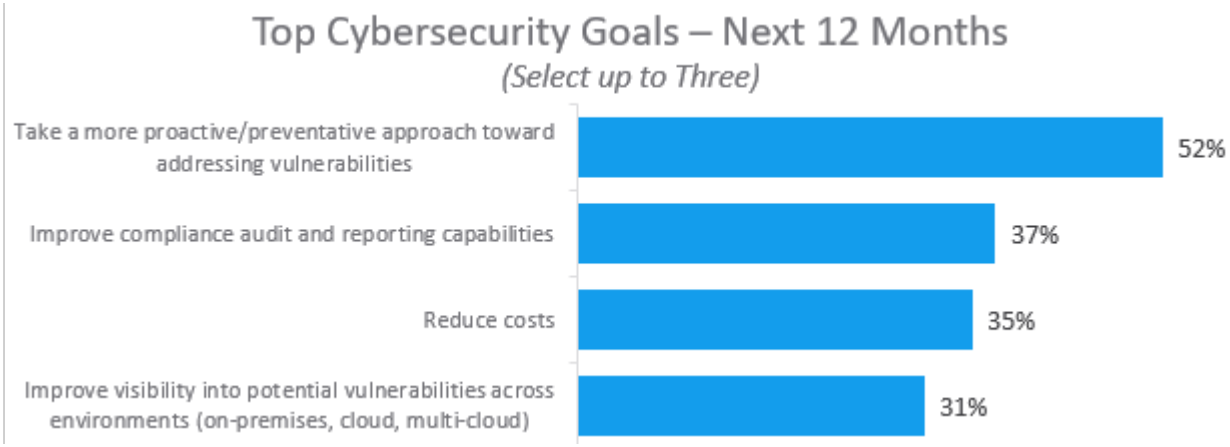
STATE OF CYBERSECURITY IN THE US FEDERAL GOVERNMENT

Federal Cybersecurity Survey Says...

RightStar and BMC last month sponsored a federal IDG survey to better understand different agencies' maturity with processes for cyber remediation, and to uncover additional capabilities that they would find value in taking a more proactive approach to cybersecurity. The survey was fielded in the US from November 28 to December 12, 2018 and consisted of 100 qualified completes. Here are the highlights.

The top cybersecurity goal for Federal organizations is to take a more proactive approach toward addressing vulnerabilities. When a security incident occurs, the most common response is the "swivel chair" approach where the Operations or Security teams use network management/analysis software, scanning tools, and eventually remediation software to analyze and fix the problem. The overarching objective, of course, is to prevent the incidents from occurring in the first place.



Government organizations have some ability to map vulnerabilities to critical or non-critical applications, but less than half (43%) are able to do so to a great extent. The increasing popularity of application discovery and dependency mapping tools such as BMC Discovery, illustrates that agencies are becoming more and more proactive about addressing vulnerabilities long before they happen. For example, BMC Discovery can map out which applications or business services run on which servers and network devices, or identify blind spots—servers and network devices that are not visible to the vulnerability scanner and are therefore not scanned. This operational intelligence makes security analysis faster, more accurate, actionable, and proactive to help organizations better manage and mitigate risk.

TrueSight Operation Management, combined with TrueSight Vulnerability Management, is BMC's "manager of mangers' solution providing a single pane of glass approach across multiple domains. By integrating with other automation and scanning tools such as Rapid7, Tenable, and Qualys, teams can quickly consume scans and automatically tie vulnerabilities to known remedi-ations.

Interestingly, last week we had a conversation with a DOD lead architect for the fourth estate, an effort to consolidate services from 16 DOD organizations into one, with 430 sites, and more than 500,000 employees. The DOD CIO's mandate is to reduce the DOD data center footprint and streamline cybersecurity infrastructure. It is, therefore, no coincidence that the DOD understand the importance of fit and function, as they move towards a standardized DOD security/operations tool platform.

Click here to view full study.