Create a "Programmatic Approach" to Cyber Security Risk reduction [1]

Peter Gailey

Cyber Security is a fundamental cornerstone of all enterprise entities. It is very complicated and riddled with risk. A "Programmatic Approach" is most effective in reducing risk.

Cyber Security is the business of measuring risk and offering solutions to reduce or eliminate risk. In its most simple form to effectively reduce enterprise risk, a series of projects need to be identified, prioritized, budgeted, executed, and tested.

To properly address enterprise cyber security the first step is to understand the business and its strategy. Most industries have cyber security mandates. Example: HIPAA in Healthcare. Consider these as minimum requirements. You must understand several components to create a strategy: Industry and its minimum requirements, vulnerabilities, standards and frameworks, risks, adversaries, and how to allocate people, process, technology, and budget $$$. Do it yourself or outsource.

Roles of individuals:

CIO – Chief Information Officer - Sets strategy, manages budget, responsible for the execution of Information Technology / Information Security IT/IS environment to drive the business to meet stated business objectives. Generally, reports to the CEO, COO or VP Finance.

CISO – Chief Information Security Officer – Generally the same as a CIO with security focus. Most always reports to the CIO.

CDO – Chief Data Officer. Generally, the same as a CISO with a focus on data. May report to the CIO or CISO.

The CIO, CISO and CDO are managing people, process and technology projects. Depending on the size of the enterprise a Program Office and or Program Manager may be involved. Regardless of corporate structure a "programmatic approach" is needed.

[1] How to cite this article: Gailey, P. (2022). Create a "Programmatic Approach" to Cyber Security Risk reduction, *PM World Journal*, Vol. XI, Issue IV, April.

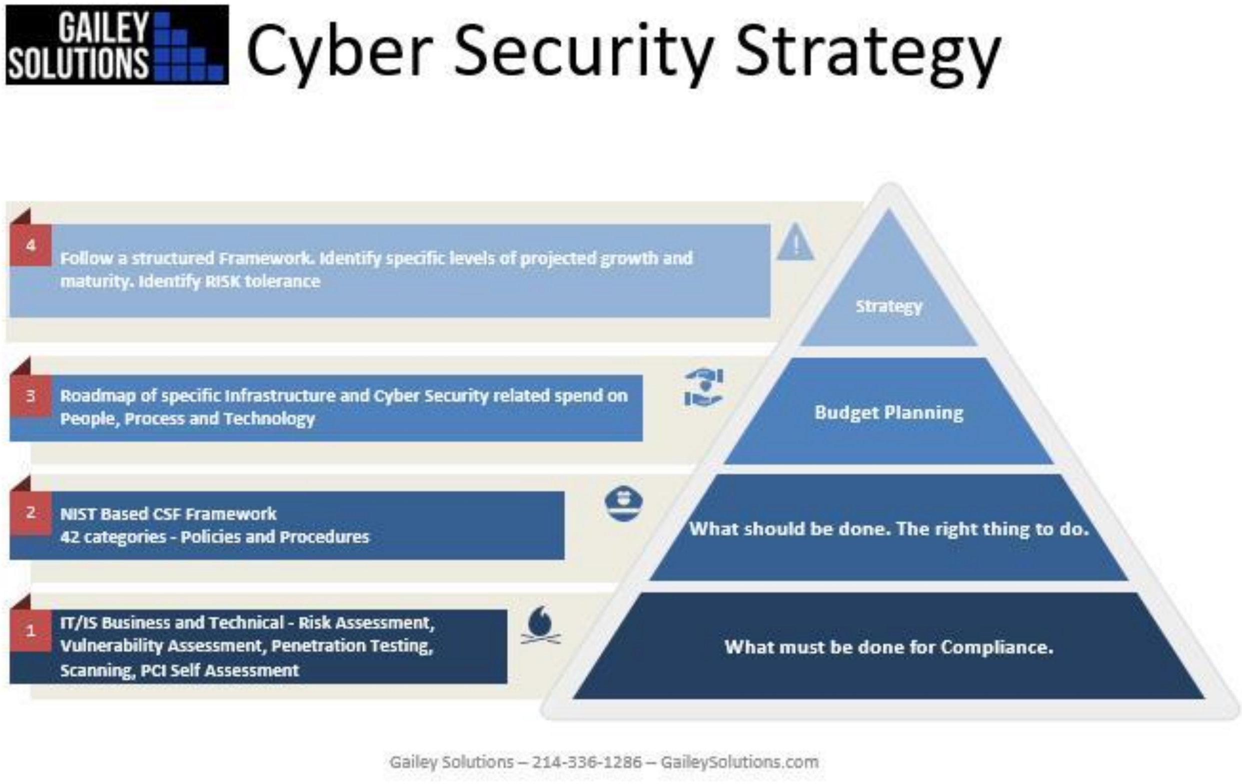
Frameworks and Standards:

Best advice is to follow industry standard practices, in the form of Industry standards and frameworks. Most will be mandated depending on the enterprise geographic location and industry. For example, in the US, NIST (National Institute of Standards and Technology) is followed. NIST consists of both Standards (Example: Measurements) and Frameworks (Example: CSF Cyber Security Framework. A library of best practices that is cross industry.)

In the EU, ISO Standards and Frameworks are followed. For large international enterprises both may be mandated to be followed.

Complicated? Yes. Detailed? Yes. A deep understanding is needed to reduce risk.

What should an enterprise risk management plan and strategy include as it relates to Cyber Security?



GAILEY SOLUTIONS Cyber Security Strategy

4 Follow a structured Framework. Identify specific levels of projected growth and maturity. Identify RISK tolerance

3 Roadmap of specific Infrastructure and Cyber Security related spend on People, Process and Technology

2 NIST Based CSF Framework
42 categories - Policies and Procedures

1 IT/IS Business and Technical - Risk Assessment, Vulnerability Assessment, Penetration Testing, Scanning, PCI Self Assessment

Strategy

Budget Planning

What should be done. The right thing to do.

What must be done for Compliance.

Gailey Solutions – 214-336-1286 – GaileySolutions.com

The above graphic represents a State of Texas mandated Agency strategy.

An enterprise Cyber Security risk plan should start with a baseline understanding of the following:

1. An understanding of the business environment. business size, scope of industry verticals, risk factors, risk tolerances, client locations etc.

2. An understanding of the types of resources involved to run and manage the enterprise. Data requirements, systems, software, services etc..

3. Full understanding of industry mandated requirements. HIPAA, FISMA, FEDRamp, CMMC, Privacy considerations - GDPR etc.

4. Understanding of people, process and Technology of IT/IS, Finance, Legal etc.

5. Governance Risk and Compliance - GRC should be structured as a program with supporting projects to deliver a programmatic approach to reducing risk. GRC is a journey with many moving parts.

6. Start with a baseline risk assessment (people and process'), vulnerability assessment, pentest and wireless network assessment (technology).

7. Consider a compromise assessment to see if you have been breached, or are experiencing symptoms of being breached, and do not know it.

8. Gather these findings and prioritize a set of remediation plans to reduce enterprise risk as it relates to budgeted funding.

9. Cost out the cumulative OpEx and CapEx funds required to execute the various projects and associated remediation efforts that: A. Are mandated by your industry. B. Should be done but are not necessarily mandated. C. The right thing to do.

10. Build out your prioritized remediation plans as they relate to available resources (Budget, People, Process and Technology.)

11. Perform remediation per #10.

12. Rinse, Repeat. Execute in a programmatic manor. Review on a quarterly basis at a minimum.

13. Build the above findings into the budget request plan. Allocated funds should represent the risk tolerance of the Board, Executive Team and Stake holders.

14. Reach out for help. It takes a community!!

In conclusion, understand that a "Programmatic Approach" is necessary for Cyber Security related risk reduction.

About the Author

Peter Gailey

North Texas, USA

Peter Gailey has worked in global Fortune 100 firms as a strategic sales leader creating strategy and building teams that have executed those strategies resulting in billions of dollars of revenue, and hundreds of millions in profits. Peter also has deep experiences in start-up firms in the high-tech space. Expertise includes Cyber-Security, Cloud, Data Center technologies and services. He can be contacted at peter@gaileysolutions.com