SECURITY AND RESILIENCE MANAGEMENT - MITIGATING RISK FOR YOUR ORGANIZATION
SPEAKERS

• Dennis Blass, CPP – Children’s of Alabama
• Lisa DuBrook, CPA – Radian Compliance, LLC
• Jim Leflar, CPP, CBCP, MBCI – Zantech IT Services
• Marc Siegel, Ph.D. – San Diego State University and M Siegel Associates LLC
SESSION OVERVIEW AND OBJECTIVES

• Panel Discussion – Perspectives on Resilience
  ➢ What is organizational resilience or what is a resilient organization?
  ➢ When does an organization move from an ad-hoc approach to a formal structured approach?
  ➢ What is the advantage of breaking down siloes?

• Change Management – Issues/Recommendations

• New Security and Resilience Standard – The recipe book

• Questions
WHAT IS ORGANIZATIONAL RESILIENCE OR WHAT IS A RESILIENT ORGANIZATION?

- Resilience is an aspirational objective – there is no endpoint nor is there one-size-fits-all.
- Organizations become more resilient by fully integrating proactive management of risk into their system of management.
  - Everyone is seen as a risk maker and risk taker, therefore, a risk manager.
  - Emphasis is placed on security and risk awareness throughout the organization.
  - The management of risk is viewed through the front windscreen, not out the rear-view mirror.
  - Risk is considered at the strategical, tactical, operational, and reputational levels.
  - Organizations are not viewed as islands but as part of a value chain.
  - It is an iterative process where you learn from mistakes.
Organizational resilience is a strategic approach to enhancing the unfettered system-wide interactions (risk, communications, cooperative relations, and social capital) in the holistic organizational environment (internal and external – includes supply chain).
WHEN DOES AN ORGANIZATION MOVE FROM AN AD-HOC APPROACH TO A FORMAL STRUCTURED APPROACH?

• The focus of any formal structured approach should be enhanced risk and business management. The move to a formal approach may be driven by:
  • Contractual requirements and client demands;
  • The need to demonstrate reliability in a supply chain;
  • The need to improve business performance and support future market development including market expansion;
  • Legal and liability protection; and
  • The need for data- and information-based business decision making.

• Certification to a standard should not be a driver – rather it is a distraction. Let it be the gravy at the end of successful implementation.
  • Implementation should be tailored to the organization’s system of management, not just the standard.
WHEN DOES AN ORGANIZATION MOVE FROM AN AD-HOC APPROACH TO A FORMAL STRUCTURED APPROACH? CON’T.

• OR becomes a formal approach when management begins to organize and recognizes the OR outcomes.

• Groups and org. culture can have informal elements.

• Communication channels are both formal and informal.

• The processes that make up the organizational system(s) can be both formal and informal – both are powerful/influential.
WHAT IS THE ADVANTAGE OF BREAKING DOWN SILOES?

• Increase communication effectiveness
• Share resources – more effective
• Risk is risk – entire organizational issue
• Increase the opportunity for social capital
WHAT IS THE ADVANTAGE OF BREAKING DOWN SILOES? CON’T.

• An efficiently run organization will have a single risk-based, information-based system of management focused on outcomes and opportunities.

• Objectives need to be considered on the strategic, operational, tactical, and reputational level enterprise-wide, division-wide, and locally.

• Security and risk management support the creation of value – they are part of the operating system.

• Security and risk awareness, communication, and training promote a culture of resilience by incorporating them in all aspects of the business.

• An integrated and holistic approach maximizes precious resources and minimizes duplication of efforts.

• Breaking down silos enhances the collaborative effort needed to address complex multi-disciplinary issues that organizations and their supply chains must address in the global market.
CHANGE MANAGEMENT ISSUES

• Resistance to Change:
  • General uncertainty about the change (Kennedy, 2011);
    • cynicism, dubious trust of leadership, and employee’s lacking confidence in each other;
  • Institutional resistance to change (Agocs, 1997);
    • Organization is slow to change;
  • Poor implementation by manager (Gilley, Gilley & McMillan, 2009);
    • Poor planning and preparation;
  • Senior leadership avoiding unknown risk (Lane, McCormack & Richardson, 2013);
    • Avoiding initiative is better than creating risk problem.
• Change failures caused by human actions, not technical.
CHANGE MANAGEMENT RECOMMENDATIONS

• Gain firm, personal approval from the CEO;

• Ensure CEO will continue to support the change initiative;

• Develop a marketing strategy for the change initiative;

• Communicate the personal importance of the initiative to the employees as well as the organizational importance;

• All employees must understand the value of the change.
CHANGE MANAGEMENT RECOMMENDATIONS

• Multi-methods of distribution (e.g., multimedia displays, newsletter, intranet messages, and team meetings);

• Seek and recruit employee involvement in the change;

• Ensure employees see involvement is necessary for success;

• Active participation increases the likelihood of personal association with the initiative.

• Pace change to the local culture and to promote success breeding success.
CHANGE MANAGEMENT RECOMMENDATIONS

• Implement a formal repeatable process consistent with organization’s culture;

• Routine status updates and reinforce the value, importance, and personal benefits to all participants;

• Top leader must be involved in the routine meetings or marketing messages;

• Leader must be seen showing absolute, sincere involvement and commitment to the initiative;

• Provide symbols of recognition from top leadership - helps maintain motivation, commitment, & personal recognition with the initiative.
STANDARD: SECURITY AND RESILIENCE IN ORGANIZATIONS AND THEIR SUPPLY CHAINS

• ANSI/ASIS Standard - ORM.1 which combines 3 previous ASIS Standards
  • SPC.1, PAP.1 and BCM.1

• Provides a risk based systematic, country-neutral approach to identify, assess, and manage risks related to an organization's operations and its supply chain.

• Places an increased emphasis on an organization’s supply chain

• Uses enterprise risk management perspective, emphasizing:
  ➢ Proactive risk and business management to support a process of prevention, protection, preparedness, readiness, mitigation, response, continuity, and recovery from undesirable and disruptive events;
ORM.1 is a holistic framework which takes into account:

- Context of the organization and its supply chains;
- Legal, regulatory, and contractual obligations and voluntary commitments;
- Needs of internal and external stakeholders;
- Uncertainties in achieving its objectives;
- Protection of human, tangible and intangible assets, and
- Continual improvement.
WHY ORM.1?

• ORM.1 enables an organization to:
  • Develop an ORMS policy;
  • Establish objectives, procedures, and processes to achieve the policy commitments;
  • Develop processes to assure competency, awareness, and training;
  • Set metrics to measure performance and demonstrate success;
  • Take action as needed to improve performance;
  • Demonstrate conformity of the system to the requirements of this Standard;
  • Establish and apply a process for continual improvement.

• ORM.1 and CPP - Either the new standard or the legacy standards may be used to study for the CPP exam
CHANGE MANAGEMENT REFERENCES


CHANGE MANAGEMENT REFERENCES


CHANGE MANAGEMENT REFERENCES


CHANGE MANAGEMENT REFERENCES


HOW TO REACH US

• Dennis Blass –
  • Email address - [Dennis.Blass@childrensal.org](mailto:Dennis.Blass@childrensal.org)

• Lisa DuBrock – 847-997-2032
  • [LDuBrock@RadianCompliance.com](mailto:LDuBrock@RadianCompliance.com)

• Jim Leflar – 267-300-1139
  • [JLEFLAR@AOL.COM](mailto:JLEFLAR@AOL.COM)

• Marc Siegel – 858-405-9855
  • [siegel@msiegel.net](mailto:siegel@msiegel.net)
Questions?