Continuity of Operations and the Capability Matrix

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

One of the key principles of business continuity planning is to eliminate single points of failure < http://www.businesscontinuityuk.net/understanding-the-process/avoid-single-points-of-failure-your-business >. Gareth Howell< http://uk.linkedin.com/in/garethhowell > writes,

> "Unless the business keeps its eyes on the principles of Business Continuity Management, it can easily get itself into a position where it is overly dependent on the services of a few key individuals. Without proper planning, that dependence can result in disaster if one of those key people is not there."< http://www.businesscontinuityuk.net/understanding-the-process/succession-planning-business-continuity >

Mr Howell urges organizations to develop *succession plans* to cope with the sudden unavailability of key people.

> "As well as being a good strategy for managing the progression of staff, succession planning is also a good strategy for minimising the impact on the business of losing a critical member of staff unexpectedly. More broadly it seeks to move the organisation to a position where none of its staff actually are critical to its continued operation as individuals." < http://www.businesscontinuityuk.net/concepts/have-got-succession-plan >

One of the principles I've taught for many years in operations management and security courses can be stated as "No institutional knowledge shall be held by only a single member of the team." Allowing single repositories of operationally significant knowledge is dangerous; one of the classic examples I cite (the reference long since lost in the mists of decades) is of a report published in a USENET group sometime in the late 1980s or early 1990s about a system manager who went on vacation for three weeks on a south-sea island with no external communications. It turned out that critical elements of the operations required knowledge that only he held. The systems were down for the entire period of his holiday.

At one organization where I worked years ago, one of the system managers was a knowledge-hoarder. She kept others from finding out the technical details of how she prevented and solved specific problems, and she refused to document policies so that anyone else could figure out what was permitted and what was not. To find out if something was allowed, the only thing we could do was ask *her*. "Control freak" and "insecurity in action" (in all senses of the word) were kind descriptions for her ham-fisted absolutist control of the production systems. I actually had a talk with the president of the organization in which I warned that – as usual – the only question was when we would have a disaster, not if. Sure enough, a few months after my warnings, the idiot system manager allowed a server to become infected with malware, spreading the toxic code throughout the network. The incident served to demonstrate that not only was she preventing others from taking appropriate security and management precautions, she was actually preventing herself from having her own errors spotted by helpful colleagues.

Copyright © 2012 M. E. Kabay. All rights reserved.

One of the tools I've long used in evaluating the resilience of organizations is the capabilities matrix< file:capabilities_matrix.jpg>. One starts by listing (or brainstorming, perhaps using Computer-Aided Consensus™< http://www.mekabay.com/methodology/cac.pdf >) all the critical functions that the organization requires and all the people in the team. The group then has to decide on a way of rating the capabilities of each person; the figure suggests one way to do it, but in no sense is this suggestion meant to constrain users. The group can come to a consensus on which of the team members can do which tasks at which level of competence and then examine the overall pattern of skills. Figure 1 shows such a matrix with made-up information.

Figure 1. Capabilities Matrix.

CAPABILITIES MATRIX FOR UNTELECOM CORPORATION

								Capabilities & Assignments			
Total points ≤	0	1	3	6	9	12		0	1	2	3
EVALUATION	ACK!!!	DANGER!	URGENT	IMPROVE	GOOD	EXCELLENT		NO CAP.	NOVICE	IS/CAN BE BACKUP	CAN BE IN CHARGE
	PERSONNEL CAPABILITIES								TOTAL	NEED	
Task	Albert	Betty	Charlie	Dahfla	Edward	Frannie	Golamo	Hur'dath			
application monitoring	3			3			2	2	10	GOOD	
application security vulnerabilities	3			3			2	2	10	GOOD	
business impact analysis		3		1				2	6	IMPROVE	
computer security incident response team			3		3			2	8	IMPROVE	
coordination with corporate counsel		3	1		1	2		2	9	GOOD	
coordination with human resources group		3	1		1	2		2	9	GOOD	
Database performance	1			3			2	3	9	GOOD	
Database support	2			3			2	2	9	GOOD	
denial-of-service monitoring				1	3			3	7	IMPROVE	
denial-of-service response				1	3			2	6	IMPROVE	
detect cyber-attacks					3			3	6	IMPROVE	
enterprise antivirus									0	ACK!!!	
governance decisions		3	1	1		2		2	9	GOOD	
identification and authentication			2		2		2	3	9	GOOD	
intellectual property protection				2		2		3	7	IMPROVE	
intrusion detection systems					3		2	3	8	IMPROVE	
intrusion prevention systems			2		3		2	2	9	GOOD	
log management systems	1		2	3	3			2	11	GOOD	
manage cyber-attacks		2		1	3	2	1	2	11	GOOD	
monitor dashboard			2	2	3			2	9	GOOD	
network behavior analysis			1	3	2			3	9	GOOD	
network discovery			1	2	2			2	7	IMPROVE	
penetration testing			1	1	2			3	7	IMPROVE	
quality of service measures	1	3		3	1	2		2	12	EXCELLENT	
respond to system alarms		2	3	1	3			3	12	EXCELLENT	
risk analysis and management				1		3		3	7	IMPROVE	
security awareness				1		3		2	6	IMPROVE	
security information and event management			3	2				3	8	IMPROVE	
service level agreements	2	3	1	3		3		2	14	EXCELLENT	
system firewalls			2		3		3	2	10	GOOD	
training				1		3		2	6	IMPROVE	
unified threat management					3		2	3	8	IMPROVE	
vulnerability assessment			2		3		1	2	8	IMPROVE	
Web site assessment					2		1	2	5	URGENT	
Web site monitoring					3		1	3	7	IMPROVE	
wireless intrusion prevention									0	ACK!!!	
TOTAL SCORE	13	22	28	42	55	24	23	81			

Copyright © 2012 M. E. Kabay. All rights reserved.

In the spreadsheet < file:capabilities_matrix.xlsx > I created for this article, I used automatic functions to highlight the danger zones. The red "ACK!!!" flags signal that two functions, "enterprise antivirus" and "wireless intrusion prevention" seem to have been neglected in assignments of duties. Other rows are flagged with other labels such as "DANGER!" up to "EXCELLENT" to give the team suggestions on priorities for improving resilience (overlap of skills).

In addition to simply identifying lacunae in operational readiness, the rows can also alert the team to potential conflicts. For example, if more than one person is rated at the top of the capabilities (in this example, labelled "CAN BE IN CHARGE"), it's important to ensure that the actual assignment of duties is crystal clear. One does not want two people each thinking that they are in charge (leading to potential conflicts) – or for that matter, that the *other* person is in charge (leaving the actual responsibility unfilled). Collegial, friendly discussions can resolve such problems and more important, prevent recurrence.

The column totals are also useful. In the made-up example, the automatic color-coding instantly shows that the lowest score is for Albert and the highest score is for Hur'dath. These scores are *not* inherently good or bad: they just point to outliers. For example, perhaps the low-scoring person is a junior member of the team who needs more training to take up more responsibilities; on the other hand, maybe Albert is a slacker who is shunning productive work. Similarly, maybe high-scoring Hur'dath is a senior member of the team who really ought to be thinking about moving to a more senior position – or maybe he's just overworked and due for a heart-attack.

Users must not make the mistake of thinking that this number-heavy approach is somehow going to make decisions for them – the method is just a heuristic tool to help people *think* about the issues, *decide* on solutions and *act* on their decisions.

Once again, remember my motto: *reality trumps theory*.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *

Copyright © 2012 M. E. Kabay. All rights reserved.