor assessment → Perform follow-up interviews with vendor → Assess likelihood and impact of security compromise → Select vendors for on-site visits per risk criteria → Perform on-site security assessment if necessary

→ Prepare findings → Report findings → Generate action plan → Communicate findings to vendor → Vendor remediates internal and external issues

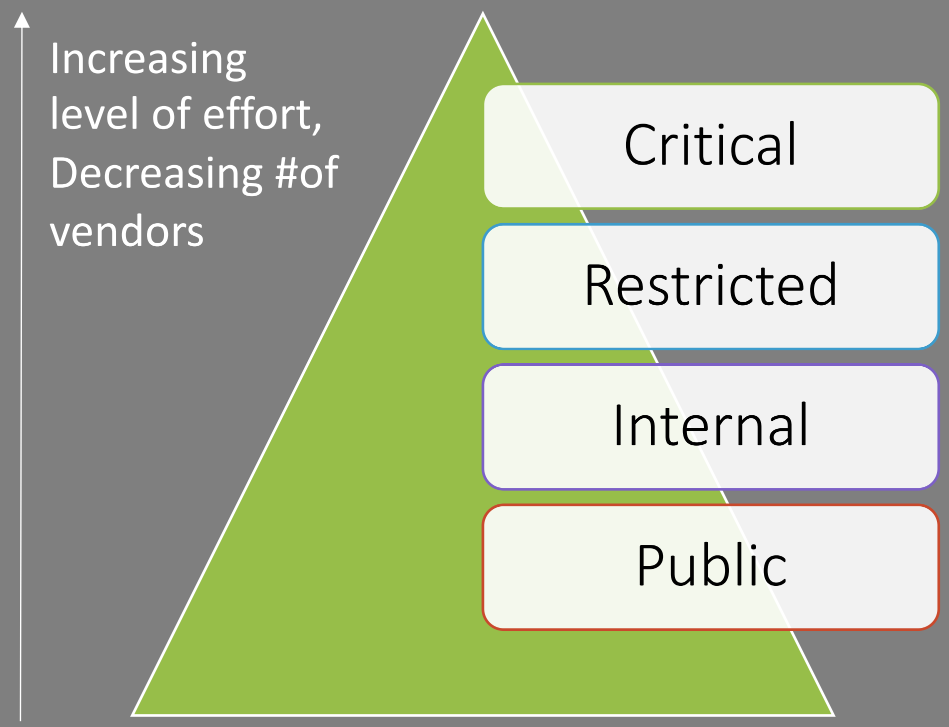
→ Requirements maintenance & Assess new vendors → Reassess existing vendors → Update central vendor repository

Assess

Remediate

Maintain & Monitor

Segment the vendors based on data classification to manage priorities and resources



Increasing level of effort, Decreasing #of vendors

Critical	Credit Card Info, Customer info (address, phone, email)
Restricted	Payroll info, employee performance data, HR data, tax info
Internal	Strategy & roadmap documents, budgets, internal reports
Public	Marketing, PR, surveys, web and media, advertising

New VRM program would identify risky vendors like the one that caused the breach

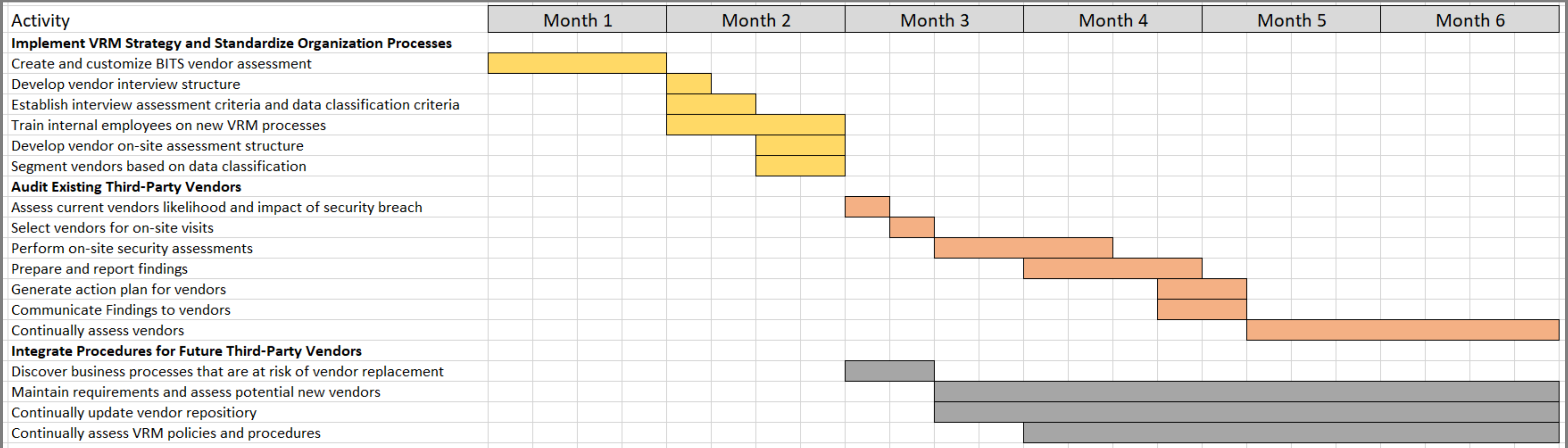
- Vendors credentials were compromised, vendor did not find out/report this issue to lock those credentials
- No Multifactor authentication set up at vendor's end. New VRM program would mandate MFA
- VRM plan would mandate that vendors be PCI compliant
- The vendor that got breached be classified as "Critical", as it had access to Credit Card Information. It would be assessed with the strictest standards of the VRM plan
- Credentials were lost through a phishing campaign. VRM plan would involve checking the security preparedness of vendor staff, including whether staff is trained through internal campaigns, whether there is external email system warning etc.
- Continuous assessment of vendor would identify lack of staff training, lack of monitoring of network access and flag vendor
- VRM program would clearly lay out liability clauses regarding breached credentials

Assessment example snapshot (table of vendor evaluation)

ID	Question/Request	Response (YES/NO)	Date of Last Check (mm,dd,yyyy)
Security			
1	Adequate Security Policy in place?		
2	Proper functions in place to support security?		
3	Flaws in data security?		
Compliance			
4	Is the vendor SOX compliant?		
5	Does the vendor follow SEC regulations?		

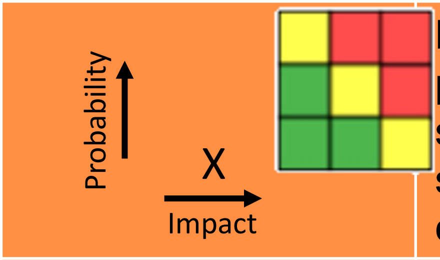
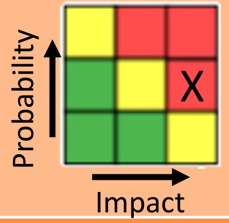
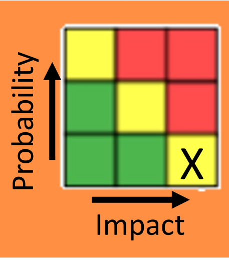
We will also prescriptively apply standardization references for specific vendor requirement requests (ISO, AUD, SOX, etc.)

Timeline



Activity	Month 1				Month 2				Month 3				Month 4				Month 5				Month 6			
Implement VRM Strategy and Standardize Organization Processes																								
Create and customize BITS vendor assessment	■	■	■	■																				
Develop vendor interview structure					■																			
Establish interview assessment criteria and data classification criteria					■	■																		
Train internal employees on new VRM processes					■	■	■	■																
Develop vendor on-site assessment structure							■	■																
Segment vendors based on data classification							■	■																
Audit Existing Third-Party Vendors																								
Assess current vendors likelihood and impact of security breach									■															
Select vendors for on-site visits										■														
Perform on-site security assessments											■	■	■	■										
Prepare and report findings													■	■	■	■								
Generate action plan for vendors																■	■							
Communicate Findings to vendors																■	■							
Continually assess vendors																		■	■	■	■	■	■	■
Integrate Procedures for Future Third-Party Vendors																								
Discover business processes that are at risk of vendor replacement									■	■														
Maintain requirements and assess potential new vendors											■	■	■	■	■	■	■	■	■	■	■	■	■	■
Continually update vendor repository											■	■	■	■	■	■	■	■	■	■	■	■	■	■
Continually assess VRM policies and procedures													■	■	■	■	■	■	■	■	■	■	■	■

Risks and Mitigation

Risks	Risk Profile	Mitigation Strategies
Certain vendors may not be able to implement security or training procedures into their own practices fast enough for Home Depot standards.		Develop an oversight committee during the early stages of the process to focus additional attention on monitoring third-party software that need more time for changing processes. In worst case scenarios, find potential replacement providers of services that cannot comply.
Potential attackers and malware technology may still bypass vendor systems despite VRM implementation.		Create a dedicated IT industry insights team that keeps up-to date with data breach incidents and technological trends. Ensure constant flow of communication between insights team and the CISO and security teams to discover any potential gaps that arise.
Third-party vendors and internal employees may be reluctant to change processes or may not understand how their role fits into the new processes.		Implement process training sessions throughout the organization so that involved associates understand the activities, responsibilities, and importance of the new VRM strategy. Adopt a top-down change management approach that encourages hands-on participation from management.

Financials

Estimated Total Cost of the Data Breach: $179 Million

+ Legal Fees

Over $200 Million

Cost of VRM Implementation:

Consulting Fees (2 consultants x $200/hr) $416,000

Third-Party Relationship Manager Training ($500 x 125 employees) $62,500

$478,500

Benefits:

Avoided Costs of Potential Future Breaches

Improved Business Continuity

Faster Value Realization From Vendors

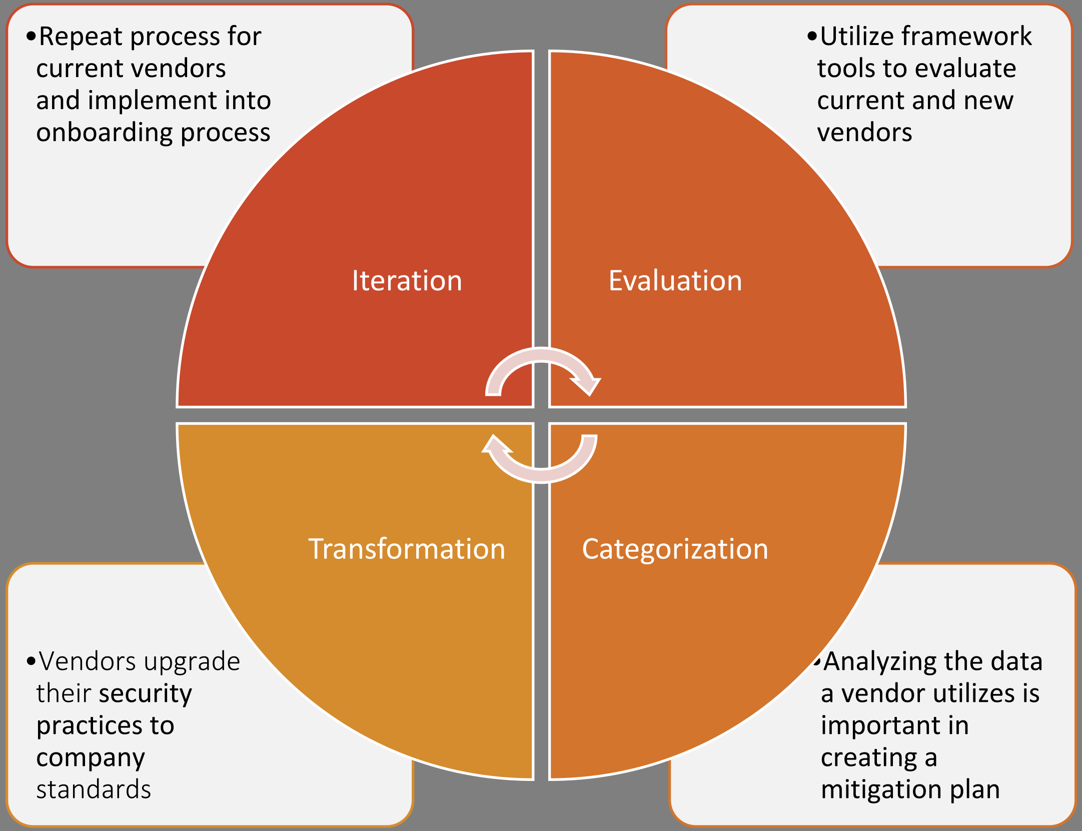
Estimated 3-Year NPV $4.7 Million

https://www.arctitan.com/blog/case-study-data-breach-cost-home-depot-179-million/

https://www.cybertrust-it.com/2020/08/cyber-security-consultant-best-tips-safe-networks/

https://www.thimble.com/blog/how-to-set-consulting-rates#:~:text=Management%20consultants%20charge%20between%20%24100%20to%20%24350%20per%20hour.

Utilize the BITS Framework and segmentation to create a standard business process in prioritizing vendor security and updating external procedures and agreements to deliver value for Home Depot



- Repeat process for current vendors and implement into onboarding process

- Utilize framework tools to evaluate current and new vendors

- Vendors upgrade their security practices to company standards

- Analyzing the data a vendor utilizes is important in creating a mitigation plan

6 Month Implementation

$478,400 Investment

$4.7 Million 3-Year NPV

Appendix

Issue Tree

Hypothesis Tree

Additional Suggestions

Home Depot Statement post-security breach

Security breach additional information

Solution ideas

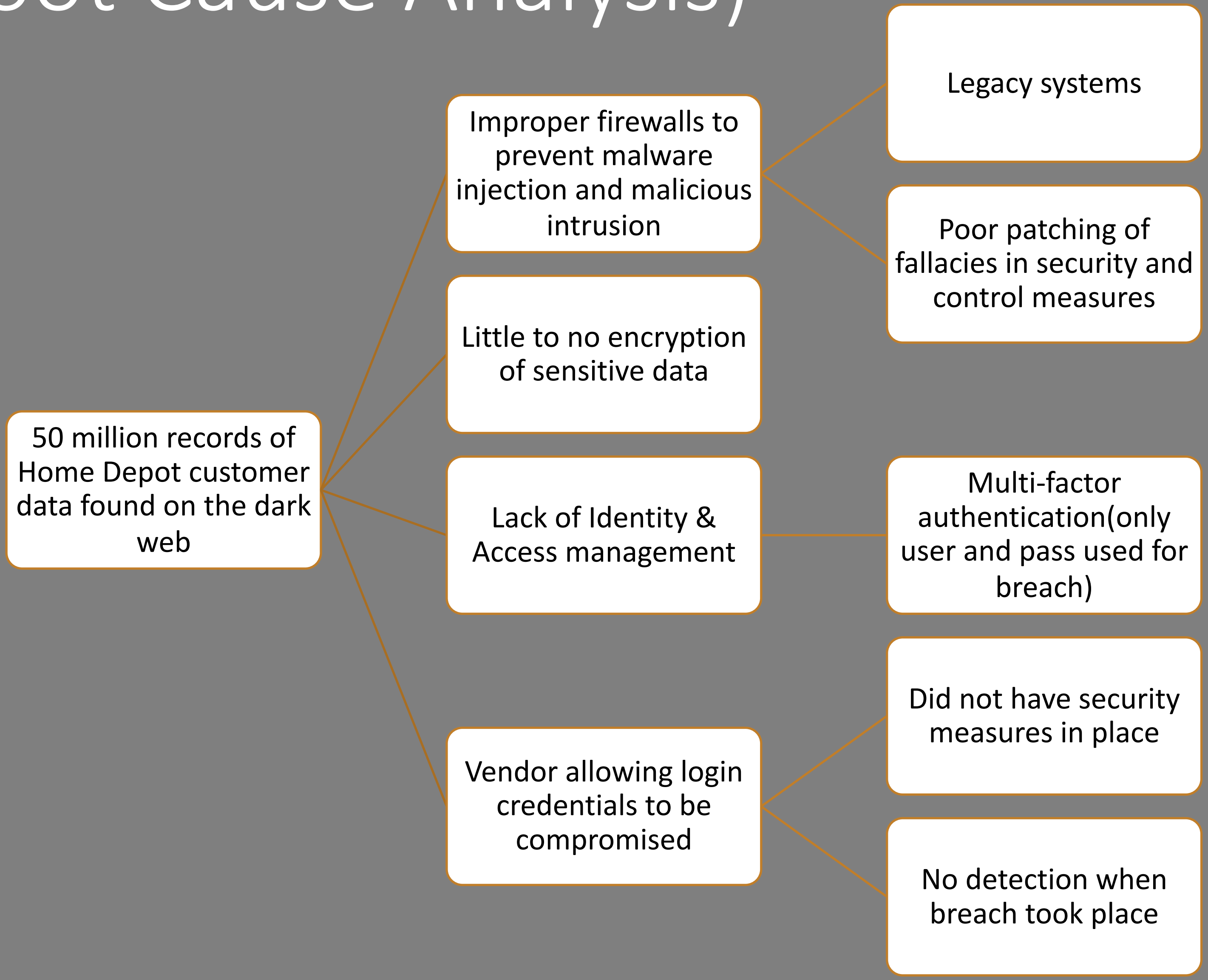
Vender Risk Assessment Requirements

Example Assessment

Home Depot Compliance Requirements

Issue Tree (Root Cause Analysis)

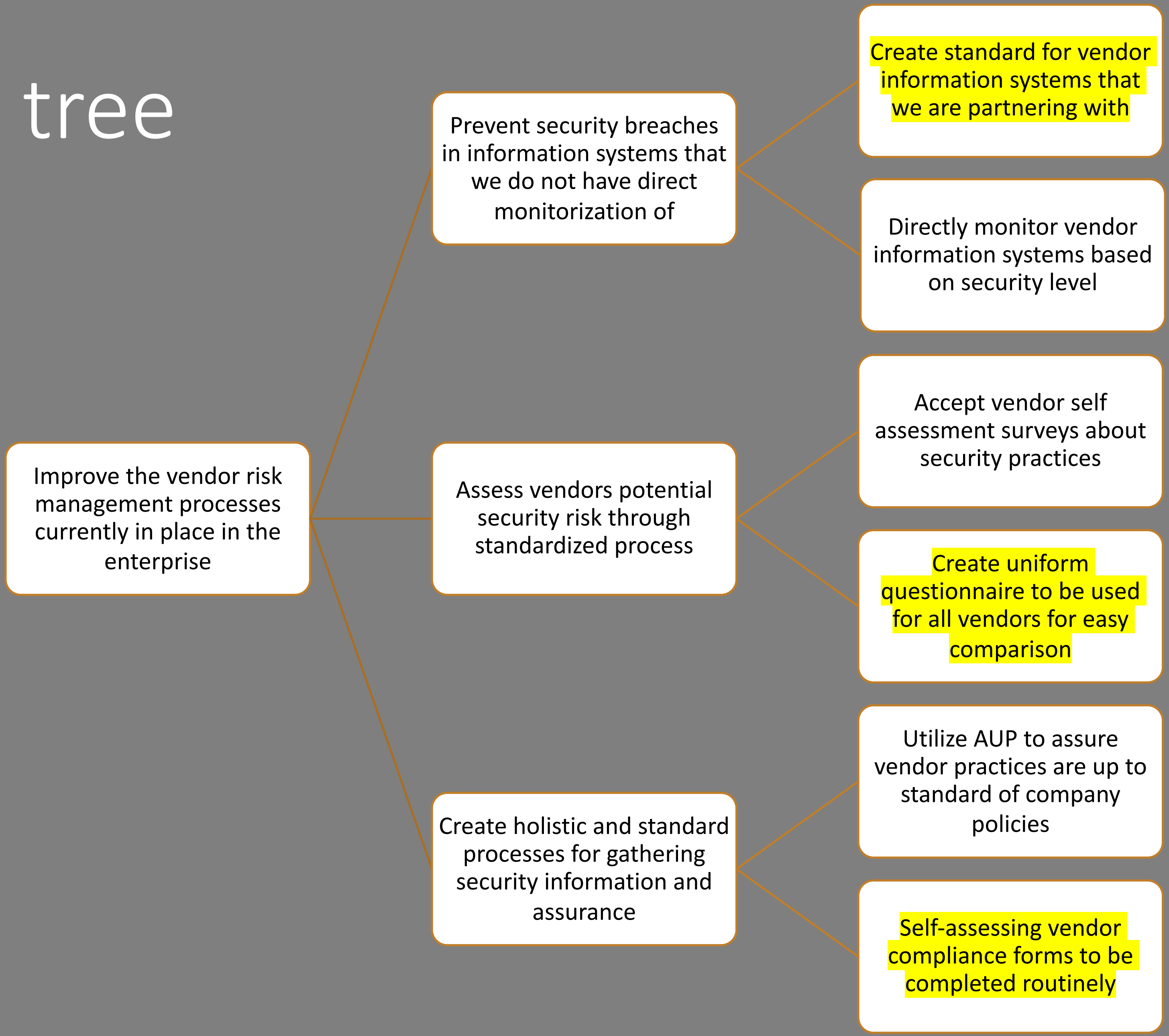
The goal of our issue tree is the address Home Depot’s mismanaged vendor security Clear and encompassing solutions are a major point of emphasis for the overall goal of the presentation.



- 50 million records of Home Depot customer data found on the dark web
  - Improper firewalls to prevent malware injection and malicious intrusion
    - Legacy systems
    - Poor patching of fallacies in security and control measures
  - Little to no encryption of sensitive data
  - Lack of Identity & Access management
    - Multi-factor authentication(only user and pass used for breach)
  - Vendor allowing login credentials to be compromised
    - Did not have security measures in place
    - No detection when breach took place

Hypothesis tree

This hypothesis tree indicates our thought process for
the solution of improving current VRM process at Home Depot. Due to recent major security breach, a new process must be implemented.



Improve the vendor risk management processes currently in place in the enterprise

Prevent security breaches in information systems that we do not have direct monitorization of

Create standard for vendor information systems that we are partnering with

Directly monitor vendor information systems based on security level

Assess vendors potential security risk through standardized process

Accept vendor self assessment surveys about security practices

Create uniform questionnaire to be used for all vendors for easy comparison

Create holistic and standard processes for gathering security information and assurance

Utilize AUP to assure vendor practices are up to standard of company policies

Self-assessing vendor compliance forms to be completed routinely

What Home Depot must do to improve its systems so that it can prevent breaches even if hackers secure vendor credentials

- Proper payment network segregation from the rest of the Home Depot network
- Point to point encryption encrypts card data at the point of swipe, all the way to the bank for approval/denial of the transaction
- Regularly scheduled vulnerability scanning of the POS environment
- Intrusion Prevention System (IPS)

Facts about the case

- 40 million customer payment card records lost in self-checkout terminals in the US & Canada
- Length of breach: ~4 months (April 10, 2014, to Sept. 13, 2014)
- Infiltrators used vendor username and password to hack network and inject malware
- $17.5 million settlement
- $198 million in pretax expenses

- https://www.reuters.com/article/us-home-depot-cyber-settlement/home-depot-reaches-17-5-million-settlement-over-2014-data-breach-idUSKBN2842W5

Home Depot Statements on the Incidents

- 53 million email records also seized
- Providing free identity and monitoring services

Implemented after the attacks:

Enhanced Encryption of payment data in the US & Canada (provided by Voltage Security)

EMV Chip-and-PIN Technology

https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315

What Home Depot could do to combat such breaches

- Manage and oversee when and who employees log into systems
  - this would have potentially caught the hackers logging in at weird times
- Periodically scan vendor software for changes in code or any specific activity (weekly scans, automated technology)
  - This would have picked up the changes to the POS system early in the process
- Establish a process for creating contracts with new vendors
- Make sure that vendors encrypt all sensitive information
  - Encrypted data will function as another safeguard against potential hackers
- Request information from the vendor about what internal campaigns they follow for phishing schemes etc.

Full List of Requirements to be checked in vendor risk assessment

- Security Policy
- Organizational Security
- Asset Management
- Human Recourse Security
- Physical & Environmental Security
- Communications/Operations Management
- Access Control
- IS Acquisition Development & Maintenance
- IS Incident Management
- Business Continuity & Disaster Recover
- Compliance

Application can be based on dependencies

Full example of assessment snapshot

ID	Question/Request	Response (YES/NO)	Date of Last Check (mm,dd,yyyy)	Compliance Document Ref Number	Compliance document Ref Text
	Security				
1	Adequate Security Policy in place?				
2	Proper functions in place to support security?				
3	Flaws in data security?				
	Compliance				
4	Is the vendor SOX compliant?				
5	Does the vendor follow SEC regulations?				

Home Depot Compliance Requirements

- Deploy a CISO into their C-SUITE
- Providing resources to fully implement their new security program
- Providing security awareness training to all personnel that have access to the company's network
- Employing security safeguards (see article for full list)
- Comply with a post-settlement security assessment which will validate the new security standards

- https://www.infosecurity-magazine.com/news/home-depot-2014-breach/

Financials Expanded

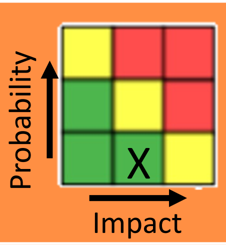
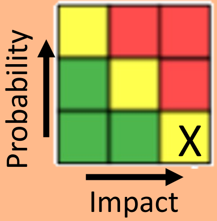
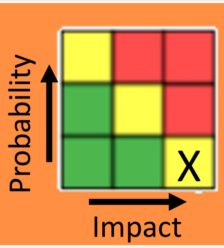
- VRM Training courses typically costs between $275 to $1,500, depending on the certification
- Home Depot new technology center houses roughly 1,250 current IT employees
  - Estimated that training 10% of this workforce would be an adequate number of managers to train
- Study for average cost savings received through various GRC tactics
  - Centralized governance = $3.01 million in savings
  - Compliance audits = $2.86 million in savings
  - Integration with security and privacy functions = $2.02 million in savings
  - Incident response processes = $1.89 million in savings
  - Enabling compliance technology = $1.43 million in savings
  - Regulatory monitoring = $1.02 million in savings
- Based on Forrester 3rd Party Vendor Risk Management Case
  - $7 Billion Fortune 500 company saved between $460,000 – $860,000 per year using VRM
  - 3-Year NPV from business continuity was $249,049.
  - Home Depot 2020 annual revenue is $132 Billion
  - Calculation: (132 Billion/7 Billion) x 249,049 = 4,696,352.57

https://www.aba.com/training-events/online-training/vendor-risk-management

https://www.dvvs.co.uk/wp-content/uploads/2018/02/Forrester_TEI_Report_The_Total_Economic_Impact_of_Prevalent_3rd_Party_Risk_Management_Solutions.pdf

https://www.dvvs.co.uk/wp-content/uploads/2018/02/Forrester_TEI_Report_The_Total_Economic_Impact_of_Prevalent_3rd_Party_Risk_Management_Solutions.pdf

Additional Risks and Mitigation

Risks	Risk Profile	Mitigation Strategies
Project may go over expected budget or timeline		Ensure that proper requirements gathering is done in the early phases of the project. Be clear about project scope and discover and bring up scope creep early in the process.
Training may need to be expanded to additional users or new certifications may come out in the industry.		Stay up-to-date with VRM certifications by delegating responsibility to internal VRM managers to periodically check industry trends. Prepare a program to train power users on how the VRM processes work and structure training sessions so that internal employees can adopt training practices to teach internal co-workers.
New standards may arise in the consumer retail industry regarding PCI or other business factors		Be prepared to maintain an agile VRM process and understand that priorities and activities may need to change in order to comply with changing industry standards.