THE PSYCHOLOGY OF NETWORK (IN)SECURITY

Is your company concerned about being connected to the Internet? If so, you're not alone. It's the fear of being successfully hacked that's keeping many companies and their employees off the Internet. In fact, according to Infosecurity News, over 25% of all companies polled responded that hackers have tried to gain unauthorized access from outside the corporate network.

What else keeps companies disconnected? Hackers are no longer just techies with a hobby. Hackers are no often highly trained professionals in places like Eastern Europe, Russia, or China, and they're out to make a profit on you. There's a mystique to being hacked. It's the new crime, it's the hottest news. And it's fun…according to hacking group Lulz Security, whose motto claims they are, *"The world's leaders in high-quality entertainment at your expense."* Well they sure aren't fun for you. If anything, this hype from the media watchers and technical experts, should be keeping you on your toes.

So why the mystique? Our ever-growing, ever-faster cyberworld makes protecting your network from intruders ever more difficult. Many people, including company executives, lack a fundamental understanding of technology. Mix this with the complexities of network security issues and you can see why many companies haven’t ventured onto the Information Superhighway. However, what you don’t know really can hurt you.

On the other side of the spectrum, there are many companies with executives who have “Teflon sensibilities.” Media hype doesn’t stick to them. Unfortunately, neither does the advice of company network administrators who want network security problems addressed. These companies go about their connected-to-the-Net business until the inevitable compromise in security happens. And when something valuable is swiped, the executives worry.

“We’ve taken steps to make sure something like this never happens again!” is the boilerplate reaction. Otherwise, they say, heads will roll. For companies that have been hacked, the cost of information security now equals the cost of the incident plus the cost of countermeasures.

So protect yourself from hackers while getting the Internet access you need. You’ll never be 100% secure, but you can dramatically reduce your risk and proactively defend your organization by containing and controlling threats, vulnerabilities, and assets. Just use the 4Ds:

- Threats need to be **detected, deterred, defended** against, and **defeated** in real-time or expect downtime.
- Vulnerabilities need to be **detected, deterred, defended** against, and **defeated** (i.e. removed by system hardening, reconfiguration, patching, etc.) as quickly as possible or expect to be exploited.
- Assets need to be controlled—which ones gain access to your network/infrastructure and those that are trusted but weak or infected need to be quarantined in real-time or expect malware propagation.

It’s a fine balancing act, but you *can* protect data and keep out the unwanted while still giving your staff access they need. A network, as it turns out, is only as secure as the people who run it, use it, and fund its protection.

Source: https://bboxblog.wordpress.com/2011/07/15/the-psychology-of-network-insecurity/