FRITS J. BOS, PMP

1602 - 145 Hillcrest Ave., Mississauga, ON, L5B 3Z1 | C: (416) 524-7790 | frits@pm4hire.com

A data center operation is a critical aspect of any business: this must be managed with a vision of growth and sustainability, security, and business continuity. It is not uncommon for budgetary restrictions to impose trade-off decisions that could have long-term consequences. It is critical to quantify those potential consequences as input to executive decisions on data center funding.

Datacenter Management Methods

Managing data centers is a challenging responsibility because of the critical nature of what is at stake. For a 24/7 operation even basic maintenance requires a careful plan to make sure no customer services will be disrupted. Customer-faced services are at risk from external attacks aimed at stealing or corrupting data to disrupt processing or breach accounts.

I can provide datacenter consulting to your organization.

With over 30 years of project management experience in managing projects, I participated in the building, upgrading, and transforming of data center operations and networks, and migrating the data between different organizations. I have been involved with planning data center backbone infrastructure (networks, power, cooling, etc.) and network and server monitoring upgrades. I have experience in PCI DSS compliance to isolate parts of computer operations, to proactively deal with hacker attacks, to begin a process of minimizing exposure and consequences. In an era of **GDPR** the company can also face severe penalties if customer private data are compromised. This kind of risk is becoming rather common and it is a stretch to consider this a true disaster: it is an oversight not unlike locating a datacenter in a high flood-risk area.

Most of these major initiatives focus on larger organizations. However, smaller companies also can be at risk by making poor choices on outsourcing operations, and potentially losing control while not diminishing their exposure to adverse consequences. While large organizations may have a team of experts on hand, smaller organizations may get their advice from people that sell computing services based on what they have to offer, not based on what the business needs. It may not occur to consider how offering business services over the internet can represent a 24/7 operation, and that an internet outage can be as disruptive as a data center outage. While your website might present your operations as larger than they are, that also makes your site a target for hackers that want a piece of your business.

With that in mind, the focus for large or small operations is the same: hardening the environment by establishing “rings of security” around your operations. While it requires additional hardware and network infrastructure you can consider this as life insurance for your company, since GDPR puts the onus squarely on you to protect customer information: the potential penalties are steep and ultimately avoidable by putting some thought into seeing your operation as a fortress.

Consider the analogy of a railroad and a rogue train that ignores the signals and breaks through into blocks that it is not authorized to enter. What happens if the switches are not set to allow it to pass is that it derails. This is how we must create a "ring of security" that bounces suspicious traffic into a quarantine server that can double-check if the credentials are confirmed before the message is passed on to the application servers.

A further analogy to the derailment is that this train goes nowhere fast, allowing opportunity for investigation into what threats the data center is exposed to. Using IP chains for known service providers used by legitimate customers, it is not rocket science to both prevent hacking and have the evidence to support a criminal investigation into the hacker attempt. If, however, the hack is successful, and your application responds, the audit trail from this "successful" transaction will be discarded, even if after the fact it is found to be fraudulent. The hacker will have extracted what he was after, and subsequently the problems may start.

The "rings of security" around your operations prevent malicious activity from penetrating to the core of your business. This is not all on operations where the consequences are first detected, it permeates throughout your information systems architecture that must intercept and mangle incoming traffic so that any embedded malware is destroyed on entry. Malware is designed for penetrating "well behaved" operations: make your operations "mis-behave" and it lacks ability to pass through the gates. Log all suspicious transactions to maintain an audit trail of intrusion attempts (we are not going into the realm of counter-hacking to destroy the perpetrators).

Just as we need a spur-line to catch a runaway train heading for a disaster, we can quarantine an incoming transaction that violates our security tests. We should use a separate security server, and while crashing a transaction is non-destructive the intent is to log the information and then to generate a response that would not be offensive to a legitimate customer accidentally routed into that quarantine server. An error has occurred in your transmission, and we are not able to complete your request – please call etc., etc. (only legitimately inconvenienced customers call). Once the routing is confirmed as legitimate the intercept logic can be updated to filter that route as legitimate. Those requests from Russia, North Korea, and other exotic places will remain as evidence should law enforcement get excited to perform a more in-depth investigation.

<u>Low cost introductory offer for commercial engagements</u>

For this ***introductory offer*** we charge $850.00 per day for commercial engagements (for out-of-town venues add $400.00 for travel time, plus reimbursement of transportation and lodging expenses at cost).

Respectfully,

Frits J. Bos, PMP