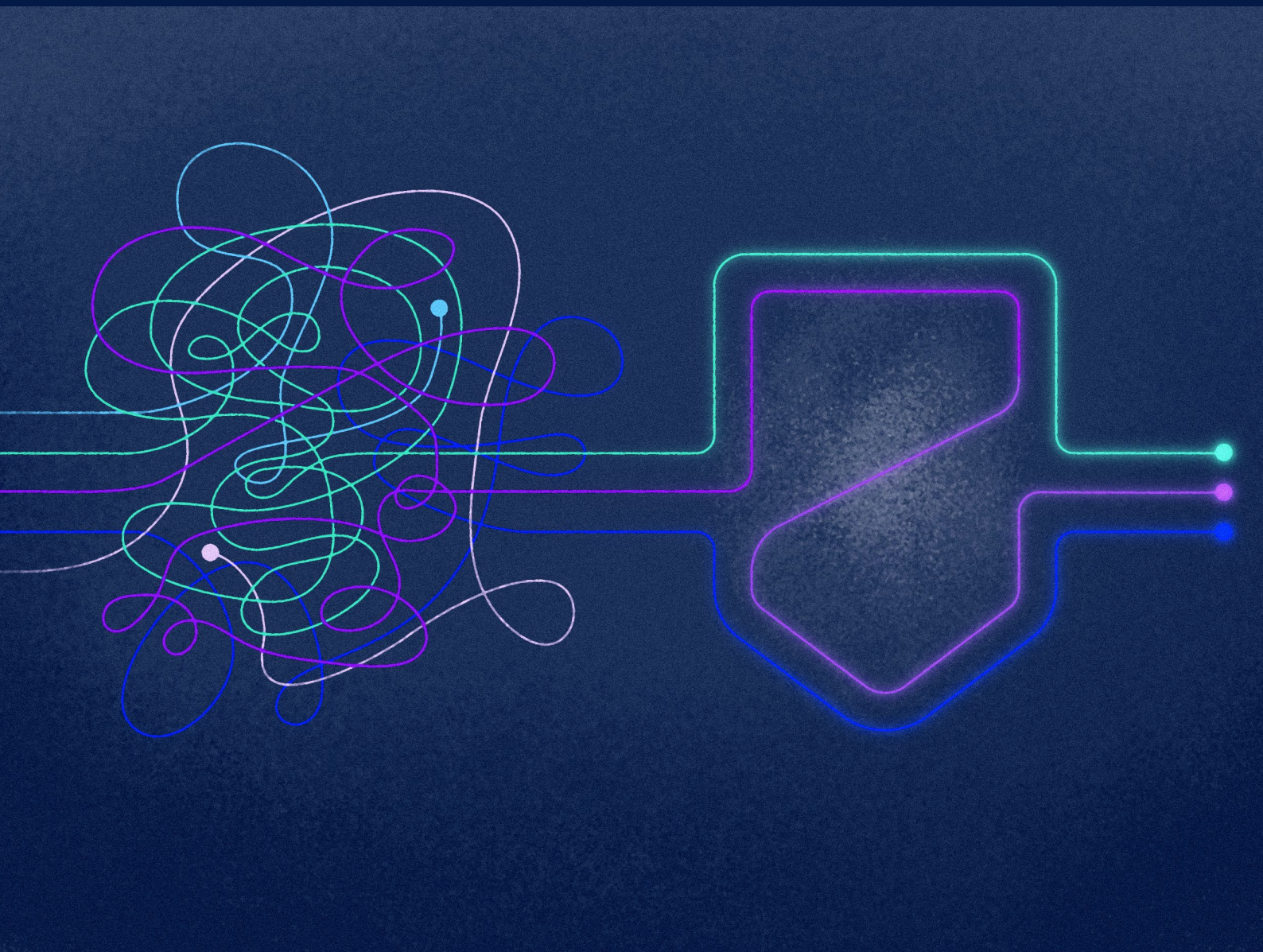
ISTARI Perspectives

How Simplicity Can Lead to Improved Security

Curtis Dalton

12 • 2021



By simplifying their cybersecurity technology stacks, organizations can reduce risk, improve cost efficiency, and minimize cybersecurity failure.

Businesses are finding themselves pulled into a new kind of arms race - a cyber arms race. As cyberattacks morph and proliferate, the number of tools designed to meet new threats increases – as do anxious buyers' purchases. Over the past several years, studies have indicated a steady increase in the number of cyber tools used. In 2019, a study indicated that the average organization was deploying 47 different cybersecurity tools. In some large companies, the average topped 130. Since then, amid rising attacks and fueled by a ransomware epidemic, the cybersecurity tool sprawl has increased even further.

Yet, despite rising security budgets and the proliferation of new cyber tools with enhanced security features, attackers appear unhindered. Even worse, all this spending may be leaving some companies less safe. A global survey conducted by the Ponemon Institute in 2020 found that enterprises that deployed over 50 cybersecurity tools ranked themselves 8% lower in their ability to detect threats and 7% lower in their defensive capabilities than companies with fewer toolsets.

Do the large number of cyber tools in our environment decrease the effectiveness of our security programs?

The Problem with Complexity

Decades ago, Yale sociologist Charles Perrow conducted an in-depth study of the nuclear power industry and uncovered a strong connection between complexity and failure. His analysis found that multiple and unexpected failures are inherent in complex systems and make accidents unavoidable. Perrow further determined that technology itself is not the problem. Instead, organizational and management factors are the leading causes of failures.

The parallels from this industry are instructive for our current cybersecurity challenges. In complex digital systems, the propensity to fail arises less from technology than from an organization's inability to properly adopt, deploy and manage its technologies. Acquiring innovative security tools with enhanced capabilities needs to be a component of our cybersecurity strategy. However, the key is to acquire these capabilities without fueling unnecessary complexity that can increase the likelihood of failure within the environment.

Steps to Achieving Simplicity

Organizations' security architectures tend to be fragmented and integrated in very complex environments. Yet, the most successful organizations are those that embrace simplicity, adopt a clear top-down strategy and only then consider their toolset.

The following three steps can help leaders simplify their environment and build a more digitally resilient enterprise.

1) Prioritize your biggest risks in terms of business value at risk.

To reduce some of the stresses placed on your cybersecurity teams and improve the effectiveness of your security program, avoid reacting to the threat of the day and craft a plan to reduce your most impactful business risks. Instead of reacting to threats, focus proactively on reducing business risk and change the conversation in your organization from threat to risk.

The first step is to identify and prioritize the data and assets most worth defending. At a high level, this step is about understanding the business's critical assets and processes, and the risk scenarios that may impact them. In the process of doing this from the enterprise level through the operational level, you will build out the threat models that are most impactful to your business. Mapping these threat models into a framework such as Mitre ATT&CK will enable you to identify both the controls you have and the controls you lack. Here, you will also be able to note

> "In complex digital systems, the propensity to fail arises less from technology than from an organization's inability to properly adopt, deploy and manage its technologies."

where you have overlapping controls and potentially some unwanted control complexity in your environment. Each threat model you build must identify what the impacts to the business are if the threat was realized.

Next, you will need to prioritize which risk gaps you will address first and determine how you will address them. Understanding what hurts is one thing, but understanding what matters most is another. To help with these decisions, quantify the impacts (resulting in a number that represents the level of impact) and if possible, monetize them (converting the level of impact into currency) to better indicate their level of financial impact to the business.

2) Simplify your cyber security technology stack.

To simplify, optimize, and improve your cybersecurity, you will need to rationalize the cyber tools within your environment. Ask yourself what role each cybersecurity tool plays in reducing risk within your environment, and what the scope of that risk reduction is across the enterprise.

As a result, you will identify gaps in capabilities in some parts of your environment and overlapping capabilities in others. Addressing gaps in your environment is where most organizations focus; however, also consider areas where overlapping tool capabilities exist. A cyber security technology stack with too much redundancy may represent another form of unwanted complexity that diminishes the effectiveness of your cyber program due to the challenges created in adopting, deploying and managing additional tools.

3) Consider the implementation barriers that any new cybersecurity tool acquisition must overcome.

Before adding another cybersecurity tool, consider how existing teams will support it. Evaluate the skills, experience, and headcount across your security teams that manage and operate your current and planned cyber tools. The proper identification and analysis of cybersecurity tool outputs and events should not be considered trivial — entrust only well-trained practitioners with these duties. Your team's workload should also enable them with enough time to dig deeper into security analysis when indicators point them in that direction.

Unfortunately, widespread understaffing conditions have led to overly demanding workloads for security teams. In 2021, an ISACA survey indicated that 61% of organizations' cybersecurity teams are understaffed. A separate report cited a high number of alerts and complexity of operation as the number one and two challenges expressed by security teams. The fact is, cybersecurity teams are already strained and stressed. Before adding another cyber tool to your technology stack, ensure your team is capable of integrating it into your environment and effectively managing it to reduce your business's most impactful risks.

About the Author

Curtis Dalton is the Managing Director of the Americas for ISTARI. As a member of ISTARI's executive leadership team, his role contributes to the strategic direction and evolution of the company.

With 30 years of experience, Curtis has a long and distinguished career in cyber security serving as a global managing director within the largest consulting organizations, as global CISO for multinational companies, and as a board advisor.

1. Bricata, How Many Security Tools Does the SOC Have? Bricata, https://bricata.com/blog/too-many-security-tools-for-the-soc/
2. Sowell, B. (2019). RSA 2019: Most Organizations Use Too Many Cybersecurity Tools. BizTech, https://biztechmagazine.com/article/2019/03/rsa-2019-most-organizations-use-too-many-cybersecurity-tools
3. IBM (2020). Cyber Resilient Organization Report 2020. IBM, https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839
4. Perrow, C. (1984). Normal accidents. Princeton university press.
5. ISACA (2021). State of Cybersecurity 2021, ISACA, https://www.thehaguesecuritydelta.com/media/com_hsd/report/424/document/state-of-cybersecurity-2021-part-1.pdf
6. Dimensional Research (2020). 2020 State of SecOps and Automation: A Survey of IT Security Professionals, Dimensional Research, https://assets-www.sumologic.com/resources/brief/2020_State_of_SecOps_and_Automation.pdf