David B. Sidon, CPA
The Navis Group
www.navis-group.com

Risk's Common Thread

People

Enterprise risk is the buzzword, the mantra, the focus, the catch-all; technology risk, credit risk, interest rate risk, operational risk, BSA risk, information security (GLBA) risk, financial reporting control (FDICIA) risk, reputation risk, compliance risk, investment risk, pricing risk, this risk and that risk. Often silo'd within our banks, often misunderstood within our banks; often assessed without thanks.

So how do we pull this together into something cohesive and useful? How do we get to the "so now what?" moment? How do we gain some efficiency? How do we make this risk exercise a "value-add"?

What's the common thread? Fraud potential, compliance gaffs, missed annual policy and training deadlines, information breaches, suspicious activity, money laundering, security lapses, identity theft, short-sighted pricing and product decisions, poor investment choices, insufficient loan underwriting, and lackluster personnel management all have one thing in common – people! People commit fraud; people make poor choices, people execute tasks poorly. Systems aren't suspicious, but the people behind them are. The beneficiaries of identity theft and the victims of identity theft are people. Our customers are people. And, the folks that work for us? Guess what? People!

How do we assess the risks inherent in our people? Our officers and staff? Our directors? Our trusted advisors? What are the risk criteria? What are the metrics? What are the monitoring, reporting and triggering mechanisms? Performance reviews doing the trick? Probably not. How often do you have to let someone go and find that the personnel file reflects a model-citizen, hard-working, team-focused individual; a far cry from reality?

In my 20 years in the industry, I have seen and experienced a full dose of "people"; belligerent, disrespectful, incompetent employees, bullying bosses, sexual discrimination and harassment, employees running their Mary Kay business on company time and equipment, porn on the job, solitaire on the job, theft, fraud in high places, fraud on the front line, fraud in the back-office, sedition, politics, as well as directors drunk, asleep, without their hearing aides, and watching I Love Lucy in the background while attending a board meeting "virtually". All true! Nothing made up. The sad common thread here? We paid 'em anyway! Little or no consequences. The good news? My description applies to only a small subset of the wonderful and brilliant folks who drive our industry. But no one who has ever worked in our industry is without similar observations about those-who-shall-remain-nameless.

People-risk recognition and measurement is a growing curiosity and challenge within the umbrella of enterprise risk management. There have recently been some thought-provoking approaches that are worth examining in my opinion.

In April, 2010, Bruce McCuaig wrote a blog (at inside-grc.com) entitled “PEOPLE RISK: THE IMPACT OF HUMAN FAILURE IN GRC AND WHAT TO DO ABOUT IT. PART 1” In his writing, he suggests four categories of potential human failure that I have taken the liberty of re-stating as follows:

A Purpose / Understanding / Alignment
B Capability / Knowledge
C Commitment Risk (over/under incented)
D Integrity / Honesty / Ethics

If we add a few more categories, we perhaps have set of metrics to consider:

E Performance standards – day-to-day – strategic objectives
F Teammate / Grown-up quotient
G Social / Cultural behavior
H Growth potential
I Management / Leadership

And a few more attributes to round things out a bit further:

J Risk level – information security (GLBA)
K Risk level – corporate / personnel information and strategies
L Essential? (in a business continuity sense)
M Succession planned for?

So ….. in the many instances where we might have a senior officer of an institution that we decided we need to let go after 10, 15, 20 years or so, with documented performance reviews with nary a negative observation, we might use the above scorecard to create this (fictional) picture of a “composite” employee:

Our subject individual might have A) good understanding and alignment; be B) very knowledgeable but not fully living up to his/her capabilities; have C) reached a compensation dead-end due to his/her tenure, resulting in a feeling of a lack of incentives; however D) honest and ethical he/she is. Performance might be E) OK at a basic level; is F) & G) disruptive in a team setting; which has H) truncated his/her growth potential and brought I) leadership characteristics into question. Since back at “D” we assessed integrity and ethics as a positive trait, J) & K) risk levels would be low; and since this person is a senior officer, the question of L) essential is clear, but our conundrum could be currently exacerbated because we’re not sure what the M) succession plan is for this position.

Does this narrative paint a different picture than the personnel file with its required impotent performance reviews? The narrative tells us why we are considering termination, the performance reviews turn out to be useless. In reality, they usually are, at least at the senior level. And where’s the first place we go at the point of

firing? The risk level; always extra paranoid that in springing this termination, the employee's ethics fall apart and we had better plan a smooth escorted exit and orderly transition.

The reality of most of these situations is that there is no documented negative in the personnel file, so we pay extra, extra and more extra in severance to avoid an ugly scene. Who's fault is that? Always a person, but you might need to look in the mirror for this one, at least for complicity. I know I've been guilty of this in my career.

Wouldn't the suggested metrics provide a bit of clarity and honesty. We might have a quite adequate employee that we would never let go, but if we see no growth potential or ascension in sight, shouldn't we so state? We know it, we just don't say it. Too impolite. Obsolescence is a key metric for hardware and software. Callous to think about the human system that way? I guess so, which is the conundrum in a nutshell – how do we get to be honest about this without looking like a hard-hearted automaton?

Coming back to Mr. McCuaig's narrative, it is beautifully crafted as he tells the tale of the airline pilots that apparently fell asleep and overflew their destination a few years ago. As a controls expert, he starts down the path of process improvement, better safeguards, improved controls and alarms, with a myriad of great recommendations and creative ideas. But then he leaves us with the punchline; the controls were not deficient, the people were.

Another interesting approach has been offered by SANS, the information security organization found at sans.org. In their "Securing the Human" program, they have put a huge spotlight on the 2-legged culprits. Suggesting metrics specific to information security, their program asks questions like:

- No. of people who fall victim to monthly phishing assessments
- No. of people who completed the awareness training
- No. of weak or shared passwords
- Employee scores from before/after testing
- % of users sampled with positive attitude towards information security
- % of users sampled who believe their actions can have an impact on security

Pick out the "human" components in the six items I have extracted from their list: victim, awareness, shared, before/after, attitude, belief. And yet, these metrics provide quite a picture of our tech users. As most of our institutions have undertaken social engineering tests, the results seem to range from fair to disappointing to dismal. There is seemingly no adequate on the scale, let alone terrific or perfect.

If evolution follows the path suggested in David Mitchell's "Cloud Atlas", we will someday have "fabricants" for each position, individuals "genomed" to serve particular roles; such as 20-hour tellers requiring no food or break, and little sleep to recharge. Model numbers such as Teller-327, and CSR-162 would be genetically free from all the problems we've been discussing. Pretty sure I have an idea of what the loan guy model would look like ☺. But until then ….

We're humans. Celebrate the diversity. Savor the complexity. Appreciate the humanity. Be patient with the newer models still learning the trade. Tolerate the tech-geeks. Respect the Model-Ts, the holders of the institutional knowledge. Put up with the minority of outliers? Your call. And one more thing, please don't let your HR director know we've had this little chat. I have probably suggested breaking more fair employment laws and HIPAA rules than I care to know about. Ignorance is bliss. I too am human.