Technology at the Top

Leaders Should Focus on Data, Access and Risk

By Rebecca Hendricks

Technology. When necessary, we deal with it; otherwise, we leave it to the geeks. If computers are running our companies, can business owners/executives afford to ignore it? Rather than trying to understand it all, executives can concentrate on three core areas: data, access and risk.

Identify critical data. Think about customer databases, business processes, financials and intellectual property. It can be the subscriber list, the secret cookie recipe, profit margin data or engineering drawings. It is any data, which, in the hands of your closest competitor, could devastate your company. Document what it is. Document the locations, as it can be in several. A customer database could be in a sales system, in the financial structure and on the CD a sales team carries around.

Know who can access the data and know from where they can access the data. If it is located on the sales manager's PDA (personal digital assistant), make sure the task of deleting the data is part of an exit process should that employee leave the organization.

According to Search Security newsletter, 60% of all corporate data assets reside unprotected on personal computers (PCs).

If it's critical to the operation, secure it. We would not print off the client list, and then leave it in plain view at a trade show. We would not leave the front door unlocked overnight with new product specs on the receptionist's counter. Why would we leave critical data on an unsecured computer for anyone to access?

Know who can access your critical data and when they access it. Most systems have security or audit logging capabilities. Is it turned on? Who has access to turn it off? When digital assets are stolen, the last thing a CEO needs to hear is security logging was available, but never turned on.

Identifying risk

Operations can be interrupted in many ways. Business Continuation Planning systems document potential business interrupters and map basic recovery steps. Before faced with the need to recover computer systems, ensure your critical data is backed up and securely stored off site. Know the name of the person who is accountable for bringing systems back online and clearly communicate this responsibility to them.

Nearly 25% of 500 small businesses surveyed in late 2002 claimed to have caught employees stealing from them.

Based on that statistic, one out of every four employees is likely to steal from the small business owner. In today's world of computers, what if the theft is digital? Stealing customer databases and intellectual property isn't difficult if it's sitting on an unsecured PC.

Rebecca Hendricks

Learning the hard way

How do you know theft occurred? At one company, it hit home at a trade show when a rival launched a competing product. Discovering their former product engineer was working for the competitor, a little digging showed an unusually short product development time. A formal investigation into theft of trade secrets quickly began.

At this point, will the digital evidence trail likely be cold? When you're working on the side of the company, improve your odds. Today, many organizations rely on Incident Response Policies. One such incident might be responding to departures of key personnel. Securing their hard drive for a period of time is a good measure. The investment is worth it if you preserved the "digital smoking gun."

A sample policy can be found at www.mirrorconsulting.com\sampleIRP.pdf.

Many organizations turn to internal information technology (IT) staff to determine if electronic theft has occurred. While intentions are good, most operational IT staffers are not properly trained to handle digital evidence investigations and spoilage will occur more times than not. Standard operating procedures dictate chain of custody documentation, bit-stream backups of original evidence and forensics processing on duplicates only. Experienced computer forensic specialists are trained in using the proper tools to preserve the evidence in an admissible manner.

Saving the evidence

In a recent computer investigation, just days before the computer examiner arrived, a disk defragmentation was performed in an attempt to conceal deleted files. Using forensic tools, more than 100,000 partial files were found as deleted yet recoverable. Of those files, 20,000 graphic files were restored completely and nearly 500 documents, spreadsheets and presentations were recovered. This was after a disk defrag.

Good risk management can save your company. An example is James Burke, the Johnson & Johnson board chairman when Tylenol tampering occurred. Leading the organization with proactive measures brought Tylenol back to its top market position within six short years of the tampering, which resulted in six deaths.

Today, 41% of CEOs, company presidents and managing directors are now actively involved in setting information security policy – 10% more than a year ago. Top business executives cannot afford to leave technology strategy to the geeks. Nor can they afford to leave computer investigations to the untrained.

INFORMATION LINK

Author: Rebecca Hendricks is president of Mirror Consulting, an Indiana-based firm specializing in strategic planning, risk management and business development. She can be contacted at (317) 862-4489 or e-mail: rebecca.hendricks@mirror-consulting.com