Pythia Cyber

Our BARC Makes Your Bytes Better

TL;DR: Incorporating cybersecurity into performance management is good business because some people don't or can't follow your rules

Starting in the late 1980s the professional psychology community has coalesced around a model of work performance with two sets of behaviors. One set, which included cognitive ability and physical skill, was labeled "Can Do" because it includes the human capacity to perform at maximal capacity. The second set included personality factors and motivational dispositions. This set was labeled "Will Do" because it includes the human tendency to perform at typical capacity. For decades, psychology made do with Can Do and Will Do

The model of work performance started broadening in the late 1990s, a trend that accelerated during the COVID-19 pandemic. People at work cannot be neatly sorted along a continuum of "poor performer" to "good performer;" people don't just do productivity-related things either well or not well. They also do counterproductive things such as destroy property, steal intellectual property or materiel, misuse company cybersystems, pad their expense accounts, or commit time theft (e.g. don't work time claimed to have worked, claim sick leave when they are not sick, etc.). Counterproductive behavior is not poor performance, it is an intentional set of actions designed to benefit the person doing them. Call these "Won't Do" behaviors because the people engaging in them are willfully ignoring standards, rules, and policies out of a sense of perceived entitlement. The entitlement arises either because the person feels the organization "owes them" or because the person feels that their (self-regarded) high performance entitles them to get away with doing things others can't get away with, thus validating their inflated sense of self.

Alleged counterproductive behaviors, generically phrased as "weakened company culture" and particularly focused on time theft, are the rationales used by companies cutting back on their work-from-home policies to being back full-time in the office. It's an open question whether counterproductivity will increase among employees forced to return to the office who in turn feel the organization owes them something for coming into the office five days a week.

Beyond normal defiance: Threats

National security psychologists and cybersecurity personnel in the mid-2000s expanded this performance model based on reviews of security incidents. At a darker level beyond Won't Do behaviors, sometimes people engage in threat behavior. Dramatic yet surprisingly common threat behaviors include extortion – denial of service attacks (DoS) are examples of extortion – and espionage, which involves betraying state secrets for ideology, money, vengeance, or to show how superior the person is compared to their colleagues. While espionage may seem to be a concern only for agencies that have classified information, this is not the case. Many organizations may not realize that their employees' (or clients') information could be valuable to entities that wish to harass or intimidate people with connections to those employees or clients. At a less headline-grabbing level, threat-oriented behavior includes harassment, sexist or racist behavior, or workplace violence. Any threat behavior can be a cybersecurity issue because of the inappropriate use, such as sending harassing direct messages over a chat or email system, or access of company systems.

Supervisors are unquestionably the first and best organizational resources for countering unproductive, counterproductive, and threatening behavior. However, supervisors may not be good at monitoring these behaviors or addressing them productively. Also, managers at higher levels of company organization charts may provide less immediate task oversight and more in terms of increased system access from having a "higher level job," increasing the chances for bad cybersecurity behavior.

An aside: Active threat situations

Workplace violence is not related to cybersecurity but is obviously a threat – and a very serious one. Any time an employee is in a state of elevated psychological distress (yelling, crying, pleading for help, etc.) or making threats of physical violence, take it seriously. Call company security or the local police.

How to defeat 'won't do' work behaviors and threats: BARC

PythiaCyber conducts behavioral reviews to determine whether and where practices exist that increase vulnerability. These reviews include qualitative (executive conversations, small focus groups) and quantitative (surveys) components. We refer to the review as a behavioral analysis of risks to cybersecurity, or BARC. The BARC includes questions and themes that identify the company's cybersecurity practices, attitudes, and understanding related to counterproductivity and threats. A manager might claim that this is already covered in an organization's annual employee survey or through its 'employee listening' process, but this is incorrect: these processes are valid for their purposes but they are focused on attitudes and perceptions that relate to productivity and leadership. BARC is focused on counterproductive/ 'Won't Do' attitudes and threat behaviors. Remember, counterproductivity is not the opposite of productivity, and it is useless to use a standard employee survey to find cybersecurity tendencies, correlates, or predictors.

Examples of themes in BARC include:

- Overall job satisfaction
- Perceptions of supervisor emphasis on ethics and good cybersecurity practices

- Feelings of organizational support
- Concerns over ‘change rage’
- Belief that managers address counterproductive behavior

Results of BARC are incorporated into a deliverable report that highlights areas within the organization that encourage, support, and expect better cybersecurity. This happens when cybersecurity is integrated with performance management. While supervisors are always the best sentinels for performance-related issues, they generally are not expected to consider cybersecurity practices in performance reviews. PythiaCyber’s approach focuses on that integration to create an organizational climate where ‘will do’ behaviors overwhelm ‘won’t do’ behaviors and threats.

BARC Process

1. Conduct executive conversations (2 – CEO & CTO/comparable, possibly also GC)
2. Conduct leadership focus groups (2 or 3)
3. Distribute survey via platform
4. Analyze quantitative data from survey
5. Integrate qualitative data with quantitative data, submit report, make presentation
6. Conduct behavioral change interventions such as:
    a. “Train the trainer” sessions with HR staff
    b. One-on-one feedback with managers based on their BARC scores
    c. Simulations of cybersecurity interventions for managers who may not feel comfortable having these conversations
7. Reassess after 6 months

Note that there are no “industry standard scores” for BARC. First, each client’s situation is different – network configurations, business model, dispersal of staff/business units (BUs), etc. Second, all too often leadership resists taking action because if their scores are “above industry standards.”

BARC Products

PythiaCyber works its clients through a process of improving cybersecurity by making it integral with productivity-oriented performance management. This directly involves understanding the attitudes, behaviors, and knowledge that prioritizes cybersecurity as part of an organization’s productive performance model. Because most managers dread spending 80% of their time with 20% of their underperforming people, and are not comfortable with having conversations about counterproductivity, and because almost no manager is qualified to have a calm and thoughtful discussion with a direct report about threatening behavior, we work with our clients to give managers the awareness and language to create a BU that prioritizes cybersecurity as part of productivity.

A significant conversation that managers may have with a direct report or a team is about the level of risk posed by an event or incident. Labeling any (possible) counterproductive behavior as a threat would paralyze any organization. Because productive people may engage in counterproductive behavior out of entitlement or inattention or lack of knowledge, managers need to have a way of engaging with staff that is exploratory without being accusative. Here are three examples:

A. One PythiaCyber staff member recalls a situation where a manager in a government agency tried to access a remote file server from her government computer to display pictures of her new grandbaby.

B. A different organization known to PythiaCyber installed an email scanning program with default settings to “solve” the problem of emails containing harassing or offensive material. While this intervention initially made the company’s General Counsel happy, the scanner quickly became problematic in its default setting when it automatically blocked emails containing words it considered possibly offensive – a specific example email was blocked when clients in a psychological experiment were asked for the sex of their participant personnel.

C. Another PythiaCyber staff member recalls a situation where someone with an advanced degree in computer science reconfigured a multifunction printer in his office to serve as a local network router.

D. A publicly known situation involved an Air Force reservist who downloaded classified documents and shared them on an external gamer site because it seemed like fun; in that case several of the Airman’s supervisors were relieved of command (i.e. they were fired) for lack of oversight.

In each case a cybersecurity risk assessment would have flagged the individuals as posing a threat, but a supervisor’s intervention would lead to different conclusions about the nature of the risk – in case A, none; in case B, none; In case C, some; in case D, high. Each situation implicates a robust cybersecurity-oriented performance-based culture that incorporates better judgment by humans and more effective monitoring by systems.

PythiaCyber specializes in creating robust cybersecurity that is part of routine performance management practices. Managers at all levels create a more effective, positive performance climate based on attitudes, behaviors, and knowledge about the role of cybersecurity. The result is higher quality supervision, better performance management, and better cybersecurity.

Examples of PythiaCyber thought leadership resources:

- *Consulting Psychology Journal* (Editor: Ted Hayes, Principle and Co-Founder, PythiaCyber): https://www.apa.org/pubs/journals/cpb

Relevant resources forthcoming in *Consulting Psychology Journal*:

- Change readiness – here is the call for papers: https://www.apa.org/pubs/journals/cpb/thriving-turbulent-times
- Emotional intelligence in organizations – here is the call for papers: https://www.apa.org/pubs/journals/cpb/emotional-intelligence-workplace