Measuring User Behavior

The 12 Key Metrics for Security Awareness

For a sample of the cultural assessment report email culture@madsecurity.com
The 12 Key Metrics for Security Awareness

Mike Murray - Managing Partner
Katrina Rodzon - Manager Security Behavior Design
Human beings adjust behavior based on the metrics they’re held against. Anything you measure will impel a person to optimize his score on that metric. What you measure is what you’ll get. Period.

Dan Airely
Harvard Business Review
Measuring User Behavior
The 12 Key Metrics for Security Awareness
Security Responsiveness
Key Metric:
Number of Reported Incidents
Sensitive Data Handling
Key Metrics:
DLP Violations
Audit for PII/Sensitive Data leakage
Online/ Browsing Hygiene
Key Metric:
Number of visits to unapproved sites (from Web Content Filter or IDS/IPS)
Email Hygiene
Key Metrics:
- Email Filter Acceptable Use Violations
- Abuse / AUP Violations reported to HR
Phishing Resilience
Key Metrics:
Phishing Audit Susceptibility
Phishing Audit Report Rate
Probable Phishing Attack Rate
Passwords
Key Metric:
Average time to crack (MTTC)
Insider Threats
Metric:
Detected Insider Attacks
Reported Insider Incidents
Working Remotely
Key Metric:
Attack Incidents through VPN
% of Infections While Remote
Device Protection
Key Metrics:
Number of lost devices
Average time to report loss
Online Information Hygiene
Metric: Social Media Audit
Computer Behavior Awareness
Key Metric: % of infections user-reported
Physical Security
Metric: Physical Security Audit
The 12 Key Metrics for Security Awareness
Frequency
Type of Collection: Assessment Real-World
For a sample of the cultural assessment report email culture@madsecurity.com