

Technological Threats in Business Communities

Cell Phone and PDA Risks and Responsibilities

By Michael G. Frank and Perry R. Safran

Advanced technology has spread throughout business communities like a brush fire. Everywhere people are conversing on cell phones, scribbling on PDAs, and typing on notebook computers. Employees can work from anywhere while maintaining contact with their main office and customers. Improvements in technology have taken businesses to unparalleled levels of efficiency, but, like any brush fire, if uncontrolled, can bring disaster.

Though this article focuses on mobile phones and hand-held PDA's, the ideas and conclusions addressed ought to be applied to all commonly used portable devices, such as:

- ?? Automobile Navigation Systems and Data Screens
- ?? Notebook Computers
- ?? Walkie Talkies

Innovative technologies are often regarded and therefore handled as toys or luxuries, but in actuality they are key business tools. In the case of cell phones and PDAs, consider a desk that one might have in his or her office: the bare essentials probably include a desktop computer and a telephone. Businesses must realize that PDAs and cell phones are much like desktop computers and landline phones, but in a mobile form. They are not geeky gadgets, but are essential tools for workers away from the office. By that token, they necessitate respect and responsibility. Because of the rapid adoption of these two technologies, many companies fail to consider the problems and liabilities that arise from their use.

Cell Phone Liability

Recently, several cases have appeared concerning car accidents that occurred while a driver was using a cell phone. This new wave of litigation can adversely affect employers who expect employees to be available while they are driving. This practice creates risk for the company, which can be held liable for employee negligence. If an employee is involved in an accident while conducting business, then the employer can be held responsible. Tremendous fines and other compensatory measures result from litigation and severely endanger a business' security and performance, especially a small business. If driving while making business calls, or even just checking messages, become routine for employees, then businesses should rethink their expectations.

PDA Security

When monetary compensation is mandated in cell phone liability cases, mobile phones appear as the biggest technological menace, when in fact, PDAs can pose an equally if not more dangerous threat. PDAs may not seem risky to businesses, but if a misplaced or stolen PDA gets into malicious hands then a business may be in danger. Not only could a computer hacker break into a corporate network using stored passwords and uncover sensitive information critical to the company, but also a novice computer user could send prank emails to customers

or colleagues, permanently damaging those relations. Even if the company's only concern is monetary, a missing PDA may contain company bank, credit card, and PIN information that could be used to acquire corporate funds.

Assume a company has dependable employees and missing PDAs do not seem like significant risks. Nevertheless, that business is still in danger. Viruses and other computer infecting programs can steal, destroy, or alter valuable information as well as expensive software and hardware. Think that a PDA can easily be replaced is often the opinion of employers on this issue, but the case is never that simple. To date, no PDA has been infected with a virus, but they act as transport devices that transmit viruses to corporate networks. If this happens, a business is in for a lot more than replacing an inexpensive PDA. The entire network may have to be reconfigured, purged or replaced, which means time and resources spent repairing what could be avoided if precautionary measures are taken.

Security and Safety Measures

So, with unexpected hi-tech hazards lurking about, how can employers avoid litigation, disruption, or catastrophe? There are passive approaches, which involve the use of hands-free devices for cell phones, and anti-virus as well as password protection for PDAs. This method is important, but is still only part of the solution. Protective equipment will not resolve all problems. Technology is only as good as the user. Knowledge and common sense are the best defenses against any misfortunes impairing to a company's performance, or worse, its existence.

How can employers make an active effort to increase awareness of prudent and reliable use of business tools in their companies? Corporate policies and procedures provide excellent ways to manage how, when, and where employees use cell phones and PDAs, but one must not overlook the issue of why employees use these devices. Making certain employees recognize and appreciate technology in the work place and that it is intended for legitimate business purposes is a sensible practice to ensure a secure business.

To establish an effective policy, employers must first assess their company's risk as related to the technology used and then determine what kind of guidelines will be appropriate to that risk. Once a plan is chosen and produced, an employer must insist on employee knowledge, understanding, acceptance, and most importantly, performance of the latest rules and regulations. Getting help from outside the company should never be ruled out. Someone who knows how to assess risk and draft and implement policy may be crucial in the success and protection of a company.

Although technology can enhance a business, there is always the possibility that it may do more harm than good. There is no reason to shun new business advancements, as long as any vulnerability that might exist is addressed and preventative measures are taken, both through specialized protective materials as well as appropriate and thorough corporate policies. It is always better to avert a tragedy than attempt to remedy one. – 07/2004