Let me belabor the obvious. Organizations everywhere realize that they need to back up their critical data and make arrangements to run their critical application systems in the event of a disruption in their data centers. So, not to put too fine a point on it, critical is covered. Critical is not the subject of this article.

**THE MYTH OF TIER TWO**

What concerns me here is everything else, the noncritical data and systems, which I will lump under the rubric of “Tier Two.” Over the years, I have heard many IT managers (and many information security professionals, for that matter) say, “We’ll take care of the critical systems and figure out what to do with the rest when the time comes.” T’ain’t so, my friends, t’ain’t so. I would like to challenge that entire way of thinking. There is no such thing as Tier Two.

There is no definitive way to ascertain what is critical and what is not based on the perceptions of the users of information systems or their developers. At best, criticality is a determination made by individuals with a prejudicial interest in what they consider to be important. While certain systems and their associated data may be of obvious importance to a department or an organization as a whole, it does not follow that that which is less evident is not vital to the organization’s welfare. In most corporations and government agencies I have dealt with, information systems are a reflection of complex organizational structures with many interrelated parts. Those managers uninterested in certain applications may not understand the consequences of the absence of seemingly unimportant applications to other functions on which they are knowingly or unknowingly reliant. It is scant comfort that the hole may be in someone else’s part of the boat.

Thus, the user who has—or who seems to have—the greatest knowledge has the greatest influence over criticality decisions. Managers who are less forceful have less knowledge of how their systems actually work, or managers who just happen to miss the meeting may find that their systems have been considered Tier Two.

**NONCRITICALITY, COST AND COMPLEXITY**

In my experience, many criticality decisions are based more on budgets than on the actual importance of systems. Because many IT functions charge back their costs, business managers have an incentive to downplay the consequences of the unavailability of their information systems. It is not inexpensive to replicate data in real time, maintain alternate equipment that would be used only in emergencies and establish telecommunication links to multiple data centers. Thus, there is a reason for some managers to say that their systems are Tier Two, knowing full well that they will insist on instant recovery should there ever be a system failure, without having to pay for recoverability every year in advance of an outage.

Adding to the murkiness of Tier Two determinations is that in many cases, application owners do not understand all the interactions among systems and data. Sadly, many application developers do not know all the interactions of their systems either. I have found that the result is shock and dismay when a critical component is missing at the time of a data center disruption—closely followed by a mad scramble to elevate Tier-Two systems to the top rank.

Systems and databases have become so large and complex that no one can accurately predict what is essential to an organization’s well-being. The 80-20 rule does not apply. A great deal more than 20 percent of all systems are necessary for an organization to function—not function at its peak, just to function tolerably well.

**THE UNCERTAINTY PRINCIPLE**

Organizations can accept that not everything is critical, or even that everything might be critical to someone, sometime. But it is extremely difficult to determine what is critical and what is Tier Two. Even that which is clearly a Tier-Two system must have some importance to an organization; otherwise, why was the system developed and the data captured? The problem is that it is nearly impossible to know the difference in advance. The Uncertainty Principle in play here may not be much of a deal by Werner Heisenberg’s standards, but it certainly
makes information security, business continuity and data management difficult.

Thus, the conundrum for management is what to do with Tier-Two systems and data. One might say, “Treat everything as though it were critical, and then nothing will be missed.” The one who might say that surely never had to justify a budget. (This approach may actually be a valid one where lives are at stake, e.g., in hospitals or in the military, but it can hardly be a general theory of data management.) While the criticality, or lack thereof, may be uncertain, the cost of protecting all the information resources equally is very clear indeed.

It does, to my mind, make sense to take the opposite approach: Treat nothing as though it were noncritical. Organizations should employ an integrated solution to data and system availability in such a way that an organization’s information portfolio is protected in a consolidated, consistent fashion, with no data element left behind.

**DISASTER RECOVERY AS A SERVICE**

That all sounds very egalitarian, but what does it mean in practical terms?

- Those applications and data judged to be critical should be backed up and recovered within the constraints of an organization’s risk tolerance and budget.
- All data, not just those deemed critical, must be backed up regularly and stored offsite. There is nothing inherently wrong with using physical tape, but it does necessitate tape drives at a recovery site, which add both time and expense to a recovery effort.
- The recovery of all data and applications must be tested. It is insufficient to figure out how to recover data after a disruption.
- This implies that there must be an equipped site in which recovery tests may be run. It need not be the same site where data and applications will be recovered if the need ever arises, although that would be preferable.
- There must be people assigned to recovering all data and applications. Following a significant data center outage, most staff will be consumed with the recovery of critical data and applications; some people need to be reserved for the recovery of everything else. To me, this suggests a contingent outsourcing solution that would come into effect only when needed.

Fortunately, meeting these requirements does not necessitate an investment in real estate and massive amounts of equipment. Much today can be accomplished using the cloud as a vehicle for data backup and recovery testing. While this is hardly a zero-cost solution, it may well bring the timely availability of all data within the financial constraints of many companies.

Disaster Recovery as a Service (DRaaS) has been much talked about for at least the past five years. Well, at least I have been talking about it, but it was always in the future tense, because DRaaS has only recently become viable—technically and economically. It may not be the best single solution just yet for enterprisewide IT recoverability, but it may offer hope to downtrodden, neglected data and applications. Tier Two is dead. Long live all data for all applications.

**ENDNOTES**

1 Nor is it about sensitivity. However, I believe that the same point could be made about the need to treat the confidentiality and integrity of data, especially the so-called “public information” that organizations make no effort to secure. It constantly amazes me how much information I am able to obtain about companies and their people from publicly available sources. I will take up confidentiality and integrity in a later installment of this column.

2 Jen Hajigeorgiou, one of the editors of this column, tells me that the ISACA Journal reaches a global audience, many of whom do not understand Americanisms. In this spirit, I offer the translation: “It is not so, my friends, it is not so.” It loses something in translation.

3 Werner Heisenberg was a German physicist who stated, in laymen’s terms, that we cannot simultaneously know the position and momentum of a subatomic particle. In nonlayman’s terms, he wrote $\sigma_x\sigma_p \geq \hbar/2$. For this, he won the Nobel Prize.

©2014 ISACA. All rights reserved. www.isaca.org