SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Metrics > Employee Awareness Program >

The Risk-Aware Organization

Created by George Campbell, Security Executive Council Emeritus Faculty

Security practitioners often equate security awareness programs with posters in break rooms, intranet alerts and informative brochures on the risk of the month. While these media serve a useful purpose, Security's risk awareness strategy must be significantly more disciplined and structured than a periodic communication exercise.

The test of sufficient awareness is found in the midst of crisis. As security professionals, we are paid to anticipate. We must proactively identify what could go bump in the night and determine how to prevent, detect and respond to it. Risk awareness is the result of planful action involving multiple steps:

1. Planning: A risk-aware organization has an established, enterprise-wide risk assessment process that provides qualitative information on the vulnerabilities of enterprise assets and mission-critical business processes. It tests the resilience of safeguards and eliminates plausible denial through focused analysis with up, down and sideways reporting. It addresses the concept of likelihood by understanding the degree of exposure gleaned from testing, incident post mortems and intelligence. It understands how combinations and multiples of risks can interact and thereby increase exposure.

2. Preparedness: The risk-aware organization operates the radar on high strength but carefully avoids what we may call the "Chicken Little" syndrome. It looks for the cues but exercises caution by testing and qualifying the data being received. It uses metrics as detective indicators that serve to inform and alert on changed risk conditions. It has pushed accountability for risk awareness down and out within the enterprise and set clear expectations on timely escalation of concern. Business processes are prioritized, risk tolerances set and responsibilities assigned. Plans that address the range of consequential events are developed and tested.

3. Training of response resources: Awareness has to be ingrained at the beginning of employment and tested over time. In the risk-aware organization, orientations of new employees and resident contractors incorporate a fundamental understanding of risk and obligations of response. Because this is a learning organization with educated, knowledgeable players in key positions, awareness is reinforced through training exercises that dissect incidents to identify root causes and test to affirm that the players know the plays.

Proven Practices from George Campbell

Looking for more metrics help? The Security Executive Council's new Proven Practices Library includes a detailed presentation by George Campbell on Building a Security Measures & Metrics Program. This 45-minute presentation includes

- a ground-level explanation of why security metrics are important;
- specific examples of measures & metrics adaptable to your data input; and
- a framework for assessing the need and building a tailored program.

4. Incident response: The risk-aware organization is proactive. This is about the interdiction of risk due to foreknowledge. If our awareness efforts enable someone to identify and report or respond to conditions that will likely lead to an incident, we have a powerful measure of security program effectiveness.
We are here because the business recognizes that bad things will occur and the organization has to be prepared to take definitive steps to minimize the consequences. Risk awareness provides the foundation of our ability to react with timely competence. This is a key performance measure of our preparedness to minimize the consequences of the risky event.

5. Consequence analysis and follow- up: Measureable reductions in risk exposure may be found in a disciplined lessons-learned or after-action analysis. This is a key element of maintaining a responsive risk awareness program. It's about learning. Through this process, we identify the gaps in our protective measures and the competence of our response.

Awareness is synonymous with watchfulness, vigilance, responsiveness and alertness. These terms work well within our security mission. Where we enable our clients to be knowledgeable of risk and their responsibilities to prevent and respond to the indicators, we have an incredibly powerful multiplier effect in the ability to deliver measurable value to the enterprise we serve.

Originally published in Security Technology Executive

Visit the Security Executive Council website for other resources on Security Metrics: Measuring Awareness Programs

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website here: https://www.securityexecutivecouncil.com/

