Just about every industry in the US has had major security breaches. Recent news articles have exposed evidence of malicious trespassers from the Internet in every corner of the US Critical Infrastructure. To name a few: the energy industry's power grid, the air traffic control network, financial transaction processing networks, department of defense strategic planning systems, and health care services data repositories.[1] This is important because it indicates a basic inability of the corresponding management entities to control their own information technology. In each case, effective and well-known computer security controls would have prevented the attack. In each case, the organization's management professed to be aware of the vulnerabilities and to be actively working on the controls. However, none have claimed that their security plans have as yet achieved their objectives, and they all still admit to having preventable vulnerabilities.

Were the identified vulnerabilities to be exploited, the computer systems that support services critical to the US economy could be controlled by potentially hostile outsiders. The degree to which the outsider could run the computer systems depends on their technical sophistication. It could be like having a backseat driver reach over and grab the steering wheel. This would be a low-sophistication-level attack that nevertheless could cause massive damage to the enterprise. Or it could be that the car suddenly appears to have a mind of its own and ignores the driver's attempts to control its course. This would be a high-sophistication-level attack, and its degree of damage would depend on how closely the attacker follows the planned route. It has the potential to be more damaging because it would be harder to immediately detect.

There should be a clear recognition among the public, not just among information security professionals, that it is simply unnecessary to expose critical infrastructure to the Internet in the course of providing services like power and air traffic control. Where information must be shared with Internet users, such as in the financial and health care industries, there is growing recognition that companies in these industries often make poor decisions on where and how to store information and provide access to it. Organizations of both types claim that the balance between security and risk had been struck at an appropriate level at one time, but that threats are new, unforeseen, and expensive to mitigate. The time in the ideal past grows fainter as the years of known threat reports increase, yet each claim faintly echoes from refrains encountered in recent experience, and their sheer volume is persuasive. The common theme behind all management defense of poor security is the high cost of information technology control measures.

Those who claim that information security is too costly to implement exist in a variety of industries and have no common lobbyist. Instead, they bond as fellow victims of technology that is beyond their ability to control. These corporations do manage to control critical infrastructure like power grids, airplanes, financial transactions, and lab tests with considerable precision. They understand Deming and Drucker enough to set objectives, deliver product, and monitor performance with respect to business process. Yet we are led to believe that technology mystifies and confuses them to the extent that they should not be held liable for their inability to control it. It is true enough that there are highly sophisticated technical attacks. However, none of the announced remediation plans for security breaches in the news called on sophisticated new security technologies, just the sound application of well-known security measures.

Where such cases have been brought to litigation, there have been findings of unfair business practices and neglect on the part of companies who have not established well-known security controls.[2] However, there are not enough regulatory bodies or courts in the country to prosecute every company that puts citizens at risk, and many regulatory agencies routinely extend deadlines for compliance with information security requirements when industry lobbyists complain how hard they are to implement. While watching this situation unfold in the news media, I have been curious why there is not more outrage among those whose businesses and lifestyles would be permanently destroyed by a successful cyber-attack on the US critical infrastructure. I find this particularly curious with respect to the power grid story.

Although all of these industries are equally guilty of neglecting to protect their customers, as the power grid vulnerabilities theoretically could wreak the worst damage, and I have some direct experience with a power company, I will illustrate what I mean by well-known security controls with an energy industry example. An energy industry lobbyist was recently quoted as saying that cost was a significant barrier to disconnecting the power grid from the Internet.[3] Given that the Internet has only been a realistic alternative for communication for the past decade, we are expected to believe that electronic communications between business partners and regulators in a highly concentrated industry could not have been economically accomplished via a privately operated network, but were only enabled by the growth of the Internet, and now cannot be easily changed.

However, my experience in telecommunications pricing tells me that virtual private networks are only an incremental cost over Internet connectivity. The difference is not exponential. My experience in the financial industry, which includes an exponentially higher number of players than the energy industry, tells me that an industry can successfully form consortiums to operate virtual private networks. It is not the kind of challenge that should allow the US critical infrastructure to be left at risk. Rather, it is the type of challenge that a graduate student in computer science could use for a Master's thesis.

As a financial services industry corporate security officer, it had been my responsibility to maintain a technology architecture model whereby business could operate safely when it needed to use the Internet. I had also to ensure that unnecessary Internet connections were unauthorized, and in addition, technically impossible for a business user to configure. My firm once acquired a power company, and we had to convert their network to follow our model. We used the same security technology that we used in the financial services part of the business to reconfigure the power company's network, and to disentangle unnecessary Internet access from the controls on the power systems. Our only obstacle was the defensive newly acquired staff who claimed that what we were doing would not work. We accomplished our goal, and nothing we did made any significant impact in the IT budget.

In the course of converting the power company to our secure network model, we found another security issue. The communications between the power company and one of its regulatory oversight agencies used an Internet communication protocol that had unsecure and easy-to-break authentication. We contacted the agency and asked if we could use a secure protocol. We were told no, the unsecure one was all that they supported. My only recourse was to have our legal department write a letter to the agency outlining the vulnerabilities to which the agency was exposing the industry. We never got an answer. For the agency to switch from the unsecure protocol to the secure one would have been a few lines in the configuration of their Internet-facing server. We were not asking for something that would cost anything but attention. The agency spent more money on their staff time communication with us, denying our request, than it would have taken to actually fix the vulnerability.

I am sure that there are computer scientists from all domains, not just security, that nodded their heads as they finished reading this example. Most basic security measures are easy to fix, and inhibitors are usually management rather than technology issues. However, many have also experienced major productivity impact due to inefficient security measures such as lengthy approval processes and hard-to-remember passwords. Historically, these experiences have led to international best practices that require all security measures to adopt a risk-based approach that ensures that security measures should all be individually cost-justified compared to some kind of quantification of business risk.[4] Unfortunately, so many organizations have judged that balance to be so far on the side of risk-acceptance that the new industry standard would seem to be one of neglect.

[1] Epstein, Keith, and Ben Elgin, “The Taking of NASA’s Secrets,” Business Week, December 1, 2008, pp 73-79.

Davidson, Paul, “Cyberspies have hacked into power grid, officials say” USA Today, April 9, 2009.

Gorman, Siobhan, “FAA’s Air Traffic Networks Breached by Hackers,” *The Wall Street Journal*, May 7, 2009.

Acohido, Brian and Jon Swartz, Zero Day Threat, Sterling, 2008. (Exposes Organized Cyber-crime in the Financial Industry)

Gorman, Siobhan, August Cole, and Yochi Dreazen, “Computer Spies Breach Fighter Jet Project,” *The Wall Street Journal*, April 21,2009.

Vijayan, Jaikumar, "'Hacker' threatens to expose health data, demands $10M," *Computerworld*, May 6, 2009.

[2] Wolf, Christopher, *Proskauer on Privacy*, Practicing Law Institute, 2008.

[3] Davidson, Paul, “Cyberspies have hacked into power grid, officials say” *USA Today*, April 9, 2009.

[4] International Standards Organization, Information technology — Security, techniques — Information security risk, management, ISO/IEC 27005:2008(E), 2008, www.iso.org.