VIEWING INFORMATION TECHNOLOGY FROM 30,000 FEET.

AN INTERVIEW WITH VIN TEDESCO.

The earth isn't spinning any faster; it just seems that way. That's the opinion of business and governmental leaders the world over. We exist in an unpredictable environment fraught with cyber hazards and threats to business continuity that were science fiction not a generation ago. Today, all businesses and the systems that operate them, are vulnerable to cyber threats, malware, data breaches and criminal intent.

Vincent Tedesco, a 30-year IT veteran and industry thought leader, looks at the frenetic IT side of the business world as a situation waiting for solutions. And in his opinion, the solutions exist and need only to be applied by skilled, knowledgeable hands.

ON CYBERSECURITY

"Cybersecurity is in every business decision makers' digital rolodex," Vin Tedesco says. "And too often that's where it stays. Cybersecurity is like exercise. No pain no gain. If you don't put it into practice, the repercussions contribute to an unhealthy life, or it might even shut you down instead of creating more quality time in the long run."

Tedesco believes that cybersecurity isn't a business option; it's the first line of defense, the initial step in developing business continuity. "Basically it stops the bad guys before they stop you. By proactively instituting a cybersecurity program for your business, you are ultimately protecting it and your people and also contributing to the business's overall productivity and success."

VICTIMS OF SUCCESS

Success and expansion all too often wreak havoc on delivery of IT services, resulting in disgruntled clients. Tedesco was COO of Tiburon's Public Safety and Justice product groups and remedied a situation spiraling out of control. "Service levels were degenerating, so we immediately created internal protocols to stabilize them, including deployments, support and contracts. We empowered our people, established realistic delivery dates and stood by the dates. In the end, we made Tiburon's offerings more efficient than ever. We brought these clients directly in line with the expectations of the multi-national public safety client base, which turned Tiburon's fortunes around."

ON PUBLIC SAFETY & IT

Public safety applications, including public safety IT, are infested with antiquated, almost byzantine governmental rules and regulations. As a result, many entities believe there are no alternatives. Tedesco feels that requests for proposals, bids and overall purchases of IT which concentrate on lowest cost scenarios do not necessarily result in the best interests of a public safety entity. By relying on antiquated, shortsighted regulations, public safety entities often end up being overwhelmed by IT costs. Then, to save money, IT purchasing decisions are all too often relegated to under-qualified

> ## "CYBERSECURITY IS IN EVERY BUSINESS DECISION MAKERS' DIGITAL ROLODEX."

individuals who lack real world IT expertise or appreciation.

"You certainly don't get the best bang for your buck that way," Tedesco noted.

LAYERED DEFENSE "PULLS SIX DISPARATE PROTOCOLS TOGETHER INTO A SINGLE OVERLAPPING CYBER SHIELD."

"There are many more efficient and cost-effective ways to acquire qualified equipment and services." He cites working with qualified outside IT consultants as a prime alternative, "because they're knowledgeable about the latest and greatest advancements. They have to be," Tedesco maintains. "It's their business; it's what they do."

Tedesco also pointed out that tunnel vision and *'that's the way we always did it'* vision often leads to erroneous IT decisions or equally dangerous non-decisions. And in a much larger sense, the process also retards the advancement of forward-thinking technologies. He unequivocally believes it is imperative to have qualified outsourced personnel lead in the decision-making process when planning and spending for public safety information technology.

OUTSOURCING V. INSOURCING IT

Information Technology is multifaceted, often ambiguous and always in flux. If Information Technology isn't your core business, it can become a cyber quicksand bog, constantly consuming and making allocated budgets disappear without a trace. Tedesco believes that tasking a company's internal personnel with ongoing mastering and implementation of the latest technologies, as well as the handling of rapidly changing IT requirements, can virtually never be cost-justified.

"For Fortune 500 companies or five-person startups, the jack of all trades approach actually costs more in hard dollars and untrackable time," Tedesco stated. "Not to mention the impact of inadequately researched or vetted systems, which might look great on paper but could be inadequate for the application. In the big picture that could inhibit inside IT staff from fulfilling their primary function, which is keeping the rest of the company staff operational on a day-to-day basis."

Tedesco maintains that outsourced individuals experienced in specific areas and technologies can

ABOUT VIN

- Founder, President & CEO Total Technology Solutions
- Creator of Total Enforcement public safety product line
- Acquired by Tiburon/Gores Group
- COO of Tiburon
- Chairman of the Board of Ten8Tech cloud-based case service application

implement new IT initiatives much more efficiently. He added, "They have to be need-based thinkers and must avoid falling in love with favorite systems or technologies. Outsourcing IT services based on need benefits companies by application of the right expertise to the right problem, resulting in the right technical solution...and better ROI."

LAYERED DEFENSE

The best protection against cyberattacks is advance protection beginning with a real world strategy. Tedesco cites the example of Total Technology Solutions' Layered Defense offering, which pulls six disparate protocols together into a single overlapping cyber shield. The strategy is to maximize an organization's overall security by strengthening all security components and aligning them in a cohesive plan that can be followed by all stakeholders.

As one might expect, Layered Defense plans are company-specific and developed based on needs, strengths and vulnerabilities. "They typically begin with site surveying and network assessment and include penetration testing and vulnerability scanning," Tedesco said. "Policies and protocols are created from the assessments. Awareness training of employees and management and their continued participation are the driving forces in the successful implementation of Total's Layered Defense planning."

NO SPIN DOCTOR HERE

The earth isn't spinning any faster; it just seems that way. In Vin Tedesco's world, the solutions for achieving business continuity in the face of burgeoning cybersecurity concerns and ROI-driven outsourcing debates already exist. They just await implementation by expert hands. ∎