Login

Archive

search

Article

Information Protection: It's Your Data Dummy

By L Burke Files, CDDP, President, Financial Examinations & Evaluations, Inc (01/07/2013)

We all rely upon computerisation for communication, the preparation of documents, the keeping of records, writing, databases, financial information, etc... Many of today's professionals do not even recognise the tools of yesteryear. As evidence of this I held up a sheet of green ledger paper and only the, ahem - seasoned executives - recognised the artifact. Even they admit to having no idea when they last used a sheet or even if they were still made. We are that dependent upon our computers. So dependent in fact that all of your critical information, the information you do not want your competitors to have, is sitting with several open doors to the world. So you have firewalls and up to date anti-virus and anti-malware installed - so what, I mean it, so what! Firewalls and anti-virus and anti-malware stop only known threats. If a threat is not known, and a virus has not been detected, it will not be stopped.

Ever hear of Albert Gonzalez? He is a computer hacker who masterminded the combined credit card theft and subsequent reselling of more than 170 million card and ATM numbers from 2005 through 2007—the biggest such theft of its kind in history. Gonzalez and his team used Structured Query Language (SQL) injection to deploy backdoors on several corporate systems in order to launch packet sniffing attacks which allowed him to steal computer data from internal corporate networks. He did this from his laptop sitting in the parking lots of retail stores that had RF registers. The registers had encrypted transactions running between the registers and the main computer. Using this pathway he penetrated the main computer networks and was able to decrypt the transactions. Before doing this he tested his SQL injection script again the 26 commercial anti-virus programs at the time to insure a level of success. None of the 26 anti-virus programs were able to detect his virus.

Think you are more secure, think you are better than all of these companies listed on these pages? http://www.privacyrights.org/data-breach - This is a scary list of companies who though they had good systems and got hacked.

Or we have a much simpler scenario for data theft. Edward Snowden, of Booze Allen, just downloaded what he wanted from the NSA to a USB drive and walked away.

A response to my assertions of our weak data security above is simple. 'These are high profile targets and my threat level is not that high." I agree, but the threat we face is for more personal and pernicious.

The primary threat we have is from employees and contractors who have access to our data. An employee comes in - downloads everything from your system on a USB drive and than sells it to a tax authority, or more common, extorts you for money. One recent case involved an unhappy secretary who took all of the data and said to her employer - I will not be showing up except to collect my check each Friday. I have all of your records and if you want to remain private this will be the arrangement. The service provider knew he had a three-fold threat, a) professional license for allowing this to happen, b) reputation to current clients for loosing control of their records, c) exposure to years of litigation if the clients found out or if any of the tax planning was considered - iffy.

So what should you do in the real world as we all work in a cross platform environment in collaborative ways to achieve client objectives? Translated - we must work and share information to get the job done, however, there are some simple steps we can take to protect ourselves;

- Background checks before hiring
- Issue effective policies that are followed on data privacy
- Create a data vault that is encrypted with restricted access
- Limit access to data on a need to know basis and track access
- Implement security software where necessary
- Implement patch, upgrade and anti-virus/malware management
- Enable audit logs, internal and external & review often
- Implement back up procedures
- Insure where possible as a full breach requires expensive cures
- Transmit emails encrypted and password protected

The bad guys do not need to break in wearing a balaclava with their tuxedos and use a Minox camera to take pictures of selected files in the middle of the night. They can wear shorts, and take all of your files in moments for the other side of the planet, balaclava - optional.

A few more suggestions not IT based but structure based include;

- Disable all CD/DVD drives by unplugging them once all of the software has been installed
- Cut the wires on the USB Ports for all computers but one or two
- Store the most sensitive data on a computer not connected to the Internet and secure the location of, and access to. Update via 'sneaker ware' by taking data from the network on a USB drive and updating the sensitive data.
- Archival data should be considered sensitive and once not in regular use should be cleared from the network and stored either on CDs or DVDs and locked up or on the sensitive data computer.
- Wipe empty space on the computers regularly, it is good maintenance anyways.
- Never use a USB dive you did not purchase new, allow no one else to plug in a USB drive to your computers - ever.

Intangible assets make up 80 per cent of the value of the S&P500. For us service providers I am sure the percentage is higher. We lock and alarm our office to secure them from theft; we must take real steps to do the same to protect our much larger assets - our information.