Forbes insights

BMC 2019 SecOps Survey

Results Summary

Overview

Forbes Insights conducted a study in partnership with BMC to better understand how organizations balance the completion of routine, tactical tasks with more broader, strategic initiatives in their security organizations.

The survey gathered opinions from security executives and managers across the globe and found:

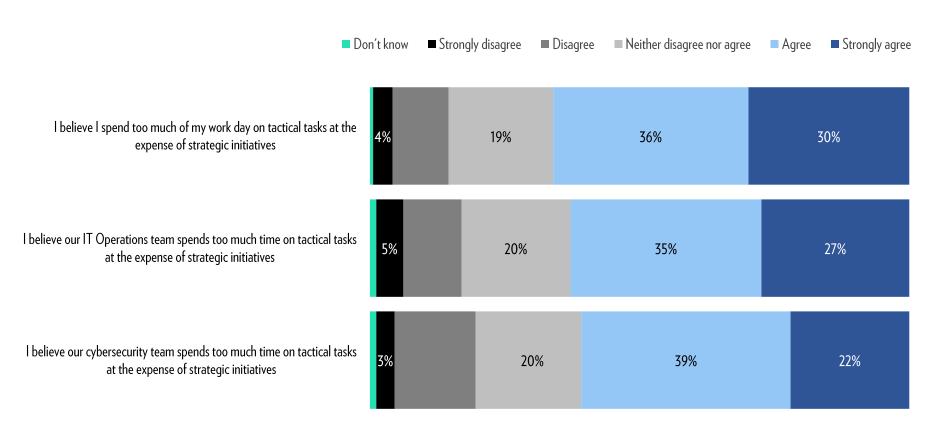
Taking employees off of the tactical and routine and allowing them to focus on the strategic and high-impact will help security organizations attract and retain the best talent, while also getting them concentrated on the most important tasks when it comes to finding a solution to cyber-risk. An effective way to accomplish this is to automate and the most tactical and routine tasks.





A majority agree that too much time is spent on tactical tasks

Q1 - To what extent do you agree with the following statements?





There are a variety of tasks that IT Operations teams hate do do

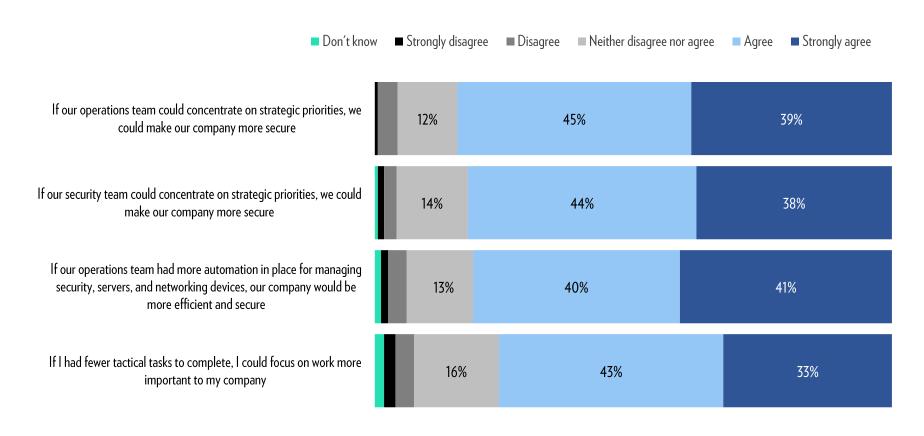
Q2 - The following are tactical tasks required by many cyber-security programs. Please select the one that you least like to work on.

	-
10%	Reviewing vulnerability scanner reports to identify assets scanned, compare with known asset lists, lentifying blind spots, and scanning known assets that were missed and are a 'blind spot' (or not scanned)
10%	Obtaining change approvals
8%	Generating reports for management
7%	Analyzing scanner vulnerability data, mapping IP addresses in the reports to actual assets, and then to business services running on those assets that are exposed to those vulnerabilities
7%	Completing audit trail of actions taken
7%	Analyzing new scan reports that may contain vulnerabilities with remediations already in process
6%	Generating the vulnerability scanner data/report (i.e. the Security team gathering data to provide to the Operations team)
6%	Making configuration changes needed to remediate a vulnerability
6%	Analyzing scanner vulnerability data and mapping the vulnerabilities to remediation content (i.e. patches)
6%	Closing the problem according to change management processes (i.e. 'closing the ticket')
5%	Assembling required information and opening remediation change tickets
5%	Updating the service desk on patches
4%	Ensuring remediation compliance with processes and regulations
4%	Prioritizing vulnerabilities for remediation
4%	Executing the remediation action (i.e. patching or configuration change)
4%	Verifying the remediation was successful



Respondents agree: if they had more time, they could focus on more important things

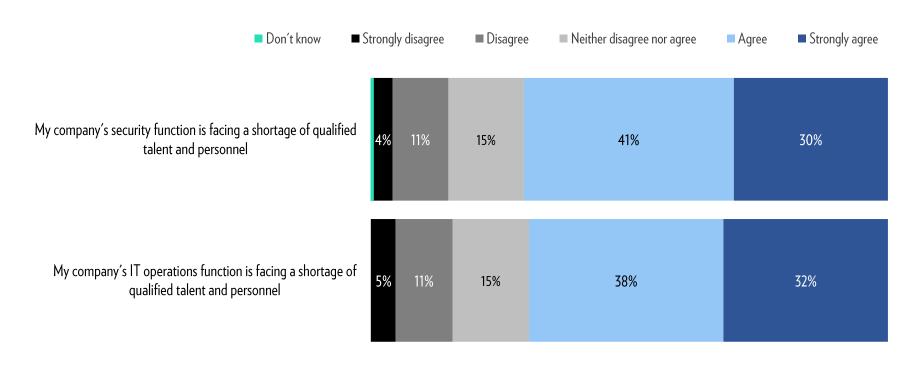
Q6 - To what extent do you agree with the following statements?





Companies are facing a shortage of both qualified security and IT operations personnel

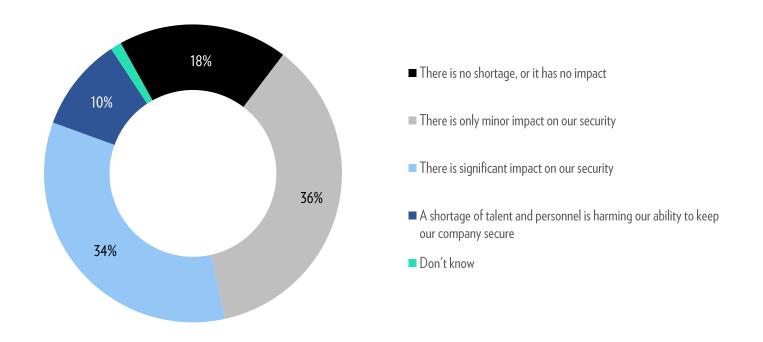
Q9 - To what extent do you agree with the following statements?





Eight in ten say the shortage of talent has an impact on their security; nearly half say it is significant

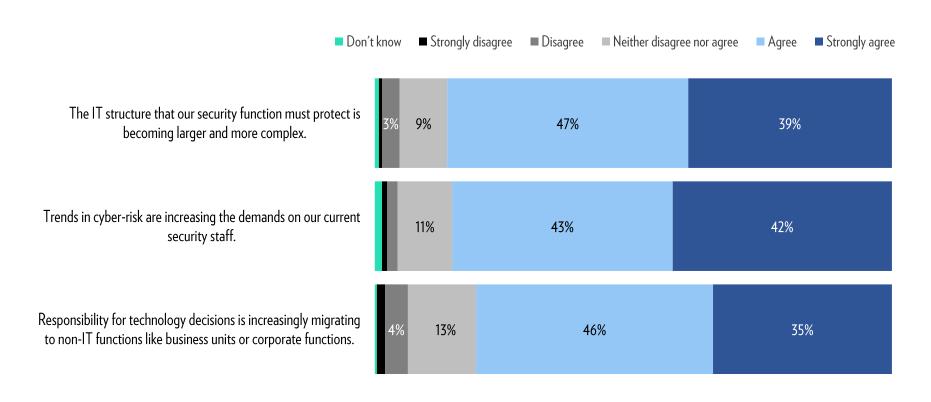
Q10 - Please assess the impact of any shortage of security talent and personnel on your company's security.





As demands increase, the responsibility for IT functions is migrating outside of IT

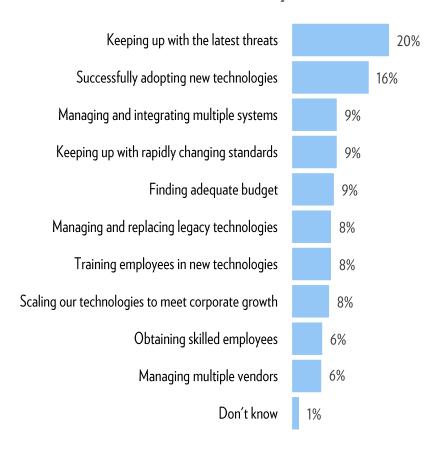
Q14 - To what extent do you agree with the following statements?





Keeping up with threats and successfully adopting new technologies are among the greatest challenges

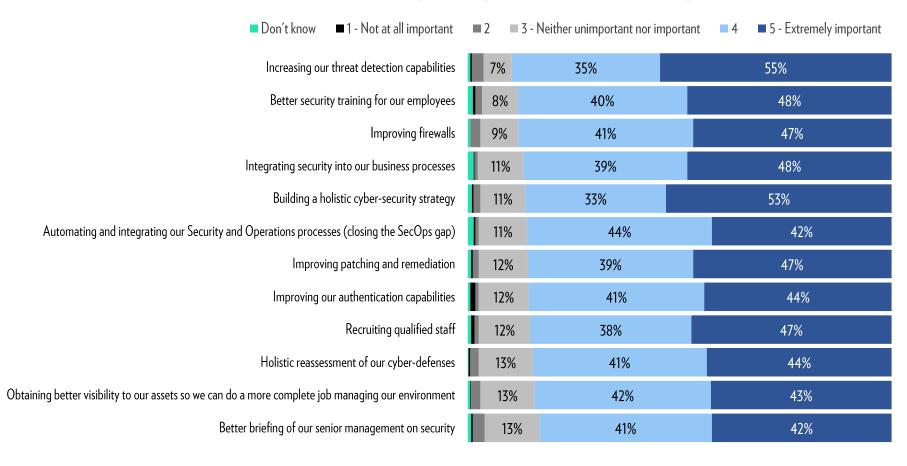
Q19 - What is the greatest single challenge your company will face in maintaining security in the next five to ten years?





Organizations place high importance on new strategic initiatives

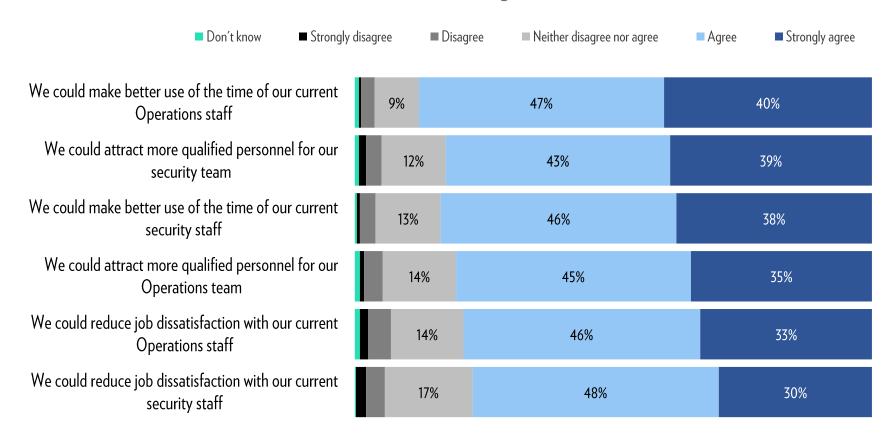
Q8 - How important are the following strategic initiatives to your organization?





If firms made work more strategic, they believe they attract better talent and make better use of their time

Q13 - To what extent do you agree with the following statements about making work more strategic?



If security leaders had more time, they would take on more initiatives, led by automating processes

Q7 - If you had more time to devote to the following cyber-security initiatives, what would be your first priority? – Ranked by Frequency

Highest Priority

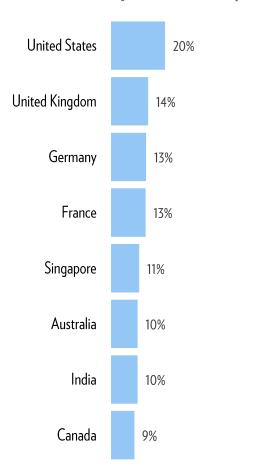
- Automating and integrating our Security and Operations processes
- ② Obtaining better visibility to our assets so we can do a more complete job managing our environment
- Better security training for our employees
- 4 Increasing our threat detection capabilities
- **5** Creating a holistic cyber-security strategy
- 6 Recruiting qualified staff
- Integrating our security solutions so they work as one
- 8 Integrating security into our business processes
- 9 Holistic reassessment of our cyber-defenses
- 10 Identifying blind spots and closing them
- Better briefing of our senior management on security
- Improving our authentication capabilities
- 13 Improving firewalls
- Reassessing our security vendors
- Improving patching and remediation

Lowest Priority

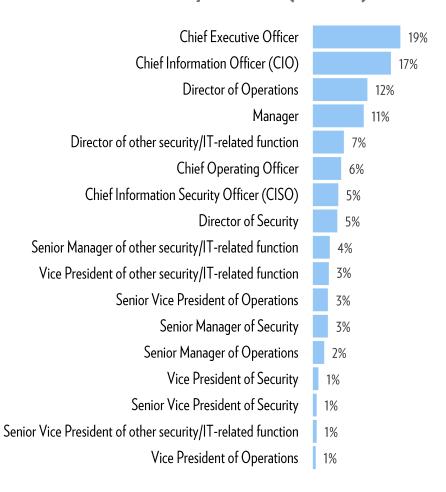


Demographics

S2 - Where are you located? (N = 500)



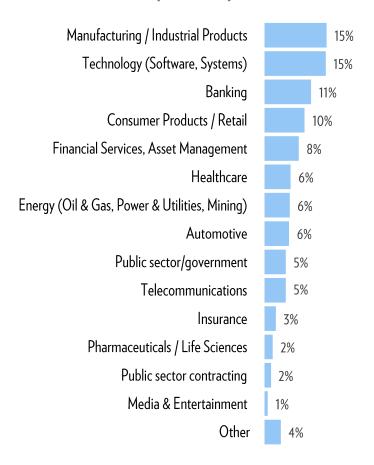
S3 - What is your title? (N = 500)



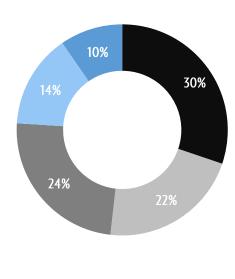


Demographics

S4 - Which best describes your industry? (N = 500)



\$5 - Approximately, what are your firm's annual revenues?(N = 500)



- Between \$500 million and \$1 billion
- Between \$1 billion and \$2 billion
- Between \$2 billion and \$5 billion
- Between \$5 billion and \$10 billion
- More than \$10 billion