Securing the Mosaic: Strategies for Strengthening Enterprise Cybersecurity

Diana Burley, PhD, Executive Director & Chair at Institute for Information Infrastructure Protection

Enterprise environments are characterized by an increasingly complex mixture of devices, networks, and computing platforms. Some of these devices are owned and controlled by the enterprise. Others are not – think BYOD and the increasing number of IoT devices. The networks often span organizational (agencies, departments, external contractors working onsite, partners, suppliers, and customers), and geographic (everything from multi-national corporations to non-local employee travel with corporate or personal devices) boundaries. Necessarily, a mosaic of policies and procedures secure this complex array of functional requirements and security assumptions.

The trouble with this fragmented approach is that while the requirements and assumptions may hold true for specific devices in specific contexts, it is in the interface between devices, systems, and organizational units; as well as in the flow of data across entities, where vulnerabilities are often exploited. The security issues and basic assumptions driving functional and security decisions across the different system components can be unknown, very different, or just too complicated for any one individual (or even one set of

individuals) to understand comprehensively in terms of security and functionality.

That said, below I identify three strategies to manage a massive global cyber attack and maintain calm with key stakeholders. First, identify the full array of stakeholders and develop a specific approach to engage each group. These individuals include senior executives, project managers, administrative and end users, network and system administrators, security operations staff, testers, developers, legal and regulatory affairs officers, … – anyone and everyone who (1) has an interest in the security of enterprise operations; and (2) can ensure that business priorities, workflows and usability concerns are considered. In determining stakeholder groups, ask questions such as: Why is this group important in the process? What is their typical background? What are the likely challenges to their participation and how can you overcome them? These questions will aid in developing a holistic approach to security awareness and in applying targeted intervention strategies. Enterprises should engage in a training that addresses the full spectrum of resistance – behavioral, cognitive, and emotional.

Second, address the knowledge gaps that prohibit the tight coupling of system processes and policies; creating vulnerabilities in the interface that expose the system and its components to exploitation. The separation of people and processes also encourages the growth of a cultural divide among different stakeholder groups that can hinder cooperation in the development and implementation of a holistic cybersecurity strategy. Security gaps persist because groups see the world differently, speak different languages, and have different (often competing) priorities.

Third, incorporate business processes and usability at the beginning and throughout security planning processes. Discrepancies occur for several reasons but

regardless of the reason, convenience matters. Users must be able to use the system without cumbersome, unnecessarily complex security requirements that run counter to natural business flows. In a battle between business flows and security – business flows will win. More broadly, in a battle between convenience and security – convenience will win. Taken together, these strategies will strengthen the security posture and enhance enterprise resiliency.

About the Author: *Diana Burley, PhD, is the executive director & chair at Institute for Information Infrastructure Protection. A full professor at The George Washington University, Dr Burley is one of the country's leading cybersecurity experts.*