Boosting Cyber Security With Data Governance and Enterprise Data Management

The relationship between cyber security and the regulatory requirements for data governance, data stewardship and enterprise data management is set to strengthen. Enterprise data management (EDM), data stewardship and data governance are concerned with the what, who and how of managing the enterprise data asset, respectively:

- **Enterprise data management (the what)**—Enabling the business to make the most of its data asset, supported by suitable tools and processes. EDM objectives include measuring data quality (and attesting to data and report quality); ensuring that reference data, e.g., product codes, are accurate (master data management); and ensuring that business has the same understanding of various business terms (metadata).
- **Data stewardship (the who)**—Identifying the people/positions involved in EDM within the business and ensuring the formal definition of their responsibilities and accountabilities. A data steward may need to measure the quality of a data element each month to support regulatory reporting; data stewardship formalizes these responsibilities and accountabilities.
- **Data governance (the how)**—Establishing, monitoring and sometimes enforcing policies, procedures, standards and guidelines that are related to the overall management of enterprise data, with the goal of sustainably ensuring data availability, usability and security. Data governance activities provide direction and structure to data stewardship and enterprise data management activities.

Guy Pearce
Is managing partner of REData Performance Consulting, which specializes in integrating data, governance, strategy, risk management and IT to produce auditable, data-driven value for enterprises and their customers. Pearce has served on the boards of directors of private and public companies in the banking, financial services and retail industries over the past decade and on their finance, risk, audit, credit, and information and communications technology committees. Pearce can be reached at pearcegf@gmail.com.

Regulators Are Driving Activities

In a joint sitting of the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS), regulators recognized the need for better data quality.[1] Banks were at the forefront of the new regulatory requirements for enterprise data management via the Basel BCBS 239, which was introduced in 2013.[2] BCBS 239 addressed the poor quality of reports that were submitted to regulators during the height of the global financial crisis and outlined the need for:

- Metadata, single identifiers and unified naming conventions for data. The latter two items are concerned with enterprise master and reference data management and are generally referred to as MDM.[3]
- Established roles and responsibilities in the enterprise—the data stewardship organization—with respect to managing enterprise data[4]
- Specific measures of data quality[5]

BCBS 239 gave rise to the creation of new bank departments and has been a driver of the chief data officer (CDO) role to head the department, often with a board or chief executive officer (CEO) mandate to meet these regulatory requirements. Although different in formality, structure and interpretation, the CDO's scope includes data governance, data stewardship and enterprise data management.

Considering the original joint sitting of Basel (banking industry), IAIS (insurance industry) and IOSCO (securities industry), similar regulations could apply to insurance and securities enterprises, too.

©2017 ISACA. All rights reserved. *www.isaca.org*

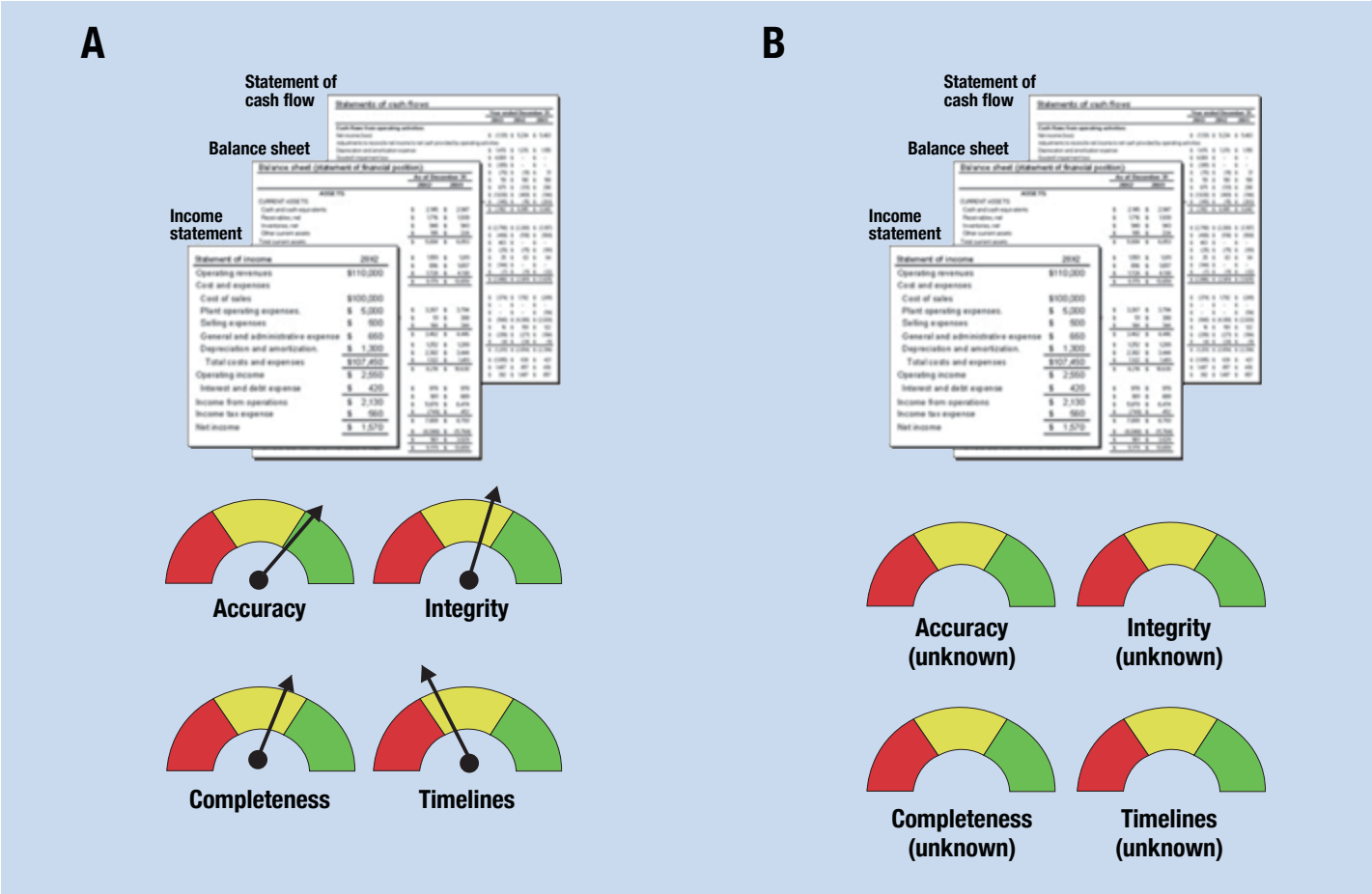
Positive Outcomes for Regulators and Data Users

Data quality processes enable users to know if a report can be trusted. For example, which report in **figure 1** is more trustworthy? Report A is certified across four data-quality dimensions—accuracy, integrity, completeness and timeliness—providing assurance of its trustworthiness. Report B has unknown quality and is unqualified, which is typical of most business reports.

The same matter applies to those enterprises that leverage analytics for enhanced business insights. If one set of insights is quality certified and another one is not certified, the former is more reliable to action, and the latter can result in unexpected and undesirable business outcomes that can, in turn, incur reputational and other risk for the enterprise.

Note that beyond absolute data quality, an enterprise should also know how well data that are copied by the enterprise from a production data source downstream into, for example, a data warehouse or data lake, remain accurate. Organizations need to know that this copy—facilitating organizational reporting and analytics—accurately reflects the production data. This example describes relative data quality that is assessed by means of data transport validation processes. Regulators are interested in absolute and relative data quality.

Figure 1—Data Quality Comparison of Report A and Report B



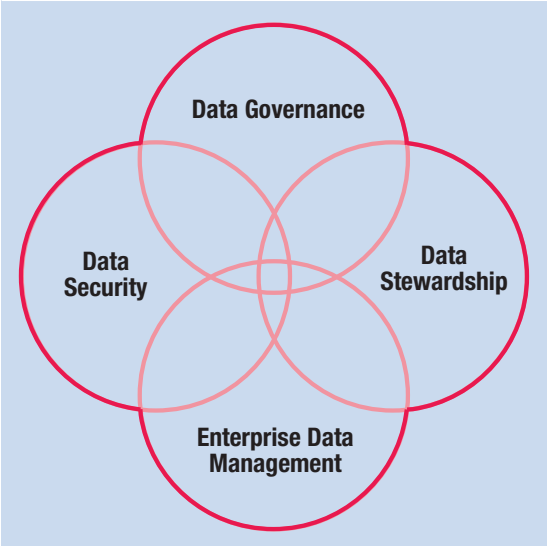
Source: G. Pearce. Reprinted with permission.

©2017 ISACA. All rights reserved. *www.isaca.org*

Relating Data Security, Governance, Stewardship and Quality

Data governance embraces all that data impact and that impacts data. For example, COBIT® 5 sees data governance as overseeing information custodianship and information security,[6] and the Data Management Association (DAMA) International places data governance at the hub of nine categories, including data quality, metadata and data security.[7] There is also an overlap between data security, data quality, data governance and data stewardship[8] (**figure 2**), specifically from the enterprise perspective.

Figure 2—Relationship Between Data Governance, Data Stewardship, Enterprise Data Management and Data Security



Source: G. Pearce. Reprinted with permission.

Incremental enterprise risk is introduced if the four categories in **figure 2** are inconsistent for any reason. The matter of organizational data management maturity comes to the forefront in plans to sustainably resolve such inconsistencies.

Good Cyber Security Deploys Multiple Lines of Defense

Cyber security strategies should create several lines of defense against attackers. One such line of cyberdefense is technology, e.g., for malware, viruses and hackers. For some enterprises, this is the only line of defense, which, unfortunately, still leaves the enterprise exposed to residual cyberrisk.

Another line of defense is ensuring that staff members are formally made aware of the risk that is associated with data and that they act according to defined data governance policies when handling enterprise data. Yet another example is third-party due diligence, in which data governance establishes the cyber security expectations of third parties.

Corporate governance—the board of directors' job—is the line of defense that looks at business culture, beginning with setting the right tone about risk at the very top of the enterprise.[9]

Four Ways Data Governance and Enterprise Data Management Boost Cyber Security

Data governance and enterprise data management augment the various lines of defense for data at risk. Data at risk are data that, if they were to fall into unauthorized hands, would compromise an enterprise and/or its customers. Identifying data at risk is a key activity, because securing all data is an impossible and very costly task for most enterprises. Data governance and enterprise data management boost cyber security in four ways.

Helping to Identify Data at Risk

Enterprise data management tools have made identifying sensitive data easier. Personally identifiable information (PII) (e.g., contact details, payment card industry [PCI] data, credit card details) and protected health information (PHI) (e.g., data containing individual medical records) constitute sensitive data. Enterprise data

Enjoying this article?

- **Learn more about, discuss and collaborate on cybersecurity in the Knowledge Center.** *www.isaca.org/cybersecurity-topic*

©2017 ISACA. All rights reserved. *www.isaca.org*

management tools can also help with identifying other data categories that the enterprise defines as sensitive. A breach of sensitive data is the cause of most reputation and financial risk for enterprises.

Hackers largely desire sensitive identity data (PII and PHI) because they have a longer shelf-life than financial data (PCI and other). Financial data are only useful to the hacker for as long as it takes the victim to inform the bank of stolen credentials.[10] With PII and PHI data, crimes can be committed in a victim's name for weeks, months or longer before anyone notices, with life-changing consequences for those affected.

The enterprise also needs to know who in the organization is using the sensitive data, the location of the data and how the data flow through the enterprise. The enterprise's data stewardship component can facilitate the identification of who has access to which data, helping to mitigate the risk of people being the biggest cause of information security incidents.[11] Enterprise data management tools can also facilitate identifying data location and how they flow through the enterprise (data lineage).

> **"Fifty percent of information security professionals worry that they do not understand the full extent of the data risk of their enterprise."**

Other ways of identifying data at risk are to:

- Analyze data flows
- Review enterprise access rights

- Perform transaction log analysis
- Perform business process analysis and audits
- Analyze job descriptions (data-intensive roles)
- Perform application audits (e.g., identify tools permitting sensitive data drill downs)
- Analyze data models, including areas of data duplication and data redundancy (data life cycle management).

Helping to Locate Sensitive Data

Heading the list of things that keep senior executives up at night is "not knowing where sensitive data reside."[12] Fifty percent of information security professionals worry that they do not understand the full extent of the data risk of their enterprise.[13]

Not knowing the location of enterprise sensitive data hampers the ability to identify enterprise data at risk, thereby compromising the enterprise's ability to design an effective cyber security strategy. Not knowing the location also hampers the ability of the enterprise to rapidly and properly respond to a data breach, which is an existing and emerging regulatory requirement in many jurisdictions and can result in significant fines and penalties.[14]

©2017 ISACA. All rights reserved. *www.isaca.org*

Some data quality tools can automatically infer the classification of data and allow custom classifications to be defined. These features are a natural outcome of the data profiling process, which accesses data stored at defined locations to perform the required data profiling tasks. The classifications, which determine whether data looks like credit card data (PCI), passport data (PII) or even fits a custom classification, can then be integrated into custom reports, enabling the enterprise to identify the location of any data of a given classification for strategic, operational or regulatory purposes.

Helping to Identify Sensitive Data Users and Ensuring Consistent Data Access Processes
Access to PCI, PII and PHI should be tightly controlled. As a result, business data stewards might lament that data security hampers them from doing their job, such as data profiling to determine data quality, while the data security team might remind data stewards that it is their job to restrict access to sensitive data to protect the data from the risk of misuse.

Data governance establishes policies and standards with respect to enterprise data. Given the relationship between data governance and cyber security, these policies and standards can also be used to guide the development of consistent data access processes across silos and across the enterprise. The policies define the principles of access for each diverse user group, and the data security team implements processes to suit each of these policies. Software tools are beginning to provide more of this type of functionality.

Helping to Ensure Safer Access to Sensitive Data
Data users do not always need to be able to see sensitive data to be able to use the data. This is important, because one of the greatest cyberrisk factors is internal staff, especially those with privileged access to data.[15] Data stewards have privileged access, especially when it comes to data profiling. How can the risk of data stewards misusing sensitive data be mitigated?

Modern data quality tools address this access risk by providing masking and tokenization functionality.

> **“Data users do not always need to be able to see sensitive data to be able to use the data.”**

Some tools also limit drill-down access to the underlying data. These features enable data stewards and other users to profile their data and assess their data quality without ever seeing the data and, thereby, potentially compromising data security.

Conclusion

Data governance and enterprise data management are key to the future competitiveness and sustainability of enterprises. The benefits of data governance and enterprise data management span areas such as cyber security, marketing, sales, strategy, finance, compliance and audit, and, from an operational perspective, business intelligence, reporting and analytics. This article outlined some benefits of the relationship between cyber security, enterprise data management and data governance.

Knowing the relationship between data governance and cyber security, enterprises need to ask if their enterprise data are consistently governed under a single umbrella. If not, an enterprise could have inconsistent and even contradictory policies deployed across the enterprise, which introduces new risk. Good corporate governance requires new risk to be recognized and documented in the enterprise risk register for board-level visibility.

©2017 ISACA. All rights reserved. *www.isaca.org*

Ultimately, leveraging enterprise data management and data governance outcomes in a cyber security context creates another line of defense for one of the modern enterprise's most valuable assets with little incremental effort.

Endnotes

1 Bank for International Settlements, *Trends in Risk Integration and Aggregation*, August 2003, *www.bis.org/publ/joint07.pdf*

2 Bank for International Settlements, *Principles for Effective Risk Data Aggregation and Risk Reporting*, January 2013, *www.bis.org/publ/bcbs239.pdf*

3 *Ibid*.

4 *Ibid*.

5 *Ibid*.

6 Suer, M.; R. Nolan; "Using COBIT® 5 to Deliver Information and Data Governance," *COBIT® Focus*, 12 January 2015, *www.isaca.org/cobit/focus/pages/using-cobit-5-to-deliver-information-and-data-governance.aspx*

7 DAMA International, "Body of Knowledge," 2015, *www.dama.org/content/body-knowledge*

8 Stanford University, "Data Governance at Stanford: A Data Governance Overview," 19 September 2011, *http://web.stanford.edu/dept/pres-provost/cgi-bin/dg/wordpress/wp-content/uploads/2011/11/DG-News001.pdf*

9 Akmeemana, C.; G. Pearce; "Tech-based Cybersecurity Can't Stop 'People Risk'," American Banker, 22 July 2016, *https://www.americanbanker.com/opinion/tech-based-cybersecurity-cant-stop-people-risk*

10 Rashid, F. Y.; "Why Hackers Want Your Health Care Data Most of All," *InfoWorld*, 14 September 2015, *www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html*

11 PricewaterhouseCoopers, "Managing Cyber Risks in an Interconnected World: Key Findings From the Global State of Information Security Survey 2015," 30 September 2014, *www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf*

12 Ponemon Institute, "The State of Data Security Intelligence in 2015," 7 April 2015, *www.slideshare.net/informaticacorp/infagraphic-ponemon-state-of-data-centric-security*

13 *Ibid*.

14 Friedman, K.; T. Hunter; J. Halpert; "Canada's PIPEDA: Consultation Opportunity for Data Breach Reporting Regulations," 31 May 2016, *www.dlapiper.com/en/canada/insights/publications/2016/05/canadas-pipeda-consultation-opportunity/*

15 Shaw, N.; "It Shouldn't Matter How Many US Bs Are Lost," *InfoSecurity*, 27 January 2016, *www.infosecurity-magazine.com/blogs/it-shouldnt-matter-how-many-usbs/*

©2017 ISACA. All rights reserved. *www.isaca.org*