Cybersecurity Strategies and Policies in Managing 3rd Party Vendor Risks:
A case for a quantitative Cybersecurity Scoring and Continuous Monitoring in the Financial Services industry

Abstract: Financial institutions, like in any other industry, use and benefit from engaging 3rd party service providers to achieve efficiency and drive enterprise value. However, hiring 3rd party service providers, some of whom undertake the most critical functions of the institution, come with risks. Third-party risk assessment has mainly relied on Due Diligence. The due diligence process utilizes lengthy and customized questionnaires sent to potential vendors via Request For proposals (RFPs) with the expectation that the potential service supplier will answer accurately and completely. The questionnaires themselves have been designed to capture not only regulators requirements on engaging 3rd party service providers in the financial services, but also follow established cybersecurity control frameworks such as NIST Cybersecurity, ISO 27001/2, SANS Institute Security controls. The institutions then, deploy thousands of employees to analyze vendors' responses for weeks to establish capability and viability of a particular service provider to deliver the expected service. Based on the qualitative answers, subject to the 3rd party's understanding of the ask, organizations decide to onboard a 3rd party service provider. Once the vendor relationship is established, an institution's monitoring effort takes place and continues during the life of the contract or terminate earlier for cause. Vendors' reviews are usually performed once or twice a year yielding limited actionable decisions. Additionally, vendor due diligence and the ongoing oversight are generally a single-point-in time assessment and lagged the actual security posture of an organization. To gain efficiency on service providers due diligence and ongoing oversight, alliances are being created in the financial services. Such alliances as *TruSight* and *KY3P* are providing *Assessment-As-A-Service* to financial organizations. However, 93% of the time spent on vendors' review onsite have been allocated to reviewing the security posture of the service provider (E&Y Vendor Risk, 2018).

This paper makes the case for a quantitative Cybersecurity Scoring and Continuous Monitoring of 3rd party vendors' technology infrastructure in the Financial Services industry. To achieve the goal, financial institutions must leverage not only the newly created alliances within their industry but also thoroughly research the methods and techniques being deployed by the early cybersecurity scoring solutions on the market today. The particularity of the proposed scoring model in this report will be to capture and map the financial regulations into its build, which none of the early adopters in the cybersecurity scoring solutions is currently offering.

Key words: Cyber security frameworks, security risk vector, SSAE 16, SOC 2, ISO 27001/2, NIST Cybersecurity framework, vendor assessment, security rating, security scoring, 3rd party vendor, Service supplier, security controls, vendor lifecycle, financial regulations, OCC, FFIEC, GDPR, 23 NYCYRR500, continuous monitoring, procurement, vendor management program, information systems, internal controls, data breach, weak link, due diligence, CyberScore

Introduction

The Office of the Controller of the Currency (OCC) defines third-party relationship as "any business arrangement between a bank and another entity, by contract or otherwise." Financial institutions outsource many of their daily operations to external parties other than the institutions' external customers or clients.

On a daily basis, many financial organizations rely on third parties to support and provide critical processes, products, programs and technology services. Some larger financial institutions engage more than 8000 vendors. The Ernst & Young (E&Y) *financial services third-party risk management survey 2018*[1] shows that 80% of the organizations surveyed have around 10,000 vendors in their inventory while 15% of the respondents had between 10,000 and 29,999. Some organizations spend on average around $20 billion each year on their third-party engagements with approximately 25,000 active vendor contracts.

But one constant concern has been an institution capability to thoroughly vet a service provider and uncover potential risks before they are actually engaged in a business relationship with the bank. Performing due diligence has been a challenge for many organizations. It is labor intensive, qualitative (i.e. questionnaire-based), subjective, and in the end, the answers at the end of an evaluation might provide an incomplete picture of the vendor's risks.

Data breach statistics have constantly pointed to third party service provider being the biggest conduit for compromised sensitive, personal and corporate information. *Ponemon* Institute's 2018 Data Risk in the Third-Party Ecosystem[2] indicates 59% of organizations' data breach occur through a business relationship i.e. a 3rd party service provider.

To gain efficiency on service providers due diligence process and ongoing oversight, alliances are being created in the financial services. Such alliances as TruSight and KY3P are providing *Assessment-As-A-Service* to financial organizations. Yet, organizations continue to spend tremendous amount of the time on vendor review on-site to assess their security posture or their business continuity plans.

It is my belief that financial institutions can take one more step in vendor due diligence process and oversight to quantitatively assign a cybersecurity score rather than relying exclusively on qualitative assessments. To achieve this goal, financial institutions must learn from the early adopters of security scoring companies such as *SecurityScorecard, BitSight Technologies*, *Prevalent* etc., to create a scoring company that will assess daily and continuously monitor the security posture of any business partners by assigning a security score. This independent Cybersecurity

[1] https://www.ey.com/Publication/vwLUAssets/ey-global-financial-services-third-party-risk-management-survey/%24File/ey-global-financial-services-third-party-risk-management-survey.pdf

[2] Ponemon_Data_Risk_in_the_Third_Party

scoring company will incorporate in its core processes the key regulatory requirements for engaging 3rd party service providers.

Engaging Third Party Service provider and the associated risks

An organization contracts with third parties to provide products and services for a variety of reasons, including: To expand product offerings; To increase efficiency (talents, technology, expertise); To reduce operating expenses; To reach an expanded audience; To gain access to the financial market infrastructure; Drive enterprise value. However, an institution's key priorities are to protect its customers and assets. When an outsourcing decision is made, the organization must consider the benefit gained from engaging a third party compared to the inherent risks. Key risk areas of concern to an institution when engaging a 3rd party:

Information security risk: The institution must identify and evaluates a third party's information security controls to protect the company and its customers

Business continuity risk: The institution must evaluate the vendor ability to recover services and minimize the impact of business disruption on the institution and its customers.

Reputational risk: The institution must evaluate a service provider's potential of negative perceptions that may adversely impact the organization.

Compliance risk: The institution must assess a third party's risk of legal or regulatory sanctions or penalties arising from the failure to comply with applicable laws, rules and regulations.

Operational risk: The institution must assess a vendor's operational performance and controls to ensure third party's ongoing capability to deliver based on the contractual agreement.

Engaging third-party vendors by financial institutions to provide products and services carries many more inherent risks compared to the one listed above. Linda Chapman[3] provided an exhaustive list of the risks that banks expose themselves to when establishing business relationships with third party service providers:

Anti-Corruption/Anti-Bribery; Anti-Money Laundering; Business Continuity Management/ Resilience; Cloud Computing; Company Officers and Corporate Viability; Contract; Financial Viability; Foreign Service Delivery Location; Human Resources; Incentive Compensation; Information and Cybersecurity; Insurance; Model; Performance; Privacy; Physical Security; Records; Reputation; SOX-Reportable Financial Loss; Subcontractor; Technology

Regulatory and Industry expectations

Regulators in the united states and around the world expect banks to apply effective risk management principle regardless of whether an action is performed internally or through a

[3] Linda Tuck Chapman, Third-Party Risk Management: Driving Enterprise Value, 2018, RMA

third-party service provider. Supervisory guidance has been communicated from regulators to banks with respect to engaging and managing third-party relationships, particularly expectations for managing the inherent risks during the lifecycle of the relationships. Following are the key regulatory bodies with specific expectations from banks with respect to their 3rd party vendors engagements.

Office of the Comptroller of the Currency (OCC)	• On October 30, 2013, the OCC issued Bulletin 2013-29 which outlines responsibilities for managing risks that arise from business relationships with third parties. • The bulletin requires third parties to be managed to the same or greater risk standards as if the company were conducting the activities directly.
Consumer Financial Protection Bureau (CFCB)	• On April 12, 2012, CFPB issued guidance on managing the risks associated with service providers focusing on prevention of consumer harm.
Federal Reserve Board (FRB)	• On December 5,2013, the FRB issued guidance on managing outsourcing risk.
Federal Financial Institutions Examinations Council (FFIEC)	• The FFIEC, a U.S. government interagency body that includes five banking regulators – the FRB Board of Governors, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the OCC, and the CFPB – is empowered to prescribe additional guidance on third parties.
Federal Deposit Insurance Corporation (FDIC)	• On June 21,2006, the FDIC issued FIL-52-2006 guidance to address the risks inherent in outsourcing relationships between U.S. financial institutions and foreign-based third - party service providers. Instructions that transfer internal processes or data to third-party service providers have the same risk management, security, privacy, and others consumer protection responsibilities that they would have if they were conducting the activities themselves.
International Regulators	• International regulators have established requirements for outsourcing that may be materially different from U.S. laws and regulations. • European General Data Protection Regulation (GDPR) has been enacted in May 2018, which demand stringent expectations of privacy from organizations doing business with EU citizens

Industry PCI DSS	• PCI DSS since august 2014 issues the PCI Data Security Standards, Third party Security Assurance[4]
New York 23 NYCRR 500	• 23 NYCRR 500 (New York's Cybersecurity Regulation) has specific provisions 3rd party[5]

Third-Party Vendor Life Cycle

The following discussion reviews the vendor life cycle or lifecycle management. It describes stages an organization goes through in managing its service suppliers and the activities performed within each of those steps.

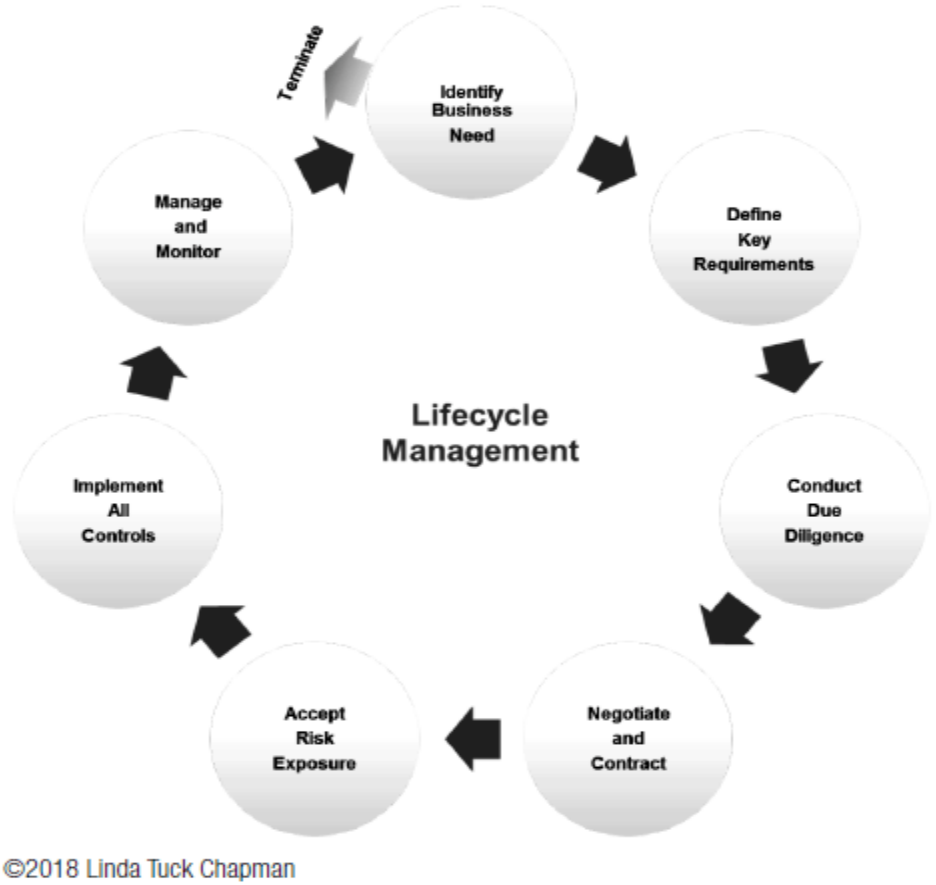

Fig.1: 3rd Party Vendor Lifecycle

[4] PCI_DSS_V3.0_Third_Party_Security_Assu

[5] https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

Identify business needs

Engaging a 3rd party service provider starts with an enterprise business unit identifying a business need for the organization. It can be a material change in the existing process. It might also be a that the competitive market has changed or it's a brilliant idea for a new product. The business unit comes to the realization that the organization's needs cannot be efficiently and cost effectively fulfilled with enterprise resources.

Define Requirements

The business unit puts together complete and detailed requirements for the need that a potential service provider will address if engaged by the organization. This is a difficult task as many requirements or assumption might not be known. The requirements must explicitly explain how a potential supplier will provide a service, what systems and data it will have access to, where access to company data and systems are allowed, the classification and categorization of the enterprise data and systems. The Business unit must also identify and map specific laws, rules and regulation covering the activities that a service provider will eventually fulfill.

Due diligence

Vendors and business partners selection must be based on due diligence. The nature of the due diligence must be proportionate to the criticality of the service expected from the vendor in relationship to the organization and the inherent risks associated with the activity. Obviously, all risks are not identifiable. There will always be residual risk associated with due diligence. Ultimately, the goal of due diligence is to assess and determine the service supplier's capabilities to not only perform the task comfortably, but also uncover the materiality of risks brought into the corporate environment by engaging in a 3rd party relationship. Regulatory bodies such as FFIEC[6] explicitly define their requirements for banks when performing due diligence.

- Existence and corporate history;
- Qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate;
- Other companies using similar services from the provider that may be contacted for reference;
- Financial status, including reviews of audited financial statements;
- Strategy and reputation;
- Service delivery capability, status, and effectiveness;
- Technology and systems architecture;
- Internal controls environment, security history, and audit coverage;
- Legal and regulatory compliance including any complaints, litigation, or regulatory actions;

[6] https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/service-provider-selection/due-diligence.aspx

- Reliance on and success in dealing with third party service providers;
- Insurance coverage; and
- Ability to meet disaster recovery and business continuity requirements.

The due diligence is generally performed using lengthy questionnaire to potential vendors via a request for proposal (RFP) per regulation requirements (FFIEC). Linda Tuck Chapman notes that some third parties are pushing back on questionnaires. Some will not respond to RFPs unless they strongly believe they will win the business. Others charge their clients for responding to due diligence questionnaires. Others send standardized responses, ignoring the actual questions. This makes it harder for financial institutions to evaluate responses and eliminates the possibility of automating any part of the evaluation processes. Also, the complexity and length of the questionnaire make it extremely difficult for many banks to get accurate and useful answers from vendors. As a result, some banks simply subscribe to external program such as the Shared Assessment Standardized Information Gathering questionnaire[7] or to the SANS Institute Top 20 Critical Security Controls[8] or the NIST (National Institute of Standards and Technology) framework for improving Infrastructure Cybersecurity[9] for due diligence questionnaire. Combining these 3 sources can easily leads to thousands of questions that a single vendor must answer. BitSight Technology[10], a security rating organization put together 40 critical questions that specifically deal with the cybersecurity posture of any vendor. These questions include Governance and Organizational Structure as well as those related to Security Controls and Technology. Once the questionnaire responses are received, the bank must review, assess and evaluate the answers.

Another aspect of due diligence includes site visits on vendors premises where on-site interviews, penetration tests, and a review of the vendor's security documentation. Vendors references are also verified and validated before their selection.

Finally, when satisfied, at least on paper, the bank decides to contract with the selected vendor. Note that an alternative to Vendor Assessment would be for a financial institution to perform an Audit of the potential vendor[11] and review the SSAE 16 (or SOC 1) and SOC 2 reports if time and cost are not an issue for the institution.

[7] https://sharedassessments.org/2019-shared-assessments-third-party-risk-management-toolkit/
[8] https://www.sans.org/course/critical-security-controls-planning-implementing-auditing
[9] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

BitSight - 40 Security Questions.p

[10]

[11] Ideally, the bank can engage an audit firm to evaluate the vendor and produce an SSAE 16/SOC 1 report and SOC 2 report. SSAE 16/SOC 1 report focuses on internal controls over financial reporting. SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system. Not only the audit process is time-consuming, it is also quite expensive. SSAE 16: The Statement on Standards for Attestation Engagements No. 16, SOC: Service Organization Controls

Contract Negotiation

Once due diligence is completed and a vendor is selected, the scope and quality of services, and any appropriate risk controls must be documented in the contract. The contract must clearly delineate the responsibilities of the vendor towards the bank as well as the bank's expectations from the vendor. The contract between the vendor and the bank is a legally binding document that must be signed by all parties with a clear understanding of the provisions in spirit and intent.

Risk Acceptance

After the contract negotiation is completed, terms and conditions have been reviewed, the type and nature of risks the business unit is bringing into the organization reviewed, the parties' acceptance must be documented.

Implement Controls

After acceptance of the risks by the financial organization, any necessary controls needed or required by the client (the bank) must be implemented before the service supplier is officially on-boarded. Site visits reports, penetration testing and other reviews of the vendor will guide whether additional controls might be needed.

Monitoring

Engaging with a service provider is the beginning of the vendor relationship. The biggest challenges are ensuring the expectations that led to the hiring of a service provider are met. Are the vendors complying with regulatory requirements as expected of them? Is the quality of service meeting or exceeding management's expectations and conform with internal operating standards? The office of the Controller of the Currency (OCC) expects a *comprehensive* monitoring of third party, particularly when the 3rd party is a critical service provider.

That includes[12]:

- *business strategy (including acquisitions, divestitures, joint ventures) and reputation (including litigation) that may pose conflicting interests and impact its ability to meet contractual obligations and service-level agreements.*
- *compliance with legal and regulatory requirements.*
- *financial condition.*
- *insurance coverage.*
- *key personnel and ability to retain essential knowledge in support of the activities.*

[12] OCC, Third-Party Relationships, Ongoing Monitoring

- *ability to effectively manage risk by identifying and addressing issues before they are cited in audit reports.*
- *process for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches or other serious incidents.*
- *information technology used or the management of information systems.*
- *ability to respond to and recover from service disruptions or degradations and meet business resilience expectations.*
- *reliance on, exposure to, or performance of subcontractors; location of subcontractors; and the ongoing monitoring and control testing of subcontractors.*
- *agreements with other entities that may pose a conflict of interest or introduce reputation, operational, or other risks to the bank.*
- *ability to maintain the confidentiality and integrity of the bank's information and systems.*
- *volume, nature, and trends of consumer complaints, in particular those that indicate compliance or risk management problems.*
- *ability to appropriately remediate customer complaints*

For its part, FFIEC specifies the scope of monitoring a service provider to include:

- *Key service level agreements (SLAs) and contract provisions;*
- *Financial condition of the service provider;*
- *General control environment of the service provider through the receipt and review of audit reports and other internal control reviews; and*
- *Potential changes due to external environment.*

In addition, FFIEC specifies the scope of vendor monitoring for technology service providers (TSP) as follow in *Appendix J*[13]:

Management should effectively monitor TSP performance throughout the life of the contract. In doing so, it assists the financial institution in ensuring the resilience of outsourced technology services. A bank should perform periodic in-depth assessments of the TSP's control environment, including Business Continuity Plan (BCP), through the review of service provider business continuity plan testing activities. The bank should also review in-depth independent and/or third-party assessments[14], and management information systems (MIS) reports[15] to assess the potential impact on the financial institution's business resilience. The financial institution should ensure that results of such reviews are documented and reported by the TSP to the appropriate management oversight committee or the board of directors and used to determine any necessary changes to the financial institution's BCP and, if warranted, the service provider contract.

[13] Appendix J: Strengthening the Resilience of Outsourced Technology Services

[14] This includes internal and outsourced audit reports, reports issued by regulatory agencies, and other independent assessments, such as consulting reports, penetration tests, and vulnerability assessments

[15] MIS reports include, for example, compliance with SLAs, TSP risk mitigation capabilities, or mediation timeframes

Termination

With any relationship, there are times when the relationship comes to an end for various reasons: The service provider is not meeting the expectations specified the contract; the vendor is not meeting the service level agreement (SLA); material security breach occurred via the third party; There is a shift in the banks prioritized products and services offerings that do not need the vendor's service anymore; the contract has expired, etc.

When an existing service contract must be renewed with a service provider, the institution must incorporate lessons learned from the current monitoring experience into the new due diligence cycle.

Current questionnaire-based assessments by banks

Figure 2 below illustrate how, currently banks, red ball, interact with service suppliers, blue balls.

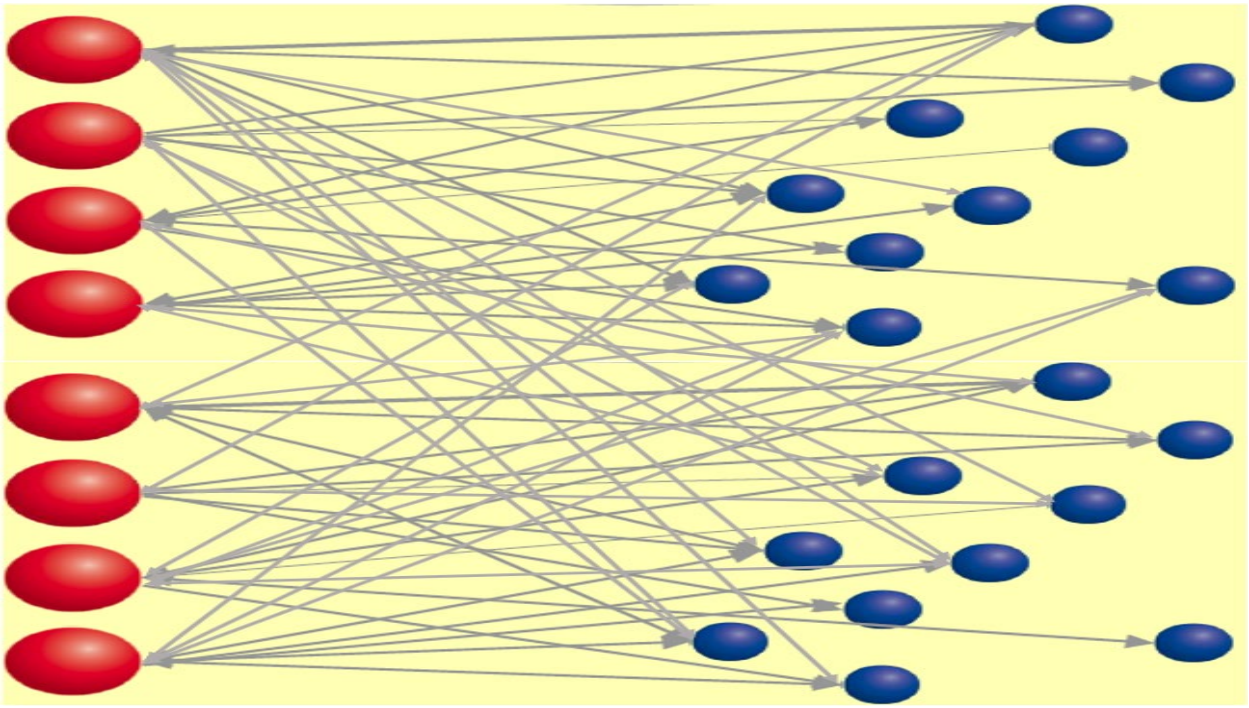

Fig. 2: current Model of Vendor assessment with questionnaires

In this model, any bank engages in a one to many relationships with service providers by issuing request for proposals (RFP) for a particular service the bank has a need for. Banks issue questionnaires to potential service suppliers. The number of questions in the questionnaire is also at the discretion of each bank. Given the elevated expectations from regulators (OCC, FFIEC, FRB) and professional organization in the industry (PCI DSS), the questionnaires will generally take into account the requirements from those regulators. In addition, banks questionnaires cover several

security controls frameworks as listed in Table 1 below to compose their security controls questions.

Organizations	Description
NIST	NIST Cybersecurity Framework[16]
ISO	ISO 27000/207001/27002 Information technology Security techniques[17]
SANS	SANS Top 20 security Controls[18]

Table 1: Cybersecurity frameworks in vendor questionnaires

Banks also do create proprietary questionnaires of their own. Finally, banks have started using standardized questionnaires such as those composed by the Santa Fe Group Shared Assessment program i.e. Standard Information Gathering questionnaire (SIG).

Vendors Assessment challenges

As one can imagine, for a global bank with more than 10,000 service providers, with this level of customization and number of questions, it is overwhelming for potential suppliers to respond accurately and completely. It is also a daunting task for banks to collect and thoroughly analyze the answers to these questions. In the end, the vetting process that is so critical to onboarding new vendors is not quite reliable. In addition, vendors monitoring which is an ongoing activity for the life of the relationship is challenging. Even with one or two assessments on a yearly basis, the amount of labor and time involved in performing vendor due diligence and monitoring over the life of the relationship is enormous.

On-site visits

To complete the due diligence assessment and monitoring effort, banks oftentimes send their own resources on the ground (on-site) to visit the service provider to perform additional reviews. These efforts generally cover such topics as Information security, business continuity, compliance and operational risk. The E&Y 2018 Global Financial Services Third Party Risk management survey[19] reveals that 93% of the duration of the on-site visits is allocated to conduct review of the vendor's information security or allocated to review the vendor's business continuity posture (87%). Clearly, this E&Y survey reveals that enormous amount of time is allocated to review the cybersecurity

[16] https://www.nist.gov/cyberframework
[17] https://www.iso.org/isoiec-27001-information-security.html
[18] https://www.sans.org/course/critical-security-controls-planning-implementing-auditing
[19] ey-global-financial-services-third-party-

posture and the cyber resilience of vendors during on-site visits. How can financial institutions improve vendors' assessment process?

Current Assessment efforts in Banking

As we discussed earlier in this paper, assessing potential 3rd party supplier is a difficult and painfully time-consuming task. To address this issue, some banks have taken steps to form alliances in order address the vendor assessment challenges. Two groups of banks have formed alliances. Barclays, Goldman Sachs, Morgan Stanley HSBC (Group 1) and Bank of America, Wells Fargo, BNY Mellon and American Express (Group 2) to form two assessments companies respectively *IHS Markit – Know Your Third Party (KY3P)* and *TruSight*. The ultimate goal is to remove the burden of performing vendor assessments within individual banks. Instead, all potential vendors must now be assessed through questionnaire either via KY3P or TruSight. If a bank needs to perform any due diligence or monitor a vendor, the bank then contacts either KY3P or TruSight for such need for fee. Clearly, Assessment-As-A-Service is what these new organizations KY3P or TruSight are offering.

Figure 3: Banking Alliances Assessment Companies: *KY3P* and *TruSight*

These alliances are great and need to be encouraged in the financial industry. However, as we have described earlier, an assessment-as-a-service is still a single-point-in-time assessment. In general bank can only perform 1 or 2 assessments per year. Single-point-in-time assessments are no longer sufficient to effectively monitor service providers, particularly their security controls.

Banks must now quit relying exclusively on qualitative security controls assessments based on questionnaires or reviewing documentation related to penetration tests of their third-party vendors. When it comes to cybersecurity, nothing is static. Even with a very positive SOC 2 report on the cybersecurity posture of an organization, the time lag between 2 assessments in the current model is a longtime for that positive SOC 2 report to stay static. When E&Y reports in their 2018[20]

[20] ey-global-financial-services-third-party-

Risk survey that 93% of the time spent on a vendor on-site review is allocated to reviewing the information security of vendors, it is a reminder that organizations need to find a better approach to monitor the cybersecurity stance of 3rd party service suppliers. The banking industry must now move to a cybersecurity scoring model, a quantitative model, to assess its vendors' cybersecurity and continuously monitor those vendors' security controls resilience.

Towards an independent Cybersecurity Scoring organization for Financial Institutions

The scenario will look similar to the model below in Fig. 4. Banks (Red balls) will interact with the independent security scoring company to request the security score of any vendor they intend to hire. Similarly, any service provider (blue balls) that intends to provide service to banks must be evaluated and continuously be monitored by an independent scoring company.

Fig. 4: Independent Cybersecurity Rating company for financial Services Suppliers.

The independent security scoring organization in the financial industry can well emerge from merging KY3P and TruSight created by the 9 banks discussed earlier (Barclays, Goldman Sachs, Morgan Stanley, HSBC, Bank of America, Wells Fargo, BNY Mellon, American Express). Any financial organization will then connect directly with the independent scoring company for their new and existing vendors due diligence as well as their daily monitoring and scoring needs. Any potential service supplier to financial institutions must now be under the independent scoring company's radar. With the independent scoring company monitoring and running the daily security score of vendors, there will be limited needs for banks to send valuable resources to perform on-site visits. The banks that created KY3P and TruSight are among the largest financial institutions[21] in the U.S. and abroad with combined assets higher than $9 trillion. These banks can agree and set the tone

[21] https://www.bankrate.com/banking/americas-top-10-biggest-banks/#slide=1

of best practices in the financial industry as a whole. Creating a Cybersecurity scoring company for financial institutions is a technically difficult task but not impossible. Banks can be inspired by the early adopters in the cybersecurity scoring business.

Early adopters in security scoring

Startups are seizing on the opportunity to provide cybersecurity risk rating solutions in a variety of industries. Some, such as *Bitsight Technolgies, SecurityScorecard, RiskRecon* and *Prevalent*, have positioned themselves as leaders in this new market as provided by *The Forrester* research below.

Fig. 5: Security Risk Rating Solutions[22]

Analyzing the case of BitSight technologies, the company uses a data-driven, outside-in approach on the rated entity, without any intrusive testing on the organization. Security Ratings are generated through the analysis of externally observable data across a variety of risk categories mapped to an organization's known networks. BitSight's Security Ratings continuously measure

[22] The Forrester New Wave™_ Cybersecuri

security performance on a scale of 250 – 900, with higher ratings indicating better security performance. The rating company scans publicly available information on the technology infrastructure of a given vendor. Next, it stores the collected information in a Collection Manager as shown in Fig. 6 below.

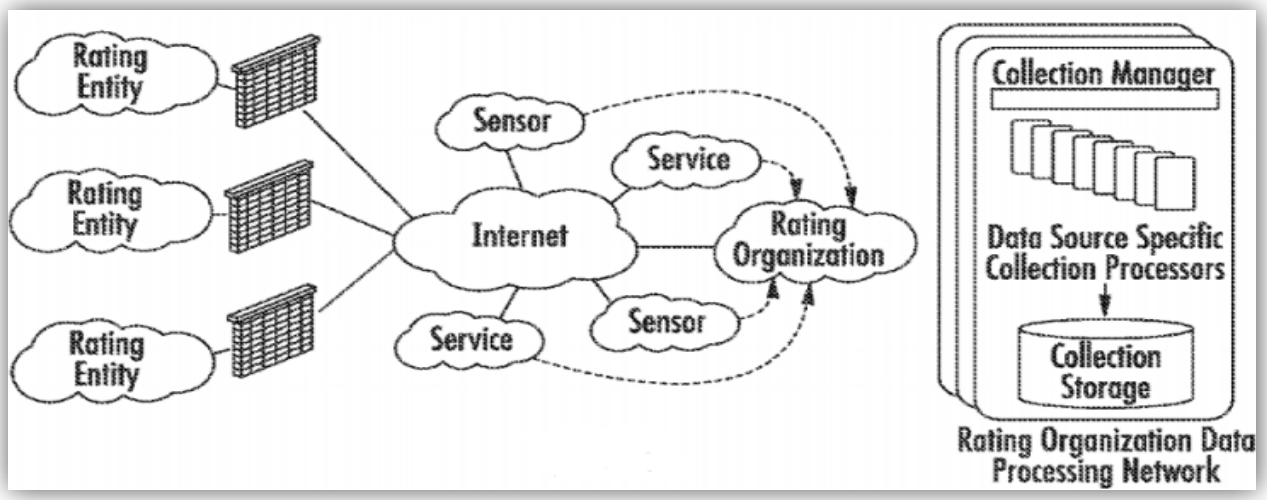

Fig. 6: BitSight's Rating Entity Information collection process[23]

To identify the rating entities, BitSight performs entity IP address mapping, by taking advantage of the Regional Internet Registries' (RIR) databases. The five RIRs used include: ARIN for North America, AfriNIC for Africa, APNIC for Asia Pacific, RIPE for Europe, Middle East, Central Asia, and LACNIC for Latin America. For IP addresses allocated to Internet Service Providers (ISPs) not captured in the 5 RIRs databases, BitSight uses a "dig" tool to collect addresses published by an entity. As of 2016, year of their patent Application, BitSight had 97 data sources identified, 82 of which have an automated data collection process. This automation helps in achieving the goal of continuous monitoring and scoring of vendors' computer systems. Key data source types include[24]:

Breach Disclosures	Spam Activity
Block Lists	Vulnerable Hosts
Configuration Parameters	Spyware
Compromised Hosts	Whitelists
Malicious Activity	Email viruses
Malware Servers	Multi-type
Reputation	Phishing
Suspicious Activity	User Behavior

[23] BitsSight, Patent Application US 20160205126A1

US20160205126A1
-BitSight Patent App

[24] ibid

Some of the collected data i.e. risk vectors that currently impact BitSight rating calculation includes the elements below:

Compromized Systems	Diligence
Botnet Infections	Open Ports
Potentially Exploited	TLS/SSL Certificates
Unsolicited Communications	TLS/SSL Configuration
Spam Propagation	Web Application Headers
Malware Servers	Sender Policy Framework (SPF)
	DomainKeys Identified Mail (DKIM)
	Patching Cadence
	Server Software
	Desktop and Mobile Software
	Insecure Systems

Fig. 7: Some risk vectors impacting rating at BitSight[25]

Computation of a CyberScore:

When the data collection completes, BitSight then, applies its proprietary scoring algorithm on the collected data to calculate the Total CyberScore (CS_{Total}).

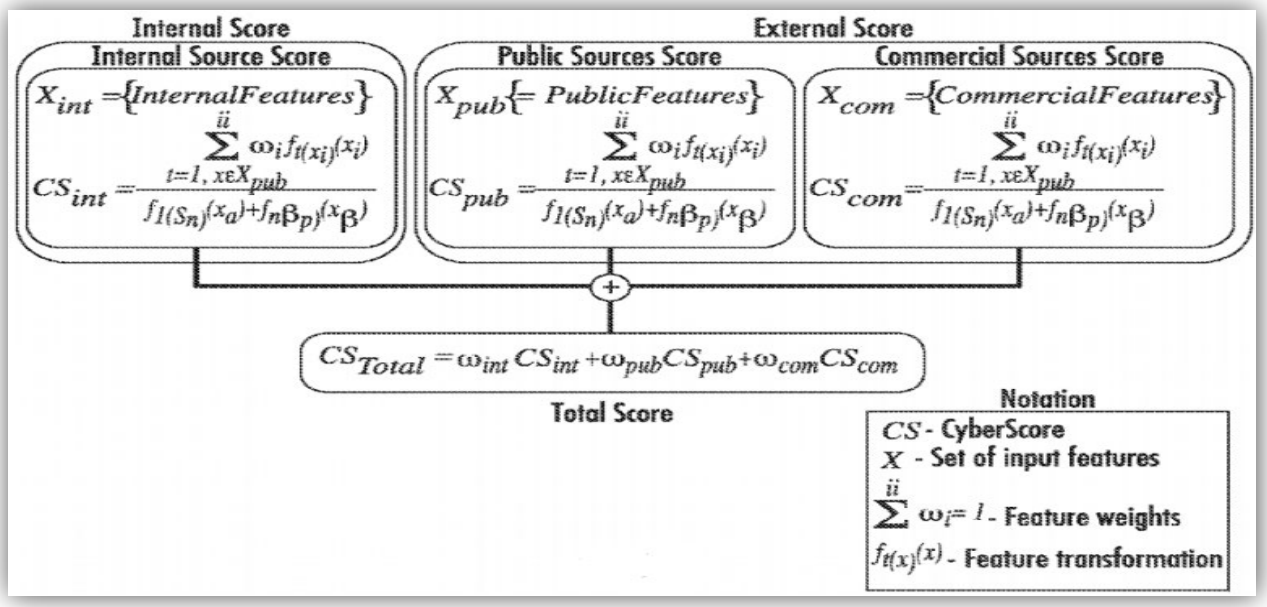

Fig. 8: BitSight's CyberScore computation model[26]

[25] https://www.bitsight.com/data
[26] BitsSight, Patent Application US 20160205126A1

US20160205126A1
-BitSight Patent Apr

The CS_{Total} has 3 components: The *internal source score* (CS_{int}), the *public sources score* (CS_{pub}) and the *commercial sources score* (CS_{com}). The *X*s in the formula represent the security features collected and stored in the Collection Manager discussed above. Each security feature has a weight that represents the degree to which it contributes in explaining the *source score* to which it belongs. Finally, each security feature has a transformation function that helps in the summation the computed scores.

BitSight explains that the *externally observable characteristics may be evidence of internal security controls or outcomes or operational execution of security measures of the third-party computer system.* Therefore, it is important to note that the internal security features in the computation are derived and includes such features as *Vulnerability scans; Firewall Rules; Incident Reports; Configurations; Software inventory; Policies; Controls; User Behavior*.

CyberScore implication

As one can expect, a lower security rating for a service supplier implies a higher probability of a client data breach through such a service provider. As shown in Fig. 10 below, a third-party vendor with a CyberScore less than 400 points has a 500% chance of being the vehicle by which its client data gets breached. BitSight Security score ranges from 250 to 900.

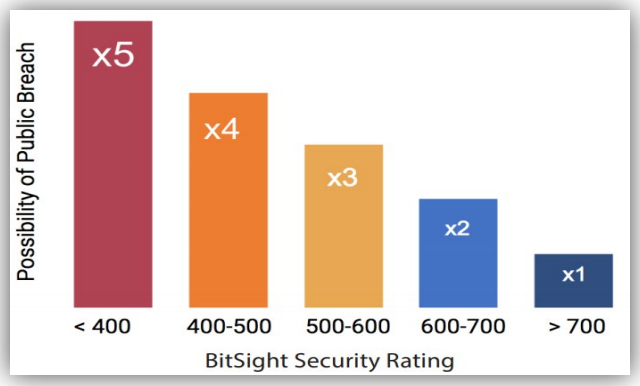

Fig. 10: BitSight Security Ratings correlates to Data breaches[27]

[27] https://www.bitsight.io/hubfs/Datasheets/BitSight_Security_Ratings_Correlate_to_Breaches.pdf

The need for a Cybersecurity Scoring model for Financial services.

It is central to note that currently, none of the new security scoring companies covers exclusively the financial services industry. In other words, none of these scoring organizations takes into considerations in their processes, the requirements of the multitude of regulatory bodies in the financial industry discussed on pages 4-5. As of the writing of this paper, *The Forrester* research indicated that only *Panorays* covers the requirements for NIST, GDPR and PCI/DSS in its processes, hence the need for a scoring organization that does address the regulations in the financial industry in its building blocks. The new independent scoring company must thoroughly research the methods and techniques discussed in this paper that BitSight is deploying, to collect key cyber security risk vectors available about the technology infrastructure of potential vendors, develop a proprietary algorithm and quantitively assign a cybersecurity score to potential service providers.

Conclusion

In closing, the questionnaire-based assessments of vendors' cybersecurity posture have proven to be inefficient and ineffective. This single-point-in-time approach, including the SOC 2 report, does not capture fully and continuously the cybersecurity risks of vendors. Given the dynamic nature of cybersecurity, and financial institutions being one of the prime targets for attackers, banks must find a smarter and quantitative approach to evaluate in real-time the security posture of thousands of service providers they hire. Such approach must incorporate in its build process, all the requirements from the regulatory bodies in the financial industry. Attackers are likely to use compromised systems of service suppliers, the weak links, to gain access to financial institutions' networks. With a scoring company in place, compromised systems of a service supplier are likely to be reflected in the supplier security scoring. Such compromised service provider will eventually not be on-boarded by any bank in the first place. As discussed in this report, some banks have already performed the ground work by creating alliances. One more step is to move to the security scoring model. To do so, banks must take a thorough look at the current scoring models produced by companies such as Bitsight to build their own structure that is targeted to financials organizations and incorporates all the financial regulatory expectations. As a reminder, Gartner Inc. predicts that by *"By 2022, cybersecurity ratings will become as important as credit ratings when assessing the risk of business relationships"*[28].

[28] Innovation Insight for Security Rating Services, Gartner, July 27, 2018 [Sam Olyaei, Christopher Ambrose, Jeffrey Wheatman]