Figure 10

NIST Framework for Improving Critical Infrastructure Cybersecurity

Note: NIST is National Institute of Standards and Technology.

Sources: National Institute of Standards and Technology; A.T. Kearney analysis

or overestimate their cybersecurity requirements in the absence of a strong vision for cyber risk management. A structured approach optimizes finite resources to deliver exceptional protection appropriate to the risk they represent if the assets are strategically prioritized and apportioned. Otherwise, as is often the case, there is little thought given to how systems are designed or deployed, and the entire organization must undergo costly remediation to protect select assets.

The National Institute of Standards and Technology (NIST) framework[16] recommends five functional capabilities for achieving comprehensive, cybersecurity defense: identify, protect, detect, respond, and recover. While businesses in the region are largely focused on the identify, protect, and detect functions of the cybersecurity life cycle, we are seeing the need for greater awareness and investment around recover and respond (see figure 10).

> "There is a lot of movement in the recovery and respond parts of the life cycle but still a lot of emphasis on protect."
> **—global director of cybersecurity solutions, global energy management and automation company**

[16] The NIST Framework for Improving Critical Infrastructure Cybersecurity is a set of industry standards and best practices to help organizations manage cybersecurity risks.