Centralized and Decentralized: Why Effective Cybersecurity Needs to Be Both

Like the Miller Light television commercials of yore ("Tastes great!" "Less filling!"), the debate between proponents of centralized versus decentralized cybersecurity sets up an intriguing but ultimately false dichotomy: To be truly effective, a corporate cybersecurity framework must embrace both.

The Case for Centralized Cybersecurity
Fans of the centralized approach argue that it allows companies to do a better job of assessing their risks by making it easier to define and measure the extent of the threats that they face.

For example, Audry Agle, senior information security auditor at Black Knight Financial Services, explains that, "If alignment across business units is important a centralized model would seem the proper choice. By directing and managing the program within a central governance body, all business units would be forced to abide by the same unified vision and policy set."[1] Agle contends centralized structure gives corporate leadership better oversight as there's only one place to go to assess the security posture of the organization. Centralized governance is generally more efficient, she adds, since resources can be leveraged across the enterprise, limiting duplication and improving cost efficiencies.

Further, the late Shon Harris, a noted information security consultant and author who had been an engineer in the Air Force's Information Warfare unit, insisted that, "Centralization allows security to be looked at as a business issue."[2]

The Case for Decentralized Cybersecurity
Proponents of decentralization counter that highly centralized solutions are fragile and extremely susceptible to environmental changes. "The high-level reason why decentralization yields greater resilience is that individual player's decisions must account both for the negative events that impact them directly, as well as the spread of fire due to the selfish choices of their neighbors," says Yevgeniy Vorobeychik, an associate professor of computer science at Washington University and a former research scientist at Sandia National Laboratories. "Thus, players build extra robustness into their configurations that is absent in a highly centralized decision."[3]

Another virtue of decentralized cybersecurity is that it increases the number of points of failure. That may sound ominous, at first. But it's actually a good thing, according to Stewart Dennis, CEO of the email service BitBounce. Dennis says it creates an environment in which a would-be attacker is forced to compromise more components and functions in order to penetrate a system.[4]

The Best Case: Centralized and Decentralized, Living Together

But just as beer drinkers came to recognize that Miller Light was both flavorful and less caloric, CISOs today should embrace a hybrid cybersecurity model with centralized and decentralized elements.

"The choice between a centralized and decentralized approach to cybersecurity isn't binary, observes Doug Grindstaff, SVP of cybersecurity solutions for the CMMI Institute. "The reality is that virtually every business should put some centralized measures in place, while allowing room for other steps to be taken in a more decentralized fashion."

Often, this is due to limited resources, Grindstaff notes, and not the outgrowth of some strategy. Likewise, there often isn't much coordination between the centralized and decentralized security teams. This could be a reflection of the company's culture, the result of one or more acquisitions that may have taken place, or some other factor.

But Grindstaff maintains that to achieve mature cyber resilience, an organization must thoughtfully develop its hybrid approach and can only achieve the appropriate balance between centralized and decentralized security measures after it:

1. Identifies the primary cyber threats it faces;
2. Prioritizes those threats based on their potential impact on the business; and
3. Aligns its cybersecurity investment to address them in priority order.

Freedom Within a Framework

To help companies systematically develop a hybrid cybersecurity approach, Grindstaff spearheaded the development of the CMMI Cybermaturity Platform. As opposed to various cybersecurity frameworks promoted by standards bodies and governmental agencies, such as the International Standards Organization (ISO) and the National Institute of Standards and Technology (NIST), which offer high-level prescriptive guidelines, the CMMI platform imposes a rigorous discipline on those organizations that seek to implement it.

"Hand 10 people a security framework and you'll get 11 different interpretations of what's required," Grindstaff quips.

To provide more concrete direction without mandating a specific set of requirements, CMMI devised an activity-based architecture for its framework. Developed as a self-assessment platform, in Grindstaff's words, "It encompasses those activities that a cybersecurity expert would seek to observe in order to determine an organization's level of cybersecurity maturity."

By requiring every group and business unit across a company to address the same set of potential vulnerabilities, for example, the platform uses a degree of centralized control to set standards for the entire enterprise to follow. At the same time, this allows for a healthy degree of decentralization and independence on the part of the various business units, which are responsible for their own self-assessment.

For example, Grindstaff says today's most popular cybersecurity framework and standards tend to treat every threat as equally important. In reality, however, "Only about 50% of an organization's assets are truly critical," Grindstaff explains. "By spreading yourself too thin and not focusing on protecting the absolutely vital assets, a business can waste up to 80% of its cybersecurity investment."

In contrast, the framework developed by CMMI requires an organization to prioritize its data assets and risks—encouraging it to concentrate its security resources where they will have the greatest impact, instead of squandering them on secondary concerns.

That makes the CMMI Cybermaturity Platform an ideal framework for building highly resilient, centralized-and-decentralized cybersecurity cultures. While it imposes a process on the enterprise in a centralized fashion, specific decisions about which assets to prioritize are made by the different business units in a highly decentralized manner. "This is programmatic guidance," says Grindstaff. "It doesn't ensure that the right cyber-security measures are in place. What it does ensure is that an organization is taking the right steps to get them in place."

---

[1] 'Information Security Governance: Centralized vs. Distributed,' *CSO,* https://www.csoonline.com/article/2123153/information-security-governance--centralized-vs--distributed.html

[2] 'Should an organization centralize its information security division?' *TechTarget,* https://searchsecurity.techtarget.com/answer/Should-an-organization-centralize-its-information-security-division

[3] 'Security and Network Effects: Centralized and Decentralized Perspectives; Sandia National Laboratories,' https://www.sigecom.org/exchanges/volume_10/3/VOROBEYCHIK.pdf

[4] 'How can decentralization improve cybersecurity?' *Medium,* https://medium.com/@stewart_dennis/how-can-decentralization-improve-cybersecurity-d9b835c69834