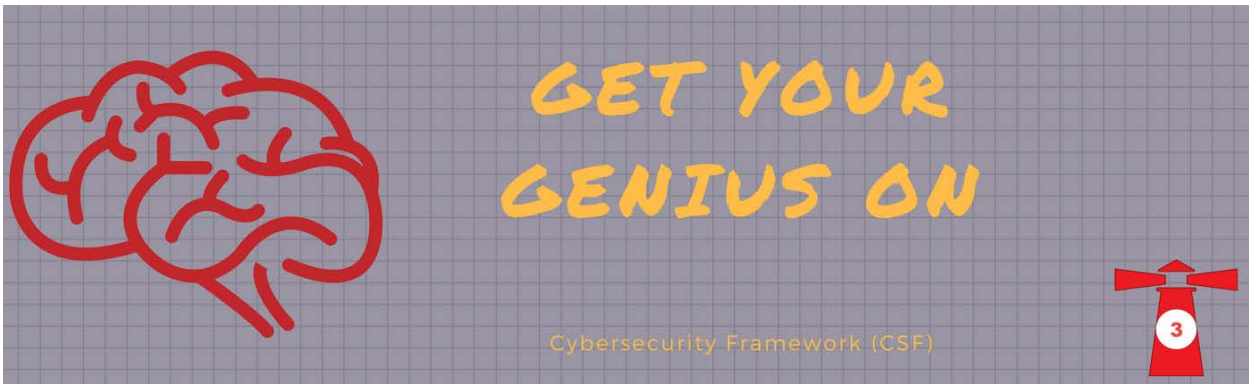

Cybersecurity threats exploit the increased complexity of business-critical information and infrastructure systems. It is an omnipresent and ever-evolving hazard that extends from enterprise-to-enterprise, rippling out into the economy. And it doesn't end there. It menaces the Nation's security—placing public safety, health and elements of the environment at risk. Cybersecurity risk affects a company's bottom line—often manifesting as financial and reputational damage. It can drive up costs and negatively impact revenue. It can harm an organization's ability to innovate, gain and maintain customers, and create value integrations with partners up and down the supply chain.

So where does an enterprise start in the quest to counter cyber threats? And more daunting, how do organizations keep pace with, and protect against the expansion and rapid advancement of cyber threats? Well, Voltaire once said, "No problem can withstand the assault of sustained thinking." Charles Kettering supposed, "High achievement always takes place in the framework of high expectation." And Albert Einstein famously whispered, "Intellectuals solve problems; geniuses prevent them." Those kernels of wisdom tally up to a practical concept centered on high expectations--adopting a framework to overcome cyber threats. A framework that supports a perpetual system to preclude, counteract and recover from adverse cyber forces. In short, it means leveraging the genius of a framework to sustain the critical activities to identify, protect, detect, respond and recover from harmful cyber events. A governance framework that is active and self-enforcing.

How should an enterprise use a framework to support Cyber Governance? The short answer is organizations should leverage frameworks to ensure Cyber Governance is 'Active.' Enterprises will continue to have unique inherent risks as the organization's products, services and geographies change over time. Add advancements and cycles in technology, infrastructure and application lifecycle management, resources and supply chain. Then imagine the complexities in maintaining the preparedness of an enterprise's people, technology and facilities to mitigate cybersecurity risks and recover from cybersecurity breaches.

Most organizations have developed sophisticated defense-in-depth strategies. They have deployed appliance and software protections North-South and East-West across their networks. So, the root-cause of their cyber problems is not that their protection strategies lack cyber technology controls. The problem is the density of dependencies stemming from the use of those

technology controls. Organizations across industries--Energy and Natural Resources, Financial Services, Public Services, Hi-tech Industries and Service Industries all cite that the root cause of their anxiety and issues around cybersecurity is--complexity. Strong governance is needed to reduce and manage the complexity in today's networks and digital businesses. Ultimately, frameworks are aimed at reducing and managing the complexity associated with cybersecurity risks and advancing Active Cyber Governance.

What are the critical components to consider of a cybersecurity framework? Frameworks should provide governance mechanisms for organizations to:

1. Assess and define their current cybersecurity posture,
2. Describe their target-state and provide line-of-sight from business operatives to technologists, to collaborate on building systems for maintaining target-state cybersecurity and resiliency systems,
3. Identify and prioritize improvement opportunities within the context of continuous and repeatable cybersecurity and resiliency systems,
4. Assess progress and generate the data to steer security actions for the next period,
5. Marry every IT activity and cyber counter measure to a business activity and requirement,
6. Communicate in business parlance, cybersecurity risk, as well as the maturity level of systems—for example partial/incomplete, performed, planned, managed, measured and defined,
7. Provide actionable intelligence for C-Level Executives and Boards to make effective policy and investment decisions (thereby elevating support for cyber risk initiatives with C-Level Executives and the Board).

The good news is that cybersecurity frameworks are not pipedreams. They exist. One framework of note was created from a collaboration between the government and the private sector. The Cybersecurity Enhancement Act of 2014 (CEA) statutorily updated the role of the National Institute of Standards and Technology (NIST) to include developing a cybersecurity risk framework. NIST was tasked through CEA to identify a prioritized, flexible, repeatable, performance-based approach to recognize, assess, and manage cyber risks. The NIST Cybersecurity Framework (CSF) continues to evolve. It uses a common language to address and manage cybersecurity—understandable by business and technical functions alike.

In addition, the US-CERT (United States Emergency Readiness Team) developed the Cyber Resilience Review (CRR), a non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The purpose of the CRR is to help enterprises measure existing organizational resilience and analyze the gaps as the basis for implementing improvements founded on recognized best practices.

There is still more good news. Gestalt Development has developed a Cyber Governance application to help organizations actively manage their cybersecurity and resiliency postures. The Cyber Governance solution leverages the NIST CSF and US CERT CRR and provides the framework and functional capabilities to actively govern, manage and reduce complexity and to

apply the principles and best practices of risk management to improving the cybersecurity and cyber resilience of organizations. Visit www.GestaltDevelopment.com to learn more.

I tend to approach things from a physics framework. And physics teaches you to reason from first principles rather than by analogy.
--Elon Musk

This is the third article in a series on Cybersecurity Governance and Cyber Resiliency. Both are broad, interrelated topics and every facet is important. We welcome your questions and comments and will directly reply or address your questions and comments in future articles. You can contact us at hello@GestaltDevelopment.com.

About the Author(s)

Jay Marqua is Managing Director of Gestalt Development's, Cybersecurity and Information Systems Consulting Practice and Board Advisory Services Consulting Practice. Jay is based in Gestalt's Durango, Colorado office. In his professional role supporting and serving Boards and Executive Leadership, Jay has led transformation efforts in the Healthcare, Energy, Financial, Communications, Technology, Software, Logistics, Hospitality and Travel Sectors. The pace and advantage to organizations of technology aligned with high performing teams has steered Jay to his concept, strategy and execution roles in the development of organizations globally. Jay can be reached at jay.marqua@gestaltdevelopment.com

About Gestalt Development

Gestalt Development is a network of consultants. We operate as one firm, bringing the most highly skilled specialists to each engagement. We develop and embed systems to leverage and integrate Technology and Human Capital. We deliver substantial improvements and sustainable performance on a global scale. www.gestaltdevelopment.com