Enterprise Security Risk Management
A Foundation of Enterprise Risk
ESRM is a strategic security program management approach that ties an organization’s security practice to its mission and goals using globally established and accepted risk management principles.
Security is About Risk Management

• Managing the security decision making process requires:
  • Educate business partners
  • Present potential security strategies
  • Implement the business leader’s choice
  • Document the residual risk and continue educating your business partners
ESRM and Security

- A mature ESRM program encompasses all aspects of security risk mitigation practices to prevent security risk impacts to the enterprise.
- Value exists because the business owns the security risk, therefore, we now provide business deliverables.
What ESRM isn’t

• It’s not “convergence”:
  • Converged integrates IT and Physical under one team
  • The degree of integration identifies the degree of convergence
  • First efforts were based on budget

• It’s not Enterprise Risk Management:
  • ERM manages all company risk
  • ESRM is a component of ERM
  • ESRM uses similar philosophy to manage security risks
So, Why ESRM?

• You gain intimate knowledge of your organization
• You get to speak to diverse stakeholders, and learn what they consider is important to them and the company
• You learn your organization’s business objectives
• You identify risks and help the business achieve objectives
• You support the legal responsibilities of the business
So, Why ESRM?

• You become “aware” of your role in the organization:
  • Identify risks to the right executive
  • Provide objective perspective on the risk(s)
  • Let the executive decide

• We don’t “accept” risks – that’s not our job!

• We identify risks, and provide SME during the risk management process
So, Why ESRM?

• Organizations have a risk based view of the protection of the business across all relevant fields. Such as, business continuity, cyber risk, personnel vetting
• Provides security structures which are best practice and defensible
So Now... ESRM HOW?
What is Risk Anyway?

Risk = Threat Event $\times$ Impact to the Organization $\times$ Probability

- You must choose...
- The world changes, so does risk
- Risk is like water
- There is always residual risk
- Define success & failure
First and foremost, you need to understand your enterprise:
- What the business does? Why? How?
- Overall enterprise objectives and priorities?
- The mission – has it changed since you started? New Products? New business models?
- What environment does the enterprise operate in?
Fundamentals of ESRM

- Who are your stakeholders?
- Who owns the business?
- Who controls the assets that need to be protected?
- Who makes the final decisions about those assets?
- ESRM is built on the concept of transferring the responsibility for security and risk decisions to the appropriate people who are responsible for the assets.
The ESRM Life Cycle

- **Identify and Prioritize Assets:** The process of identifying, understanding, and prioritizing the enterprise’s assets.

- **Identify and Prioritize Risks:** Identifying, understanding, and prioritizing the security risks to the enterprise and their relationship to the assets value.

- **Mitigate Prioritized Risks:** Taking the necessary, appropriate, and realistic steps to protect against the most serious security threats and risks.

- **Improve and Advance:** The risk paradigm of managing security risks is a cyclical approach to continuously improve and advance the security posture of the enterprise.

* Figure 1-1. The Phases of the ESRM Life Cycle, *Enterprise Security Risk Management: Concepts and Applications*
ESRM Essentials for Success

- Transparency
- Independence
- Authority
- Scope
ESRM Essentials for Success

- Be open and honest with your stakeholders about:
  - What security is doing.
  - Why security-related tasks are being performed.
  - What risks those tasks are mitigating. (How they fit into the program)
  - Who (which risk stakeholder) made the decisions to perform the security tasks.
  - What we need from them to ensure the ongoing protection of enterprise assets.
ESRM Essentials for Success

- Consider security vulnerabilities wherever they exist.
- Identify risks and maintain risk transparency.
- Understand all business operations and the business’ assets.
- Respond to an incident, investigate, and clearly identify its root causes in any area of the enterprise.
ESRM Essentials for Success

This is not about being the “boss” or the “enforcer”.

• Authority is the ability of the security manager to:
  • Access the appropriate level of business leader to discuss security risk issues.
  • Escalate security risk decisions to higher levels of leadership, if necessary.
  • Discuss security risks with complete transparency at all levels of the organization.
  • Investigate security incidents in any area of the enterprise, as needed
ESRM Essentials for Success

• Scope is the direction given to your department by the Business. Which risks fall into the realm of “security risk” and which do not.
References

- ISO 704, Terminology work — Principles and methods
- ISO 860, Terminology work — Harmonization of concepts and terms
- ISO 3534-1, Statistics — Vocabulary and symbols — Part 1: General statistical terms and terms used in probability
- ISO 9000, Quality management systems — Fundamentals and vocabulary
- ISO 10241, International terminology standards — Preparation and layout
- ISO 31000:2009, Risk management — Principles and guidelines
- ISO/IEC Guide 2, Standardization and related activities — General vocabulary
- ISO/IEC Guide 51, Safety aspects — Guidelines for their inclusion in standards
ESRM @ ASIS
2018 Update
ESRM Board Initiative: Background

• In 2016, the ASIS Board of Directors determined that Enterprise Security Risk Management (ESRM) would be a driving underlying force in the global ASIS, International strategic plan.

• Goal: “to make ASIS members more effective security professionals and more valuable members of their organizations by enabling them to better identify and manage the various aspects of security risks they face... [leading to an] empowered membership, safer enterprises, a more strategic approach to risk, and a more cost-effective security function”.
ESRM Board Initiative: 2018

• Our Board of Directors has made a significant commitment to integrating the principles of Enterprise Security Risk Management into the very fabric of ASIS.
• Our entire library of security programs and practices are now undergoing an ESRM approach.
ESRM Board Initiative: Project Scope

• The 2018 project managed four working “Value Streams”

  - ESRM Framework Standards and Guidelines
  - ASIS Member ESRM Education / Certification / Research
  - Internal and External ESRM Marketing / Communications / Branding
  - ESRM Tool / Matrix / Model

  ESRM DNA
ESRM Board Initiative: Accomplishments

- Draft ESRM Guideline:
  - URL HERE
- ESRM Education at GSX
- ESRM articles and Communications in Security Management Magazine and ASIS Connects
- Coming in 2019!
  - Dedicated community area for ESRM topics on ASIS Connects
  - Online ESRM Webinars and Education
  - ESRM Program Maturity Assessment Tool
  - June 2019 – ESRM Workshop in Atlanta, GA
<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Session Details</th>
<th>Speaker/s</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sunday, Sept 23</td>
<td>The ESRM Lifecycle and Convergence of Physical and Cyber Security</td>
<td>David Feeney, CPP Rachelle Loyear</td>
<td>Pre-Conference Workshop</td>
</tr>
<tr>
<td>8:00am – 5:00pm</td>
<td>(Additional Fee Required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monday, Sept 24</td>
<td>Bring Better Data to Top Management</td>
<td>Brian McIlravey, CPP Jeff Sieben</td>
<td>Panel Discussion</td>
</tr>
<tr>
<td>10:30am – 11:45am</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monday, Sept 24</td>
<td>ESRM and ASIS: Know More About Enterprise Security Risk Management</td>
<td>Rachelle Loyear Tim McCreight, CPP Tim Wenzel, CPP</td>
<td>Panel Discussion</td>
</tr>
<tr>
<td>10:30am – 11:45am</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monday, Sept 24</td>
<td>Practical Tools for Complex Risk Management Assessments</td>
<td>Genevieve LeDuc Derrick Stewart</td>
<td>2-Hour Workshop</td>
</tr>
<tr>
<td>2:00pm – 4:00pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monday, Sept 24</td>
<td>Running on a Shoestring Budget: A Case Study</td>
<td>George Hainer Aaron Juarez Nick Weber, CPP PSP</td>
<td>Case Study</td>
</tr>
<tr>
<td>3:45pm – 5:00pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuesday, Sept 25</td>
<td>What You Need to Know About ESRM</td>
<td>Rachelle Loyear Tim McCreight, CPP Brian McIlravey, CPP</td>
<td>Panel Discussion</td>
</tr>
<tr>
<td>11:00am – 12:15pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuesday, Sept 25</td>
<td>Is Enterprise Security Risk Management Relevant to Retail Asset Protection?</td>
<td>Alan Greggo, CPP</td>
<td>Panel Discussion</td>
</tr>
<tr>
<td>2:00pm – 3:00pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuesday, Sept 25</td>
<td>Manage Your Security Organization Through ESRM</td>
<td>Tim McCreight, CPP Tim Wenzel, CPP</td>
<td>Panel Discussion</td>
</tr>
<tr>
<td>2:00pm – 3:00pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuesday, Sept 25</td>
<td>Securing Big Data in an Evolving Regulatory Landscape</td>
<td>Gary Bucholtz</td>
<td>Lecture</td>
</tr>
<tr>
<td>3:30pm – 4:30pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuesday, Sept 25</td>
<td>ESRM Best Practices for Security Leaders in Complex Environments</td>
<td>Nathan Monshin</td>
<td>Case Study</td>
</tr>
<tr>
<td>3:30pm – 4:30pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wednesday, Sept 26</td>
<td>Security Risk Versus Compliance: A Cultural, Technical, and Budgetary Shift</td>
<td>Daniel Renfroe, PSP Nancy Renfroe, PSP</td>
<td>Case Study</td>
</tr>
<tr>
<td>11:00am - 12:15pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wednesday, Sept 26</td>
<td>Building a Brand for a Security Department</td>
<td>Jim McConnell</td>
<td>Lecture</td>
</tr>
<tr>
<td>3:45pm – 4:45pm</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Join Us!

• The ESRM Program is looking for dedicated security professionals who are using the principles of ESRM in their careers, and want to help ASIS and this project move further down our ESRM path.

• Contact us directly at esrm@asisonline.org to volunteer!