Pilots choose a course of actions and follow procedures for navigation dependent upon conditions. They follow Visual Flight Rules (VFR) or Instrument Flight Rules (IFR) as circumstances dictate. A pilot can fly VFR if conditions are unobstructed but will navigate by IFR if there is any chance that conditions might change (IFR is suitable for VFR conditions—the reverse is not true). The struggle for many organizations today is that they are following the equivalent of VFR for cyber when IFR is required. The equivalent of navigating by IFR for today's digital businesses is Active Cyber Governance.

Another way of thinking about Companies that employ Active Cyber Governance versus Companies that do not is operating with the "lights on" versus operating with the probability of "lights off." Organizations are operating in two parallel universes—one highly visible and engaging (lights on) and one not readily visible and so often deferred (lights off). Those universes are:

1. Thriving in a society and marketplace where rapidly changing technology and unanticipated user adaptations is a constant, and a source of untold opportunities—lights on.

2. Vulnerable to the tactics of infection, attack methodologies, and changing development and distribution techniques used by cybercriminals, and a source of untold business disruptions and impediments—lights off.

So why are so many organizations still navigating a digital world as if 'lights off' is improbable? The reason seems to be a difference in awareness, concern versus commitment. There is a lack of appreciation regarding the vast differences in insight and effectiveness afforded by the level of awareness. There are those organizations that are committed to keeping the lights on and there are those organizations that are concerned with the lights going off. It is a seemingly subtle difference but with an enormous disparity in consequence. Committed companies have adopted Active Cyber Governance as a matter of operating norm. Their security posture is aggressive—they actively focus on keeping the lights on by staying out ahead of the Cyber Quandary Curve[i]. Concerned companies have not adopted Active Cyber Governance as a matter of operating norm and so their security posture is happenchance—operating behind the Cyber Quandary Curve. They characteristically depend on heavy investments in cyber technology controls and countermeasures to placate their concern of the lights going off, and then roll along (unless or until something happens).

To illustrate the point made above, without exception, the source of all high profile cyber breaches in recent years are organizations that operate with security postures compelled by cyber-concern instead of commitment. The breaches have occurred despite the compromised organizations having had sophisticated defense-in-depth strategies. They had deployed appliance and software protections across their networks. So, the cause of their breaches was not that they lacked cyber technology controls. The cause was their lack of Active Cyber Governance to manage the complexity in their networks, digital businesses and the cyber universe in which they operate. They were concerned; they were not committed—and they failed their brand, customers, employees, partners and shareholders.

The CEO and the board of every organization needs objective, current information and a cyber posture that is forward focused—security is forward focused, or it is happenchance. The required mastery for security to be forward focused is Active Cyber Governance. Cyber technology controls without Active Cyber Governance is like trying to maintain a heading while flying in low visibility conditions without a directional gyro or compass. It works until it doesn't. The role of Active Cyber Governance in a company's position relative to the Cyber Quandary Curve is so substantial that it's better to have below-average cyber technology controls with solid Active Cyber Governance than be a company with solid cyber technology controls and below-average Active Cyber Governance.

The problem with which organizations are confronted is unrelenting change and open-ended systems complexity. Inability to reconcile the intricacy of all the moving parts often leads Organizations to deem cyber tools and countermeasures as adequate defense. But without a robust Active Cyber Governance system to reconcile cybersecurity structures, technology controls and cyber resiliency capabilities, a Company's cyber posture is more happenchance than adequate. Imagine a financial system that did not perform rolling reconciliations and provide periodic reporting to snapshot health, highlight trends, and provide actionable information to improve outcomes in the coming period . . . Without the financial reconciliations and periodic reports, that financial system and Organization would blindly roll forward–until it didn't.

Now imagine, an Organization with a cybersecurity and resiliency system that does not perform rolling reconciliations and provide periodic reporting to snapshot health, highlight trends, and provide actionable information to improve outcomes in the coming period . . . If you can, if that is your Organization, don't just be concerned, commit to Active Cyber Governance. The alternative is that your business will roll along—until it doesn't.

So, what does it mean to commit to Active Cyber Governance? It means to implement and run cybersecurity and resiliency with the same diligence and rigor as we do our financial systems. Organizational awareness and prowess of cybersecurity and resiliency is a competence, as necessary as financial competence, to compete and gain advantage in the digital marketplace. Without Active Cyber Governance, organizations lose the ability to be nimble, opportunistic and evolving because at some point a cyber event will cause them to stall.

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 ACG connects cybersecurity activities to business mission and activities. That connection provides 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 system for managing cybersecurity and resiliency in the same way companies need financial and ERP systems to manage costs and resources. ACG 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 awareness 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.

"It is not only what WE do, but also what WE do not do for which WE are accountable."
--John Baptiste Molière

This is the fourth article in a series on Cyber Governance, Risk Management and Resiliency. All are broad and deep topics and every facet 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.

[i] See the second article in this Cyber Governance series, 'The Cyber Quandary Curve—it is fraught with risk and danger and it is here to stay'.