The Cyber Quandary Curve

It is fraught with risk and danger,
and it is here to stay

Organizations remain concerned about cybersecurity and cyber resiliency-- the protection of sensitive data and the availability of their information systems. Company's digital landscapes are continuing to expand to maintain relevance and competitive advantage--creating a larger attack vector, at the same time the cyber threat landscape is rapidly changing and advancing. The dilemma is that the technology controls implemented today to address the threat landscape quickly become inadequate. That dilemma, let's call it the Cyber-Quandary Curve, is a new operating reality for organizations. It is fraught with risk and danger, and it is here to stay. That's no way to operate an enterprise. So how can organizations keep cybersecurity and cyber resiliency ahead of the Cyber Quandary Curve? Governance—appropriately matching every digital transaction and information activity to business mission and goals.

Let's start with the end-state we are looking to achieve.

1. Institutionalizing a culture of digital awareness and digital accountability
2. People behaving securely
3. The company operating resiliently
4. Enterprise-wide knowledge share
5. The advancement of business operations and successful cyber postures as a matter of norm
6. Realtime, actionable intelligence for effective policy and investment decisions
7. Active governance--always executing ahead of the Cyber Quandary Curve

Now let's look at some first steps to achieving Active Cyber Governance—the driving force to achieve the behaviors needed to show-up every day, with everyone across the enterprise. First and foremost is to institutionalize a culture of digital awareness and digital accountability—from IT and business operations to the boardroom.

Accountability and awareness are the key-stones to prevention. What many organizations fail to keep top-of-mind, is that surrounding every business transaction is a swirl of digital activities. Simply stated, every company is running a digital organization. It's how we connect with customers, vendors and each other. Every piece of data is shared, manipulated and stored digitally. Consequently, every business activity must have built-in preventative measures and accountability for the protection of sensitive data--and an awareness as to the appropriate availability and access of the related business information systems.

Without digital awareness, and digital accountability, cybersecurity is often treated as an IT problem instead of a business problem (the fact that the negative impacts of deficient cybersecurity and resiliency defenses harm the company's margin, mission and reputation make it a business problem). The consequence is to disjoint the organization's cyber posture from its business activities and mission, leaving organizations to deem cyber tools and countermeasures as adequate defense. Security capacities are siloed retarding knowledge share, separating cybersecurity from business support requirements and thereby inhibiting cyber resiliency and increasing the cost of loss expectancies. Further, C-level executives and Boards are left with a lack of actionable intelligence to make effective policy and investment decisions--which defuses the Board's and executive's abilities to accurately support and elevate cyber concerns.

Without Active Cybersecurity Governance to reconcile systems to business activities and mission—a company's cyber posture is more happenstance than adequate, and destined to fall behind the Cyber Quandary Curve.

In summary, Active Cybersecurity Governance is paramount. Its power stems from strategies based on digital awareness and accountability. But every strategy needs structure to support it—so what is the structure needed to support Active Cybersecurity Governance? A Cybersecurity Framework is needed to persist awareness and accountability. It is crucial for establishing Active Cyber Governance. Many enterprises operate in highly regulated spaces with complex cybersecurity challenges. Without a Cybersecurity Framework, the density of complexity associated with cybersecurity and resiliency actions often causes more money invested on countermeasures than loss expectancies. A Cybersecurity Framework supports Active Cybersecurity Governance that is the basis for developing successful countermeasures-reasonable, measured and achieve the best possible economics. The cyber security framework joins cybersecurity and resiliency to business mission and requirements (operative, resilient and ahead of the Cyber Quandary Curve).

An active, robust Cyber Governance Framework is also critical in keeping pace with the rate of change on all fronts—technology, lifecycle management, business shifts and cybercrime. Without on-going assessments and cyber resiliency targets, the business mission is at unnecessary risk. It is incumbent for every organization to not only get ahead of the Cyber Quandary Curve, but to adopt the Active Cyber Governance systems to make it irrelevant.

"The secret of getting ahead is getting started. The secret of getting started is breaking your complex overwhelming tasks into small manageable tasks, and starting on the first one."
-- Mark Twain

This is the second 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