

Creating a plan the planner never sees

Securing the plan

John Glenn, MBCI

Enterprise Risk Management/Business Continuity practitioner

This article appeared first in DRJ's Summer 2009 issue

Does a business continuity planner need a security clearance?

In 99% of the time, the answer is a strong "No."

That doesn't mean some organizations don't insist on a clearance - usually Top Secret or higher.

Like a Masters degree, anything less than Top Secret (TS) is hardly worth considering, and even a TS is - well, it hardly equates to a PhD in the clearance scheme of things.

Trouble is, most managers in the "classified" world have no clue as to what risk management, a/k/a business continuity or Continuation Of Operations (COOP), is all about.

Many seem to have an ostrich-like mentality that tells them spies - governments on governments and industrial on competitors - can't figure out recovery plans from the media and the Internet.

That's nonsense.



For example

Recently a major spy agency advertised for a business continuity planner.

The advertisement fairly well laid out what this organization did - in the simplest terms:

The group receives information from operatives in the field.

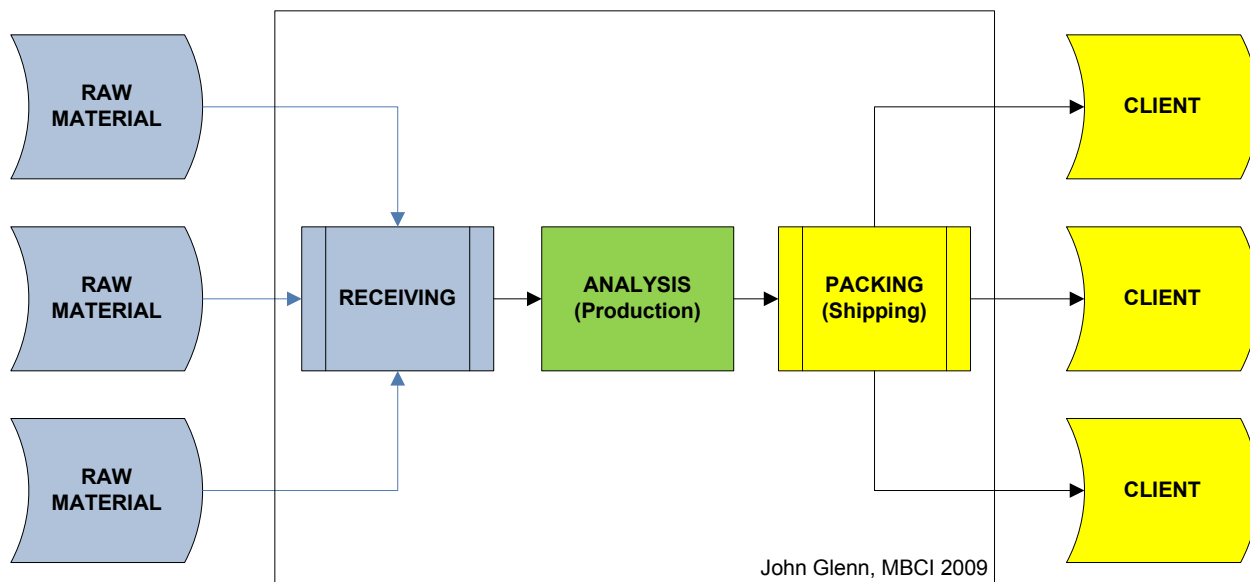
The information is analyzed by a select few and reports are created.

Others sort the reports and set classification levels for the information.

Once neatly packaged, the reports are transmitted to the organization's customers - primarily other government agencies.

OK.

Let's say that John Glenn is engaged to create a business continuity or Continuation Of Operations (COOP) plan for our spy agency.



I need to know how information is collected, at least in general terms. (The most common methods are reading the local papers and smoozing with the locals. Honest.)

I will leave the risks unique to covert operations to the Subject Matter Experts (SMEs) in covert operations. Does this need to be in **MY** document? No. Does it need to be in any document? Yes, but that document can be referenced in my document and the secret sections can be kept inside a safe inside a safe (hopefully at the recovery site - wouldn't want it to be buried under the rubble of the production site).

As for as depending on SMEs, that's SOP (Standard Operating Procedure) for all comprehensive plans, be they for a secret organization or the church league. Planners should not be expected to be expert in anything other than planning and, perhaps, program management.

As the planner, I really don't need to see the SMEs' documents.

Of course I can't be responsible for the content, accuracy, completeness or "readability" of the SMEs' document. It would be better if I could read the SMEs' work, but if my mentoring skills are any good, I should be able to guide the SME toward creation of a usable document even without actually seeing the contents.

Generic information vs. specifics

I do need to know **HOW** information is transmitted, but again, in general terms.

For example, does the information originator call in via telephone - either public using codes (that I do not need to know) or via a special phone or carrier pigeon

or ... If I know how the information is relayed, at least generically, I can recommend means to avoid or mitigate risks to that method and to identify alternate methods.

I was asked at a security session if knowing this information wouldn't make the planner a security risk? Possibly if the alternate was esoteric and only one option was available and if the planner was privy to management's decision to implement specific measures.

Ah, but what about the planner having to know the options to the primary method?

Answer: The responder is told to implement the alternate process documented in another, classified, document.

OK, let's assume, always a dangerous thing, that the information arrived safely at the center where the analysts will put their talents to work on the data.

According to Bush-era COOP requirements - and like him or not, his action this time was on the mark - the first requirement is "protect the people." The second is to get back into at least a minimum level of functionality within 72 hours - maximum. That means sufficient resources must be available - people, telephones, facilities, IT, and all the rest.

My job, then, is to assure the people are safe. That starts in the parking lot, if not before.

It also is my job to generally assess the facility - is it in an airport's final approach, near a sea port or hazmat-carrying railway? Is it on a fault line? The "standard" concerns every planner has for every facility.

Ditto utilities. Telco comes in at two demarcation points? Power is backed up by a generator that's big enough to support business functions in addition to IT.

As with any organization, I need to plan to relocate the analysts - and all the support staff.

Do I need to know where?

Not necessarily.

I do need to know and provide my client with information about space requirements, power requirements, and security requirements.

Source material

Where do I get this information?

From the SMEs.

True, if I know space requirements and power requirements, were I a spy I might be able to guesstimate the number of people employed at the site, but I easily could find that information any number of "innocent" ways, including monitoring the gate to the facility.

Spying, I have been told, mostly is paying attention to things out in the open. Attention to detail is a spy's greatest asset. That's not to say that there are no miniature cameras or bugs under tables or other spy novel toys; it *is* to say that most spying is paying heed to the obvious and "adding two plus two."

Given the fact that space and power requirements are fairly "public," the planner probably could have access to this information.

The planner's primary concern must be to relocate the analysts and support people to an equally secure facility. (That sometimes is a more difficult task than it first appears.)

So far, all pretty much SOP - Standard Operating Procedure - for any comprehensive business continuity or, in Fed-speak, COOP plan.

Naturally the secure facility must accommodate the analysts' communication resources. If they are not already in place, e.g., secure lines, someone must string them. Call the local phone company? Probably not, but there are people with both the security level and technical expertise to do the job - check the nearest military base.

The planner's job is to ***recommend*** avoidance and mitigation measures. Even in the most open environment, the planner rarely decides which measures to implement; that's a management decision.

In the "normal" environment, the planner would, once management decides on what measures to implement and sets an implementation schedule, create response plans.

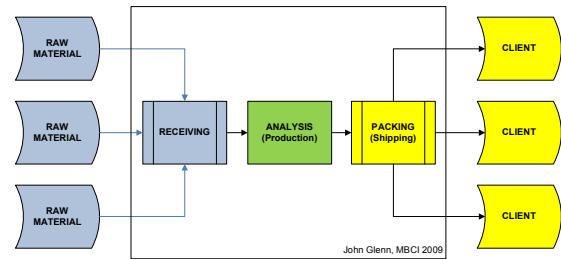
In the "secret" world - be it government or commercial/industrial - the response plans may be left to the responders to create. Not wise, but possible.

As with other parts of a plan, there may be information in the "base" plan and references to "secret" paragraphs and entire "sub-plans" kept under lock and key.

Back to the process

Once the analysts have done their work, the information is moved to - for want of a better term - the "packers" or shippers, the people who assemble the

information for each of the customers. Some might get "very" classified information, others less sensitive, and still others only unclassified data. Who gets what is "out of scope" for the plan and, aside from assuring the "packers" have a secure area in which to work and the tools they need to do their job, the planner's job is pretty routine. As before, what do the people need in so far as space, security, power, communications - the "standard" requirements that any organization needs.



This exercise started by collecting data and transmitting it to the analysts.

It ends almost the same way - transmitting data.

As before, the concern is how to assure the information gets to the clients without being compromised.

The outgoing product may be more sensitive than the incoming information since the analysts have not only worked with information from Point A, but from Points B through Z as well, information the originator of Point A may never see or know about.

In the real world of business continuity planning for classified operations, the planner may not be privileged to see all the information he or she might see in a "normal" plan, but even the parts the planner can't see can be influenced by the planner.

Planners need to be documentation pros, or at least "semi-pros," to create templates for the classified sections. The planner also needs to be a mentor to the SMEs who actually create the secret sections.

Bottom line is no secret

The bottom line: good business continuity/COOP planners do not absolutely need to hold a security clearance to create a plan for a secure facility.

The planner needs to know general processes.

The planner needs to help the SMEs develop classified documentation.

The planner needs to mentor and encourage the SMEs without asking too many sensitive questions.

From my perspective, it makes no difference if the plan is for Spies-R-Us or Worldwide Wizard Insurance.

Either way, the planner works with available information and then promptly forgets any client-specific information as he or she wraps up the project or moves on to the next phase of an on-going program. It also makes no difference, as I see it, if the planner is a contractor or in-house staff.

Does a planner need Top Secret clearance to do the job?

Lots of people in the world of secrets might disagree, but from this planner's perspective, a classification is about as necessary as a PhD is to fix a toilet.

Spy vs. Spy image: <http://www.ybcw.com/strip1.php>