BLOWBACK: STUXNET AND THE ONGOING RISK TO MANUFACTURING WORLDWIDE

Dear Chevron: Thanks for letting us know you've been infected with Stuxnet. It's difficult to muster sympathy for your management or shareholders, because you were warned.This guy quite clearly warned your industry, as did other firms specializing in technology security.

Every single manufacturer around the world using supervisory control and data acquisition (SCADA) driven equipment in their processes was warned. Businesses at particular risk are those relying on certain ubiquitous applications in a networked environment.

Perhaps you heeded the warning months ago but didn't disclose widely that your business was working on eliminating the exposures. If your business has been hardening your systems, great. However, the public does have a right to know know if your plant located in their backyard might blow up or release toxic chemicals because your firm was exposed to cyber warfare elements our country sponsored in some fashion.

This goes for any other firms out there that are dealing with the same exposure. Perhaps you believe it's a business intelligence risk to let your competitors know you've got a problem—frankly, we're way past that. The potential risks to the public outweigh your short-term profitability, and if your plant blows up/dumps chemicals/produces unsafe or faulty products because of Stuxnet, our public problem becomes your public relations/long-term shareholder value problem anyhow.

By the way: perhaps it might be worthwhile to actively recruit American citizens who qualify for security clearance when hiring SCADA application analysts to fix your Stuxnet

problems. Why compound your problem for lack of foresight with regard to national security risks? We can see you're hiring. Ahem.

Dear Senate Intelligence Committee: You are in way over your heads when it comes to technology. You need to rethink how you handle anything involving software and the hardware on which it runs as well as any technology attached to a network. That includes phones.

You let this thing loose when you signed off on it—you signed off on a weapon payload that was inherently insecure, or designed deliberately to be insecure, because it relied on delivery applications requiring security and upgrade patches every frigging month, delivered via network in nearly all cases. It's laughable that you think there was a leak requiring investigation when this insecure cyberweapon of mass destruction was released with your blessing.

What was it you thought you were authorizing? Did you not realize that this bug could spread because its was designed for delivery via an insecure application? Or did you permit an undisclosed quid pro quo to some unidentified entity so that all SCADA-based manufacturing could be affected at will at some point in the future?

There were at least three countries involved in this process, too. Did you rely too heavily on one of the two partners to keep a leash on the other? Have you asked how one of the partners is protecting its own manufacturing environment from exposure? Or did it never occur to you that they are our competitor for manufacturing jobs and have less exposure to this weapon because they don't rely as much on a private corporation's inherently buggy applications in their manufacturing? Did it ever occur to ask if there were secondary agendas on the part of any participant in the design, development, and distribution of this weapon?

And now that we the public know your little

xenomorph has gone rogue and into the wild, when are you going to mitigate the risks of proliferation by ensuring manufacturers as well as SCADA users like utility companies, mass transportation providers, and any site requiring physical maintenance and security controlled by computers are informed of the risks and take action to limit potential failures? Recall Congress' reaction to the risks from Y2K; Stuxnet and its precursors and variants may pose a far bigger risk than Y2K, worthy of deeper consideration.

Perhaps the Permanent Subcommittee on Investigations should review this mess to prevent future snafus like the Stuxnet debacle. Perhaps if you can't or won't tell us, you'll tell that committee what other monsters you've unleashed that might blow back on us all.

Dear Fellow Americans: Welcome to the 21st century, where proliferation is about bits and bytes of information, and not physical fissile materials. Perhaps it's time for voters to ask whether we have a 21st century government, capable of understanding the risks that technology poses. Or are we really comfortable with elected officials who think of the internet as a series of tubes, don't understand *The* Facebook, and wouldn't understand the concept of futureshock if it came up and bit them on the nose like it did with Stuxnet?

[*Note: Video embedded here features preeminent Stuxnet expert Ralph Langner of Langer Communications, "The first deployed cyber weapon in history: Stuxnet's architecture and implications" presented at NATO's International Conference on Cyber Conflict, Tallin (Estonia), June 2011. The definitive presentation to the SCADA industry from January 2012 can be found at this link; it is not embeddable. The most important portion of the video is in the last third, though the entire video, if rather technical, is worth watching*.]