



“To Secure Your Business, Consider the Access Points”

By Rebecca A. Morgan
Inc.com • 2006

Potential threats come in many forms: computer connections, supply chains, your employees, visitors – even your front door. Know where the holes may be, then work to fill them.

Though we wish we still lived in a world of unlocked doors and keys left in the ignition, a few instances early this year brought a reminder that those days are gone: The January killing of six people at a California postal facility; multiple reports of laptops containing critical information being lost or stolen; and the contentious debate around Dubai Ports World’s potential involvement with U.S. ports. All highlight the variety of risks faced by businesses today. Even if yours is a small company, the threat of theft, industrial espionage, computer hacking, workplace violence, and terrorism are all too real to ignore. Every business needs a security plan to protect itself and its employees, investors, and customers.

An effective security plan addresses multiple avenues of risk, as threats can emerge from almost anywhere. The first step is simply acknowledging that it can happen to your business; then, take a realistic look at your vulnerabilities and prioritize your efforts to address them. A few suggestions to consider:

What Lying Might Lead To

Lying on resumes and job applications is an all too **common fraud**. While such personal puffery is often viewed as harmless, it may be indicative of a willingness to mislead on other matters of importance. To be more certain of candidates you’re considering, conduct background checks, including both criminal and financial; you may unearth information key to the hiring decision. Ensuring all paperwork is valid, whether social security cards, green cards or other documents that indicate identity, is an important part of that process. While these verifications of the hiring decision you want to make are not inexpensive, moving forward without them can be a costly mistake.

Visitors Need to Be Kept in Check, Too

Employee background checks will only go so far to protect your business if you don’t also consider others who come in to your building. Package

delivery personnel may appreciate access to restrooms and vending machines; that seemingly reasonable request should not sanction unattended wandering throughout the building. Visits by customers and suppliers may be common, but what do you really know about them? Develop a policy about where those visitors can go, and with whom, even though you may feel a little funny about asking customers to wear a visitor badge or move around only when accompanied. The alternative is feeling worse if you don’t do it. Encourage employees to question any strangers walking through the building. Employee and visitor badges can help recognize someone who shouldn’t be there.

Lock Your Doors and Electrify Them

Many businesses no longer have a receptionist at the front desk, but leave the front door unlocked; elsewhere, warehouse and other doors are occasionally left open hoping for a cool breeze. Think about whether your physical access allows just anyone to simply walk in an open door and walk to critical areas without being stopped. If so, you might implement electronic security systems that control the opening of doors according to the rights associated with any specific employee badge. Set up lobby phones for visitors to notify someone of their arrival, before they walk in the door.

Computer Connections Can Be Insidious

We all know that computer viruses and worms can be a pain, but we usually expect antivirus

Continued on back



Contact Rebecca A. Morgan at:
Fulcrum ConsultingWorks, Inc.
voice: 216-486-9570
fax: 216-486-9922
cell: 216-210-9109
morgan@fulcrumcwi.com
www.fulcrumcwi.com
© 2007 Fulcrum ConsultingWorks, Inc.

software, firewalls, and our IT folks to keep us safe and help us recover quickly when something goes wrong. But good cybersecurity should be a top-down initiative. Without it, you open your company to serious loss of business and other risks.

An important aspect to review in shoring up your cybersecurity is the connectedness of your systems and machines: For instance, does any of your equipment utilize automated systems (PLC's or other) connected to your business applications? If so, any virus/worm or hacker that reaches your business systems can also reach that equipment. Is equipment linked to an OEM for monitoring or updates? Can your employees link in from home, where they may have unsecured links to the Internet? Any electronic link of equipment to the outside world, including the laptop the service tech brought with him, presents risks. Manipulation of machines or the theft of data doesn't require going on site; it can be done by someone seated comfortably half way around the world.

There May be Holes in Your Supply Chain

Heated debate around whether the U.S. should allow a Middle Eastern company to manage U.S.

ports surfaced when Dubai Ports World acquired the British-run firm that currently manages several major U.S. ports in March. The episode brought the issue of supply chain security front burner.

Most importers already know about C-TPAT, the acronym for Customs - Trade Partnership Against Terrorism, a joint effort of U.S. Customs and business intent on accomplishing both security and speed of imported goods. FAST – Free and Secure Trade – is a similar program for those importing directly from Mexico or Canada. C-TPAT and FAST emphasize principles of risk management and supply chain security. Your suppliers, the transportation company and your company may all be well-intentioned operations, but any hole in the system presents the opportunity for a security breach damaging to your business and others. Domestic supply chains carry similar risks. Identifying holes in the system and fixing them can save all of you money in the long term, as well as increase the level of broad based security.

Security is smart business. Without thinking through access points thoroughly, you leave your operations open to risk.



Contact Rebecca A. Morgan at:
Fulcrum ConsultingWorks, Inc.
voice: 216-486-9570
fax: 216-486-9922
cell: 216-210-9109
morgan@fulcrumcwi.com
www.fulcrumcwi.com
© 2007 Fulcrum ConsultingWorks, Inc.