HOW TO MEASURE THE EFFECTIVENESS OF YOUR CYBER SECURITY PROGRAM

01 Increase in Reports of Phishing, Lost Devices & Other incidents
When security awareness is going up, you expect to see an increase in the accurate number of reports coming into InfoSec.

02 Decrease In Clicks From Phishing Tests
Phish testing puts the effectiveness of security awareness training to the test by reinforcing what has been presented.

03 Decline In Confirmed Incidents
When your cyber security awareness training is effective, you should see an overall decline in the amount of incidents year over year.

04 Decrease of Policy Violations
Adhering to security policies is usually a result of understanding why we implement these controls. Instead of bypassing them, people feel comfortable reaching out to the security team.

05 Increase In Employee Questions
A great way to measure engagement is to track how often employees ask questions. A ticketing system, google forms or in-person all work.

06 Increase In Security Team Involvement
Measure how often people are asking the security team for help to ensure their projects are “secure by design.”

07 Increase In Requests For New Technology
If people are asking for permission to use new technologies, it is a sign they understand the risk and wish to mitigate it. It also shows a healthy collaboration with the security team.