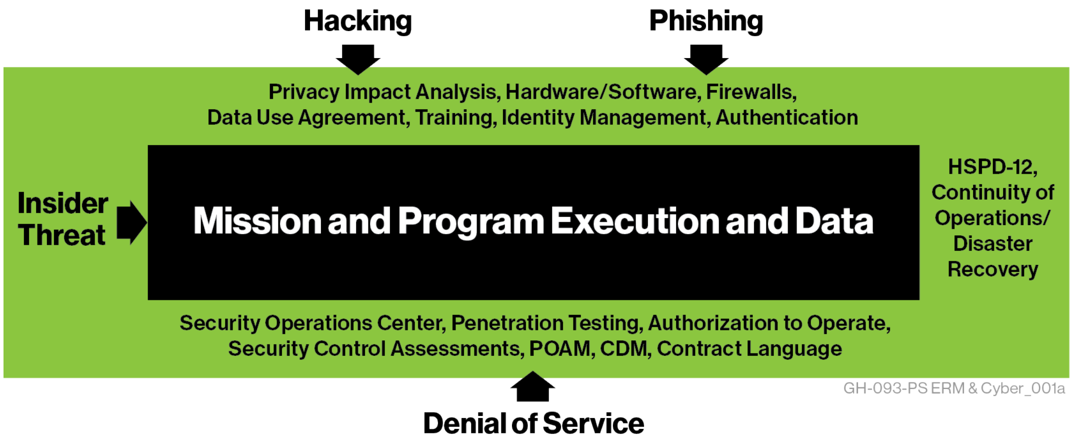
Enhancing Decision-making through the collaboration of ERM and Cybersecurity

All organizations are facing increasingly persistent and complex threats at all levels to data, information, mission, and programs. Adversaries are continuously seeking new and creative ways to gain and exploit network access and information resources. Increased levels of hacking, malware, phishing, rogue mobile apps, mobile device infection, as well as targeting specific individuals, are some of the more common attack methods used by adversaries today.



Hacking

Phishing

Privacy Impact Analysis, Hardware/Software, Firewalls,
Data Use Agreement, Training, Identity Management, Authentication

Insider Threat

Mission and Program Execution and Data

HSPD-12, Continuity of Operations/ Disaster Recovery

Security Operations Center, Penetration Testing, Authorization to Operate,
Security Control Assessments, POAM, CDM, Contract Language

GH-093-PS ERM & Cyber_001a

Denial of Service

This increase in efforts by adversaries and the sophistication of their methods, is similar to the growth in the amount and complexity of databases, systems, and devices that house or process Federal information assets. **The combination of these issues, combined with the speed of onset, and immediate impact from Cybersecurity threats is forcing a reexamination of reliance on "compliance" and a "hardened perimeter" mindset as the primary means to protect from external threats, and convey risk information to senior leaders**.

Instead of relying on "armor" to protect organizational capabilities, missions, and resources, Cybersecurity and risk decisions need to be made part of the "fabric" of everyday operations. Protection of mission essential functions and enabling data and technologies can no longer be a discipline that is only handled by the "IT" or "Cyber" people. Business owners need to understand their responsibilities for cybersecurity risk management in the context of the overall mission objectives of the organization. They need to partner with the cyber team to evaluate their cyber risk posture and determine where to invest in mitigation within the context of the *business's* risk appetite (which may be different from the cyber team's risk appetite). Leaders need to ensure their workforce is adequately trained on effective cyber risk activities, and not simply outsource that responsibility to IT. To effectively manage cyber risk, business leaders must engage with all relevant stakeholders, just as they would with any other risk to the strategic or operational risk to their enterprise.

Who is Guidehouse?

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We are successfully supporting numerous large-scale ERM and cybersecurity programs across the Federal government, including design, implementation, and ongoing maturation. Our Cybersecurity professionals are providing high impact strategy, technical, and risk management support to Chief Information Officers, and Chief Information Security Officers across the Federal Government.

What value is derived from this approach?

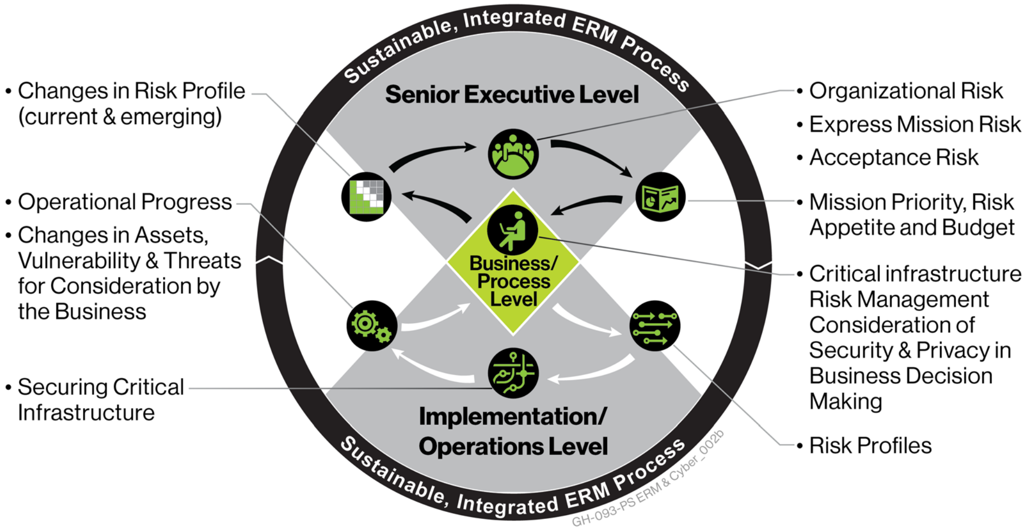
An enterprise risk management approach to cybersecurity risk, provides the following benefits:

- Understand residual risk
- Enhanced decision-making through better information flow
- Improved resource deployment
- Enhanced strategic discussions
- Reduction of threat surfaces
- Increased risk awareness
- Improved senior management communication and collaboration
- Application of risk appetite to cybersecurity decision making
- Understanding of cyber risk in context of other enterprise risks

Our Approach to Enterprise Cybersecurity Risk Management

At Guidehouse, we approach Cybersecurity and Enterprise Risk Management (ERM) holistically within the context of the organization, its mission and objectives. This approach is based on leading industry practices such as the 2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO) *ERM – Integrating with Strategy and Performance Framework*, and Federal Guidance such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 – *Managing Information Security Risk: Organization, Mission, and Information System View*. This methodology introduces a cohesive, integrated approach to identifying, communicating, and managing organizational risk, while providing the opportunity to manage Cybersecurity for greater impact in risk reduction. This approach fosters increased communication of risk and Cybersecurity information such as risk profiles, risk appetite, and changes to the business context within the organizational tiers as identified in NIST SP 800-39. Our high-level approach is as follows:

- Identify potential risks and mission impacts
- Map existing governance structures
- Identify risk information to inform enterprise cyber risk decisions
- Identify organizational strengths, weaknesses, and points of failure for risk information and decision making processes
- Define levels of tolerable and intolerable risks
- Provide organizational change management analysis with roles and responsibilities, ranging from cyber technical professionals to agency leaders responsible for mission outcomes
- Develop a strategy to provide risk information to inform decisions



• Changes in Risk Profile (current & emerging)
• Operational Progress
• Changes in Assets, Vulnerability & Threats for Consideration by the Business
• Securing Critical Infrastructure
Sustainable, Integrated ERM Process
Senior Executive Level
Business/ Process Level
Implementation/ Operations Level
Sustainable, Integrated ERM Process
GH-093-PS ERM & Cyber_002b
• Organizational Risk
• Express Mission Risk
• Acceptance Risk
• Mission Priority, Risk Appetite and Budget
• Critical infrastructure Risk Management Consideration of Security & Privacy in Business Decision Making
• Risk Profiles

- Agencies can take the following steps to enhance awareness of Cybersecurity risk:
- Incorporate the consideration of Cybersecurity into strategic decision-making.
- Change organizational mindsets that Cybersecurity is a service, or just a hardened IT perimeter serviced by “someone else” - it involves everyone at every level of the organization.
- Make cyber mainstream in the business conversation and vernacular by describing Cybersecurity activities and vulnerabilities in the context of the impact on the ability to protect information and transactions and the overall impact on mission objectives.
- Reduce the attack surface (devices, databases, emails, interfaces, etc.) with informed, risk-based business decisions about where data is maintained and how programs can be designed with Cybersecurity and privacy in mind.
- Balance cybersecurity and privacy protection with the needs of the business (or mission delivery needs) through discussions weighing tradeoffs between risk and performance.