THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF ACCOUNTING

THE IMPACT OF EFFECTIVE VENDOR RISK MANAGEMENT IN RAPIDLY CHANGING BUSINESS ENVIRONMENTS AND A NEW PROPOSED RISK UNIVERSE PROFILE

SANG YEOP LEE
SPRING 2016

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degrees in Accounting and Information Science and Technologies
with honors in Accounting

Reviewed and approved* by the following:

Scott Collins
Clinical Assistant Professor of Accounting
Thesis Adviser

Henock Louis
KPMG Professor of Accounting
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

After the 2008 financial crisis, regulatory scrutiny has been rising to reach not only financial organizations but also to the vendors and third parties that supply them. As responsibilities cannot be outsourced, financial institutions are being held responsible by regulators for not only their actions, but also for those of their vendors and suppliers. Financial institutions now have started looking at ways to broaden their risk profiles of their suppliers and vendors with an increased emphasis placed on preventive, detection, and mitigation controls.

This thesis shines light on the importance of vendor risk management (VRM) and its rising need for businesses with IT related vendors. The specific industry analyzed is the financial services industry where, on average, more than 20,000 vendors supply major financial institutions. Big Four public accounting firms are analyzed as main VRM service providers in the financial industry. Through analysis of current VRM methodologies and risk profiles, this thesis draws a conclusion on the impact of the VRM for businesses to manage emerging risks and stay competitive in the market. From research, a new proposed VRM risk universe profile is introduced and applied to a case of Target's data breach incident to demonstrate how VRM could prevented such tragedy.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to Scott Collins, my thesis supervisor, for his patience, continuous academic and personal guidance, and willingness to help me at all time. Scott's valuable insights and lessons, from both inside and outside of classes, motivated me to have genuine interest in the topic of vendor risk management. His encouragement and motivation have been paramount to the completion of my thesis. I would also like to acknowledge Professor Henock Louis, my honors advisor, for his guidance and wisdom that kept me on the track and fulfill all of the requirements on time. Dr. Louis' expertise in accounting and accounting research have helped me immensely from the planning phase to editing of my final submission. Lastly, I would like to thank Dr. Orie Barron for overseeing my thesis process from the beginning to the end through BA 412H and ACCTG 494H. Dr. Barron's continuous support and trust in my research on a trending topic in accounting truly encouraged and motivated me to stay on track and to leverage insights from professionals and professors with expertise in the practice.

INTRODUCTION

Vendor risk management (VRM) is a comprehensive management plan for preventing, identifying, and mitigating potential business risks and legal liabilities inherited from information technology (IT) products and services, data exchange services, business process outsourcing (BPO), and other related services provided by third party vendors. Vendor risk management has been rapidly increasing in various industries, as more businesses became specialized and therefore leveraged expertise from third parties through outsourcing products and services. Many businesses have, however, been blinded by the immediate benefit of outsourcing their products and engaging third parties, only recently they have realized the importance of managing risks of engaging third parties. The industry standard has been established for an institution's board of directors and senior management to be ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution. As, on average, financial institutions typically have more than 20,000 vendors, many institutions were stuck with figuring out where to start with their vendor risk management plan.

The purpose of this publication is to illustrate the importance of proper vendor risk management in preventing, detecting, and mitigating emerging risks from third party vendors. Recently, vendor risk management has made headlines as organizations struggle with managing third party vendor risks. Four leading public accounting firms, Deloitte, PwC, EY, and KPMG have implemented structured vendor risk management program into their internal audit engagements and became the major VRM providers.

Through analysis of the four accounting firms' current VRM methodologies and risk profiles, this research draws a conclusion on the impact of the risk modeling in preventing, detecting, and mitigating vendor risks and improving overall company competitiveness. This research also presents a new risk universe profile that encompasses both core and emerging risks derived from the four firms. Target's data breach incident is conducted as a case study to demonstrate the impact of a proper vendor risk management plan in preventing, detecting, and mitigating vendor-related problems.

INDUSTRY BACKGROUND

Since the most recent economic recession of 2008, regulatory environment of financial services has become stricter than ever. As business processes became more complex with the rise of outsourcing and advanced technologies, it is not only necessary but also now mandatory for the companies to have a proper management tool to comply with new regulations as well as managing business risks from third parties. Many companies have started to implement vendor risk management services with the help of external consultants to evaluate, track, and measure third party risks to access its impact on business and develop preventive, detective, and mitigation controls to lessen the impact of the business risks. However, vendor-management programs have focused predominantly on risks to the bank and the financial system such as business continuity, financial strength, and credit risk. Since financial institutions are ultimately responsible for their suppliers' actions, vendor risk management has been rapidly evolving to encompass emerging risks and regulatory requirements. Emerging risks in advanced technology and regulatory

requirements include regulatory and compliance risk, cyber security, cloud computing, IT compliance, mobile, identity theft, corporate governance and internal control failures.

EMPHASIS ON VENDOR RISK MANAGEMENT

Extending the enterprise by third parties has allowed companies to focus on core competencies, pursue growth and innovation, improve time to market, and reduce costs. Most organizations agree that outsourcing benefits have outweighed the challenges. However, after the 2008 financial crisis, regulators are holding not only financial institutions but also third party vendors that supply them. Since activities can be outsourced, but responsibilities cannot, the Consumer Finance Protection Bureau (CFPB) and other regulators are holding financial institutions responsible for not only their actions, but also for those of their vendors and suppliers. (Samandari, 2013). There is an increased awareness and emphasis placed on preventive, detection, and mitigation controls as businesses are starting to worry about the liability issues as well as business risks shared with their suppliers and vendors. As a result, more regulations are being proposed to require institutions to properly manage business risks and prevent another financial crisis.

Vendor Risk Management has many benefits that will provide security and efficiencies to businesses. Vendor risk management seeks to assist businesses to reduce risk and increase agility and resiliency—enabling them to pursue growth while also reducing areas of vulnerability (Twerdok, 2013). Businesses will be able to establish appropriate policies, processes, and controls to manage vendor risks. The result of this research encourages organizations to implement and upgrade their VRM technology according to their particular mission/business objectives, goals,

threats, and operational environment. Effective VRM should allow business organizations to minimize the risk of less direct oversight or control and maximize the benefits gained through a well-managed vendor relationship.

NEW REGULATORY ENVIRONMENT FOR VENDOR RISK MANAGEMENT

Vendor Risk Management is no longer an option for businesses as regulations are being proposed to regulate institutions to manage their vendors properly to not repeat 2008 financial crisis. Regulations such as the Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS) and the Health Information Portability and Accountability Act (HIPAA) mandate that risk management policies extend to third-party vendors, outsourcers, contractors and consultants (Vendor, 2011). Institutions started to acknowledge that third parties have the potential to insert risk into their environment and network because they are outside your direct sphere of control.

Updated regulatory expectations focus heavily on board involvement for onboarding and management of suppliers. In July 2009, the US Securities and Exchange Commission, proposed new regulation on requiring public company's board of directors to disclose their role in managing business risks such as credit risk, liquidity risk, and operational risk (SEC, 2013). New regulatory changes focus on appropriate pre-contract due diligence, based on risk, prior to engaging with a significant or customer-facing third party. Specific focus has also been given to understanding expectations and requirements for services with stricter regulatory compliance implications.

In late 2013, Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), and Federal Deposit Insurance Corporation (FDIC) guidance issued guidance on third party

risk management. Most large financial institutions improved their third party risk management capabilities to comply with the new regulations. OCC Bulletin 2013-29 broadened the scope of the financial services institution's risk-management responsibilities to encompass any business relationship between the institution and another entity, including affiliate relationships (OCC, 2013). The FRB's regulatory guidance enforce institutions to treat third party risk management as a formal, enterprise-wide risk discipline, and to follow a process that is commensurate with the level of risk and complexity of the given activity (OCC, 2013). Lastly, FDIC guidance focuses on increased complexity, magnitude, and nature of the arrangement and associated risks. FDIC also provides four basic elements of an effective third-party risk management program: risk assessment, initial and ongoing due diligence in selecting a third party, contract structuring and review, oversight (FDIC, 2013).

IMPORTANCE OF EFFECTIVE VENDOR RISK MANAGEMENT

Vendor Risk Management is no longer an option for businesses as vendors are essential to almost every business. When an enterprise outsources business processes to an external vendor, sensitive data may be transmitted, stored and processed on both company and vendor networks. Recently, vendor risk management have been on news headlines as major credit card and giant retailers have been hit with data breaches caused by their improper vendor risk management programs. During 2012, for example, inadequate vendor management costed American Express, Capital One, and Discover Bank had a total of more than $530 million to settle complaints of deceptive selling and predatory behavior (Samandari, 2013). Inadequate risk management on its vendors caused major data breaches on giant retailers like Target and Home Depot. In December,

2013, Target was attacked by a hacker and 40 million credit and debit cards were stolen and up to 70 million individuals were affected by the additional stolen information through the use of stolen third-party vendor credentials and RAM scraping malware (Fowler, 2015). In September, 2014, Home Depot lost 56 million debit and credit card numbers and 53 million email addresses by hackers who accessed the network through the use of stolen third-party vendor credentials and same RAM scraping malware that was used for Target (Fowler, 2015). A proper vendor risk management program would have potentially prevented the data breach from the start. Specifically, Target's data breach case will be further analyzed in details later in this paper to demonstrate the impact of vendor risk management in preventing such tragedy.

COMPANY PROFILES

Four leading public accounting firms, Deloitte, PwC, EY, and KPMG have now become the major providers of VRM in financial, insurance, brokerage, healthcare, retail and telecommunications industry, leveraging their wide clientele, previous internal audit relationships, advanced technology capabilities, and partnerships with up-to-date software and vendor risk management tools. Even though all of the four firm share the goal of assisting organizations to understand, manage, and monitor potential risks effectively and efficiently, each firm has a unique focus on specific risks that reflect their expertise as well as their forecasts on emerging risks and markets.

Deloitte

Deloitte has become one of the leaders in VRM as it leverages its broad IT services portfolio and as its risk and security capabilities integrated into one risk management practice a few years ago. Deloitte's Third Party Risk Management (TPRM) framework and teams are renowned for their rapid market responsiveness and strong IT capabilities. Deloitte has been most rapid to adapt and respond to changing market conditions among the Big 4 public accounting firms (Heng, 2014). Deloitte's TPRM team constantly seeks to improve its services and close gaps of capabilities through in-house training. Deloitte also has strong partnerships with prestigious organizations such as Kaggle, a data analytics firm, and Singularity University, a Silicon Valley think tank and a business incubator that offers educational programs (Heng, 2014).

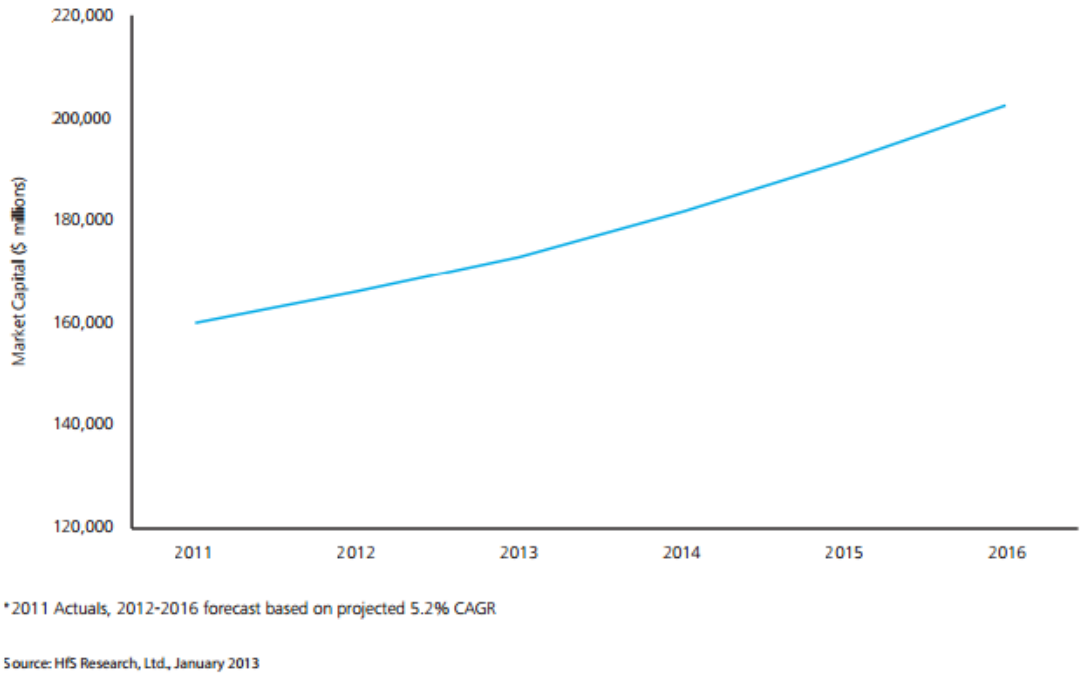

Figure 1. US banking and financial services outsourcing market

The graph above shows how information technology and business services outsourcing in US banking and financial services are expected to increase by more than 25 percent from 2011 to 2016 (Deloitte). While the benefits of using third parties is obvious, Deloitte acknowledges the existence of added risks from outsourcing to third parties. Deloitte believes that even though vendor risk management will differ for each organization, there is a common goal to consistently and effectively evaluate and monitor third-party performance and risk. Deloitte also highlights that multiple business areas should contribute to have a good corporate governance. Effective financial institutions are the ones that extend risk management programs and compliance to their vendors to leverage compliance as an engine for creating competitive advantage and organizational value. Deloitte's third party risk framework focuses on compliance with Office of the Comptroller of the Currency (OCC) and Federal Reserve Board (FRB) guidance.

Deloitte recommends institutions to stop awarding work to third parties based solely on price or financial value. Rather, institutions should evaluate outsourcing decisions based on broader concepts of foundational and emerging risks and decide which areas of the business are "off limits" to outsourcing. Institutions should also be aware of total compliance costs, and assess how they align with compliance risks that could impact your brand or result in costly fines or litigation. Lastly, it is critical for institutions to assign ultimate responsibility in managing, implementing, and overseeing roles to business lines in each third-party engagement, while recognizing that accountability for TPRM resides with the board and senior management.

Deloitte also emphasizes three best practices in third party vendor risk management to institutions. First, Deloitte recommends in investing in real risk-management tools, processes, and skill sets to focus on higher risk relationships or help uncover hidden dangers that pose strategic

risks. Institutions should be aware that third parties may not have the resources to implement risk controls themselves. Second, institutions should rationalize and rank third-party relationships at an aggregate portfolio level, taking into account that different entities carry different types of risks, and then manage them based on how much risk they present to your institution. Third, verify that your internal organization is doing what it needs to do to execute your TPRM processes, while making certain that vendors are performing to expectation. Although it may not be feasible or cost-effective to audit all third-party relationships, some level of formal assessments conducted through internal audit or by independent parties may make sense.

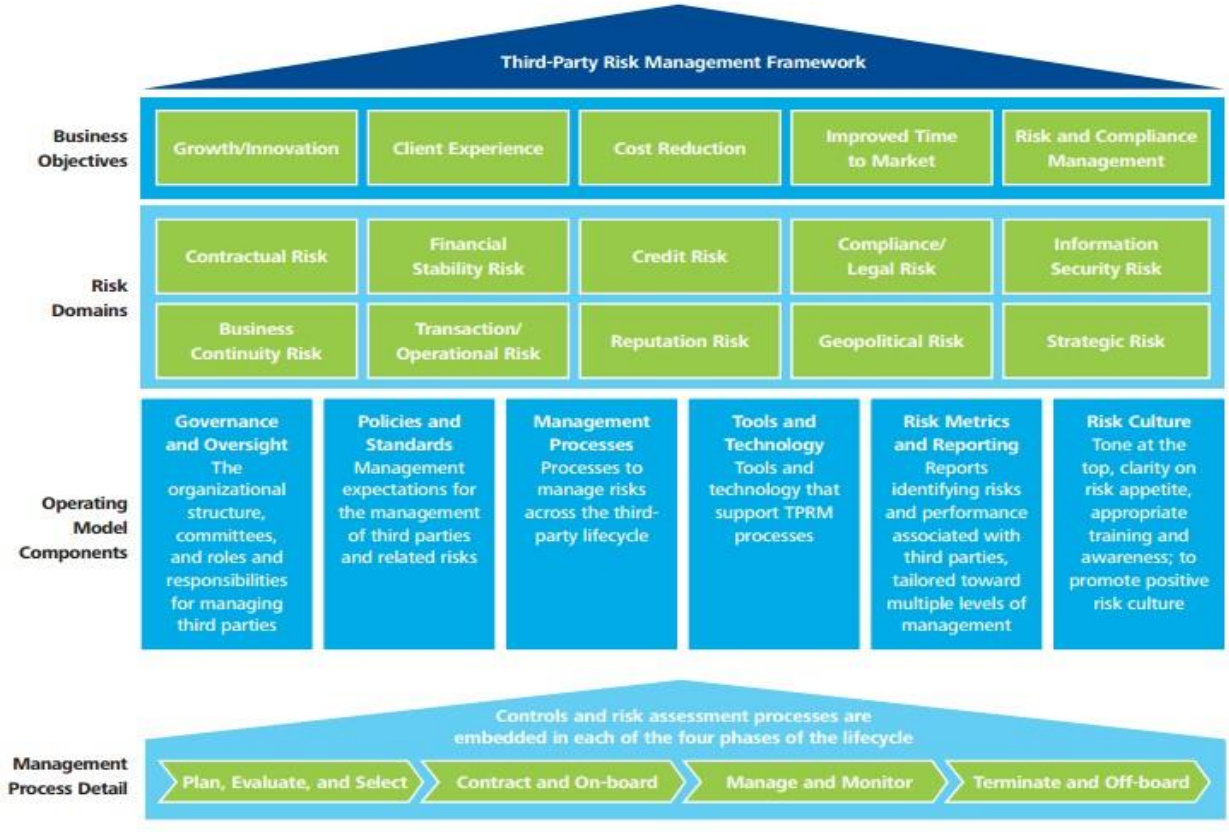

Figure 2. Deloitte's Third-Party Risk Management Framework

PwC

PwC has a Trust but Verify as their main engine for their effective vendor risk management program. PwC acknowledges that IT vendors are a major source of data breaches and highlights insecure third parties as one of the top three threats to an organization. PwC's 2014 survey indicates that disruptive events have become more frequent and their consequences have become even more costly. The Ponemon Institute's survey shows that 41% of the companies experienced a data breach caused by a third party vendor, and the consequent loss of brand value typically ranged from $184 million to more than $330 million (Nocera, 2015). "Financial services respondents ranked assessment of security capabilities of third-party vendors as the top challenge to their information security efforts. Accordingly, more than half said they would increase spending to better monitor third-party security in the coming 12 months. Others are improving third-party cooperation with risk based security frameworks. These guidelines can also help companies more easily exchange information with third-party business partners and suppliers, and communicate expectations and concerns about services that are being provided." (Nocera, 2015).

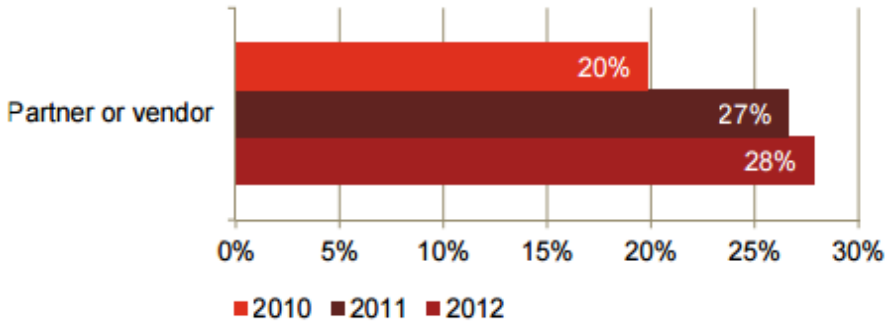

Figure 3. Number of security incidents attributed to vendors

PwC Analysis based on PwC 2011-2013 Global State of Information Security Surveys shows that the number of security incidents attributed to vendors have been constantly increasing.

Along with security incidents, PwC acknowledges various risks on natural disasters, cyberattacks, data breaches, supply chain disruptions as it only takes one or two of these sudden shocks that could stun institutions' vendors and result in unhappy customers and stakeholders. PwC's third party risk management model focuses on assisting its clients to ensure proper assessment to prevent, detect, and mitigate vendor's emerging risks. PwC strongly emphasizes the importance of strong vendor risk management program as any organization in today's business environment is exposed to fiscal, operational, regulatory and reputational risk, just to name a few (Nocera, 2015).

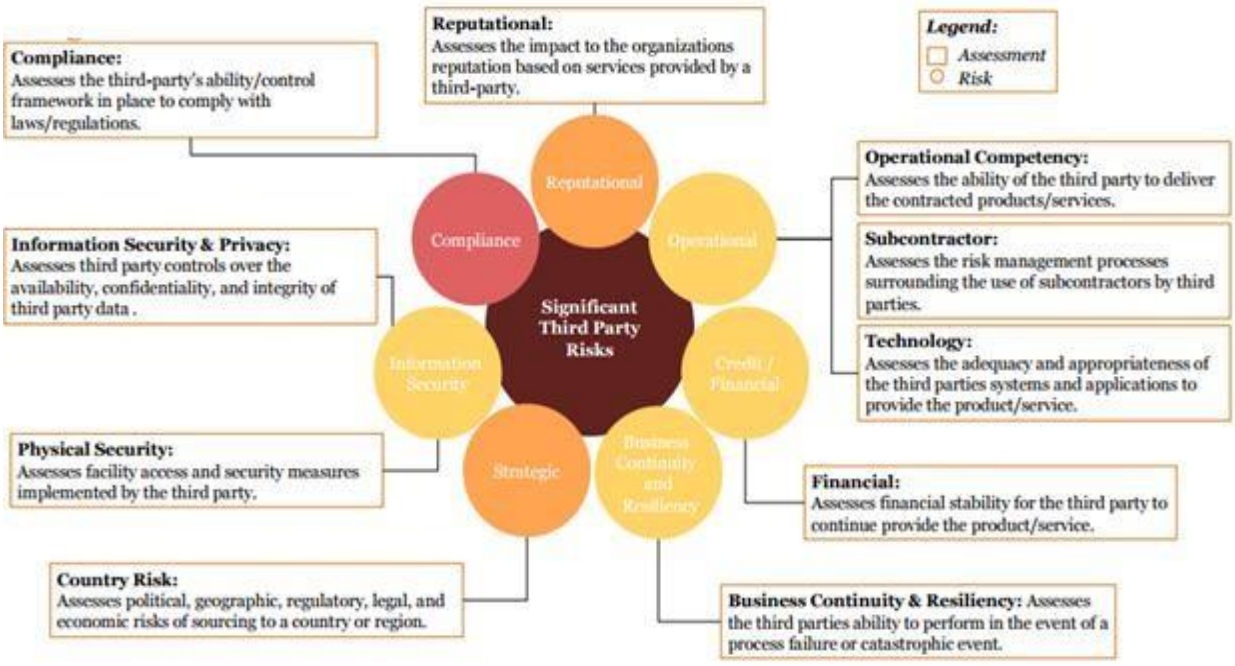

Figure 3. PwC's Third-Party Risk Management Model

EY

EY's Vendor Risk Management (VRM) practice focuses on transforming the risk and control functions by using an integrated "risk transformation" methodology that includes GRC (Governance Risk and Compliance) technology delivery and enterprise GRC technology transformation. EY has been continually building its ecosystem through collaborating with major software vendors (SAP, IBM and Oracle), GRC and security software vendors (such as RSA [The Security Division of EMC], Symantec, Guidewire, Cura Software, BlackLine, Websense, Saviynt, Damballa, SailPoint, McAfee [an Intel company] and Mandiant), and content providers (such as Thomson Reuters and Cloud Security Alliance) (Heng, 2014). EY seeks to leverage its partnerships to provide up-to-date technology services to its clients as cyber security and information technology were the most vulnerable and emerging risks. EY provides tailored problem solving approach for each of its clients to meet their needs and providing a new and practical solution (Heng, 2014).

In addition, EY has integrated its risk assurance, risk transformation and security groups into one risk management practice, reducing duplication of risk resource across the firm and leveraging relevant skills from adjacent practices such as finance. (Heng, 2014). EY has established COEs to develop innovative approaches to integrate risk and performance models. These include its Global Family Business COE, Global Talent Hub and Emerging Markets Committee from which EY's VRM teams benefited in assessing emerging risks within financial industries

EY acknowledges that banks must be compliant with regulations and therefore their vendors must hold the same standards. EY's VRM team assesses compliance of bank, help build

frameworks, and then apply these methodologies to the vendors that support the bank. EY's unique focus on 4th party risks are very critical as most organizations tend to overlook. EY realizes that an organization's vendors might also their own vendors with whom they share proprietary information and require client facing or retail functions, which all bear operational, reputation, and regulatory risk. EY's VRM team therefore assess the shared risks of the vendors and provide proper risk mitigation plan. EY also incorporates internal audit on vendor risk management to test internal controls that will effectively prevent, detect, and mitigate risks. EY's goal is to establish and execute a risk-based program that meets regulatory guidance and reduces the risk of the vendor base.

Figure 4. EY VRM- Risk Universe

KPMG

KPMG's Value Delivery Framework focuses on disciplines related to risk strategy and appetite, risk governance, risk culture, risk assessment and measurement, risk monitoring, and risk reporting, including a focus on data analytics and information technology (Heng, 2014). Through KPMG Capital and KPMG's innovation solutions drive, the firm has invested in and developed new risk solutions. KPMG also developed integrated GRC solutions, cyber information security, risk data and analytics, and regulatory compliance. KPMG clients cited examples of KPMG's pragmatism and practicality in the company's tailored approach to clients' needs. KPMG leverages its global Service Networks and industry-focused COEs to provide risk insight to clients across the globe. Along with other firms, KPMG integrated its accounting advisory, forensics, internal audit, GRC, enterprise RM, regulatory, financial RM and IT advisory service lines into one RM practice, enabling synergy and end-to-end solution delivery under one senior leadership team.

KPMG focuses their vendor risk management program on two main entities, banks and "non-depository consumer financial service companies," that use third-party vendors. KPMG recognizes that banks use third party vendors to outsource internal operations, offer more products and eservices, lend their name and regulated status for a fee (Twerdok, 2013). Whereas nonbanks leverage third-party vendors to make-up for resource constraints, develop additional products or services, and provide expertise that would not be otherwise available internally (Twerdok, 2013).

KPMG also acknowledges that many regulators derive authority to reach out to third-party vendors from the Bank Service Company Act, which states when the third party is performing functions of the bank's internal operations, federal regulators treat these third-party functions as subject to the Act as they are considered as performance of the bank itself. Third-party vendors

should also realize that the Bank Service Company Act may apply directly to them along with the Dodd-Frank Act. In addition, the new Consumer Finance Protection Bureau (CFPB), has also granted the CFPB jurisdiction over "any person that provides a material service to a bank or nonbank in connection with offering or provision by the bank or nonbank of a consumer financial product or service" (Twerdok, 2013). Moreover, the CFPB seeks to supervise financial institutions and hold them responsible for effective risk management on service provider relationship.

KPMG's third VRM focuses on aligning VRM activities with enterprise risk management programs. KPMG's VRM mainly assesses enterprise-level risks inherent in vendor relationships, vendors performing core business processes, vendor health and financial viability, relationship specific risks, and risks associated with client/customer facing activities.

Figure 6. KPMG VRM- Risk Profile

COMPARISON ON RISK PROFILES OF MAJOR VRM PROVIDERS

Each of the firm has VRM risk profile that they leverage as a base for all of their VRM engagements. Their risk profiles share a lot of common VRM risks such as financial, compliance, regulatory, legal, information security, reputational, business continuity, transaction/operational, and credit. However, each of the four firm has unique risks that they specialize in leveraging the firm's expertise and client base. The table I. below is the comparison of risks in four major VRM service providers with two sections: common risks and unique risks. Table II. shows definitions of all of the risks that are listed in Table I.

Table 1. Comparison of risk profiles in four major VRM providers

Service Provider	Common Risks	Unique Risks
Deloitte	Financial Compliance Regulatory Legal Information Security Reputational Business Continuity Transactional/Operational Credit	Geopolitical Strategy
PwC		Strategy Physical Security Country
EY		Country Exit Strategy Cyber Risks Tier 2/3 Suppliers
KPMG		Tier 2/3 Suppliers Green Sustainability Fraud Intellectual Property Rights

Table 2. Risk Definitions

Core Risks	
Financial Risk	Risk that the Vendor cannot continue to operate as a financially viable entity. The potential risk for financial loss due to Vendor failure or non-performance. Also, the risk that our client's involvement with a vendor/service provider may result in a negative financial impact on profitability or results.

Compliance Risk	Risk that our client's involvement with a vendor/service provider may result in a negative impact to the organization's processes, systems and people adversely affecting the ongoing business operations. Contracts, Standards,
Regulatory Risk	Risk that a Vendor fails to comply with a required regulation, thus causing your company to be out of compliance. This is commonly the most complex risk to quantify and assess.
Legal Risk	Risk that the institution is not in compliance with laws, ethical standards, or its own policies, standards, procedures because a third party does not have adequate compliance management processes and controls over its products, services, or systems.
Information Security Risk	Risk of inappropriate disclosure, corruption, or destruction of the institution's information due to a third party's failure to provide appropriate security and privacy controls over the institution's information. Risk to an organization resulting from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction of information and/or information systems..
Reputational Risk	The risk of brand damage to the institution due to a third party's inability to meet the institution's expectations.
Business Continuity Risk	Assesses the risk of Vendor failure on the continuation of business as usual for the organization.
Transactional/Operational Risk	Risk of a financial loss to the institution and/or an adverse impact to the institution's product/service delivery due to inadequacies in a third party's internal processes, people, systems, and/or other third-party issues.
Credit Risk	Risk of a financial loss to the institution that arises when credit exposure is caused by a third party holding, settling, or collecting the institution's funds; or issuing a guarantee to the institution; or creating a liability for the institution that is not adequately managed.
Focus Risks	
Strategic Risk	Risk of inappropriate sourcing decisions by the financial services institution due to a lack of third-party alignment with the institution's business strategies and objectives.
Service Risk	Risk that a Vendor fails to meet your needs as a company from a service delivery perspective. Common metrics include SLAs, scalability and overall performance reviews.
Country Risk	Risk of doing business in a specific country and includes legal/regulatory, geo-political and social-economic considerations.
Physical Security Risk	Risk of failure in managing identities and provisioning access in physical security infrastructure such as physical identity management, role-based access, and back-ups.

Technology Risk	Risk of failure to implement, monitor, and assess risk on technology that might contain intellectual property ,
Contractual Risk	Risk that the institution does not receive products/services in line with expectations due to incomplete or inadequate third-party contract provisions, or a third party's inability to meet contract terms and conditions.
Tier 2/3 Suppliers Risk	Risk that the vendor fails to perform proper vendor risk management on its vendors that are related to the institution. Any information, data, and services shared with the 4th parties are not at risk.
Cybersecurity Risk	Risk that refers to an institutions' vulnerability to potential threats and cyber-attacks from hackers for proprietary information such as credit/debit cards, employee information, login credentials, intellectual property, and any financial information that are now publically available.

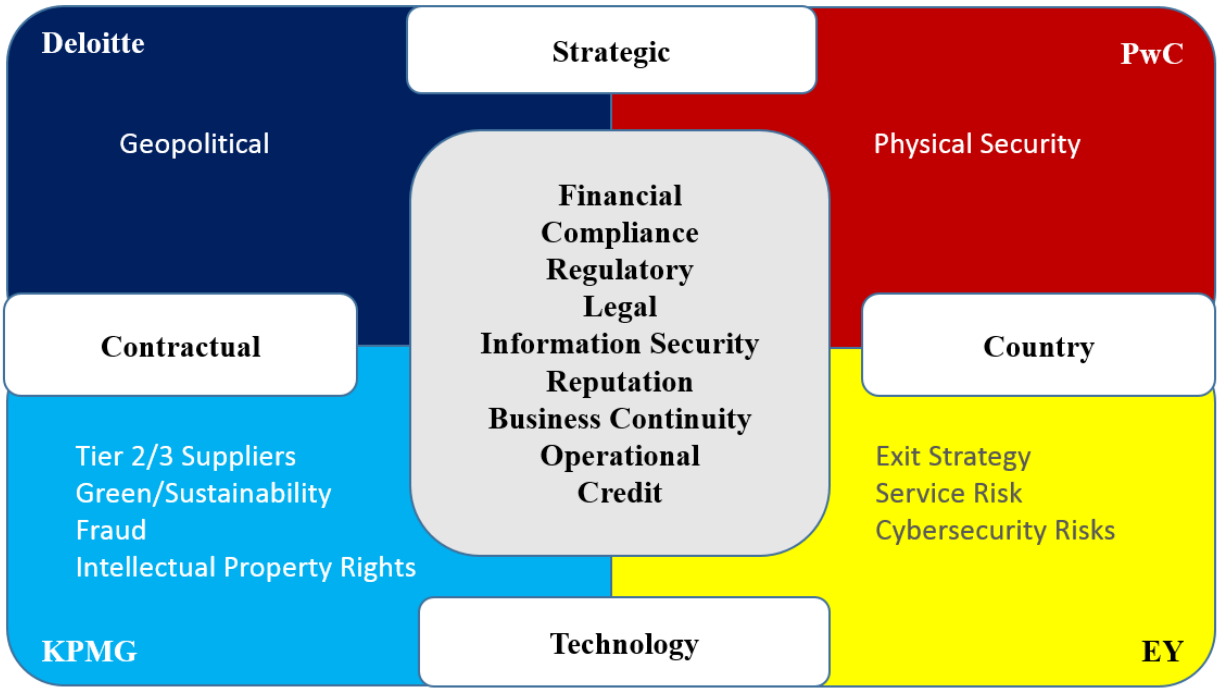

Figure 5. Big 4 VRM Risk Matrix

The diagram above shows the main risk matrix consolidated after studying the Big four major service providers. The risks that are in the light gray box at the center of the matrix are shared core risk services that are prevalent in all of the four service providers. Each firm has

additional risks that are unique to themselves or only shared with one other firm (displayed in the white box). These additional risks provided by each firm represent individual firm's competencies in the market.

Each of the four firms has unique risks that reflects their expertise, emerging risks, and market forecasts. Deloitte puts heavy weight on geopolitical risk on vendor selection process to minimize the risk of disruption to the institution's operations due to economic, social, and political conditions and events in a country that may adversely affect a third party's operations or viability. PwC has concerns on physical security as physical items such as documents, laptops, confidential strategy, business intelligence, and inventories bear risk to businesses. The human factor in physical security is regarded as one of the most important risks to mitigate as human errors are always the top concern as they are more difficult mitigate than computer systems and controls.

EY focuses on service risk to ensure that the engaged vendor provides the promised service that adds value to the parent company in achieving its business objectives. EY also focuses on exit strategy risk to ensure that the business would not suffer a negative impact should the relationship with the vendor need to be exited from and commonly internally controlled via a formal exit strategy. EY's emerging competency in the market is its investment and expertise on cyber risks where EY's VRM team seeks to mitigate and protect their clients vulnerability to potential threats and cyber-attacks from hackers for proprietary information such as credit/debit cards, employee information, login credentials, intellectual property, and any financial information that are not publically available.

Lastly, KPMG focuses on tier 2/3 suppliers to ensure that the vendor performs proper vendor risk management on its own vendors that are connected to the parent institution. Any

information, data, and services shared with the 4th parties are now at risk if not properly identified and mitigated. KPMG also focuses on fraud risk to ensure that the institution has a proper insurance and disaster recovery plan should a fraud occur from its vendors. In addition, KPMG also focuses on protecting its clients' intellectual property rights by ensuring proper vendor selection, periodic vulnerability testing, and risk assessment tailored to each of the main vendors. Moreover, KPMG has Green/Sustainability risk focus to ensure that the vendors are meeting the industry trend of using resources more efficiently, consume less, and reduce any natural harms.

NEW PROPOSED VRM RISK UNIVERSE PROFILE

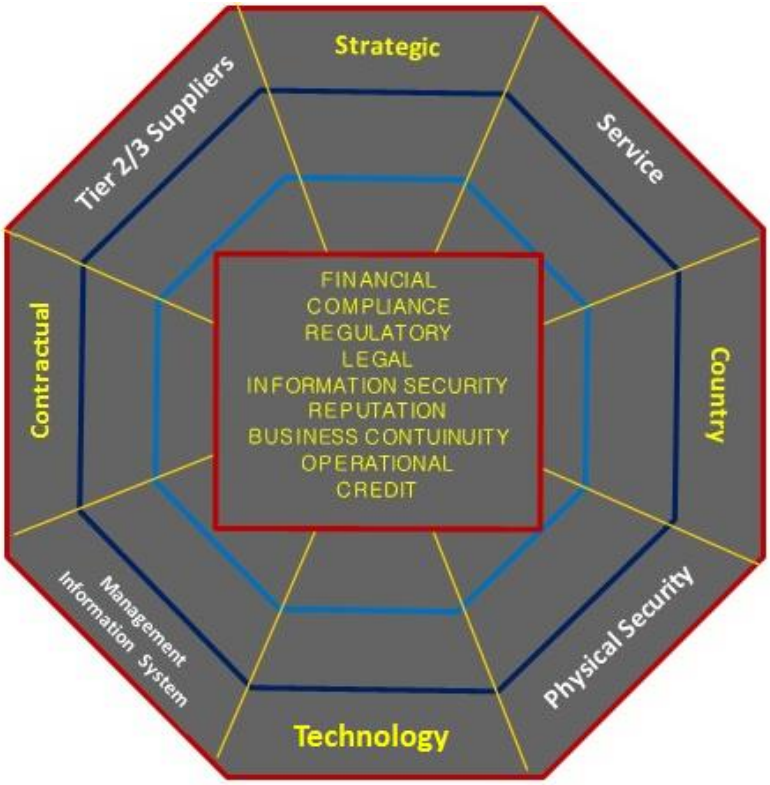

Figure 6. New Proposed VRM Risk Universe Profile

As the risk profiles of the four major service providers have been continuously changing according to market conditions, advanced technology, and emerging business requirements, the new model is proposed to demonstrate the need to update of existing models in order to proactively assist institutions in managing vendor risks. This new model encompasses nine commonly shared risks and eight specific risks from the major risks that are emerging in the financial industry. This model adds value to existing models through not only encompassing the core risks, but also on focus risks that bear higher risks in the market. Service providers can apply this model to assess their client's vendor risks by creating a unique risk profile for each of the major vendors as every business has different functions, needs and risks.

The four risks that are highlighted in yellow on the outer circle represent risks that are shared with two of the four service providers, which have more chances of being included in the risk profile for businesses. Core Risks are financial, compliance, regulatory, legal, information security, reputation, business continuity, operational, and credit. Focus Risks are country, physical security, technology, management information system, contractual, tier 2/3 suppliers, strategic, and service. I believe that the new model accurately represents the industry's emerging risks profile that service providers could leverage to provide better VRM solutions for their clients.

VENDOR RISK MANAGEMENT CASE - TARGET'S DATA BREACH

Target's data breach case is a great example of information security. Information security risk is a risk of inappropriate disclosure, corruption, or destruction of the institution's information due to a third party's failure to provide appropriate security and privacy controls over the institution's information. Risk to an organization resulting from unauthorized access, use, disclosure, disruption,

modification, perusal, inspection, recording or destruction of information and/or information systems.

In 2013, Target was attacked by a hacker and 40 million credit and debit cards were stolen between Nov. 27 and Dec. 15 and up to 70 million individuals were affected by the additional stolen information. Shortly after the initial announcement, Target's profits dropped 46% in the fourth quarter of 2013, compared to the previous year (Krebs, 2014). Target's CEO Gregg Steinhafle had to step down. Target did not have Chief Information Security Officer (CISO) or Chief Security Officer (CSO) who would have been responsible for the organization's information security (Krebs, 2014). An Anti-fraud analyst has commented that "We can't say for sure that all stores were impacted, but we do see customers all over the U.S. that were victimized" (Krebs, 2014). Target data breach could end up totaling $1 billion or more in damages before all is said and done (Seals, 2015).

The attack came through Target's vulnerable POS (Point of Sale) security systems along with inadequate risk assessment of its vendors (Vijayan, 2014). Even though the number of targeted vendors is unknown, it only took one for the access to Target's network. The attackers first gained access to Target's network on Nov 15. 2013 with a username and password stolen from Fazio Mechanical Services, a Sharpsburg, PA- based company that specializes in providing refrigeration and HVAC systems for giant retailers (Vijayan, 2014). Attackers were able to get the login credentials when a phishing email containing Citadel, a variant of the Zeus banking Trojan, was sent to at least one employee. It is assumed that Fazio did not have proper anti-malware protection lacking real-time protection since Citadel malware was common at the time of the breach and major versions of anti-malware were capable of detecting the Citadel (Kassner, 2015). What could have also prevented the access from the attackers is a simple two-factor authentication to contractors who have

internal access to sensitive information. With Fazio's access, the attackers went on to Target's network and injected the Trojan.POSRAM into Target's POS system. The "RAM-scraping" portion of the POS malware stole credit/debit card information from the devices every time when cards were swiped (Kassner, 2015).

Target chose to allow a third party vendor access to its network, but failed to properly secure and manage the risks. Even if Target had a valid reason for Fazio to have access to all stores network, the network access could have been segmented to prevent access to its payment systems (Krebs). Even though Target did not release the exact details on the attack, however it is found that the data breach was preventable in several ways. One of the major ways that has been discussed is the use of effective VRM. Target had a third party vendor, FireEye, which is a computer security firm. Six months earlier of the attack, FireEye installed a $1.6 million malware detection tool, however it was found that no proper assessment configuration or testing was done with Target's monitoring tools that were connected to FireEye (Riley, 2014). Had there been a proper assessment and testing done, Target could have allowed the security system to automatically terminate the threat by running the tool on autopilot.

Due to lack of configuration and proper controls assessment, Target's security team was bombarded with frequent warnings from FireEye, which led them to ignore the alert on the data breach as Target's security team thought of it as just another exaggerated alert (Krawczyk, 2014). Even the Payment Card Industry Data Security Standard, which companies like Target are required to follow, specifies network segmentation as a way to protect sensitive cardholder data (Jaikumar, 2014). It was Target's responsibility to ensure that those practices were followed. The fact that

attackers were apparently able to leverage their third-party access to reach Target's payment systems suggests those practices were improperly implemented.

With a proper VRM plan, Target could have leveraged their security investment to prevent the attack from the start. Target could have configured frequent warnings which were all marked as high severity by segmenting their severity levels to be more detailed and accurate. Target could have segmented their network access with network-connected outsiders. In addition, autopilot and auto termination could have been implemented and monitored which would have stopped the whole initiative attack.

With proper vendor risk management plan implemented and reviewed by external consultants from one of service providers, Target would have received recommendations to review and update of its network access privileges which would have limited or disabled vendor accesses to network. Recommendation would also include implementing POS management tool along with configuration and testing on malware detection tool from FireEye. Lastly, Target would have also been advised to improve monitoring and logging of system security along with update on its firewall rules and policies. Just like most data breaches and vendor fraud issues, a proper vendor risk management would have been able to prevent, detect, and mitigate the Target’s data breach attack from the start.

CONCLUSION

All of the new headlines on data breach cases that have hit 2013 and 2014 on data breaches with major credit card companies and giant retailers are evident that VRM is no longer an option. With stricter regulatory environment with rapidly changing IT environment, proper and proactive

VRM will be critical for businesses to survive in doing their business. “Invest now or pay later this is the message from one of the largest data beaches reported to date” (Prince, 2015). Steve Hultquist, chief evangelist at RedSeal, said in his article that institutions should consider the ROI (return on investment) for investment in proactive security management that could have blocked the breach before it even started (Prince, 2015).

As demonstrated from the Target’s case example, VRM is no longer an option. Rather, VRM is an operational strategic investment, just like outsourcing, that is imperative for institutions to mark as a top priority that might cost them their valuable business if not done correctly. Business organizations in all industries should leverage proactive vendor risk management program to safeguard their business from potential attacks. With proactive review and update on their VRM risk profiles and methodologies, service providers will be able to prevent, detect, and mitigate emerging risks more efficiently.

BIBLIOGRAPHY

Auerbach, J. (2014). Third party risk management. Retrieved December 2, 2015, from http://www.ey.com/Publication/vwLUAssets/ey-third-party-risk- management/$FILE/ey-third-party-risk-management.pdf

Samandari, Hamid. (2013, July). Managing third-party risk in a changing regulatory environment. Retrieved January 15, 2016, from http://www.mckinsey.com/business-functions/risk/our-insights/managing-when-vendor-and-supplier-risk-becomes-your-own

SEC. (2003). Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports; Rel. No. 33-8238. *U.S. Securities and Exchange Commission*. Retrieved February 12, 2016 from http://www.sec.gov/rules/final/33-8238.htm

Siriano, Glenn. (2012, October 29). Vendor risk management – leading practices. Retrieved January 15, 2016, from http://www.continuityinsights.com/sites/continuityinsights.com/files/B7_Siriano_ CINY.pdf

Heng, Jacqueline. (2014, October 7). Magic Quadrant for Global Risk Management Consulting Services. Retrieved Janurary 15th, from http://www.ey.com/Publication/vwLUAssets/EY-magic-quadrant-for-global-risk-management-consulting-services/$FILE/EY-Magic-Quadrant-for-Global-Risk-Management.pdf

Hoogmoed, Walter. (2015, January 8). Managing third-party risk in financial services. Retrieved Jan. 2015, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-third-party-pov-05-010815.pdf.

Fowler, Bree. (2015, July 10). With data breaches, bad news can show up well down the road. Retrieved February 18, 2016 http://bigstory.ap.org/article/5a24a6f6ea634228b8ee326a889298fa/data-breaches-bad-news-can-show-well-down-road

Krawczyk, Konrad. (2014, March 14). Target ignored warnings before hackers stole 70 million credit cards, says new report. Retrieved Feb 21, 2016, from http://www.digitaltrends.com/computing/target-credit-card-theft-warnings-ignored/

Kassner, Michael. (2015, February 2). Anatomy of the Target data breach: Missed opportunities and lessons learned. Retrieved Feb17, 2016 from http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Krebs, Brian. (2014, May 14). The Target Breach, By the Numbers. Retrieved February 12, 2016, from http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

Maynor, John. (2015, Oct 16). Risk Management: IT Vendor Management and Outsourcing. Retrieved January 2016, from http://www.isaca.org/chapters5/Cincinnati/Events/Documents/Past Presentations/2015/IT Vendor Risk Management_October 2015.pdf

Nocera, Joe. (2015). Turnaround and transformation in cybersecurity: Financial services. Retrieved December 13, 2015 from file:///X:/Downloads/pwc-global-state-of-information-security-survey-20.pdf

Prince, Brian. (2015, February 26). Target Data Breach Tally Hits $162 Million in Net Costs Retrieved December 15, 2015 from http://www.securityweek.com/target-data-breach-tally-hits-162-million-net-costs

Protiviti. (2015). 2015 Vendor Risk Management Benchmark Study. Retrieved January 15, from http://www.protiviti.com/en-US/Documents/Surveys/2015-VendorRiskManagement-Benchmark-Study.pdf

Riley, Michael. (2014, March 13). Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. Retrieved Feb 21, 2016, from http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Seals, Tar. (2015, Feb 28). Target Breach Costs Could Total $1Bn, Retrieved February 12, 2016 from http://www.infosecurity-magazine.com/news/target-breach-costs-could-total-1bn/

FDIC. (2013). THIRD-PARTY RISK. Retrieved February 15, 2016 from https://www.fdic.gov/regulations/resources/director/presentations/dallas/2013-Third-Party-Risk.pdf

OCC. (2013, October 30). Third-Party Relationships Retrieved February 15, 2016 from http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Twerdok, M. (2013) Vendor Risk Management in the New Regulatory Environment. Retrieved December 3, 2015, from https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/vendor-risk-management.pdf

Vendor Risk Management (VRM) (2011) Retrieved January 15, 2016 from http://searchcio.techtarget.com/definition/Vendor-risk-management

EY. (2015, December 7). Vendor Risk Management Overview – Microsoft PowerPoint Presentation. Received December 7, 2015 from Andrew Dunheimer

Vijayan, Jaikumar. (2014, Feb 6). Target breach happened because of a basic network segmentation error. Retrieved January 15, 2016, from http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html

Academic Vita of Sang Yeop Lee

EDUCATION

The Pennsylvania State University, University Park **May 2016**

Smeal College of Business, College of Information Science and Technology

- Major: Accounting BS, Integration & Application BS
- Minor: Supply Chain and Information Sciences and Technology, Security Risk Analysis

Schreyer Honors College

RESEARCH

Thesis Title: What is vendor risk management and its future?
Thesis Supervisor: Scott Collins
Honors Advisor: Henock Louis

WORK EXPERIENCE

Ernst & Young. LLP **June 2015 – August 2015**
FSO RAP ITRA Intern New York, NY

- Tested various IT controls for two banking clients in Wall Street for preparation of their SOC 2 report
- Led a team of four in delivering professional presentation to an audience of 100+ ITRA professionals on vendor risk management
- Actively participated in conference calls, walkthrough meetings, audit proposal rehearsals, and engagement team meetings

Beta Alpha Psi - Beta Theta Chapter **January 2015 – May 2015**
Internal Auditor University Park, PA

- Plan and perform internal audit on internal control environment of Smeal College of Business

Penn State ITS Lab Consulting **December 2014 – May 2016**
ITS Lab Consultant University Park, PA

- Deliver level 1 technology support to Penn State students, faculty, and staff in 57 computer lab locations on campus
- Perform troubleshooting and reporting hardware and software issues for computers, scanners, and printers in the labs

SM Accounting Firm **June 2013 – July 2013**
Accounting Intern (Strategic Accounting & Financial Reporting Income Taxes)
Seoul, Korea

- Addressed the strategic accounting and financial reporting challenges facing clients' business and implemented solutions
- Completed firm-wide training on client interaction, presentation, and Duzon accounting software

LionTutors, LLC (Private Tutoring Center) **September 2013 – May 2015**
Marketing Director University Park, PA

- Construct the brand's marketing efforts on campus with creative ideas by analyzing the need and interest of 15,000+ students
- Spearhead a team of four to promote the brand and services by presenting to diversity student organizations on campus
- Lead monthly meetings with the CEO to best assess the students' needs and implement ideas

The Pennsylvania State University **August 2013 – December 2014**
Head Economics Undergraduate Teaching Assistant University Park, PA

- Coordinated undergraduate teaching assistants to best facilitate students' learning environment for 1,100+ students
- Implemented creative ideas on improving class environment, academic integrity, and course issues by consolidating feedback
- Managed assignments, quizzes and exams, and assisted students with any problems on understanding macroeconomic concepts

EXTRACRURICULAR ACTIVITES

Schreyer Consulting Group **September 2013 – January 2016**
Workshop Chair University Park, PA

- Host consulting workshops with professional accounting/consulting firms to demonstrate applications of various models
- Lead workshops on building decks, public speaking, navigating Excel, case interviews and problem -solving frameworks

Wall Street Boot Camp **January 2015 – May 2015**
Participant University Park, PA

- Accepted into an exclusive group of 40 students to participate in weekly sessions presented by Wall Street professionals
- Participate in highly competitive 15-week program to become educated in career paths in financial services in Wall Street
- Develop interviewing, networking and interpersonal skills that are crucial for success in the financial services industry

Smeal Innovation & Quality (IQ) Team **September 2014 – December 2014**
IQ Team Leader University Park, PA

- Identified barriers to learning and exploit them as opportunities to improve 1,300+ students class
- Led biweekly meetings with a professor, teaching assistants, and IQ team to enforce business ethics and sustainability
- Assisted professor with consolidating feedback about the impact of course designs to enhance the learning environment

Students Consulting for Non-profit Organizations **September 2013 – September 2014**
Consultant University Park, PA

- Consulted for a non-profit organization, the Mommy Shoppe, in a team of five with creative solutions and recommendations
- Co-created new inventory management system, mission statement, logo, new hierarchy of board members, and marketing plans

ACHIEVEMENTS

Dean's List: All Semesters
Case Competition: Ascend & Nittany Consulting Group (1st place – Team Leader), Deloitte Consulting (4th place/53 teams), KIVA (3rd place)
Programming Language: SQL (Basic), C++ (Basic), Java (Basic), Python (Basic), Duzon Accounting Software (Basic)
Certifications: Engineer Information Processing and Word Processor 2nd Degree

Language: Fluent in Korean
Award: Recipient of Certificate of Recognition for Outstanding Service for First Year Students