

Webinar uncovers tip of proverbial iceberg

Practitioner's ethics

John Glenn, MBCI
Enterprise Risk Management Practitioner

I just eves dropped on an interesting Norwich University-DRJ Webinar that focused on professional ethics. The unseen duo on the other side of the WWW connection were John Orlando, the Program Director for the Master of Science in Business Continuity Management program at Norwich University and President Bob @ DRJ.

Unfortunately, the nature of the beast prohibits give-and-take discussions, but it does (should?) get people thinking.

I think everyone signing in to the "Ethical Issues in Business Continuity Management" webinar agrees that People Are Priority One. I confess that this came as a bit of a surprise to me since many people claiming to be "business continuity" planners put "Save The Data" as their top priority.

Grab laptop or not?

The question that prompted the "where do people stand" issue was "Should a business continuity plan insist that employees take their laptop computers with them when the alarm sounds?"

The general consensus was "No." I suppose many of the responses were based on user experience. My "out-of-synch" response was based on mine.

I used a laptop at my last staff job; it sat in a docking station with a one-finger quick release. On several occasions I did a quick R&R - Release and Run.

This is being created on a laptop that has three cables connected to it: a USB hub, power cord, and a speaker wire. Trust me, if the alarm goes off, I can disconnect everything in a matter of 3 seconds - probably less. The only difference between the "staff" laptop and my own is battery - my machine is battery free for at home use, which means that when I pull the power plug, I'm probably going to lose any work in progress. (Do I hear someone say "Save early and often?")

One of the participants suggested that as long as the person was at the computer, take it and run, but if the person was elsewhere, leave it and get out. Seems reasonable.

Then someone threw a legitimate money wrench into that (but easily handled). What, the query went, if some malcontent pulled the fire alarm and people exited leaving their computers on their desks and turned on. Good point.

All machines, especially those that may have sensitive information, should have short automatic shutdowns and require at least one password to reboot or even wake up. (Single authentication bothers me, but it's "better than nothing.") In a networked environment, there should be at least two levels of authentication: one for the machine and one for the network.

Guard the gate

There were 4 "security" questions.

Two addressed "improper" entry - tailgating, a/k/a piggybacking, and over-the-shoulder code snatching.

The first should be covered by policy - no tailgating allowed, period. State Farm Insurance had a rule that both the tailgater and the tailgated were fired if someone was caught coming in "two on a swipe card."

The peek-over-the-shoulder issue has import beyond the workplace ... think ATM.

I don't know how many offices still use push buttons for access, but staff must be aware that they need to protect the numbers - just as they (should) do when they are at the ATM.

It came to mind that personnel in both cases need awareness and safety training.

Training to make them more alert to their surroundings and the people inhabiting those surroundings.

At one client, I recommended a series of ID badges with different colors for different categories of people - normal photo ID cards for employees, and different screaming, fluorescent colors for vendors and visitors, both of which require escorts.

I know of one private school and one hospital that requires visitors to be photographed for a paper badge. The school used first rate technology - after a certain time, the badge picture and text faded away, much like the Cheshire cat in Alice in Wonderland. The hospital tag was dated and was supposed to be collected as the visitor exited. (The hospital tag also showed the entry door, very handy when the visitor failed to find his way out through the lobby's maze.)



© Walk Disney Studios

One of the security challenges was do you test a person's ethics by having someone offer that person a bribe to share corporate secrets?

This was voted down by the participants for a number of what this scrivener considers legitimate reasons including the idea that this was a no-win test for everyone.

Reveal and recuse, or just reveal?

The question was asked "If you are asked to review vendor plans for a critical product or service, and if you had created a plan for the vendor, and if you knew the plan was deficient, should you (a) excuse yourself from the review, (b) tell your current employer.

I have no problem telling my current employer that I worked for the vendor - it's probably on my resume anyway - but I would not recuse myself from the task at hand. Why? Glad you asked.

Let's say I created a plan for XYZ Company a couple of years ago. I know that XYZ failed to implement all of my recommendations. I know that's hard to believe, but budgets being what they are - or aren't - that sometimes happens.

But my recommendations were made two years ago - maybe (and in the case I am thinking about I know it's true) my recommendations were revisited and implemented.

Would it be fair for me to tell Current Employer than XYZ Company's business continuity plan is deficient? No. I don't know that it is; it was two years ago, but today is today. What I would do - as I have done - is ask to see plans, or at least what I deem critical parts of plans - from each of the competing vendors. (Truth be told, I make it Standard Operating Procedure, SOP, to ask all critical vendors for plans for all my clients.)

Over the years I have had potential clients ask to see plans I did for other organizations. My answer always is the same: No. I explain that plans contain sensitive information about the business. Then I ask if the potential client would want me to show their plan to other potential clients. Most quickly understand and withdraw their request.

All-in-all an interesting hour that could have easily expanded into several interesting hours.

John Glenn, MBCI, has been helping organizations of all types avoid or mitigate risks to their operations since 1994. Comments about this article, or others at <http://JohnGlennMBCI.com/> may be sent to Planner @ JohnGlennMBCI. com.

© 2010, John Glenn, MBCI