Recent Sony's Hack Damage

There's been a lot of press, speculation and intrigue regarding the recent "hack" on Sony Corporation. I have already been asked by a number of people "Could you have prevented that?" A very simple question with a complex answer. Here's the quick response:

1. We could not have prevented the attack - no one on Earth can. Attacks can and will come and no one can prevent those.
2. **We could indeed have prevented the attack from doing any damage! THAT's what really matters anyway.**
3. To accomplish #2 above, Sony would have to re-architect their IT systems (the ones that they care about, *de minimis*) in accordance with our IQware architecture.

Once I explained that to a few people yesterday, they said, "Well, this should be an easy sale, then!". Ah, the enthusiasm of those not in this business. It's refreshing but misguided. To explain that - and to answer similar questions before they are asked - here's the reasons why contacting Sony would be a colossal waste of time - and why I'm typing this email instead of speed-dialing Sony's CEO:

1. Sony produces movies, among many other things
2. Most movies require a great deal of CGI work (Computer Graphics Imaging)
3. CGI is labor-intensive and uses a lot of really cool "animation" and frame-building/editing tools
4. The "CGI skillset" is becoming global and hence follows the cheapest labor pool
5. The various CGI "subtasks" are farmed out, often done by unknown individuals / parties working under a various (usually known) "corporate umbrellas".
6. **Thus, Sony can, does (and in fact MUST) share (=make available for access & editing) digital "assets" across the globe so that its "animators" can do their work and collaborate globally on one film**
7. Sony's operational practices, architecture, CGI tools, CGI techniques and CGI storage and archiving systems make them necessarily vulnerable to attacks, especially with a global labor force.
8. **Speculation #1:** some of Sony's workforce may indeed be in N. Korea - and Sony might not even know. Sony may have contracted with India, who often contracts with China (or Russia) and they, in turn, sometimes contract with N. Korea.
9. **Speculation #2:** N. Korea likely does not possess all of the software technologies required for the attack on Sony. That's something for the CIA or NSA to determine. Regardless, it's pretty easy for N. Korea to "contract out" this "digital hit" to disaffected folks in Chechnya, various places in the Middle East and elsewhere who'd love a quick buck and a chance to "get back" at anything USA-related.

All of that plays directly into #2 above - and represents an emotional+intellectual+financial "wall" that we do not have the resources to scale or breach.

Additionally, it's highly likely that all the "major players" in the cyber security business are chartering planeloads of salespeople and going after Sony right now at all levels, spending millions of dollars in that endeavor. It's 100% impossible to be heard above that noise. Again, we simply do not have the resources to compete with that volume on any level.

A Note On Our Sales Approach

Wisely, we do not lead with security in our sales approach. Even today, with the "cyber war casualties" mounting daily, people do not want to listen. They are akin to drug addicts who will not listen to a way out of the declining "death spiral". They are too far gone for reason. They go with what they know and that's net-centric defense and "defense in depth". More net-centric defense and anti-virus software is always better and will surely work THIS time. Right....:-D

So, what do we do?

We lead with "operational capability" which means that we give the customer more "things that they can do" which usually involve the creation of new revenue streams for them. We "toss in" security as a closer if required. Our rule-based design (now covered by 2 patents, US# 7,322,028 and US# 8,924,928) makes that a simple, effective pitch that we can "back up" with our delivery.

I hope that this little note helps everyone understand our measured approach. Of course, if you personally know the Sony CEO and have his private email/cell phone number, I will at least give it a shot ;-)

Regards,

Dr. Steve Belovich