BEST PRACTICES FOR BUILDING AN INSIDER THREAT PROGRAM

1 Consider the why

so you can understand the intent of behavior—malicious or compromised

2 Adapt language to culture and audience

to ensure organizational adoption

3 Present the program as a partnership

through transparent, clear, and honest communication

4 Focus on the positive outcomes

with a collective approach that addresses both company and employee benefits

5 Prioritize the role of culture

to guide users to make smarter decisions about data

6 Align around executive and board responsibility

to foster continual support

7 Focus technology investments on the outliers

with forensic capabilities that establish the norm so you can quickly identify when it deviates

"In an insider threat program, you're looking for strange behaviors that are not normal for an employee—be it because someone else is using his or her credentials, or because the employee may be doing something accidental or malicious."

Gary Harbison, Monsanto Company

FORCEPOINT.COM

FORCEPOINT