Cyber Best Practices

Preparing organizations for the adoption and adaption of cyber best practices

What Are Cyber Best Practices?

Cyber best practices are a series of frameworks, methodologies and standards that provide guidance on what organizations should be doing to manage the security and resiliency of its cyber services portfolio.

A best practice is a framework or method that has consistently shown results superior to those achieved with other means, and that is used as a benchmark. In addition, a "best" practice can evolve to become better as improvements are discovered.

Companies like Axelos and others have created professional qualifications and training programs for the adoption and adaption of a cyber best practice program across an organization and its supply chain.

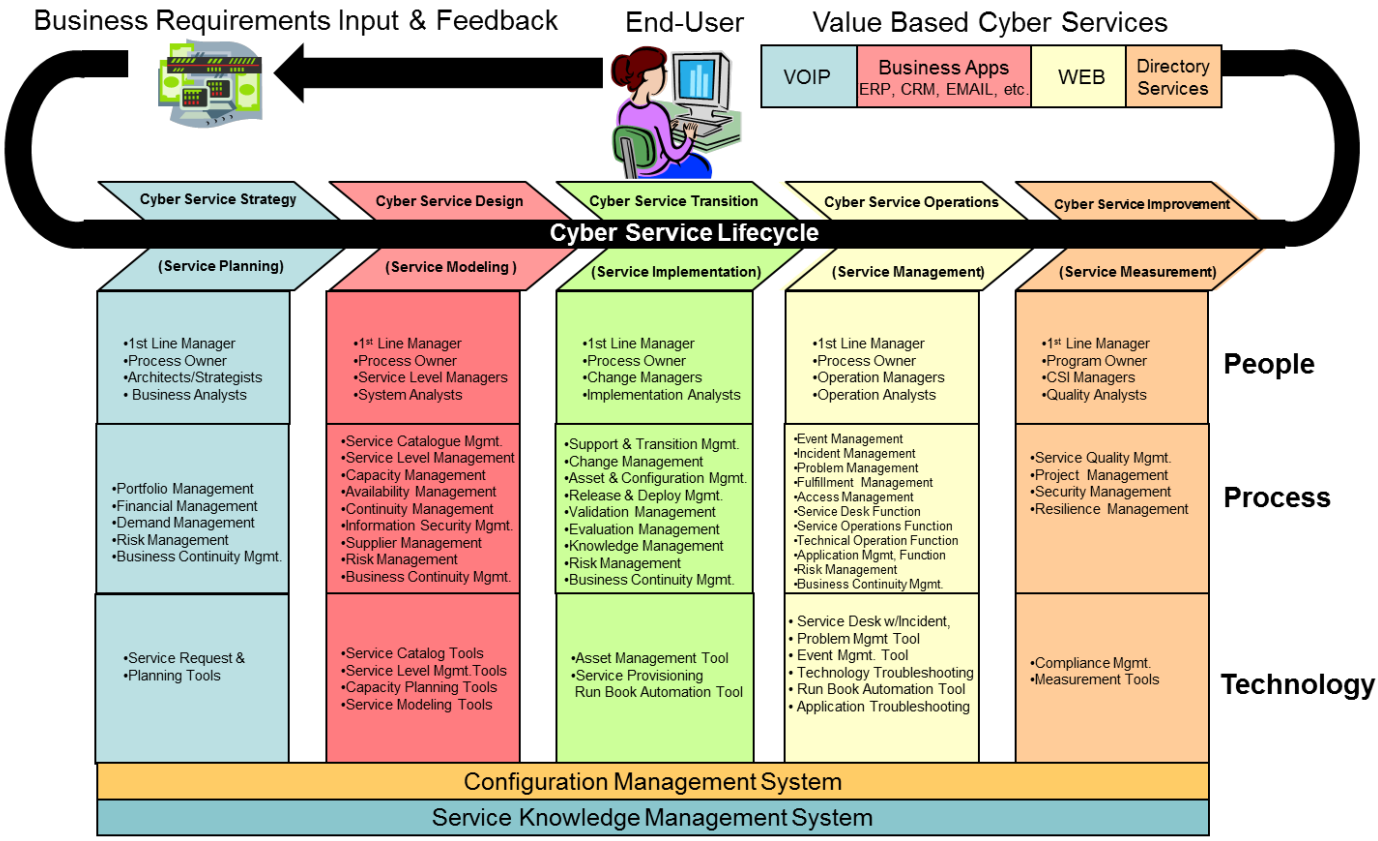
What Is the Cyber Service Lifecycle?

To sustain high levels of business performance in today's digital economy, organizations need to be agile in bringing new services to the market that customers will value, buy and use. Adapting quickly to changes in the market can bring organizations value in terms of competitive advantage but it can also bring with it risk in terms of cyber security and business resiliency. Organizations need to have a balanced view between risk and opportunity providing guidance on an appropriate balance of the two

The cyber service lifecycle ensures an organization's ability to deliver cyber services that are optimized for cost, quality, compliance, security, risk and business continuity. The cyber resilience lifecycle is split into 5 stages:

- Cyber Service Strategy
- Cyber Service Design
- Cyber Service Transition
- Cyber Service Operation
- Cyber Continual Service Improvement

Each stage relies on cyber service principles, processes, roles and performance measures, and each stage is dependent on the other lifecycle stages for inputs and feedback. A constant set of checks and balances throughout the cyber service lifecycle ensures that as business demand changes with business need, the services can adapt and respond effectively in alignment with the risk management policies established by the organization. The following diagram provides a high level overview of a cyber service lifecycle.



What Are Examples of Cyber Best Practices?

Cyber Service Management - Cyber service management best practices (ITIL® etc.) provide guidance on how to shift from managing services as stacks of technologies to customer-facing services that help an organization achieve its business goals.

Cyber Project Management - Cyber project management best practices (Prince2, PMP etc.) enable organization to incrementally improve its cyber security posture by using knowledge, skills and techniques that tie project results to business outcomes.

Cyber Security Management - Cyber security best practices provide guidance on how enterprises can leverage existing cyber security frameworks (NIST etc.) and standards (ISO 27001, ISO 31000, ISO 38500 etc.) to enable the organizational capability of cyber security

Cyber Resilience Management - Cyber resilience best practices (RESILIA™ etc.) provides guidance on how enterprises can leverage existing cyber service management systems (ITIL®) and cyber security frameworks and standards (NIST, ISO27001 etc.) to manage an organizations cyber risk and business continuity best practices.

What Are the Five Stages of Adopting and Adapting Cyber Best Practices?

Probably everyone has been exposed to the Kotter 8-Step Change Model in college or management seminars. In Kotter's 8-step model for organizational change, the first few steps help organizations overcome the status quo;

- Establish a sense of urgency
- Create a guiding coalition
- Develop a vision and strategy

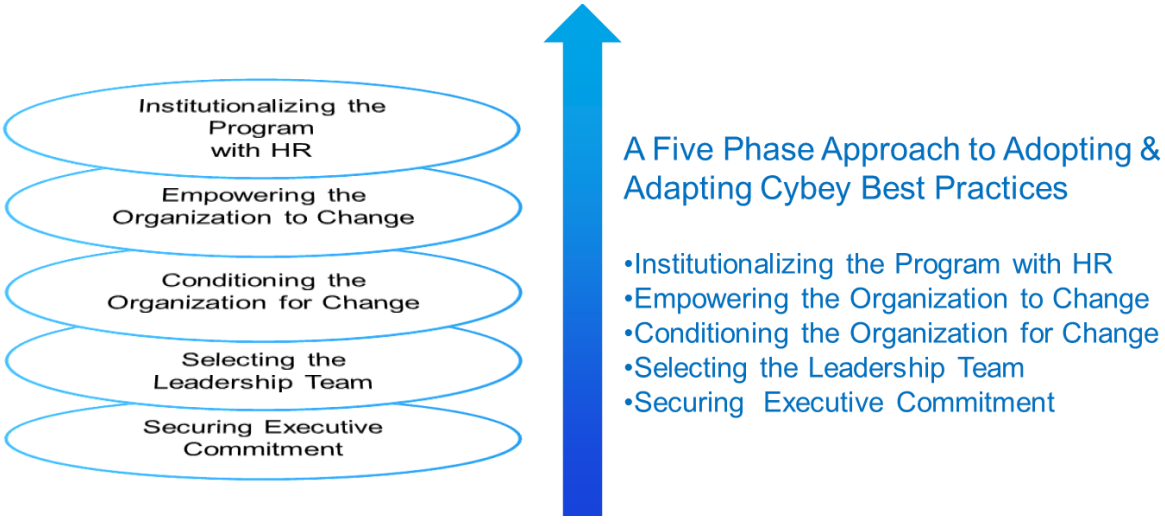
The next steps focus on communication and the realization of the change vision;

- Introduce new practices
- Empower a broad base of people to take action
- Generate short term wins
- Consolidate gains and produce more change

The last step ensures that the change sticks;

- Institutionalize the new practices.

The 5 five phase approach for adopting and adapting cyber best practices listed below aligns nicely with the Kotter 8-Step Change Model listed above. This five phase structured approach to training also ensures that an organization will optimize its training assets in terms of time, money and people.



What is a Cyber Best Practice Training & Mentoring Program?

Successful adoption and adaption of a cyber resilience best practice program requires organizations to invest in training and mentoring program capable of delivering the following knowledge and skills:

Leadership Training Leaders understand risks and the potential impacts these risks can have on their strategic objectives. However, understanding and responding to cyber risks, in today's highly complex and fast moving environment is challenging. The challenge for many leadership teams is to define what good cyber resilience looks like, understanding the risks and the information provided to them so that an effective resilience strategy can be achieved.

Organizations need to implement innovative and compelling awareness products tools and guidance specifically designed to increase understanding, insight and action in the boardroom. These programs should include:

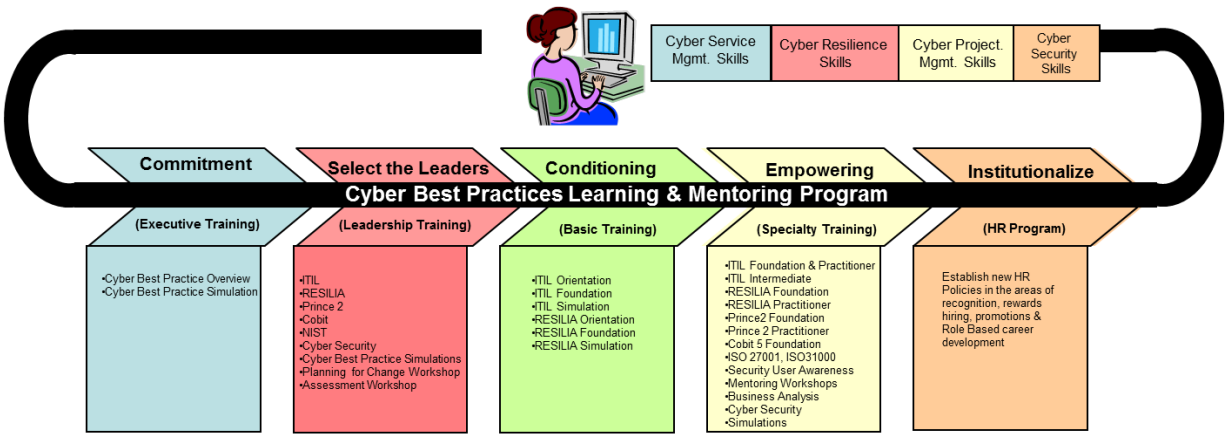
– Professional development and learning for executive and non-executive directors – Cyber boardroom simulations – Cyber resilience risk management training for senior risk management decision makers

Certification Training Organizations need to implement Foundation and Practitioner level certification programs that teach the knowledge and skills required to integrate cyber best practice frameworks into an organization's service management architecture.

Business Stakeholder & Supply Chain Awareness Training Organizations need to implement awareness learning solutions that give people the knowledge, skills and confidence they need to embed cyber resilient behaviors into their day-to-day behaviors. Modules should include: phishing, social engineering, online safety, social media, BYOD, removable media, password safety, personal information, information handling and remote and mobile working.

Continuing Education Training Organizations need to acquire cyber service continuing education programs that teach the ongoing knowledge and skills for organization to maintain and improve its cyber service program on a continuous basis.

The following diagram outlines the five stages of a cyber best practice training and mentoring program.



Summary

A spray and pray approach to the delivery of cyber services has real consequences; wasted time, wasted money and most importantly opening doors for the bad guys.

The 5-step approach mentioned above in the context of organizational change will ensure an organization's ability to deliver cyber services that are optimized for cost, quality, compliance, security, risk and business continuity thereby enabling it to survive and thrive in the global digital economy.