
# No longer a 'nice to have' . . .

ACTIVE CYBER GOVERNANCE
INFORMAITON SYSTEMS

This is the 5th article in a series on Active Cyber Governance and Active Cyber Governance Information Systems (also known as, ACG Information Systems, ACG Info Systems, and ACGIS).

In the same way that AIS, MIS and ERP information systems bring control, transparency, effectiveness and coordination to financial and business transaction flows, an ACGIS brings accountability and coordination to the digital security and resiliency of those business and financial transactions and systems. Because business activities are accomplished via digital transactions amongst business units, vendors, partners, and customers–implementing an ACGIS is no longer a nice to have; it is a must have.

The previous four articles in this series built on ideas that are summarized in this article. Several of the ideas focused on an understanding of cyber as a required enterprise-wide business discipline (not just for IT). Here are the understandings needed to effectively tackle cyber requirements:

- **Every Company is running a digital organization.** It's how we connect with customers, vendors and each other. Virtually every piece of data is shared, manipulated and stored digitally—from voice and video to information and images. Digital lives in cyber and without cyber competencies—digital perishes in cyber, or worse, is penetrated by bad actors.

- **Cybersecurity is a business problem, not an IT problem.** When cyber breaches occur, it is our Company's margin and mission that suffer the consequences—from business interruptions to reputational damages. All of these carry negative confidence and economic repercussions to our brand, customers, employees, partners and shareholders.

- **Cybersecurity and cyber resiliency are capabilities to build and deploy in every corner of the organization**—in every customer, vendor and partner interaction and in every business activity. Embracing the reality that we are all running digital organizations and understanding that cybersecurity and cyber resiliency are necessary core competencies for any business is the fundamental awareness needed for our digital organizations to thrive in a cyber dominated world (all digital, all the time)—from financial transactions to business boundaries with vendors, partners, customers and employees.

- **Companies are continuing to expand their digital landscapes 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,

the Cyber-Quandary Curve, is a new operating reality for organizations. It is fraught with risk and complexity, it is here to stay, and organizations need an Active Cyber Governance Information System to stay out in front of it.

So where is the best place to start in persisting secure and resilient cyber practices throughout the enterprise and what provides the most leverage in building cyber discipline? As with most significant shifts, it starts with awareness and is continued by leveraging the discipline afforded by accountability.

Cyber diligence and rigor (awareness and accountability) is as important to an organization's forward progress as Financial diligence and rigor (awareness and accountability). Without digital awareness, and digital accountability, cybersecurity is often treated as an IT problem instead of a business problem. As a consequence, the organization's cyber posture is disjoined from its business activities and mission, leaving organizations to deem cyber tools and countermeasures as adequate defense. Siloed security capacities retard 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 executives' abilities to accurately support and elevate cyber concerns.

If we were to snapshot situational awareness across industry, we would find that 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.

ACG Information Systems provide organizations the ability to govern enterprise cyber risk by managing the organization's inherent cybersecurity risk, determining the organization's resiliency and measuring the system maturity levels of cybersecurity and resiliency systems and countermeasures. ACG Information Systems guide users from the IT department and business units, to the Board of Directors through a Governance and Management system of assessment, accountability, system evaluation, intelligence and reporting.

At their core, ACG Information Systems provide a governance framework that is active and self-enforcing. The immediate and ongoing benefits of implementing an ACG Information System is the ability to:

1. Define and understand the organization's current cybersecurity posture,
2. Describe the 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. Marry every IT activity and cyber counter measure to a business activity and requirement,
4. Identify and prioritize improvement opportunities within the context of continuous and repeatable cybersecurity and resiliency systems,
5. Assess progress and generate the data to steer security actions for the next period,
6. Communicate, in business parlance, cybersecurity risk as well as the maturity level of systems,
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).

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.

Financial and Enterprise Resource Planning (ERP) information systems integrate applications to manage departments and functions such as production, sales, purchasing, logistics, accounting, project management, inventory control, orders, payroll, etc. Those points of integration and the flow of transactions are digital. Digital integrations and transactions require cybersecurity and resiliency to be built-in and that is what an Active Cyber Governance (ACG) information system brings. At its most basic level, an ACGIS connects cybersecurity activities to business activities. That connection provides end-to-end transaction accountability, promotes resiliency, limits loss expectancies, reduces exposure to the threat landscape and ensures the best possible economics for protecting against tactics of infection, attack methodologies, and the changing development and distribution techniques used by cybercriminals.

Companies need an ACG Information System for managing cybersecurity and resiliency in the same way companies need financial and ERP systems to manage costs and resources. ACGIS builds cybersecurity and cyber resiliency capabilities as well as awareness and accountability into every customer, vendor and partner interaction and business activity in the same way financial and ERP systems build process control and financial accountability into every customer, vendor and partner interaction. ACG Information System solutions provide the framework and functional capabilities to manage and reduce the cyber complexity inherent in today's digital business environment.

The following are the end-states an ACGIS is leveraged to achieve.

1. Institutionalizing a culture of digital awareness and digital accountability
2. Ensuring people behaving securely
3. Advancing the company in operating resiliently
4. Cultivating enterprise-wide knowledge share
5. Disseminating business operations and successful cyber postures as a matter of norm-- from IT and business operations to the boardroom. No weak links.
6. Realtime, actionable intelligence for effective policy and investment decisions
7. Active Cyber Governance–always executing ahead of 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 and Active Cyber Governance Information Systems provide that structure. Active Cyber Governance distilled down to its simplest form is: Matching IT resources to business mission and activities, and enforcing the principals of governance, awareness, security, resiliency, maturity, and accountability on the entire organization—including business unit leads and third-party vendors. Vincent Van Gogh understood, "If one is master of one thing and understands one thing well, one has at the same time, insight into and understanding of many things." Active Cyber Governance is that one thing for organizations to understand in today's digital business landscape.

"In each business, there is a process, or delivery system, that is changing rapidly under them.
--Ken Moelis

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