Bloomberg BNA

BNA's Banking Report™

Cybersecurity

Basel III and the Dodd-Frank Act require certain financial institutions to develop, implement and maintain enhanced data information technology to accurately assess and aggregate a variety of potential financial, legal and other operational risks. As such, bank regulatory counsel should be aware that the choice between two commonly used approaches to the external indexing and querying necessary for such risk aggregation – data warehousing and federated data access – might well prove to be a key component of the enterprise's ongoing efforts to implement the required type of ''reasonable'' data security and cybersecurity protection.

BNA INSIGHTS: Basel III Cybersecurity Requirements for Data Storage

BY RICHARD A. BLUNK AND ERIC W. ARMSTRONG

The recent global financial crisis has led to the recognition that major financial institutions — both domestic and international — need to better understand and inform their management and directors about the enterprise's aggregate risk exposure. Emphasis on key features — including the development of appropriate corporate governance, infrastructure, reasonable cybersecurity, the ability to provide management and regulators with accurate, timely and useful reports and overall supervisory review – serve as the foundation upon which the Bank of International Settlements (BIS) implements Basel III.[1] The Federal Reserve has followed suit in mandating enterprise risk management programs that provide similar required identification, assessment, quantification and aggregation of key organization-wide risk.[2]

Since the majority of international financial transactions are consummated through BIS, ''globally significant'' U.S. banks that participate in this type of transaction will be subject to these Basel III directives. Among them is the requirement that the bank design, build and maintain its data architecture and information technology in a manner that fully supports the required quality of risk aggregation. Following this mandate, U.S. financial institutions must obtain both a baseline of the organization's current and desired risk profile to implement and maintain those proactive steps that would bring the baseline risk into compliance with the enterprise's desired risk profile.

As with all matters that bring similar sea changes, these new requirements received their fair share of criticism prior to adoption. These financial institutions must now be able to assess and aggregate risks recorded in disparate and frequently incompatible databases. In so doing, the enterprise's directors must be made aware of any material deficiencies in these efforts

[1] Basel Committee on Banking Supervision, Bank for International Settlements, ''Principles for effective risk data aggregation and risk reporting,'' (January 2013), available at http://www.bis.org/publ/bcbs239.pdf.

[2] See generally Board of Governors of the Federal Reserve System, Press Release, Release Date December 6, 2013, available at http://www.federalreserve.gov/newsevents/press/bcreg/20131206a.htm.

 ISSN 0891-0634

as well as efforts to remedy those deficiencies. Regrettably, some data may not be fully accessible or even if available, it may not be usable.

If not corrected, these defects could significantly impair the determination of the enterprise's aggregate risk as well as potentially questioning the results obtained in the absence of the needed corrections. Some risk, such as determining the aggregate credit risk to a large corporate borrower and liquidity risk, may be relatively easy to quantify. But others, such as time-critical operational risk, may not be. Given its laudable underlying policy goals, this approach seems well reasoned and appropriate, even though it may frequently prove to be challenging in ''real world'' efforts to successfully implement and maintain ongoing compliance.

Robust Procedures

Basel III requires that these financial institutions have robust data architecture and information-technology infrastructure that provide an automated process to correctly identify and combine all material enterprise risks — frequently referred to as ''risk data aggregation'' — to provide management with timely, accurate, complete and useful reports. Such reports must be available upon demand for all business lines, legal entities, asset type, industry, region and other enterprise-specific grouping. Basel III is quite explicit in requiring that the bank design, build and maintain its data architecture and information technology in a manner that properly facilitates the required quality of risk aggregation.

To be most effective, these risk aggregation procedures should be adopted across the entire enterprise simultaneously. The manner in which these risks are assessed, quantified and reported is an ongoing technical debate. But bank regulatory counsel assigned the task of coordinating compliance with these two major initiatives, must understand that the manner in which data is maintained, accessed, indexed and queried may have a direct and substantial impact on the institution's ongoing data privacy and security compliance efforts.

Capgemini identified seven major issues currently preventing many financial institutions from fully realizing the benefits of properly leveraging the availability of big data.[3] The inability to access data across the entire organization, which is frequently due to the inability to access and query differnet types and version of legacy databases, the amount of time it takes to properly analyze the available and usable data and the shortage of skilled analytics personnel are common concerns. Cap Gemini also noted difficulties in interpreting unstructured data and the expense of storing and analyzing large data sets.

On balance, then, each bank's senior executives must be able to understand and weigh the cost and any possible enhanced functionality available in each new data structure proposed by their chief technology officer against the sunk and operating cost and functionality provided by their current architecture.

Two methods of database management are most commonly used in similar situations. In data warehousing, data is extracted from its original source before being cleansed, replicated and loaded into a new centralized repository. Queries addressing the risk assessment and adjustment actions are then directed to this new database in order to retrieve the requested results. Under the other approach, federated data access, data is analyzed in its original data source. Queries are submitted through adapters that translate the queries into custom forms for each of those original data sources for execution and the production of results. The results from those individual queries are then cleansed, transformed, standardized and combined into final results — frequently in middleware.

Replicating the old database in data warehousing versus the ability of the federated data access approach to access and use the data in its original source is the key, obvious difference between these methods. As a result, the cybersecurity obligations inherent in the data warehouse approach must be assessed at both the original data sources maintained by the enterprise as well as in the cloud storage. Therefore, access available to both databases must be done in the analysis done for proper risk aggregation. Enterprises using the federated access approach, on the other hand, will retain their legal obligations to maintain the original database. But financial institutions that implement either approach, or a hybrid of the two, must still be mindful of the potential liability that may arise from improper or insufficient risk aggregation activities. These obligations exist under both the principles-based approach advocated by Basel III as well as the more functional guidance provided by the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool.[4]

No Safe Harbor

Unfortunately, no safe harbor exists under either of these methods upon which practitioners can structure their cybersecurity protection work and feel comfortable that they have satisfied these rapidly evolving obligations. Given this uncertainty, the goal is to structure, implement, maintain and continuously improve the type of required ''risk data aggregation'' program while also maintaining a ''reasonable'' cybersecurity program. This approach should comply with applicable governmental and regulatory obligations and recent guidance while also protecting the enterprise from civil liability. As a result, careful analysis must be conducted in each individual situation to determine which features must be included to satisfy this amorphous standard of reasonableness.

Given the frequency and seriousness of current and potential, future breaches, it is quite possible that no such safe harbor will be available in the future. Consequently, bank regulatory counsel would be well advised to help analyze, structure, implement and continuously improve their programs along the lines explored by the based upon the key policies and issues addressed in the FFIEC Cybersecurity Assessment Tool. That tool was structured along the same lines as the National Institute of Standards and Technology's Framework for Improv-

[3] Capgemini Consulting, ''Big Data Alchemy: How can Banks Maximize the Value of their Customer Data?'' available at https://www.capgemini.com/resource-file-access/resource/pdf/bigdatainbanking_2705_v5_1.pdf.

[4] Federal Financial Institutions Examination Council, ''Cybersecurity Assessment Tool'' (June 2015), available at https://www.ffiec.gov/cyberassessmenttool.htm.

  BBR ISSN 0891-0634

ing Critical Infrastructure Cybersecurity, which some see as the ''industry standard'' for such matters.[5]

Which Method is Better?

In terms of functionality, data warehousing is a superior approach in many ways. It is frequently viewed as being more scalable and adaptable for use in a broad variety of architectures, it cleanses the original data more efficiently so it may be more usable and it has a higher query success rate due, in part, to its complete control of that process. While federated data access is limited by the constraints inherent in the underlying data systems, data warehousing is able to produce consistent, multiple indexes as well as pre-calculation and pre-aggregation values.

Since it replicates the original source and conducts all of its operations in the copied database, it is not surprising that data warehousing does not impose much additional load on the original database, cause any interference with its post-replication operations or enable the original database to be aware of any activity conducted in the replicated database. After the replication of the original data source, data warehousing, unlike federated access, is not dependent upon the continuing availability of the original data source or need to install any activators in the original data source.

Data warehousing, however, does come with a unique set of challenges. Real-time access to data will always be an issue due to the need to copy, transfer and cleanse data. In addition, as the size of an entity grows, it may become increasingly unlikely that 100 percent of the data required for property risk aggregation is transferred to a cloud-based data warehouse. Additionally, the costs associated with a data warehouse grow as more data is transferred and maintained in the duplicated database since the volume of daily data transfers and the amount of stored data are frequently key components in the pricing model used by many big data and analytics platforms.

Of critical importance to counsel is the possible deletion of metadata stored via data warehousing, clearly a possible negative in the data warehousing column. Federal data access typically does not have this risk. What it does have, however, is better functionality in a number of key areas, such as its ability to ''drill down'' into the original data source and to actively monitor all data sources while having easier access to the most recent data. Given these differences in functionality, a very strong case can be made that data warehousing is a superior method for information technology management.

But functionality is not the sole test in reaching a thoughtful conclusion on this choice since the implemented system must be able to perform its required tasks in a cost-efficient manner without the possibility of deleting the metadata that may be demanded in future litigation. Here the pendulum swings clearly in favor of federated data access. For example, it does not incur the expense of copying, transferring, storing and supporting the duplicated database. Generally, the cost of data extraction, transformation, loading and updating is higher in data warehousing, which may also require additional data marts to perform any significant analysis, including business intelligence analysis. Federated data access, on the other hand, frequently has a higher cost to modify the adaptors it uses to assemble the data as well as a greater cost — in both time and money — in adding new data sources. But these aggregate incremental costs in the federated data access approach may be minor in comparison to the overall cost of data warehousing.

Wyndham Case

Bank regulatory counsel should ensure that the institution's management is aware of these major differences in cost and functionality. In both systems, the institution should incorporate requirements of the Gramm-Leah-Bliley Act Safeguards Rule[6] and evolving case law, such as the landmark *Wyndham* case.[7] In this Third Circuit case, the Court upheld the Federal Trade Commission's authority to regulate the cybersecurity systems for entities involved in financial transactions — in this case, customer credit card information — even in the absence of existing, detailed regulations outlining the requirements for such a system. This case was resolved in mid-December 2015 when Wyndham agreed to implement and maintain for 20 years an enterprise-wide ''comprehensive information security program that is *'reasonably designed'* (emphasis added) to protect the security, confidentiality and integrity'' of customer credit card and related data.[8]

Aspects of this program were explicitly described in the order. For example, Wyndham will identify an employee that will be accountable for this program. The company must have employee training and management, review its network and software, and take additional steps to prevent, detect, and respond to attacks, intrusions and other systems failures in an appropriate manner. However, this program retains the current uncertainty surrounding the required oversight of independently owned parties whose data is processed by the defendant and the key requirements in the selection of acceptable outside vendors. Lastly, the order imposed additional recordkeeping obligations and the requirement that an independent, qualified expert and senior corporate officials certify to ongoing compliance.

While the *Wyndham* case sets out some aspects of a ''reasonable'' cybersecurity program, much subjectivity remains in applying its lessons. As a result, bank regulatory counsel should ensure that their clients cybersecurity programs address the deficiencies highlighted in recent FTC enforcement actions. With the benefit of counseling that incorporates these points, senior man-

---

[5] National Institute of Standards and Technology, ''Framework for Improving Critical Infrastructure Cybersecurity,'' (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. See ''Appendix B: ''Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework,'' (June 2015) available at https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf.

[6] Electronic Code of Federal Regulations, Title 16, Part 314.

[7] *Federal Trade Commission v. Wyndham Worldwide Corporation, et al.*, U.S. District Court, District of New Jersey, No.13-01887.

[8] Stipulated Order For Injunction, U.S. District Court for the District of New Jersey, Civil Action No. 2:13-CV-01887-ES-JAD, entered December 11, 2015, available at https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf.

agement and directors should recognize the need to implement appropriate cybersecurity controls. Areas highlighted by the FTC in such actions include:

- controlling general access;
- requiring the strong passwords and appropriate authentication;
- network segmentation;
- securing remote access;
- monitoring activity across the network;
- using a ''white'' list of programs that are permitted access to sensitive areas of the network;
- employee training and disciplinary action;
- appropriate data destruction methods; and
- an emphasis on continuous improvement in a culture in which cybersecurity is a daily, key consideration.

Additional guidance can be found in FTC publications, such as ''Protecting Personal Information: A Guide for Business,'' which provides some more concrete steps on physical, electronic and laptop security, password management, the proper use of firewalls, digital copiers as well as controlling wireless and remote access, specific guidance on threat detection, employee training and the concerns that arise from the use of contractors and other third party service providers.[9]

These steps should be followed in both data warehousing and federated data access since they must each address the risks inherent in database maintenance. To be sure, both methods also require manipulation of the underlying data. However, the need to duplicate the original database in data warehousing presents expanded logistical concerns as well as the possibility of increased regulatory requirements and civil exposures. Arguably, these latter concerns may be twice as problematic in data warehousing since it clearly presents the incremental risk of ''External Dependency Management,'' which is so important in the application of the FFIEC Cybersecurity Assessment Tool.[10]

This type of risk may be dealt with in properly structured outsourcing agreements with qualified and well-financed cloud providers. But the general belief in the security provided by the ''cloud'' should not be accepted in lemming-like fashion. Information technology professionals and bank counsel should be involved in the early and careful analysis of the desired level of third-party involvement, including the use of data warehousing or federated data access, and the relative expertise and competence of available internal and external resources. Since many corporate executive and directors may not be aware that the federated data access approach may provide a different cybersecurity risk profile, levels of functionality and cost, bank regulatory counsel must make sure that both the C Suite and the Board are aware of a different method of data access, integration and querying exists that does not require the separate, and potentially significant, risk inherent in data warehousing in the cloud.

Conclusion

We may see actionable guidance in the development of a total or partial safe harbor for use in designing, implementing and updating the cyber security programs as financial institutions access, quantify and calculate their respective aggregate risk profiles. For example, bills were recently introduced in both the Senate and House of Representatives that would establish strong and uniform national data security and breach notification standards that preempt state law while providing the FTC with express enforcement authority in such matters.[11]

Until that day, however, bank regulatory counsel should be well versed in the key difference between data warehousing and federated data access since each new database implementation may present individual risk aggregation and cybersecurity challenges and requirements. As discussed above, a strong case can be made that the federated data access approach is a structurally superior method to achieve cybersecurity compliance. This, combined with its lower cost, may offset, to a certain degree, the superior functionality currently available in data warehousing. Bank regulatory counsel must make sure that senior management and the board of directors are aware of the pluses and negatives of both federated data access and data warehousing.

Given the rapidly improving functionality available in all technologies, it is possible that ongoing efforts to retain the overall structure of federated data access while addressing its current deficiencies may shrink the current gap in functionality while retaining its advantage in cost and regulatory compliance. Addressing the present inability of either method to access, integrate and query information across disparate and frequently incompatible data sources — described as ''interoperability'' — would be an excellent start.

---

[9] Federal Trade Commission, ''Protecting Personal Information: A Guide for Business'' (November 2011), available at https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

[10] FFIEC Cybersecurity Assessment Tool, pp. 47 – 50.

[11] ''Data Security Act of 2015'' introduced in the Senate (114th Congress) on April 15, 2015, as S. 961, ''Data Security Act of 2015'' introduced in the House of Representatives (114th Congress) on May 1, 2015, as H.R. 2205.

BBR ISSN 0891-0634

BBR ISSN 0891-0634