Regulation & Governance (2008) 2, 480–484 doi:10.1111/j.1748-5991.2008.00051.x

COMMENT

The cybersecurity challenge

Michael Chertoff
Secretary, US Department of Homeland Security

Of the many challenges facing the global economy in the 21st century, one of the most complex and potentially consequential is the threat of a large-scale cyber attack against shared information technology and cyber infrastructure, including the Internet. To be sure, the exponential growth of the Internet over the past two decades has created manifold benefits for society and the economy, but with these benefits has come a commensurate increase in cyber threats and vulnerabilities, making it imperative to act with urgency and purpose to protect the cyber domain from crippling attacks and disruptions.

Of course, the world of cyberspace is one in which we are unlikely to see airplanes crashing into buildings or bombs exploding on trains. But we could see human and economic consequences that are very much on par with traditional acts of terrorism. A successful cyber attack could shut down essential government services, imperil business operations, erode public trust in financial transactions, and disrupt electronic communications. The impact of a cyber attack could be far-reaching indeed, threatening multiple sectors of the economy at once and creating cascading effects across interdependent systems and operations.

But while the potential consequences of a cyber attack are every bit as concerning as those of a physical attack, managing the risk is not the same. Cybersecurity is not exclusively or even largely a government responsibility or something that can be imposed upon businesses or individual users of the Internet. In the US, the federal government does not own the nation's information technology networks or communications infrastructure, and it would not want to force a burdensome and intrusive security regime on one of the most dynamic and reliable engines of the US economy.

On the other hand, cybersecurity is not solely a private sector responsibility either. The private sector may own the vast majority of cyber infrastructure, but its benefits are so widely distributed across the public domain and so integrated into various sectors of the economy – from banking and energy, to transportation and communications – that everyone faces clear security risks and consequences if the infrastructure is not adequately protected.

Further complicating matters, we know that no single person or entity controls the Internet or IT infrastructure and there is no centralized node, database, or entry point. No single person, company, or government can fully protect the IT infrastructure. And a security failure in even one company, or at just one link of the chain, can have a cascading effect on everybody else.

How do we address this shared problem in an era of increasing global dependency on cyber systems and infrastructure? How do we ensure the integrity of the Internet without compromising its fundamental openness and fluidity and unique culture? And how do we minimize the impact of cyber attacks while increasing economic and communications resiliency?

Recognizing cyber threats

It is important to understand the serious nature of the current threat. As we know, the Internet has been around for roughly two decades. For about the same amount of time, we have also seen cyber attacks in one form or another. Some may be tempted to suggest that cyber attacks are merely a cost of doing business – a nuisance dealt with in the past that can be readily dealt with in the future – and that there is no real reason to treat this threat as a concerted national or international priority. I think this would be a misguided approach.

The US intelligence community has publicly stated its assessment that some nations, including Russia and China, have the technical capability to target and disrupt parts of the information infrastructure, or to use that infrastructure to collect intelligence and other kinds of information. Nation states and criminal groups target governmental and private sector information networks in order to gain competitive advantage in the commercial sector, as well as in the area of security.

Terrorist groups, including Al Qaeda, Hamas, and Hezbollah, have expressed the desire for using cyber means of creating harm. Criminal elements show a growing and alarming sophistication in technical capability and targeting, operating a pervasive, mature economy in illicit cyber capabilities and services that are available to anybody willing to pay.

Cyber threats can impact individuals and nations alike. During the Georgia–Russia conflict earlier this year, we saw perhaps the first instance of military action with a clear cyber component. The denial of service attacks launched from Russian IP addresses against Georgia occurred with military action taken by Russians against the Georgian government. A large number of Georgians could not access any information about what was happening in their country. Government websites were defaced and the delivery of government information and services was curtailed.

In the US, criminal networks have exploited cyber systems for significant personal gain. In August 2008, the federal government disrupted the largest cyber identity theft ring in US history, involving 40 million credit card numbers stolen from nine major retailers through a sophisticated, international scheme perpetrated by capturing wireless transmissions of information from commercial computer systems. This scheme led to millions of dollars being withdrawn from the bank accounts of innocent consumers across the world.

The reality is that cyber attacks are not decreasing; in fact, they are increasing in frequency, sophistication, and scope. They include a broad range of nefarious activity: a single individual or an organized criminal group trying to steal personal or financial information; a hacker trying to breach a system to show that he or she can do it; nation states engaged in cyber espionage against governments and businesses. There is also the prospect of a terrorist group hijacking and exploiting the Internet to cause very real damage to information and communications systems and to the economy.

Defending systems and networks

All of these threats have major implications for national and economic security. As such, they raise the question of how best to address them.

The first thing we must do is ensure that government networks are adequately protected. In essence, we need to look across government's civilian domains to assess

vulnerabilities, reduce points of access to the Internet that could be sources of intrusion, put into effect tools that will reduce or eliminate the possibility of an attack, and use around-the-clock monitoring to stay ahead of an evolving adversary.

In January 2008, President George W. Bush issued a classified national and homeland security directive that for the first time will unify, accelerate, and expand the US government's cybersecurity efforts under a Comprehensive National Cybersecurity Initiative. This "Cyber Initiative" has three major components: establishing clear lines of defense; defending against all threats; and shaping the future environment by educating the next generation of cyber professionals as well as producing new, game-changing technologies.

As part of this effort, the US government will continue to ensure that privacy and civil liberties considerations are at the center of cybersecurity. The government has no interest in sitting over the Internet or attempting to control what people see. No government should disrupt the open architecture and culture of freedom that are the hallmarks of the Internet – to do so would undermine the very thing we must try to protect.

In the US, the federal government currently faces a situation in which it has thousands of connection points between government domains, civilian domains, and the Internet. This is simply too many and creates unnecessary vulnerabilities. To build a set of capable defenses, the number of connections must be limited. The US is now in the process of reducing the number of connections to less than one hundred.

In addition to reducing potential avenues of attack, government must have robust monitoring of and proper coordination between agencies. Every part of the civilian network must have appropriate levels of security for what is allowed to enter from the Internet and must show how system security will be maintained. A single weak link could compromise the entire system. To provide this coordination, the US Department of Homeland Security has established a new National Cyber Security Center to improve overall threat awareness and to ensure coordination among various federal cyber centers.

The Department of Homeland Security has also taken action to expand and strengthen its intrusion detection system, known as "Einstein." This system sounds the alert if a malicious intrusion has occurred, providing information about the signature and code of the attack, which we can disseminate to agencies across the network. We are in the process of deploying a more advanced system that will enable us to detect, in real time, if an attack is underway. In the future, the Department intends to move from intrusion detection to intrusion prevention, ultimately developing a system that will allow us to actually stop an attack before it permeates and infects our systems.

The second focus of the US Cyber Initiative is to protect against a full complement of threats: not only threats from hackers, criminals, nation states, and terrorists, but also insider threats, such as individuals downloading sensitive information, including passwords, that will afford them access to a system, or planting a bug that would enable the capture of information over the Internet. Although this is a relatively unsophisticated threat, it can cause as much damage as a traditional cyber attack.

Protection must also be provided against compromised hardware or software that have been embedded in electronics during manufacture or before they are sold on the open market. This is a particularly difficult challenge in a global environment where the components of a finished product are often produced in multiple places or countries, each with uneven quality control.

To counter these types of threats, steps must be taken to protect the global supply chain, and we must work with the private sector to achieve better validation of the source of critical elements of software and hardware, particularly for systems that contain high value, sensitive information. At the same time, governments must continue to use old-fashioned counter intelligence: working to prevent people from committing espionage, stealing data or passwords, or implanting trapdoors in systems.

The third and final element of the US Cyber Initiative is to shape the future environment by recruiting and developing the next generation of cybersecurity professionals. Specifically, it involves working with the private sector to boost cyber education, training, and recruitment, as well as funding for leap-ahead technology and game-changing capabilities that will increase cybersecurity at an accelerated pace. Just as past generations of highly skilled workers met the challenges of their times, we must build a new generation of cyber professionals to address the current threat.

Expanding partnerships

Ultimately, the value of the Internet and the vast social and commercial activity it enables will only continue to multiply if its users are confident they will not lose their identities or their sensitive information when they enter cyberspace. The government alone cannot provide such assurance, nor can it mandate a top-down, command-and-control approach to a fundamentally decentralized, networked system.

On the contrary: Securing cyberspace will require an unprecedented series of partnerships among the public and private sectors, owners and operators of cyber infrastructure, businesses, and even individual users. To build such partnerships, the US federal government has reached across all sectors to set goals and priorities and exchange information about security as it relates to a particular sector's threats and vulnerabilities. The Department of Homeland Security has asked the private sector to look at cyber risks and mitigations as well as interdependencies that could affect multiple sectors and have cascading consequences on their ability to function. We also have explored the possibility of sharing federal capabilities, including our intrusion detection system, so the private sector can benefit from our efforts on a voluntary basis if it chooses.

Because managing risk is often an inexact science, the Department of Homeland Security is working with the private sector to establish metrics that will allow us to chart our progress and focus on how to mitigate risks apparent in the globalization of the commercial technology industry. It is important to create standards that will allow the private sector to gauge the integrity of the systems it purchases: it must have confidence in what it is getting on the open market and what it is delivering to its customers. Recently, we have seen a rising concern in the global environment about the safety of and potential contaminants in certain foods and toys. The security of software and hardware that finds its way into homes and businesses must also be of great concern.

Finally, individual citizens have an important role to play in cybersecurity. Simple steps taken at home or work can have an immense impact on overall protection and will help increase defenses. For example, individuals can ensure antivirus software is properly functioning and up-to-date, change passwords regularly and keep from writing them down, and avoid suspicious emails and websites. Unfortunately, too many individuals fail to take these steps on a regular basis, creating unnecessary vulnerability.

Conclusion

The challenge of cybersecurity is both significant and complex. Achieving effective regulatory governance in this area calls for a comprehensive strategy that involves coordinated action by government, the private sector, and individual citizens. Of course, an undertaking of this size and magnitude cannot be completed overnight – it requires a sustained, multi-year effort with significant governmental and private sector cooperation. More than anything, it will require developing and sustaining a sense of urgency and commitment because unfortunately the threat is mounting. The global community has a clear, common interest in protecting the security of cyber systems which calls for immediate action and cooperation, as well as ongoing attention and study.