Building Resiliency into Your Security Program

ASMGi

INFORMATION SECURITY SUMMIT
Building Community Through Education

Charlotte ISSA Summit May 10, 2018

Introduction

linkedin.com/in/garyjsheehan/

Gary Sheehan

As CSO of ASMGi, Gary has responsibility for all security matters of the organization and is responsible for managing the design, delivery and implementation of GRC customer solutions.

Abstract

Are you satisfied with your security program and its effectiveness, or is it time to take a new approach to protecting your organization and your organization's assets?

Agenda, Overview and Objectives

- Understanding Resiliency
- Using Resiliency Concepts for Security and Security Concepts for Resiliency
  - People
  - Process
  - Technology
- Wrap Up

Understanding Enterprise Resiliency

Enterprise Resiliency

Resiliency is the ability of an organization to anticipate, prepare for, and respond and adapt to incremental or chronic change and sudden disruptions, as well as minor everyday events and acute shocks in order to survive and prosper.

- Resiliency is a strategic objective intended to help an organization to survive and prosper.
- Resiliency is a goal, not a fixed activity or state.
- Resiliency is a relative, dynamic concept and, as such, an organization can only be more or less resilient.
- Resiliency is not just disaster recovery and business contingency planning.

Understanding Enterprise Resiliency

Enterprise | Organization | Company | Business

- Not necessarily interchangeable, but are often used to mean the same thing.
- Can represent a hierarchy within a company.
- Be aware of the subtle difference in meanings between organizations.

Understanding Enterprise Resiliency

Enterprise Resiliency is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity.

Governance, Risk and Compliance are critical components to Enterprise Resiliency.

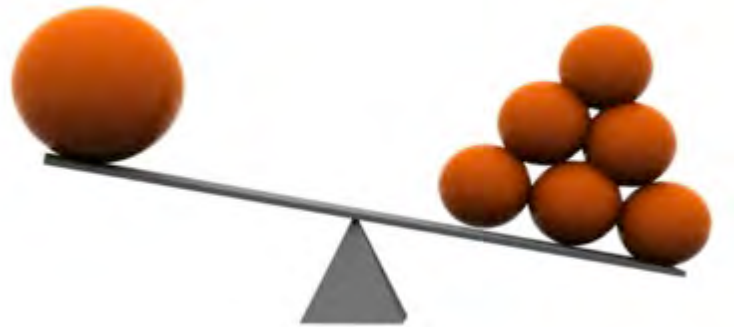
Understanding Enterprise Resiliency

Security Program Resiliency

You know your Security Program is resilient when:

- It can anticipate, prepare for, and respond and adapt to incremental or chronic change and sudden disruptions in the organization
- It can anticipate, prepare for, and respond and adapt to incremental or chronic changes in your organization's business, security and compliance requirements.
- It can anticipate, prepare for, and respond and adapt to incremental or chronic changes in the threats, threat agents and threat trends that affect your organization.

Benefits / Challenges



Each organization comes to its own decisions on these issues according to the amount and type of risk it is willing to pursue or retain, and the amount it is willing to invest in resilience.

Understanding Enterprise Resiliency

Benefits of Resiliency

- **Competitiveness:** The behaviors that an organization develops as part of a resilient culture can also help to build innovation and common values and vision, and develop an ability to anticipate and adapt to change and evolve the business model.
- **Coherence:** Resilience both requires and allows organizational silos to become more integrated and interoperable.
- **Efficiency and Effectiveness:** Working within a coherent and integrated framework has time- and cost-saving implications.

Understanding Enterprise Resiliency

Benefits of Resiliency (continued)

- **Reputation:** The coherent framework built by resilience supports the organization in understanding and acting on the interdependency of brand, trust and reputation, thereby managing and enhancing its reputation.
- **Societal/community Resilience:** Resiliency can also give assurance to other interested parties, such as regulators, third parties, government, customers, partners and shareholders.

Understanding Enterprise Resiliency

Challenges

- Understanding when to take action.
- Resolving potential tensions between cost and resilience in building just-in-time processes and just-in-case redundancy.
- Determining an appropriate trade-off between controlling costs and achieving greater resilience.
- Identifying when to embrace new values rather than persisting with existing behaviors.

Understanding Enterprise Resiliency

Challenges (continued)

- Resolving conflicts between the need to keep information from competitors and the need to share information for resilience when collaborating with others.
- Identifying legal and regulatory constraints, as well as voluntary codes adopted by different sectors, that can limit desirable resilience actions.

Each organization comes to its own decisions on these issues according to the amount and type of risk it is willing to pursue or retain, and the amount it is willing to invest in resilience.

RESILIENCY

The New Model For Security

Resiliency – The New Model For Security

ASMGi

BASED ON FRAMEWORKS

A framework is an extensible structure for documenting and implementing a set of concepts, processes, methods, technologies, procedures and cultural changes necessary for a complete product.

By aligning the framework objectives to enterprise strategies, the framework helps to keep the focus on achieving the goals of the enterprise.

Provides :

Consistency

Standardization

Measurement

Efficiencies

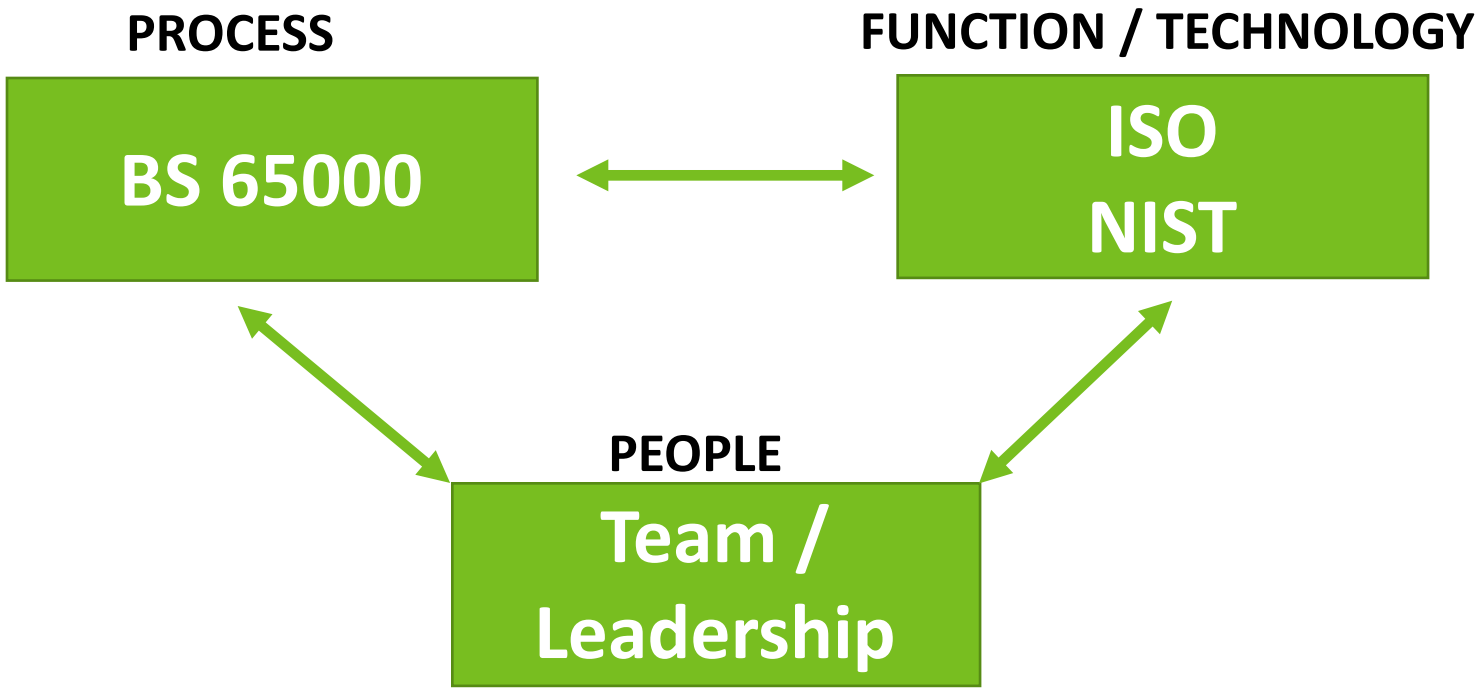
Resiliency – The New Model For Security

PROCESS

FUNCTION / TECHNOLOGY

PEOPLE

Resiliency – The New Model For Security



Resiliency – The New Model For Security

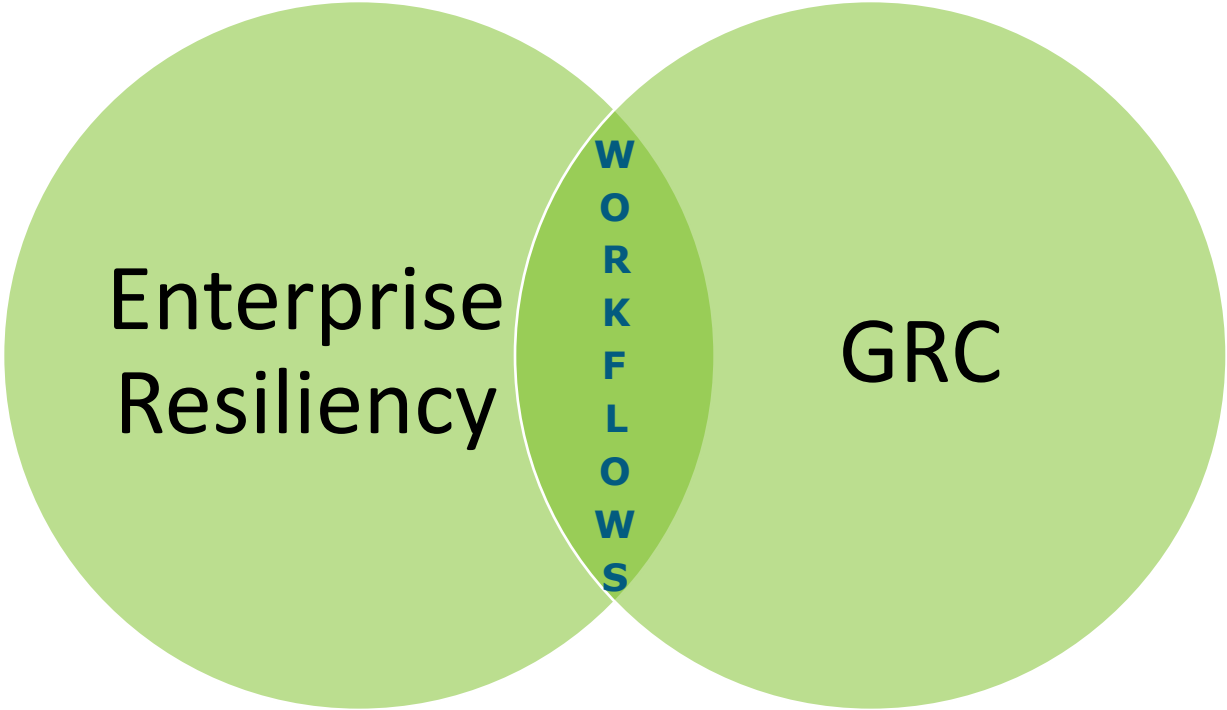
This model will provide:

- Clarity
- Commitment
- Alignment
- Collaboration
- Standardization
- Measurement

This model requires:

- Cultural Change
- Commitment
- Accountability
- Leadership
- Participation
- Support

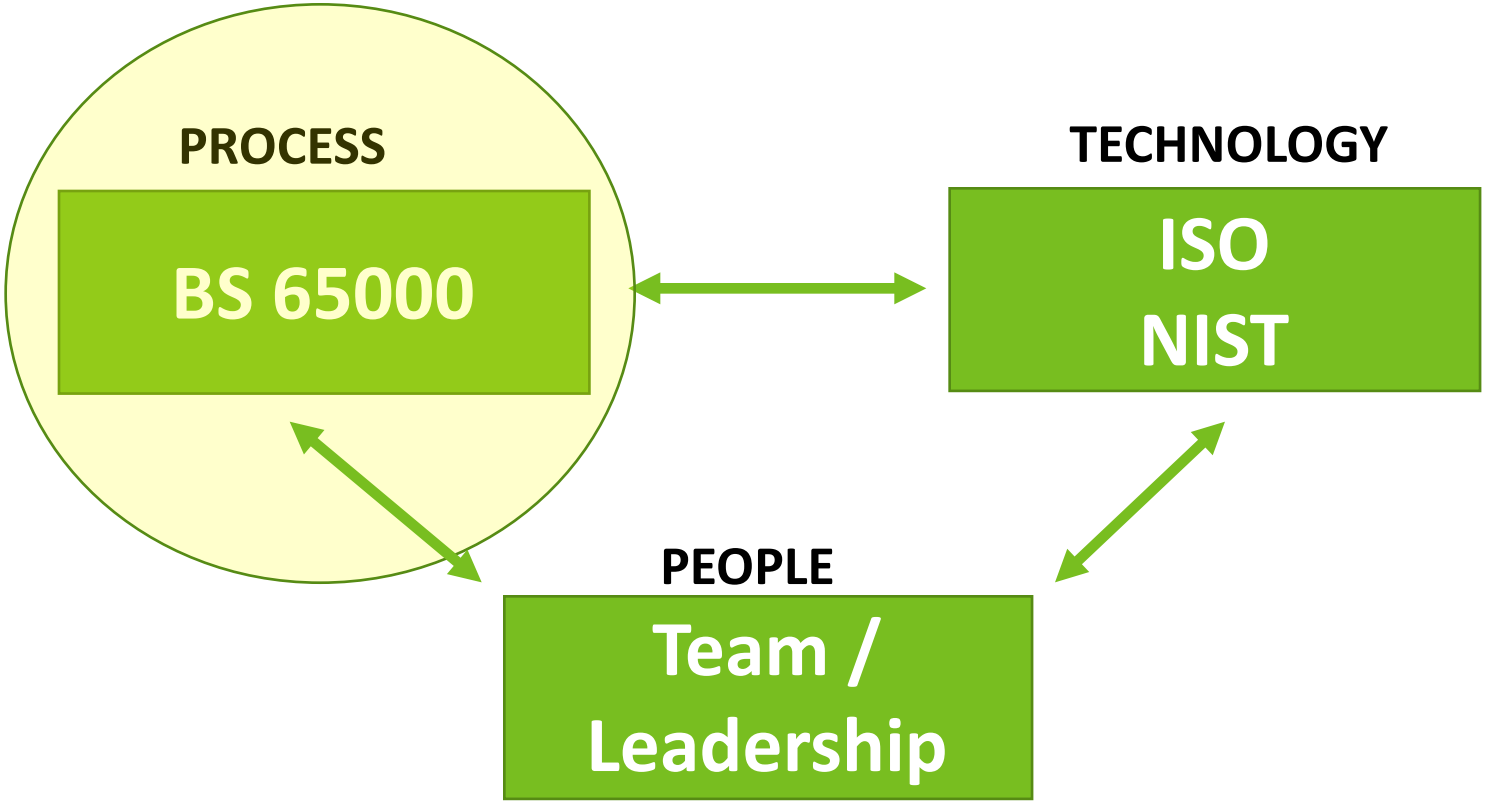
Resiliency – The New Model For Security



Understanding Enterprise Resiliency

Are You Informed, Aligned and Engaged?

Resiliency – The New Model For Security



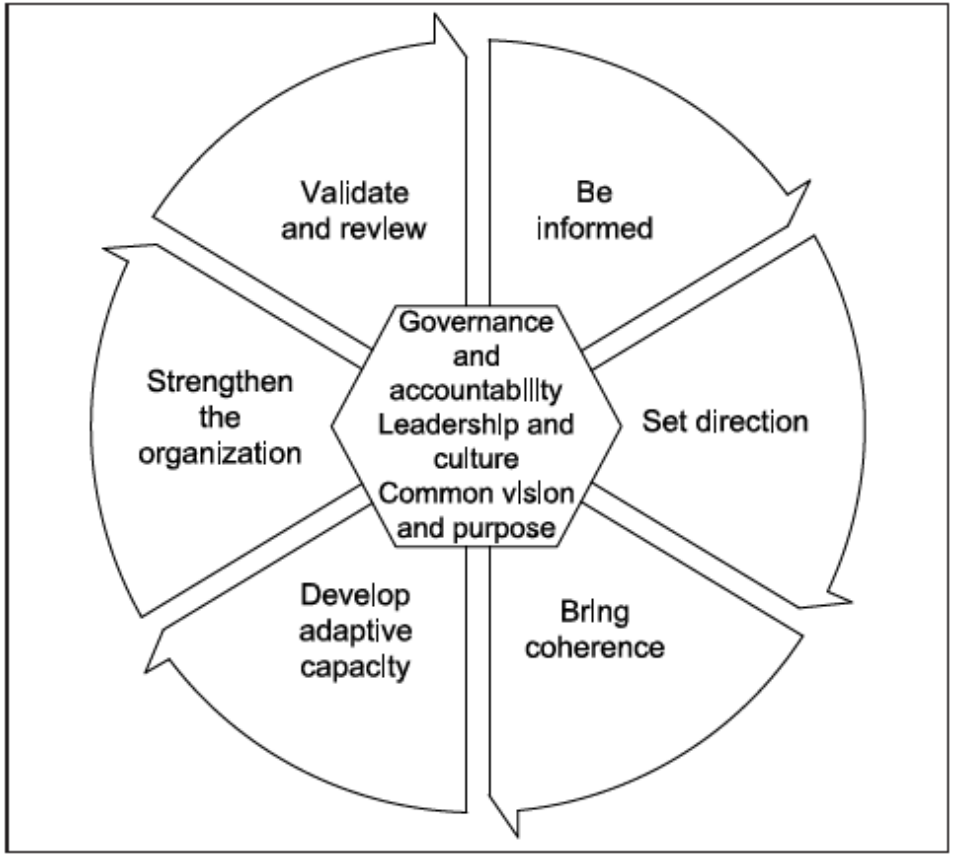
BS 65000:2014

BS 65000:2014 gives guidance on building enterprise resilience by:

- Clarifying the nature and scope.
- Identifying the principal components of resilience.
- Identifying and recommending good practice.

BS 65000:2014

Actions necessary to make the organization more resilient.



The British Standards Institute - 2014

Resilience requires the ability to make good decisions informed by an understanding of what the organization stands for and where it is trying to go, the organization's environment, what matters to the organization and what resources it has at its disposal.

BS 65000:2014

Building a Foundation for Resiliency

The fundamental attributes define the attitudes that shape decisions and actions, and ultimately underpin resiliency are:

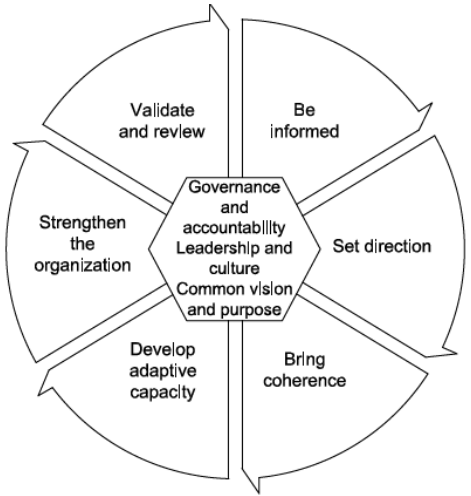
- **Governance and Accountability**
  - The systems of rules, structures and processes that drive coherent decision making within acceptable parameters of cost, risk and speed contribute to resilience.
- **Leadership and Culture**
  - Staff should be appropriately empowered by a culture of trust, openness and innovation.
- **Common Vision and Purpose**
  - Should be recognized and shared throughout the organization.

BS 65000:2014

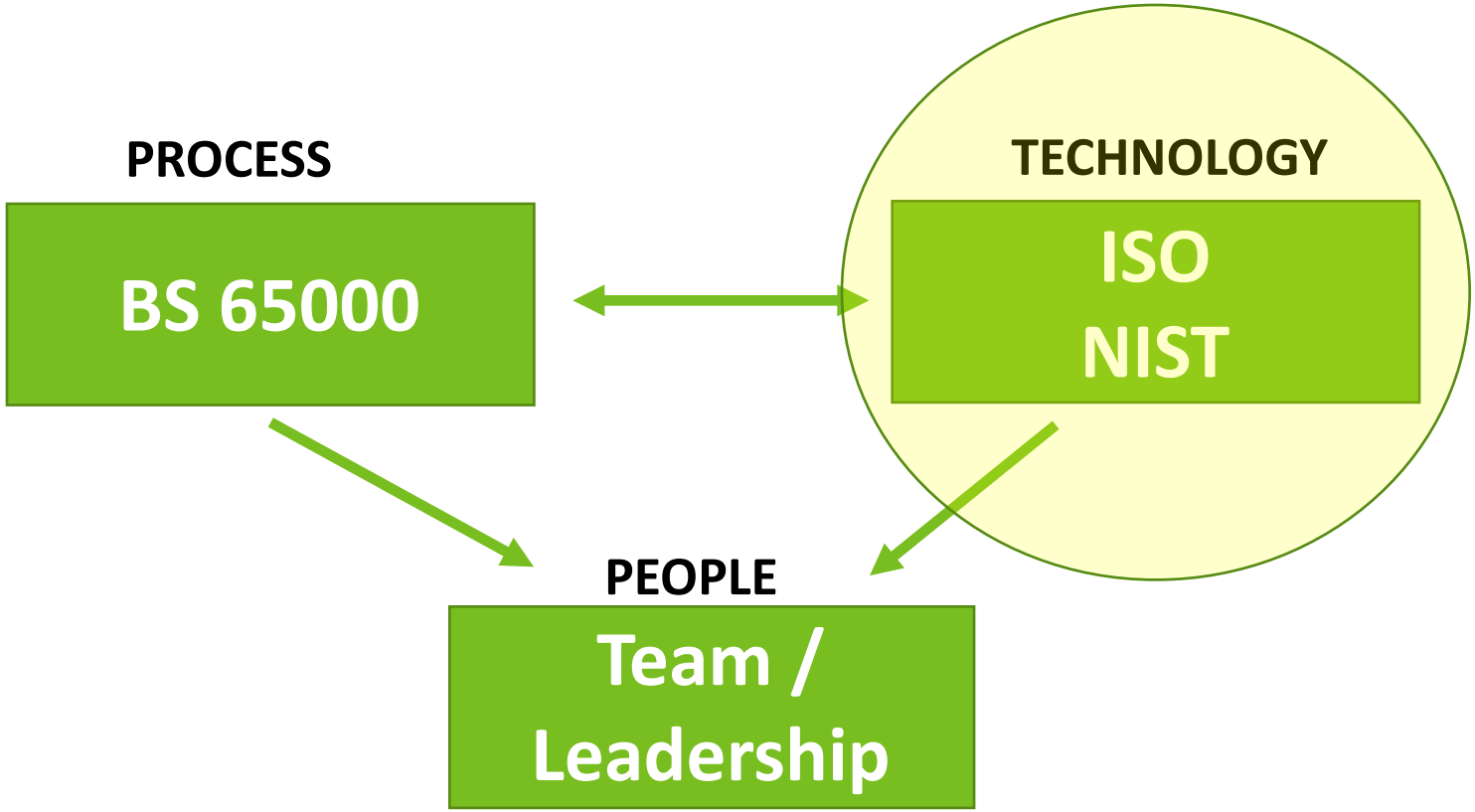
Building Resiliency

Resiliency requires the ability to make good decisions informed by an understanding of what the enterprise stands for and where it is trying to go, the business environment, what matters to the enterprise and what resources it has at its disposal.

- Actions include:
  - Be informed
  - Set direction
  - Bring coherence
  - Develop adaptive capacity
  - Strengthen the organization
  - Validate and review



Resiliency – The New Model For Security



Security Frameworks - ISO 27x

- The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization“.
- The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment.
- The standard is also intended to provide a guide for the development of organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

Security Frameworks - NIST

International Harmonization and Context

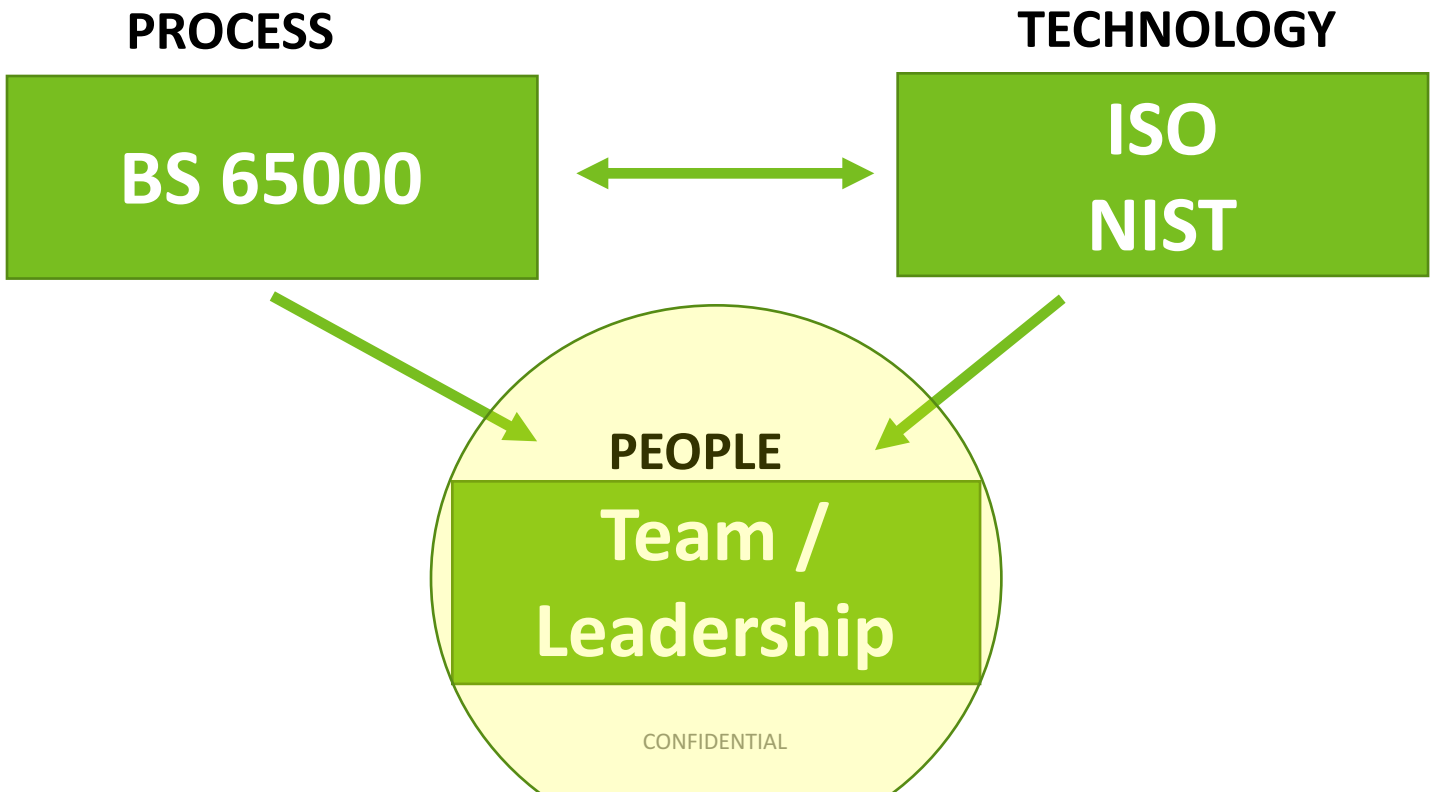
- The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure.
- The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Security Frameworks- NIST

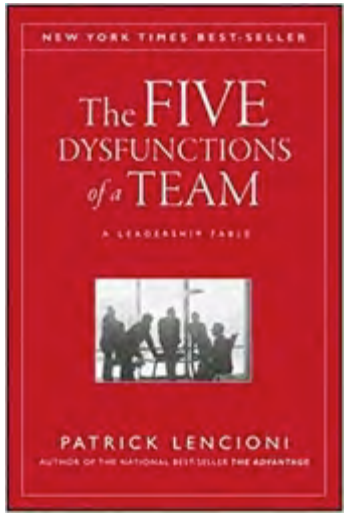
In February 2013, President Obama issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013. It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cybersecurity risks.

> *"The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats"*
> *~Section I of the Executive order~*

Resiliency – The New Model For Security



7.0 - Building a Team for Resiliency



7.0 - Building a Team for Resiliency

ACHIEVING TRUST

- Trust is knowing that when a team member does push you, they're doing it because they care about the team
- Good intentions - no reason to be protective or careful around the group
- Take risks in offering feedback and assistance
- Appreciate and tap into one another's skills and experiences
- Focus time and energy on important issues, not politics

7.0 - Building a Team for Resiliency

MASTERING CONFLICT

- The desire to preserve artificial harmony stifles the occurrence of productive ideological conflict
- Great teams do not hold back with one another. They are unafraid to air their dirty laundry. They admit their mistakes, their weaknesses, and their concerns without fear of reprisal
- Have lively, interesting meetings
- Extract and exploit the ideas of all team members
- Solve real problems quickly

7.0 - Building a Team for Resiliency

ACHIEVING COMMITMENT

- The lack of clarity or buy-in prevents team members from making decisions they will stick to
- Organizations need trust and conflict so people can fully commit
- Most reasonable people just need to be heard and to know that their input was considered and responded to
- Creates clarity around direction and priorities
- Aligns the entire team around common objectives
- Develops an ability to learn from mistakes
- Leaders must communicate the results to their teams

7.0 - Building a Team for Resiliency

ACCOUNTABILITY

- Every team member is responsible for holding the team accountable
- Applies to ALL LEVELS of the organization
- Accountability to Trust, Conflict and Commit
- Helps poor performers improve
- Identifies potential problems quickly
- Establishes respect among team members
- Avoids excessive bureaucracy

7.0 - Building a Team for Resiliency

RESULTS

- The pursuit collective success must be #1
- Clarity - Make results so clear that no one would even consider doing something purely to enhance his or her individual status or ego
- Retains achievement-oriented employees
- Minimizes individualistic behavior
- Enjoys success and suffers failure as a team

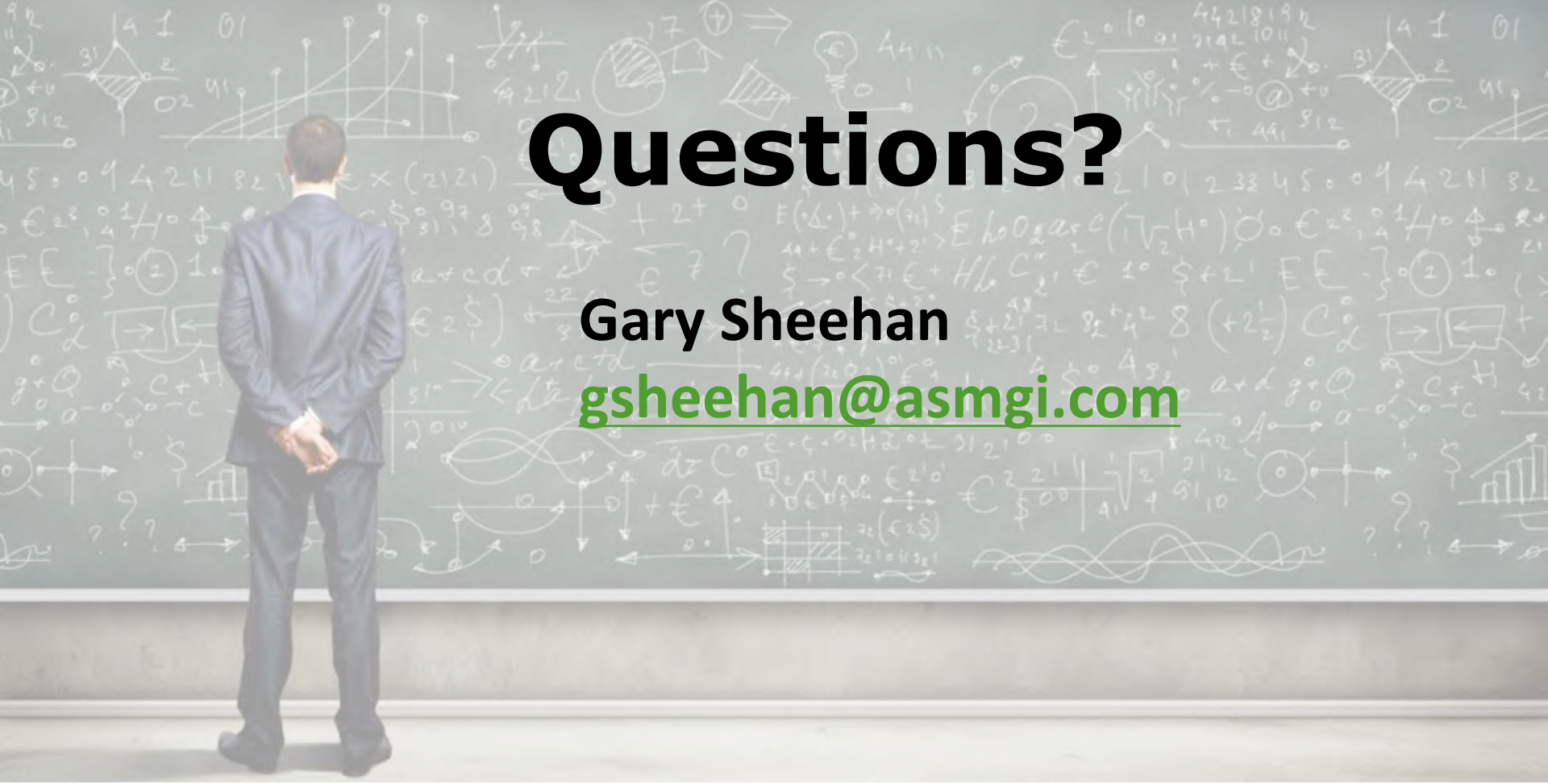
Wrap Up

Resiliency/Security must be embedded throughout the organization, cutting across silos, organizational structures and hierarchies, with operational activities aligned to strategic priorities.

Building a resilient workgroup, department, business unit, organization, company or organization is hard work - for EVERYONE.

Resilience/Security is inherently relative, and no organization, person, network or system can be absolutely resilient or secure, as they experience constant change and operate under varying degrees of uncertainty and risk.

- Everyone in an organization plays a role in **resiliency/security.**
- You must understand your business and the role you play in helping your organization achieve **resiliency/security.**
- All employees must be active participants in the **resiliency plan/security plan**.
- **Don't be the missing piece!**


Questions?
Gary Sheehan
gsheehan@asmgi.com