

September 8, 2011

Regarding case in Western District Court, Waco Division regarding United States v. David Holt Palmer:

Waco, TX – On Thursday, September 1, David H Palmer, a former employee of McLane Advanced Technologies Commercial Division (MAT Comm), pled guilty to computer intrusion. Palmer is set for sentencing on November 2.

Mr. Palmer used existing user names and passwords to access servers at Lonestar Plastics and Capstone Mechanical on Thursday, January 21, 2010 beginning around 5:30PM. By the early hours of the morning on Friday, January 22, 2010, MAT Comm had discovered that the problems experienced on these servers was intentional and malicious. MAT Comm engaged in forensic evaluation and was able to lockout all further activity from Palmer on these servers. It was not until the weekend that MAT Comm knew with some certainty that Palmer was involved. All of the damage caused by Palmer was intended to cause harm to MAT Comm and no data was stolen or copied off the systems. Although the time to recover all the files deleted or damaged was lengthy, MAT Comm's advanced backup and disaster recovery services ensured that eventually all the data could be restored. Business operations at Capstone Mechanical and at Lonestar Plastics, both in the Garland, TX operation and the Prattville, AL operation were temporarily impacted.

On Monday, January 25, 2010, MAT Comm contacted local authorities who referred them to the Department of Homeland Security's Secret Service in Waco because the incident involved operations that crossed state lines.

At no time were any other systems involved that were managed by MAT Comm. Furthermore, no access to MAT Comm's or McLane Group's systems other than Lonestar was ever attempted or gained. MAT Comm's standard protocols dealing with departing employees ensured that the risk of such a situation was mitigated.

This particular incident may have been avoided by reminding users of computers systems that user names and passwords should not be handed out carelessly. If a password needs to be provided, then the password ought to be changed as soon as the need is satisfied. Using a best-practices approach to password management including sufficient complexity and a requirement to change with some frequency is the best measure for prevention.

Media Contact:

Steven Phillips
(254) 771-6414
steven.phillips@mclaneat.com
www.mclaneat.com