INTELLECTION
strategies

"Perspectives"

The Deterioration of Trust and Confidence

Questions are rising around the world over the implications of trust and confidence placed upon information technology systems and environments. One particularly compelling question is how does this affect the outsourcing of business process operations that has become a massive component of globalized businesses? This includes the emerging world of virtualized data centers constructed using VMware and other virtualization solutions as well as distributed computing services. Grid computing, cloud computing, outsourced sales systems, outsourced security software support, outsourced log management, outsourced email and more are spreading throughout enterprises. A fitting analogy is companies contracting with a big four audit firm instead of grooming employees to conduct audits.

In the event of a crisis, recoil invariably occurs. For example, the US is suffering from an energy crisis, causing gas prices to go higher, which slows the sales of SUVs, which then causes auto makers to adjust their entire business operations. When any such recoil happens, the question business leaders need to foresee how it will affect the operations of their companies. And, equally important is how will it impact the technology industry? Will it stimulate another boom? Lessons from the past show us that systems and businesses extend until they cannot extend again. Without a risk management philosophy, the bounds of that extension are never drawn and the penalty is generally underestimated.

Consider the financial crisis gripping the world today that was fostered by the self-professed financial experts who actually caused the mess. Is the same not possible in technology and operational services? As organizations further extend their IT environments—virtually and remotely—they lose the ability to manage these functions internally. A company that relies on IT outsourcing lacks the staff, facility and in-house expertise to bring these services inside the business, creating a deep dependency on their third-party providers. What's more, competitors who outsource to the same service provider cannot gain a competitive technological edge, because they share the same virtualized servers and data centers and, therefore, have similar technical operations costs. Any competitive advantage or cost savings due to an improvement in IT operational efficiency benefits the service provider; not the customer. This fact, combined with recurrent crises, create a natural cyclical event where technology is repeatedly centralized, decentralized and centralized again.

Even the typically short life span of technology environments shows this regular sequence of events.

Trust has deteriorated; of that, there is no doubt. It ebbs and flows as the mind forgets and the losses are washed away under the normal business cycle that history repeatedly recounts. In the recent past, cyber attacks were created by amateurs using worms and viruses meant to cause business disruptions. Today, the attacks are propagated by professional cybercriminals and data is the target. The attacks are international, multi-continental, unique, conducted as a business and seek to profit from your company's technology, property and people. Because these criminals gather more data from victims over time, systems are worth more money if they remain online as zombie and host machines and are then used in for-hire attacks. Therefore, the lack of trust in the machine is becoming commonplace. While businesses are seeking to understand, safeguard and leverage these systems to maintain business functions, consumers are unable to regain trust as quickly.

Environmental risks—despite the disassociation applied to the technology services themselves—also remain a concern to organizations. In the physical risk management space, factors such as factory locations, weather patterns, geopolitical activities and the region’s economy are analyzed and carefully weighed before important business decisions are made. Insurance is used to transfer risk or, alternatively, to minimize it. Yet, a gap exists in most enterprise operations when the technology aspects are considered. Most risk managers are tasked with the operational integrity of operations such as the placement of servers, the reliability of the power being delivered to the facility, the availability of network bandwidth, the pathways taken by Internet traffic and the implications of nation-state disputes on network traffic. Note that a common problem and oversight of using secondary backup data centers is that these are used due to a disaster or event. Therefore, many customers are using it at the same time, thereby clogging the traffic. This is similar to everyone leaving a city at the last moment before a hurricane hits. It’s not an intelligent way to safeguard important data.

Organizations can respond to this type of risk by recognizing the necessity of a proper control environment that addresses the businesses’ operational integrity requirements. It is advisable to take a holistic approach by conducting a complete evaluation of your organizations’ sourcing network and use this information to construct a risk table that allows you to understand its extended risk, the cost/benefit, the operational integrity safeguards, the disparity between reality and expectations and the "action list". The action list, similar to the essential shopping list—the one you keep in your pocket of prime targets for acquisition should a specific event occur—should include your organization’s next steps. These steps might include, for example, bolstering the internal audit function; bringing outsourced processes in-house; the purchase of technology; or hiring new staff.

The original comparison of outsourcing vs. big four audit firms within an organization is not wholly true based upon the risks and nature of problems illustrated above. While it is true that the risks for each sourcing solution have their challenges, the difference is this: external audit firms rotate and establish the rules of engagement to

ensure integrity of their services. The rotation of audit firms and the continued external evaluation of external audit firms establish a control environment that seeks to keep the risks in check for the organization.