

The Here and Now of Cyber Security

A Q & A with Chris Furlow

We're hearing a lot in the news recently the perils of cyber space. Why do you think cyber security is becoming increasingly more relevant in the public and private sectors?

Very few infrastructures remain that are not in some way connected to the cyber world. Our financial service industries are reliant upon cyber to perform transactions—from a consumer making an ATM withdrawal to the transfer of funds between major corporations. In the energy sector we've seen concerns over threats to our power generation capabilities and now see the development of a "smart grid" to ensure more secure, resilient bulk-power production and distribution. These are just a couple of examples. The ability to support our economy, commerce and way of life are dependent on these systems. Therefore, they are attractive potential targets for nation-states, terrorist organizations and independent actors.



Cyber warfare – is this the new sleeper threat? And how should governments be preparing for this new battle tactic?

Well, what we are seeing is the rapid *evolution* of cyber warfare—it's just that most people are not aware of the serious nature or reach of this global threat.

During the recent conflict between Russia and Georgia, cyber tactics were used to disable critical infrastructure for the civilian population, such as public power and communication capabilities. Media reports suggest that hackers stole U.S. identities and utilized social networking sites, in part, to facilitate these attacks.

So cyber warfare is not warfare of the future; it is warfare of the here and now. It has the capability not only to disable military targets, but also to inflict direct or collateral damage on civilians around the world—even those without computer access.

With the interdependencies that exist between government and private sector networks, securing cyberspace is a massive and complex undertaking. Additionally, from a government interagency perspective there are challenges posed by the missions of military, intelligence and civilian agencies—which are sometimes crystal clear and separate, and, at other times, are inter-twined.

So it will take leadership from the top to more clearly establish clear roles/responsibilities and to open communication channels in order to educate and engage both public *and* private stakeholders at all levels. Much progress has been made in this regard over the last few years, but there can be no let-up. Tough decisions need to be made immediately to establish authorities and break up turf battles—at the federal executive and agency levels as well as on Capitol Hill. But difficult or not, we become more vulnerable every day that we allow bureaucracy and indecision to delay addressing this threat adequately.

Difficult or not, we become more vulnerable every day that we allow bureaucracy and indecision to delay addressing this threat adequately.

It seems that the new cyber criminal has grown to include more than lone wolf hackers – the kid in his garage. Can you talk about today's new crop of cyber criminals and their various motives?

We pay bills online. We manage our checkbooks and retirement accounts online. We shop and make purchases online. Credit card data, social security numbers, passwords and other sensitive information may be used for these activities. And, increasingly, people communicate personal data to friends and family via social networking sites. This is prime hunting territory for criminals.

Our society is dependent on technology, therefore lone-wolves and organized crime will continue to utilize technology as means to achieving their ends. Just in recent days, reports surfaced about organized crime organizations from Eastern Europe targeting U.S. businesses by stealing legitimate banking credentials via malicious software.

Other actors that are politically or ideologically motivated will also utilize technology to communicate their agenda, to disrupt systems on which we depend, and they will use cyber-crime as a means of financing their activities.

Corporate espionage is also a very real concern—particularly for companies that conduct international business. Protecting their company networks and information systems—all the way down to individual laptop and desktop level—is critical to protecting intellectual property, trade secrets, confidential internal data and business strategies. And certainly, customer data protection is critical as well, when you consider liability concerns. At the end of the day, international business deals can put millions or billions of dollars on the line, so there are very real consequences to not adequately protecting your systems.

Meanwhile, we have seen government struggle with protecting the information of veterans and employees when individual laptops have been stolen or misplaced. And government networks are clearly being targeted for infiltration by cyber actors at all levels. As we just pointed out, identity theft—which has been viewed as a cyber-related crime carried out by random hackers—is suspected of being perpetrated to carry out the goals of a nation-state. Foreign governments are suspected of having probed into networks at the White House, the Pentagon and agencies with significant security requirements.

Should the international community condemn cyber security attacks in the way it responds to traditional attacks of organized disruption and terrorism?

A cyber attack can have the same effect as a conventional weapon such as a bomb, albeit without the bang. The goal is the same. That is to damage critical nodes of infrastructure and the interdependent systems on which government, industry and the general population rely. So the answer is yes, the international community should clearly condemn unjustified, destructive cyber acts as it does physical attacks. The problem is that the technology and the tactics used to carry out such attacks have thus far outpaced the ability of international organizations to formally address them. So we will need to adapt. But this will remain a challenge in the near term and will only encourage actors at all levels to test the limits of international law—or the lack thereof.

Earlier, you mentioned the smart grid. What characteristics are needed to make the smart grid work?

The Blackout of 2003 demonstrated the kind of disastrous and cascading effects that a disruption to the bulk power grid can produce. It's been estimated that the total economic impact of that event was in the \$6 – 10 billion range. When manufacturers and other businesses lost power, they lost production. Cities lost water treatment capabilities and other vital services, not to mention putting a massive strain on already stretched public safety personnel and resources.

If security fails and your operations are shut down or crippled, there is a real bottom-line impact.

So in addition to achieving economic efficiencies and environmental improvements, as it specifically relates to cyber aspects of the smart grid, two key requirements are that it be more secure and resilient. We must assess and reduce vulnerabilities, repel attacks whenever possible and have the ability to bounce back quickly when significant events occur—whether they are man-made or caused by natural disasters.

The Congress, the FERC and the NERC have and are continuing to advance standards to ensure better security and reliability. Public/private partnerships are working to ensure that government and industry stakeholders are addressing areas of mutual concern. And billions of federal dollars are being invested in building smart grid infrastructure and capabilities. There is still more to do. But in the end, security and resiliency, to include cyber and network protection, must be an integral part of planning, design and re-design alongside efficiency and environmental elements of the smart grid.

Many corporate leaders started embedding network protections in the early days of launching their e-commerce businesses, but cyber criminals have since become more technologically savvy. What is your advice to today's

business leaders trying to protect their networks, their customers and their reputations in a new, globally networked world?

Budgets are often the drivers. Unfortunately, security generally continues to be viewed as an expense or an “add-on.” The question is, “why?” If security fails and your operations are shut down or crippled, there is a real bottom-line impact.

In relation to cyber, some companies have installed some level of protection, but have done so without really assessing their vulnerabilities upfront. This means they have serious gaps. Other companies may not want to know what vulnerabilities they have or what new threats exist on their networks, because they would have to fix them—and that means dollars out of the budget. Unfortunately, the worst scenario is *knowing* that you’re exposed and not doing anything about it or hoping remediation won’t be so bad. It’s the equivalent of burying one’s head in the sand and is as much of a risk as the threats themselves.

Instead companies should view building, managing and constantly improving security and resiliency as an investment. If your networks are more secure, then your IP and other assets are safer. If your systems are resilient, and you are prepared to take contingent action when disruptions occur, then your supply chain is stronger. Ultimately, this ensures reliability for your customers—and that is a competitive *advantage* in the marketplace.



At Ridge Global, we have an exclusive package of training, consulting and software called Total Security Management or TSM. TSM helps companies build security, preparedness and resiliency into corporate-wide business activities—and makes them marketable assets.

This is critical as companies often experience spikes in their levels of security and preparedness, and these spikes are usually event driven. TSM helps to set focus points and metrics and manages processes in such a way that your level of security and preparedness are not only maintained, but are always getting better. TSM builds off of Total Quality Management and is poised to replicate TQM’s success as a business game-changer for companies that pride themselves on being industry leaders.

Chris Furlow currently heads up the U.S. Public Sector practice at Ridge Global and is the former Executive Director of the Homeland Security Advisory Council.