Governance distilled down to its simplest form is matching resources to business mission. Within the context of a business enterprise, effective governance provides guidance, line-of-sight and alignment between business activities, mission and goals—especially in times of significant change when business and industry alter direction.

Business enterprises are often and fairly referred to as ecosystems. Businesses evolve, and that evolution causes gradual change and random periodic shifts. In periods of change, most enterprises are adept at managing the change—adjusting incrementally. Conversely, when shifts happen, there is not a process to manage the shift because shifts are a tipping point--the end of a chain of trends. A chain of trends that are often seemingly unrelated or random. Or, more dramatically stated—shifts happen, and we feel as if we have suddenly been dumped out in a new jungle on the other side of a world we don't fully understand and to which we aren't prepared to adapt.

Shifts require transformation--embracing the realities of the new ecosystem and the key swings in Governance vital to accurately match resources to business activities. The most recent shift in business is 'digital', and the new business ecosystem is 'cyber'. The realities of the new ecosystem demand we embrace the need to build Governance capacity and rigor on two fronts--cybersecurity and cyber resiliency. Cyber Governance is the ecosystem's oxygen and it needs to extend to every business unit in the organization if the enterprise is to ever catch its breath.

Rightfully so, Cybersecurity has become a topic of concern in every boardroom—but where does an organization that feels the pressure to respond to the new threat landscape begin? I have asked the following two questions to dozens of business executives and boards that have raised that concern.

1. Is your Company running a digital organization?
2. Is Cybersecurity an IT problem?

The questions are broad enough to be vague and illicit a range of responses, but the answers are surprisingly similar. The reaction to "Is your Company a digital organization?" is usually along the lines of "We employ some digital technologies, but we aren't a digital media, digital equipment or cloud company". In other words, "No we are not a digital company." And to "Is cybersecurity

an IT problem?" the response is typically "Yes. Of course." While both perspectives ring of accuracy, the diluted precision of the assessments prevents companies from making the shift to a digital mindset, accepting the realities of cyber in the new ecosystem landscape, and accepting the need to build cyber governance into every business activity.

A business operating without the conviction that they are running a digital organization causes cybersecurity and cyber resiliency to be compartmentalized as technology issues for IT. The misperception blocks the awareness of the need to weave cybersecurity and cyber resiliency as core operating competencies into every business unit in the enterprise.

Here are the new realities.

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. The only exception is that occasional super-secret sticky note with a hand-written P@$$w0rd dangling from a user's monitor.

Cybersecurity is a business problem, not an IT problem. Here's why. When cyber breaches occur, it is our Company's margin and mission that suffer the consequences--from business interruptions to reputational damages. All of which 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 new reality that we are all running digital organizations and understanding that cybersecurity and cyber resiliency are necessary core competencies are the new business fundamentals. And active Cybersecurity Governance is needed to make such a sweeping course correction and successfully re-align our resources to our business mission.

> "Forward movement is not helpful if what is needed is a change of direction."
>
> — David Fleming, Lean Logic: A Dictionary for the Future and How to Survive It

This is the first 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@ACGInfoSystems.com.

About the Author(s)

Jay Marqua is CIO of ACG Info Systems Cybersecurity and Information Systems Consulting Practice and Board Advisory Services Consulting Practice. Jay is based in ACGIS Info Systems' 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@acginfosystems.com

About ACG Info Systems, LLC

ACG Info Systems has developed an Active Cyber Governance Information System (ACGIS) to help organizations actively manage their cybersecurity and resiliency postures. The Active Cyber Governance Information System solution leverages the NIST CSF and US CERT CRR and provides the framework and functional capabilities to actively govern, manage and reduce complexity and risk. The ACGIS provides the functional governance capabilities to apply the principles and best practices of risk management to improving the cybersecurity and cyber resilience of organizations. The application guides enterprises in 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.