Security Risk Governance: A Critical Component to Managing Security Risk

Brian Allen
Global Security Risk Management Alliance

Timothy Kelly
Global Security Risk Management Alliance

Rachelle Loyear
Global Security Risk Management Alliance

Amy Poole
Global Security Risk Management Alliance

Adegbenro Awojulu
University of Connecticut School of Business

Andrew Kmetetz
University of Connecticut School of Business

Michel Rakotomavo
University of Connecticut School of Business

Zhuoran Wang
University of Connecticut School of Business

Heli Xu
University of Connecticut School of Business

Mengzhu Xu
University of Connecticut School of Business

Huaijin Yuan
University of Connecticut School of Business

This paper proposes that security risk be managed at the same corporate level and with the same focus as financial risk, regulatory risk, or operational risk. It reviews related corporate governance and risk

management concepts and shows applications into a variety of case studies from real businesses across the traditional risk management footprint. Using the framework of enterprise security risk management, it illustrates how security risk can be managed as any other type of risk and suggests some oversight and governance models for the security risks that could impact and damage business assets and functions.

INTRODUCTION

Enterprise business leaders must understand and manage many kinds of risk in the course of ensuring the organization can fulfill its mission: meet the goals set for it by the board of directors, satisfy the expectations of the customers or clients they serve, ensure continued operation for the good of shareholders, and provide ongoing employment for personnel. While most business leaders have a deep understanding of managing financial risk, regulatory risk, or operational risk, there is a segment of the risk picture that is often treated in a different manner, and that is security risk.

Security risk is defined in the book The Manager's Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security as:

"anything that threatens harm to the enterprise, its mission, its employees, customers, or partners, its operations, its reputation."

Security risk can range from a risk of workplace violence to a data breach, from a natural disaster to a stolen shipment of supplies, a break in to a facility to a break in on a network. And yet, protecting the organization from these types of risk is often handled, not as business risk, but as day to day task management of locks, passwords, supply tracking, badges, cameras, etc. Rather than managing risk through a holistic approach in line with other types of risk, these aspects of business protection are seen as the job of IT or security, and not approached from the executive leadership level with the same stringent risk-based controls that other types of risk are.

Security risks are continually evolving and changing as the enterprise evolves and changes. Each new product line, new facility, change in business direction, move into a new market, personnel increase or reduction, or other business change, bring with it a change in potential for some internal or external factor to bring harm to the assets of the organization. And this dynamism is not limited to change in the business. The global environment in which the organization functions is also changing just as rapidly. Global human migrations caused by political instability or environmental changes can have enormous impacts on the business. New technologies in the hands of criminal organizations can make operating in the cyber-environment more difficult. Environmental factors like water shortages or weather changes can lead to political instability and new threats to the operation of business in unstable areas. All of these security factors must be dealt with by business leaders, and simply cannot be left to the hope that a single business unit such as IT or security can protect the organization in a vacuum without the input of the impacted business stakeholders.

This paper will first explore an overview of governance concepts as they apply to business risk management, then delve into a variety of case studies from real businesses, showing how existing business organizations apply governance and risk management across the traditional risk management footprint. Finally, through the lens of a new security management paradigm, Enterprise Security Risk Management (ESRM), it will show how security risk can be managed in the same fashion as any other type of risk and explore some potential practices for business managers to set up oversight and governance for the security risks that could impact and damage their business assets and functions.

CORPORATE GOVERNANCE AND RISK MANAGEMENT - AN OVERVIEW

As mentioned above, this paper will espouse the idea that the most effective way to deal with the constantly changing security risk environment that businesses operate in today is to enact a clear security risk governance model. To begin the discussion of how to implement that, we will first consider the two more general topics of corporate governance and enterprise risk management. Together, these fundamental business concepts will provide the base for managing security risk in a more business-

oriented fashion that allows the business to take appropriate and acceptable risks within a framework of identified acceptable levels of risk and proper education about threats to business assets.

Corporate Governance

Corporate governance can be described at a high level as the set of systems and processes that a well-managed company puts in place to ensure that it acts correctly in its relations with all of its stakeholders – including, but not limited to, shareholders, employees, clients, customers, and the public.

Typical corporate governance documents and standards address issues such as the role of the CEO and chairman of the board, the role of the board of directors, the need for audit and oversight of business activities to ensure they are in the best interests of the stakeholders of the company, the rights of all stakeholders, and the need for disclosure and transparency in management.

Corporate Governance is complex due to the many factors that influence it. Factors such as laws, regulations, industry standards, stock ratings agencies, shareholder activism, and many more. These factors vary widely, from country to country, from region to region, and from industry to industry. The US, for example, defines and mandates some aspects of corporate governance through the financial transparency requirements of the Sarbanes-Oxley Act of 2002, while the European Union (EU) has its own corporate governance requirements. There is not, however, any single international standard that all countries and all industries are required, or even expected, to follow (Dowdney, 2005).

Although there is no legal standard required internationally, a number of organizations have worked over decades to provide guidance and definition around the topic of corporate governance.

The Cadbury Committee.

A frequently cited description of corporate governance was written by the Cadbury Committee, a working group that was set up in the UK in 1991 to promote the adoption of standards in corporate governance: "Corporate governance is the system by which companies are directed and controlled" (Cadbury Committee, 1992).

That definition was the beginning of the creation of a body of knowledge around corporate governance. As time went on, and in response to ongoing examples of poor governance in many business organizations, other groups concluded that there was a need to provide further documentation and models of governance.

International Federation of Accountants (IFAC).

In the 2004 report: Enterprise Governance, Getting the Balance Right, another group, the IFAC, defined 'enterprise governance' as:

"…the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly." (IFAC, 2004, p. 6)

In this definition, the IFAC began specifically mentioning managing risks properly – a critical step in the evolution of corporate governance and the management of all types of organizational risk.

Organisation for Economic Co-Operation and Development (OECD).

Continuing the evolution of concepts around corporate governance, the OECD put out a document in 2015 titled G20/ OECD Principles of Corporate Governance. It is a document that business leaders can look to now for a model on how to govern their organizations appropriately.

Some of the key governance principles of the OECD document are:

1. Ensuring the basis for an effective corporate governance framework.

   "The corporate governance framework should promote transparent and fair markets… It should be consistent with the rule of law…" (OECD, 2015, p. 13).

2. The rights and equitable treatment of shareholders and key ownership functions.

"The corporate governance framework should protect and facilitate the exercise of shareholders' rights and ensure the equitable treatment of all shareholders…" (OECD, 2015, p. 18).

3. Institutional investors, stock markets, and other intermediaries.

"The corporate governance framework should …provide for stock markets to function in a way that contributes to good corporate governance" (OECD, 2015, p. 29).

4. The role of stakeholders in corporate governance.

"The corporate governance framework should recognise the rights of stakeholders…" (OECD, 2015, p. 34)

5. Disclosure and transparency.

"The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company" (p. 37).

6. The responsibilities of the board.

"The corporate governance framework should ensure … the board's accountability to the company and the shareholders" (p. 45).

Enterprise Risk Management

Corporate governance is tightly tied to another concept, Enterprise Risk Management (ERM). ERM is often an established program within the enterprise, sometimes separate, or sometimes part of Internal Audit or Compliance, designed to manage risks for the business. ERM is used in business organization as a framework to manage financial and investment risk, supply chain risk, operational risk, resource risk, and more.

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

The ERM concept was first developed, defined, and codified by the financial services industry. The originator of ERM was the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a joint initiative of five major professional associations: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Internal Auditors (IIA), and the National Association of Accountants (now the Institute of Management Accountants [IMA]). The Treadway Commission also included representatives from industry, public accounting, investment firms, and the New York Stock Exchange.

In its 2004 Integrated Framework document written to help businesses and other entities assess and enhance their internal control systems, COSO describes ERM "as a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

This ERM framework is geared towards achieving an entity's objectives, as set forth in four categories:

- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of reporting
- Compliance – compliance with applicable laws and regulations.

COSO's guidance illustrated the ERM model in the form of a cube (Figure 1). COSO intended the cube to illustrate the links between objectives that are shown on the top and the eight components shown on the front, which represent what is needed to achieve the objectives. The third dimension represents the organization's units, which portrays the model's ability to focus on parts of the organization as well as the whole.

FIGURE 1
THE COSO ERM MODEL

According to the document:

"The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity's units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit, or any subset thereof" (COSO, 2004).

It further suggests that everyone in an entity has some responsibility for ERM with principal responsibility residing with the most senior officers. The Chief Executive Officer (CEO) is ultimately responsible and should assume ownership while other managers support the entity's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility.

COSO's is just one of several industry frameworks for ERM.

The Three Lines of Defense

Another risk management oversight and strategy-setting methodology actively used by many organizations although with varying adjustments to make for peculiarities and organizational differences is the three lines of defense structure (See Figure 2).

FIGURE 2
THE THREE LINES OF DEFENSE MODEL

Adapted from ECIAA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

"The Three Lines of Defense model provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties. It provides a fresh look at operations, helping to assure the ongoing success of risk management initiatives, and it is appropriate for any organization — regardless of size or complexity" (Institute of Internal Auditors, 2013).

The three lines of defense effectively distinguishes between three groups that are usually involved in the risk management process.

Group 1 – Functions that own and manage risks are considered the first line of defense. It is their role to set risk appetite and ensure that controls are in place.

Group 2 – Functions that oversee risks are the second line of defense. These groups are the ones that carry out the actions of the controls set by management.

Group 3 – Functions that provide independent assurance are the third line of defense. Their role in ERM is to check and ensure that the controls are carried out and provide the protection they are meant to provide.

International Standards Organization Standard 31000:2009 – Risk Management: Principles and Guidelines

The International Standards Organization, in ISO Standard 31000:2009 – Risk Management: Principles and Guidelines outlines highly effective standards for risk management.

A few examples of key principles from the ISO Standard 31000 (2009) are that risk management should:

- Be part of decision making process.
- Be transparent and inclusive.
- Be dynamic, iterative, and responsive to change.
- Be capable of continual improvement and enhancement.

These are just a few snippets from the standard. The entire standard is voluminous and quite comprehensive and cannot be fully explored in this setting. However, it is a foundational document that,

if a risk management approach is used in business organizations, is highly recommended as a baseline of setting up the program.

Additional ERM Models to Consider

While a comprehensive exploration of all risk models is not possible in this setting, there are many different risk models that any organization could consider when implementing a formal ERM program. In Table 1, several are listed for consideration.

TABLE 1
WIDELY USED SECURITY AND RISK MODELS

European Union Agency for Network and Information Security (ENISA) Risk Management/Risk Assessment (RM/RA) Framework	https://www.enisa.europa.eu
International Organization for Standardization (ISO) Enterprise Risk Management Model	http://www.iso.org/iso/home/standards/iso31000.htm
National Institute of Standards and Technology (NIST) Cybersecurity Framework	http://www.nist.gov/cyberframework/
ISACA Control Objectives for Information and Related Technology (Cobit 5) Framework	http://www.isaca.org/cobit/pages/default.aspx
Federation of European Risk Management Associations (FERMA) — Risk Management Standard	http://www.ferma.eu/risk-management/standards/risk-management-standard/
EU Solvency II Directive (2009/138/EC)	http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0138
OCEG GRC Capability Model (Red Book) 3.0	http://www.oceg.org/resources/red-book-3/

CASE STUDIES: BUSINESS IMPLEMENTATIONS OF CORPORATE GOVERNANCE AND RISK MANAGEMENT

Formal models and definitions are an excellent starting point for implementing governance and risk management program. But no two business organizations are alike, and the real world often requires adaptation of academic best practices. Some examples of current ERM implementations in real enterprise organizations follow to illustrate how vastly different these implementations can be in practice while still upholding the spirit and goals of governance and ERM. Additionally, the diverse nature of the businesses in the case studies shows the ubiquity with which this critical business philosophy has crossed industries and geographic boundaries due to its importance in enterprise management.

OLAM Group

Olam Group is a leading agri-business organization that operates in five significant business segments including edible nuts, seeds, confectionary ingredients, and other food staples. They operate, in their own words, “from seed to shelf in 70 countries, supplying food and industrial raw materials to over 16,200 customers worldwide” (Olam, 2016). This global business operates in a volatile environment with significant risk exposure and has implemented an overarching risk management plan.

The Olam Board of Directors chose to delegate oversight of risk management to a sub-committee of Executive and Non-Executive Directors. They call this the Board Risk Committee, and it acts as the directing body for risk management. The responsibilities of the risk committee are:

1) examining the effectiveness of risk program components
2) reviewing risk policies, etc. and risk exposure and risk treatment plans.

The risk subcommittee also assists with risk tolerance posture by recommending the overall company Value at Risk (VaR) to the Board for approval at the start of the financial year. Figure 3 shows the risk governance structure of Olam Group and attendant responsibilities (Olam, 2016).

FIGURE 3
OLAM GROUP RISK GOVERNANCE

Johnson & Johnson

Johnson and Johnson operates in a far different field than the Olam group. As such, they have a significantly different structure for managing risk. But as with Olam, they recognize the importance of that formal structure and program for ERM.

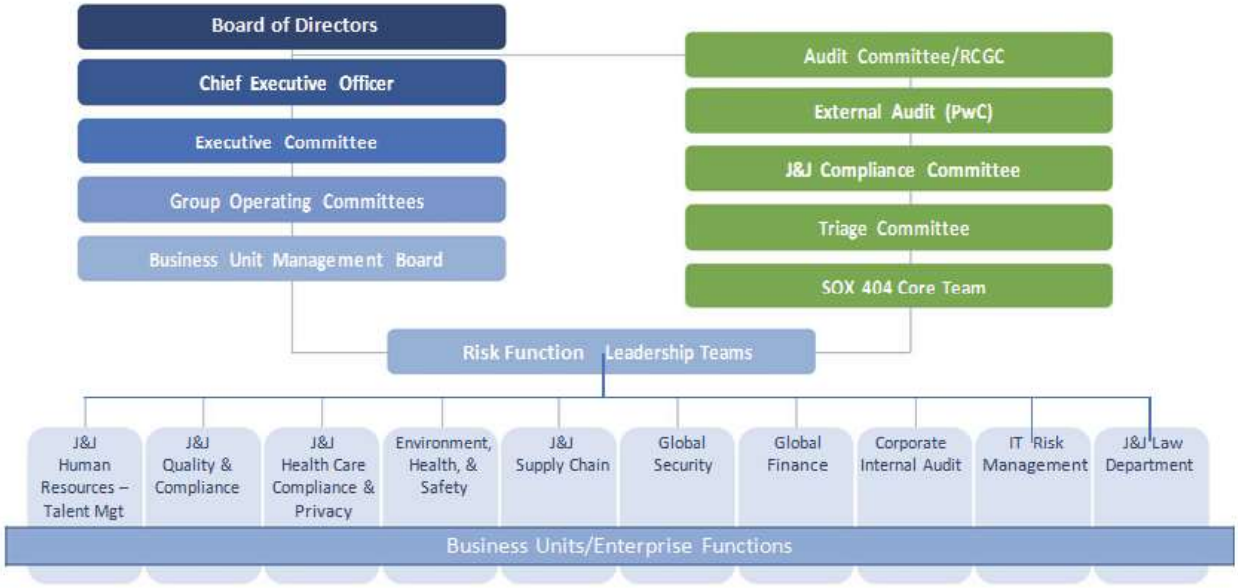
Johnson & Johnson is an umbrella corporation with a number of different companies operating under its control. It is primarily in the business of research and development, manufacture and sale of health care products and operates in almost every country across the globe.

According to the company's Framework for Risk Management, each of the many business units and functions has its own risk group that is responsible for communicating the risks and the risk response strategies they have identified as part of the program to their respective leadership teams. If needed, the risks can continue along an escalation path to an Executive Committee, which is the overall risk posture and policy setter for the entire organization, or directly to the Audit Committee, which is an overseer of the risk program.

With each individual company in the group responsible for managing risk, the firm is able to understand and respond to the specific risks to individual groups, while allowing them the flexibility to manage them in the way that best fits their situation; however, the structure allows for cross-functional councils and committees to share emerging risks and common practices and deal more effectively with

risks that require an integrated response or might impact more than one group (Johnson & Johnson, 2013). Figure 4 illustrates the structure put in place by Johnson and Johnson.

FIGURE 4
JOHNSON & JOHNSON RISK GOVERNANCE & OVERSIGHT



Brit Global Specialty Insurance

Brit Insurance is an example of risk governance in a service-oriented industry rather than a product-oriented space such as the health care or agriculture industries. Brit is a global insurance and reinsurance firm that focuses on commercial insurance in the property, casualty, and energy business segments. They offer coverage on a variety of assets and business areas from aerospace to marine and covering both physical and cyber environments.

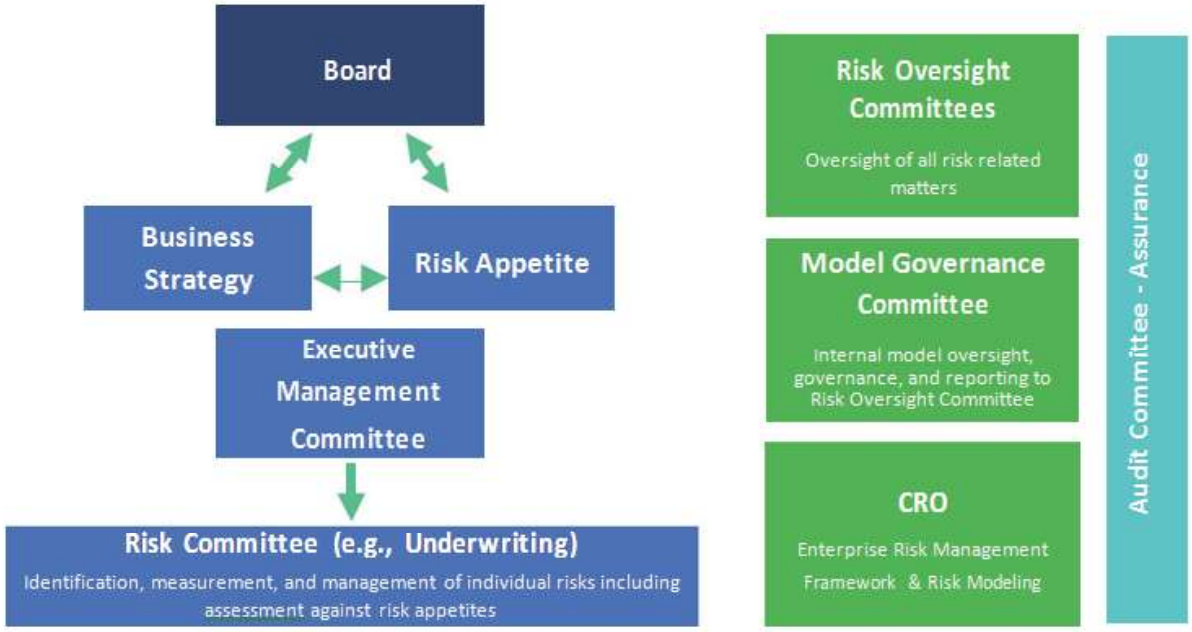
At Brit Insurance, the Board holds the overarching responsibility for risk management and internal control. The program splits segments of risk management among multiple Risk Oversight Committees and Audit Committees to support a more granular risk governance framework.

The role of the Risk Oversight Committees is to monitor and review the risk profile under their area of control and ensure the effectiveness of all risk management activities. They also ensure company conformance to set risk tolerances.

To provide additional assurance of proper risk management, the Internal Audit function oversees the Risk Oversight Committees, Audit Committees and Boards with regular audits and external audits provide independent assessments of the program.

An illustration of Brit's risk governance framework is shown in Figure 5. This model is based on the three lines of defense model discussed in section 2.2.2. The first line of defense is the individual risk committees. Risk management is the second line of defense, and the Audit Committee provides the third line (Brit Group, 2015).

FIGURE 5
BRIT INSURANCE RISK GOVERNANCE STRUCTURE



APPLYING PRINCIPLES OF CORPORATE GOVERNANCE AND RISK MANAGEMENT TO SECURITY RISK

As identified in the introduction of this paper, the goal of this document is to describe how fundamental risk management principles based in the philosophy of corporate governance and ERM can be used by business management in an organization to manage security risks. Security risks are, after all, simply another type of risk that can impact the mission and function of the enterprise operation. Traditionally, many risk management programs have shied away from security risk topics such as cyber security risk, workplace violence risk, physical security risks like intrusion or theft, and other specialized forms of risk that fall outside of the typical financial and operational silos. This is often because business managers do not have a deep understanding of security risk and have a tendency to think of it as an IT issue, or the job of the security department, or Human Resources. This attitude towards these types of risks is exposing business organizations unnecessarily to two problems. One, these risks might be ignored and impact the company negatively at a future time due to lack of management, or two, the risks might be over-mitigated, far out of line with overall enterprise risk tolerance levels, simply due to a lack of in-depth understanding of the potential threats, exposures, and impacts possible. The solution to this lack of governance around security risk is a philosophy of managing security risk called Enterprise Security Risk Management.

Enterprise Security Risk Management (ESRM)

According to the 2016 book The Manager's Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security, at its most simple, ESRM is defined as:

"Enterprise security risk management is the application of fundamental risk principles to manage all security risks - whether information, cyber, physical security, asset management, or business continuity - in a comprehensive, holistic, all-encompassing approach."

Security Risk

Risk is a very broad term, and ESRM deals, quite specifically with security risk. A security risk in context of ESRM is anything that threatens harm to the enterprise, its mission, its employees, customers, partners, its operations, or its reputation. This could mean a troubled employee with a gun, an approaching hurricane, a computer hacker, a robber or a thief, an angry customer in a company facility, or an employee with access to sensitive information that is willing to sell it to a competitor.

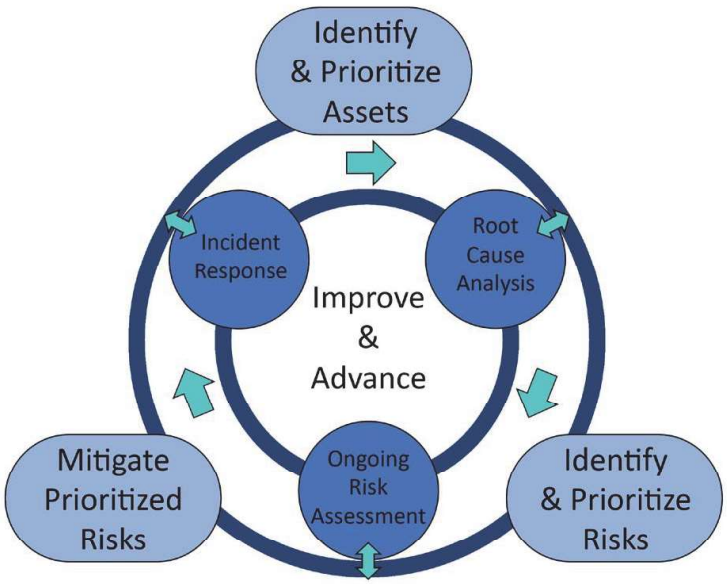
Security risks take many different forms, and new ones are being introduced all the time. Recognizing those risks, making them known to the enterprise, and having security assist internal functional business partners to mitigate them is central to the ESRM philosophy.

The ESRM Life Cycle

ESRM is a cyclical program. Although there must be a starting point in every program, once begun, the cycle of risk management is ongoing with multiple steps as seen in Figure 6.

1. Identify and Prioritize Assets: Identifying, understanding, and prioritizing the assets of an organization that need protection.
2. Identify and Prioritize Risks: Identifying, understanding, and prioritizing the security threats the enterprise and its assets face - both existing and emerging - and, critically, the risks associated with those threats
3. Mitigate Prioritized Risks: Taking the necessary, appropriate, and realistic steps to protect against the most serious security threats and risks
4. Improve and Advance: Conducting incident monitoring, incident response, and post-incident review - learning from both successes and failures - and applying the lessons learned to advance the program.

FIGURE 6
THE ESRM LIFE CYCLE



From: The Manager's Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security

The Role of Security and Functional Leaders in ESRM

ESRM uses risk management principles to manage any and all security-specific risks across an enterprise. It does not define an organization, specific job roles, or a required management structure, but

simply establishes a management philosophy and process the security organization can use to guide the business in identifying, managing, and accepting security risks.

There is a key delimitation of roles in ESRM between the security team and business leaders. Each has a part of managing the risk. The role of security is to provide analysis and education to business leader around security risk topics to allow those business leaders to make informed security decisions. These roles are outlined in Table 2.

To further break down the roles:

a) The role of security is to manage security risk.
b) This means - the security team provides security guidance and subject matter expertise to business function leaders to help them make quality security risk decisions in their areas of responsibility.

TABLE 2
THE PARTNERSHIP BETWEEN SECURITY AND OTHER ENTERPRISE BUSINESS FUNCTIONS

The Role of Security	The Role of Business Function Leaders
Manage security risks to enterprise assets.	Understand the role of the Security department in helping the businesses carry out its operational mission
Monitor risks to ensure impacts stay within defined tolerance levels.	Define an acceptable level of security risk tolerance to assets in their area of responsibility.
Provide subject matter expertise on risk mitigation options.	Make quality, educated decisions on security risks to assets in their area of responsibility.
Carry out risk mitigation tasks that require technical security skills in support of the security/business partnerships.	Carry out risk mitigation tasks that require business function involvement in support of the security/business partnership.

Governance Models for Security Risk

The key to managing security risk in a governance model is to understand that security risk is merely a subset of all risk that must be managed holistically across the enterprise. While security risk may have very specialized risk response and mitigation actions required, the process of managing the risk with fundamental risk principles is the same for security, financial, operational, or any other kind of risk.

In the ESRM philosophy of security risk management, the security practitioner works directly with the business leader and risk stakeholders of the enterprise asset at risk to determine risk tolerance, and implement an acceptable response that the business determines best covers the asset at risk. It is critical that both the security team responsible for mitigation tasks and the managers responsible for the assets under consideration are clear on their respective roles so that the subject matter experts in topics relating to security like cyber defense or workplace violence prevention, or access control and monitoring can provide appropriate knowledge to the business leader who ultimately owns the risk in question. A formal model of risk governance can help significantly in this task, as oversight committees can direct and control risk response while the mitigation actions are performed and managed by the personnel with the technical backgrounds needed. But even an informal approach, with committees or working groups, can provide a critical level of governance in an organization that might not have the resources and personnel to implement the infrastructure of formal governing councils.

Models of Security Governance

The final decision on how to manage security risk as part of an overall risk program can take many forms. As show in the case studies, the key to risk-based security management is that the model must be flexible and adapt to the need of the enterprise in which it operates. From an ESRM point of view, the most important factor is that the business leadership makes the decision to manage security risk in the same or similar manner as any other type of risk: with executive governance and oversight of the risk in line with tolerances derived by business criteria.

However, although the governance must be flexible and adaptable, there are three basic models that can be used as a framework to organize security risk governance in almost any enterprise.

Security Risk Council.

In the Security Risk Council model, all types of security risk are governed by a single council of risk stakeholders. In this model, the scope of the council is defined to handle any risks that the enterprise considers to fall under the security topic. This council would report findings into either the executive level or an overarching risk management program governing body. The key feature of this council model is that a single council governs and oversees the tolerance and response to all security risks with one set of council members. In Figure 7, one approach to this council model is shown with some possible stakeholder groups identified as participants in the council. This model would need to be adapted to the key risk stakeholders of any particular enterprise organization in which it was adopted.

FIGURE 7
EXAMPLE OF SECURITY RISK COUNCIL APPROACH

Security Risk Council with Subcommittees.

The security risk council with subcommittees model, a possible example of which is shown in Figure 8, also features one main body responsible for all security risk. However, in this model, there are working groups or subcommittees tasked with oversight of specific disciplines of risk. For example, the security council might determine that it would handle most types of security risk at the central council level, but that certain topics such as workplace violence and threat management, cyber security, or other critical topics required members of a subcommittee that had more technical expertise to oversee the risk more closely. Those subcommittees and working groups would still report into the main council who would represent the entirety of the program with a single face to higher level management.

FIGURE 8
EXAMPLE OF SECURITY RISK COUNCIL WITH SUBCOMMITTEES APPROACH.

Security Discipline Councils.

In the model of multiple security discipline councils (See Figure 9), there is no central body with scope over all security risks. In this model, the enterprise might have such specific and critical focus on individual disciplines of security that a single body to manage risks associated with topics as diverse as personnel hiring and clearance, business continuity risk, or cyber security might not work to provide adequate risk management for the firm. In this case, specific councils might be put in place to deal with each critical discipline as determined by the risk posture of the firm. They might report into an executive body, as shown in the example in Figure 9, or the enterprise might function best with the councils operating without any direct reporting. As with all these models, the best structure is the one that works for the enterprise it is applied to.

FIGURE 9
EXAMPLE OF MULTI SECURITY RISK COUNCIL APPROACH.

Security Networks / Working Groups.

In each of the models above, and in the case studies included earlier in this paper, the key is that there is some determination made by executive management to manage security risks to the enterprise in the way that fits in with the overall risk posture of the enterprise. While formal models of governance with named councils and committees is one way to apply governance to security risks, the critical factor in managing security risk is for there to be some kind of governance in place. In the ESRM philosophy, formal and documented governance is preferred, however, even informal governance allows better decision making to occur due to having input from a variety of risk stakeholders in the security risk decision making process. An informal governing process might include networks of department leaders who perform some aspect of a security risk mitigation plan, or working groups of business functions who are most heavily exposed to security risk. Flexibility in security risk governance is important, to ensure it fits the culture of the enterprise it is managing the risk in.

CONCLUSION

In an ever more competitive business environment, enterprise leaders must take every advantage they have to manage risk to their organization's ability to accomplish its mission. Security risk is one risk element that has often been overlooked in the executive suite in the past, but is coming more and more to the forefront of potentially enterprise- impacting topics that must be considered on a holistic basis. Embracing the concepts of corporate governance and ERM, and applying those fundamental risk concepts to the domain of security risk is an excellent way to protect the business against security risk and to prepare it to handle the impact of any security incident that might occur. Governance is a key component to managing security risk and should be considered by any business leader that has security responsibilities in an enterprise or who is a stakeholder in a process or over an asset that could be impacted by a security risk.

REFERENCES

Allen, B, & Loyear, R., (2016). *The Manager's Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security.* Brookfield, CT: Rothstein Associates, Inc.

Brit Group. (2015). Risk governance. Retrieved from http://www.britinsurance.com/governance/risk

Committee on the Financial Aspects of Corporate Governance (Cadbury Committee) & Gee and Co. Ltd. (1992). *The financial aspects of corporate governance*. London: Gee, pp. 14 – Sec 2.5. Retrieved from http://www.ecgi.org/codes/documents/cadbury.pdf.

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (September, 2004). *COSO Enterprise risk management - Integrated framework Executive Summary* (2004). Durham, NC: American Institute of Certified Public Accountants [AICPA].

Dowdney, A. (2005). Corporate governance in the UK and U.S. comparison. Metropolitan Corporate Council. Retrieved from http://www.metrocorpcounsel.com /articles/6173/corporate-governance-uk-and-us-comparison

Institute of Internal Auditors (IIA). (2013) Position paper: The three lines of defense in effective risk management & control. Altamonte Springs, FL: IIA.

International Federation of Accountants (IFAC). (2004). *Enterprise governance, Getting the balance right.* (pp. 6) New York: IFAC,.

ISO/IEC, (2009). ISO/IEC 31000:2009 *Risk management – Principles and guidelines.* Geneva, Switzerland: ISO/IEC.

Johnson & Johnson. (2013) Framework for enterprise risk management. Retrieved from http://www.jnj.com/sites/default/files/pdf/JnJ_RiskMgmt_ERMFramework_guide_v16a.pdf

Olam Group. (2016) *Risk Governance Structure.* Retrieved from http://olamgroup.com/about-us/risk-management/risk-governance-structure/

Organisation for Economic Co-operation and Development (OECD). (2015), *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264236882-en