Top Five Cyber Security Myths for Industry

The industrial control automation industry has seen a lot of change with the migration from analog based switching, to programmable PLCs to today’s complex DCS systems. None of the industries have been more impacted than the Power Generation, Chemical Manufacturing and Water Processing facilities. While their network control systems have evolved from older proprietary hardware and software architectures to digital networks running on TCP/IP on Ethernet—the very same protocols and architectures that run the corporate IT networks — the attitude towards cyber security has not.

Despite the fact that there were over 286 million threats detected in 2010 and the number of daily web attacks has increased steadily over the same period to 20 million per day, as reported by Symantec’s Internet Security Threat Report. Even the US Government has recognized that ‘Targeted’ attacks such as Hydraq (aka Aurora) and Stuxnet are on the rise and considered the number one threat. However, in many cases, old ideas and myths still shape the network systems in the field today. The old adage of “if it ever happens” must now be viewed as “when it happens”. A number of cyber security myths that fuel these misperceptions include:

**Myth:** I have deployed an anti-virus software on my network; therefore, my systems are safe.

**Myth Busted:** While anti-virus software is an important element in protecting your network information, it cannot prevent an attack. New threats and technology are constantly evolving and changing the cyber landscape.

**Myth:** I have a firewall, so I am safe.

**Myth Busted:** Firewalls provide secure access to the networks they protect. Hackers understand typical firewall strategies and codes, and they exploit common IT mistakes and oversights to achieve their goals. The Breach Investigation Reports states that, “Only 17% of cyber security threats were designated to be highly difficult”; this means, in turn that hackers make 83% of cyber security threats easily. However, these cyber security threats are avoidable.

**Myth:** I run on UNIX. Only windows-based computers are susceptible to cyber security threats.

**Myth Busted:** The Cyber Alert system has identified over 90 new or updated vulnerabilities. Of these, 12% targeted Windows systems, 50% affected UNIX/Linux (aka Apple), and 38% affected other Operating Systems. The SANS organization findings have indicated that the number of vulnerabilities being discovered on applications is far greater than the number on operating systems.
Myth: My computer is not connected to the internet or network, a virus cannot attack my system.
Myth Busted: Unfortunately, no computer is an island. Computers need software updates loaded and patches downloaded. In most cases, the network does not deliver the virus, the user does in the form of a USB device such as a free trade show thumb drive. Research done by Avast!® found that 1 out of every 8 attacks on computers now enters via a USB device. Many cyber security experts see the USB Thumb Drive as the greatest threat to cyber security.

Myth: Advanced hacking techniques render cyber security pointless.
Myth Busted: Nearly 90% of all external attacks exploit poorly administered, misconfigured or inadequately managed systems, that any moderately competent hacker could exploit. There are many more moderately competent hackers than good ones, due to the large number of mediocre cyber security deployments in the industry today.

While there is no magic hardware or software product that will guarantee 100% protection from cyber security threats, Invensys’ Critical Infrastructure and Security team specializes in cyber security solutions and architectures. Invensys’ solution is unique in that it is a platform independent lifecycle methodology that integrates seamlessly between manufacturing operation and corporate IT networks.

Invensys’ Cyber Secure Portfolio solution takes a holistic approach to cyber security, based on these four tenets of security compliance:

- Assessment
- Development
- Implement
- Management

Is your network secure and safe? Contact Invensys for a comprehensive cyber security GAP analysis. Be a Myth Buster—not Myth Busted.