
Overview and Background

Organizations are continuously exposed to a host of evolving threats which create a multitude of security risks. Security risks to the enterprise have not consistently been viewed or managed through defined risk-management principles and processes. A consistent and holistic approach will enable organizations to effectively manage security risks and the impacts on the business.

This document will frame the practice of Enterprise Security Risk Management (ESRM) and provide a high-level perspective of the concepts and management processes that should be used to manage security risks to and across an organization. A common understanding of ESRM will help practitioners and organizations to more effectively manage security risks.

ESRM needs to be fully integrated into corporate processes at every level of the business and by every security risk professional. Therefore, the audience is anyone involved with identifying, understanding, and/or managing security risks, including:

- **Business Leaders**: Executives and managers throughout the organization will gain a better understanding of industry-accepted best practices related to the management of enterprise security risk.
- **Security Practitioners**: Security professionals at every level will find in these ESRM principles a common and repeatable set of practices which will help identify, quantify, prioritize, and manage security risk in a consistent manner.
- **Audit and Risk Professionals**: This document will provide a common framework of generally accepted practices related to the management of security risks across an enterprise.

Definition of ESRM

ESRM is a management process used to effectively manage security risks, both proactively and reactively, across an enterprise. ESRM continuously assesses the full scope of security-related risks to an organization and within the enterprise’s complete portfolio of assets. The management process quantifies threats, establishes mitigation plans, identifies risk acceptance practices, manages incidents, and guides risk owners in developing remediation efforts.
DIFFERENCE BETWEEN ESRM AND ERM

ESRM uses risk-management principles to manage security-related risks across an enterprise. ESRM does not define an organizational structure. Enterprise risk management (ERM) uses risk-management principles to address enterprise risk issues and often defines an organizational structure. The security department may be represented within an ERM program if one exists, but ESRM is simply the processes under which the security department manages security-related risks.

DIFFERENCE BETWEEN ESRM AND CONVERGENCE

ESRM is a risk-management process used to manage security risks regardless of reporting lines or organizational structures. Convergence relates to the degree of integration within organizational structures that combines physical-security and information-security teams. This could include the integration of processes, procedures, or tools for the purpose of aligning security responsibilities.

VISION, MISSION, AND GOALS OF ESRM

The Vision of ESRM is to manage the protection of an organization’s enterprise-wide assets, enabling the business to advance its mission.

The Mission of ESRM is to provide consistent identification, evaluation, and treatment of security risks to mitigate potential impacts to the business and prioritize protective activities.

The Goals of ESRM are to establish organizational policies, procedures, best practices, and capabilities to identify and manage security risks to the enterprise in an effective, consistent, and efficient manner.

CONCEPTS AND GUIDELINES FOR IMPLEMENTATION

An enterprise security risk management program must be built upon a culture of managing security risks that follows a common approach to risk management practices, which includes the following key components (see Figure 1 below):

1. **Identification and Valuation of Assets**
   a. Identification of assets and the proper stakeholder(s)/department(s) responsible for each asset. Valuating assets involves engaging stakeholder(s) in identifying the short- and long-term value, actual and perceived, of those assets, as well as their value in relationship to individual owners, departments, and/or relevance to the enterprise.

2. **Identify Security Vulnerabilities and Risks to Each Asset**
   a. Identification of risks and vulnerabilities includes the assessment of the intentional or unintentional exploitation of each vulnerability, the effect on each asset, and the potentially disruptive effect on the business and its goals if a vulnerability were to be exploited.

3. **Prioritize the Security Risk and the Security-Risk Relationship with Each Asset**
   a. An evaluation of security risks ensures that decisions can be made on which risk treatments can be implemented, and helps to prioritize the resources needed to address the identified security risks.

4. **Develop Risk Treatment Plans**
a. **Mitigation**: Mitigation processes, coordinated with the proper security risk stakeholder(s), serve to identify and develop available remediation plans. Proper assessment of these plans would measure the impact on the targeted risk. Mitigation plans could include:

i. *Termination of the activity that causes the security risk.*

ii. *Mitigation of the plans to limit the probability or impact of the security risk.*

iii. *Transferring the risk to another party, e.g., insurance.*

iv. *Acceptance of the risk.*

b. **Remediation**: Both security representatives and the risk stakeholder(s) have responsibility for implementing the mitigation and remediation plan. Simply because mitigation plans have been developed doesn’t mean that security’s role ends.

c. **Risk Governance**: If the security risk is to be accepted, the role of security is to verify that the proper security risk stakeholder(s) has evaluated the risk and ensure that the security risk is accepted at the appropriate levels (and by each security-risk stakeholder if necessary). Ensuring that security risks are accepted at the correct levels can be the most difficult part of the security role in ESRM. Escalation or broader conversations may be necessary to make sure that all of the security risk stakeholders are engaged in proportion to the risk and associated potential impact.

5. **Continuous Improvement**

a. **Intelligence Gathering**: Information can be gathered on evolving security threats through both reactive and proactive means. An “incident” can be a security event, an investigation, an article in the paper, a court decision, or other event.

b. **Root Cause Analysis and Post Mortem**: Throughout the incident response, security must examine and analyze the root causes of the incident to properly understand the nature of the threat as well as the potential controls that could help to avoid or mitigate similar events in the future. Issuing the post-mortem recommendations does not mean that these must be implemented, or that security should take on the role of implementing any recommendations; it is simply an acknowledgement of available remediation opportunities. Security professionals should not be the only ones weighing in on the recommendations. The post mortem should be distributed to every security risk stakeholder, as well as any responsible party engaged in managing security risks (e.g., internal audit, the controller, compliance, etc.).

c. **Reassess Security Risks**: After any event, a reassessment of the asset and the related security risk is necessary to gauge whether the risk’s impact has changed and if prioritizing of the security risk should occur. Reassessing security risks should occur on a regular basis (not just in response to an event) due to the changing nature of security risks. This could include a new threat, a change in the regulatory environment, a recent lawsuit, an unrelated security event that has gotten notoriety, or even a conversation with an executive.
CASE STUDIES

The case studies that follow will help to demonstrate ESRM concepts in practice.

**Who Owns a Lighting Problem?**

A security practitioner is conducting a security assessment at a retail establishment. A recommendation to light the parking lot was previously made and turned down by the finance group as excessive. The finance group, one of the risk owners, has accepted a security risk. The security practitioner feels that there is still an existing risk to customers and employees due to inadequate lighting, and that this risk was not accepted by the proper risk owners.

The security practitioner uses ESRM principles as follows:

1. **Identify and Quantify the Enterprise’s Assets.** In this scenario, the assets to be protected are customers and employees; risks to cash movement; and potential liability issues should a security event occur.

2. **Identify and Quantify Security Risks to Each Asset.** The risks identified in this scenario are crimes occurring in the parking lot and various safety issues.
3. **Prioritize the Security Risk and the Security Risk Relationship with Each Asset.** The lighting in the parking lot has a direct relationship to crime targeting customers and employees. The prioritizing of this risk may change based on how the company places value on its customers, employees and any concerns of liability. The prioritization of this risk may be based on prior events at that location, crime statistics in the area, or even an article in the local newspaper bringing attention to crimes in parking lots that may be unrelated to the practitioner’s company.

4. **Develop Risk Treatment Plans.** The security professional will work with each asset owner to discuss the continued risk. The asset owner may be the customer care managers, human resources, legal team, and potentially others. The discussion about the risk should allow others to weigh in. The group should walk through the potential mitigation plans:
   a. **Terminate the risk.** Don’t build the store there. This is not the likely option.
   b. **Mitigate the risk.** Use commonly accepted security principles to reduce the risk of an incident. For example, add more lighting.
   c. **Transfer the risk.** For example, add insurance
   d. **Accept the risk.** There may be agreement by the risk owners to simply accept the existing level of risk. At this point, as long as the correct risk owners were consulted, the security practitioner’s involvement in this process is complete and the risk acceptance is appropriate.

5. **Continuous Improvement.** The security group will always monitor events and the environment for risk-changing factors that may cause the risk and the prioritization to change. This could include an event in which criminal activity occurred, statistics indicating that crime in the area has increased, incidents where employees have complained for their safety, and so on.

**An Event Faces Unexpected Risks**

A security manager was contacted by the marketing department concerning a special event that will take place at a high-profile location in midtown Manhattan. The security manager conducts an assessment of the event, focusing on the attendees, venue and surrounding locations, and citywide events that will take place simultaneously. The security manager then provided the completed protective-services proposal to the marketing department. The proposal detailed a strike and protest scheduled to occur on the same block as the event’s venue. The proposal effectively mitigated the potential risks by a deployment of security resources and preplanned ingress and egress routes.

However, the proposal was challenged by the marketing department and turned down due to the inconveniences the rerouting of arrivals and departures would create. The marketing group has chosen to accept the risk to employees and guests. However, the security manager determines that the owners of this security risk are legal, human resources, safety, and the executive-services group. The security manager feels that this is risk needs to be elevated to the appropriate departments to work through ESRM principles:
1. **Identify and Quantify the Enterprise’s Assets.** In this scenario, the assets are the safety of the employees, executives, and guests of the company during the special event.

2. **Identify and Quantify Security Risks to Each Asset.** The risk is the potential of protest activities spilling over into the ingress and egress of the events. Additionally, due to the volume of activity within the confined area, there is a concern for the potential increase of crimes against visitors to the event.

3. **Prioritize the Security Risk and the Security Risk Relationship with Each Asset.** Crimes against persons attending the event and disruption of the overall event are the prioritized risks of this event.

4. **Develop Risk Treatment Plans.** The security manager works with the asset owners to discuss the overall risk. The discussion surrounding the risk of the event should allow each party to weigh in and determine what steps should be taken or if the risks should be accepted.
   a. **Terminate the risk.** Either cancel or postpone the event.
   b. **Mitigate the risk.** Implement all or a portion of the controls/countermeasures highlighted in the proposal.
   c. **Transfer the risk.** Add insurance.
   d. **Accept the risk.** After the risk owners are consulted, there may be agreement to simply accept the existing level of risk. At this point, as long as the correct risk owners were consulted, the security practitioner’s involvement in this process complete and the risk acceptance is appropriate.

5. **Continuous Improvement.** The security group will always monitor events and the environment for risk-changing factors that may cause the risk and the prioritization to change. This could include an event in which criminal activity occurred, statistics indicating that crime in the area has increased, incidents where employees have complained for their safety, and so on.

**Payment Center Problems**

A security professional is contacted by the facilities and real-estate department seeking approval on the security-system design for the new model of payment centers. The security practitioner reviews the plans and identifies numerous vulnerabilities with the design. The security practitioner creates a new proposal which effectively mitigates the potential risks. The new proposal is turned down by the facilities and real-estate department due to the increase in security-system cost. The facilities and real-estate department has chosen to accept this security risk but the security professional recognizes that the true owner of this security risk is the payment services group. The security practitioner feels that this is still an existing security risk to customers, employees, and financial assets due to an inadequate security design.

The security practitioner relies on ESRM concepts to plan next steps:

1. **Identify and Quantify the Enterprise’s Assets.** The assets identified here are safety of the customers, employees, and the income received during payment transactions.
2. **Identify and Quantify Security Risks to Each Asset.** The risks in this scenario are crimes against persons occurring within the payment center and fraudulent transactions or theft of financial assets by employees and/or contractors.

3. **Prioritize the Security Risk and the Security Risk Relationship with Each Asset.** Customer and employee safety and the security of financial assets have a direct relationship with the crimes targeting cash transactions in the payment centers. The prioritization of this risk may be based on the volume and value of anticipated transactions, prior events at like-owned facilities, or crime statistics in similar non-owned facilities.

4. **Develop Risk Treatment Plans.** The security practitioner will work with the primary risk owner to discuss the identified security risks. The discussion will focus on the facts surrounding previous events and the mitigating controls or countermeasures for each of those respective risks. The asset owner can then choose to accept or mitigate the risk for each control or countermeasure within the proposal.

5. **Continuous Improvement.** If there are certain risk controls which are not implemented, the security practitioner will work with management and the payment center management team to identify future financial resources when they become available. The security group continuously assesses events at like facilities and provides updated countermeasures accordingly.

### Field Access to Information

The CIO group is working with the leadership team to develop strategies which will enhance customer relationships. Enhanced capability and productivity of the field-consulting workforce is targeted. The core of idea is to enable the workforce to achieve longer productive periods at client premises and enhance interactions with them.

One proposed strategy centers on the organization making its proprietary tools, data, and consulting processes available to its consultants in the field, instead of solely within the office. The security group is consulted because some of the processes and methods utilized are trade secrets which differentiate the business and give it a competitive advantage. There are also concerns about the proprietary database of data becoming exposed or copied.

The consulting group has made a strong case for access to the tools and data, speculating about additional ROI to the business, and have also suggested utilization of **Bring Your Own Device (BYOD)**. The security professional engages the business stakeholders in a consultative fashion using ESRM processes to evaluate the asset value, vulnerabilities, and risks to the business.

1. **Identify and Quantify the Enterprise’s Assets.** The assets are the trade secrets used by the knowledge workers. The security group works with several stakeholders in the business including consulting and legal to identify and value the assets which consist of proprietary
consulting methods and processes, and data in proprietary databases. The economic value of the information assets to the business is identified.

2. **Identify and Quantify Security Risks to Each Asset.** The risks to the trade secrets and data are *confidentiality* (risk of unauthorized exposure); *integrity* (risk of corrupting or destroying core data); and *availability* (continued access by practitioners to do their job). Fewer concerns exist around integrity or availability. An ALE (annualized loss expectancy) is already known for smartphone and laptop technology which is an appliance containing or accessing the information.

3. **Prioritize the Security Risk and the Security Risk Relationship with Each Asset.** Unauthorized access to a complete trade-secret process has a direct relationship to the security of the information appliance, the workflow and structure of the software, the motivation of the individual to help protect the trade secret, and the effectiveness of security culture and controls.

4. **Develop Risk Treatment Plans.** After help from security to value the information assets, the business owner realizes that the financial impact of trade-secret exposure exceeds the designated financial authority of any single leader, and thus will require Board approval. A case is provided to the Board with the CSO supporting the business owner. The Board considers on a risk-reward basis and the proposal from the business and approves the plan for risk treatment. The risk treatment involves several steps.

The first step in the risk strategy is to significantly reduce the impact that exposure of the trade secret would have, by breaking the trade-secret process into several pieces, and implementing each piece in different parts of the enterprise software, so that the entire secret cannot be exposed at any given time.

Further steps to decrease the likelihood of exposure of the trade secret include undertaking a secure-software design in partnership with IT. An information-security awareness culture is implemented which trains and provides incentives to field practitioners in line with company culture.

Technical controls at implementation time include encryption and strong-authentication technologies. Further mitigation is achieved by use of thin-client software which limits access connectivity and access to core system resources.

5. **Continuous Improvement.** Security and the business owner will monitor incidents according to the target metrics developed and agreed.
Acknowledgements (in alphabetical order)

Recognition is given to the following individuals who have donated their time and energy to assist in the research, development and preparation of this documentation which defines and explains Enterprise Security Risk Management.

Marene Allison  
Johnson & Johnson

Brian Allen, CPP  
Time Warner Cable

Shayne Bates, CPP  
LMC Consulting Group

Kevin Donovan  
Johnson & Johnson

Peter Piazza  
ASIS International

John Petruzzi, CPP  
Time Warner Cable

John Turey, CPP  
TE Connectivity

Version: February 4th 2014

January 30, 2015