MiniCase for Quiz-No3 – Multimedia Information Strategic Planning

Subject: Homeland Security Tries To Get Its Cybersecurity House In Order

By Eric Chabrow, InformationWeek, Oct. 2, 2006
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=193100332

Washington has so far fallen short of its goals for safeguarding the Internet, and if it's going to succeed, it will need more cooperation from private industry.

The idea of terrorists bringing down the Internet is as unfathomable today as the collapse of the Twin Towers was on Sept. 10, 2001. But the threat cyberattacks pose to the Net is real.

Government policy-makers, corporate leaders, and cyberwonks agree that it's ultimately the federal government's responsibility to coordinate protection of the Internet. But Washington has so far fallen short of its goals for safeguarding the Net, and if it's going to succeed, it will need more cooperation from private industry.

The Internet has come under attack before. In October 2002, a coordinated denial-of-service attack disrupted 13 domain-name root servers, making numerous Web sites unavailable. Early this year, a hacker brought down 1,500 Web sites by hijacking PCs and sending traffic to servers with a DNS query and forged source address. A larger-scale attack, one that effectively shuts down the Internet, is a genuine danger, experts say.

"It's not science fiction; it's not theoretical," says Larry Clinton, chief operating officer of the Internet Security Alliance, which works with CERT (Cyberattack Emergency Response Taskforce). "It's happening today, and in all likelihood will get worse."

Most eyes focus on the federal government, and particularly the Department of Homeland Security, to take the lead in developing the mechanisms to prevent large-scale attacks and a process for reconstituting the Net if a colossal disaster occurs. In fact, it's the law. The Homeland Security Act of 2002 and a presidential directive put the department in charge of orchestrating activities to support the IT systems that safeguard the nation's critical infrastructures. "Our job isn't necessarily to do it all, but to make sure we get all the players to the table and to make sure it all gets done," says George Foresman, the Department of Homeland Security's undersecretary for preparedness.

Expectations of Homeland Security have grown in recent weeks. The agency named Gregory Garcia as its first assistant secretary for cybersecurity and telecommunications, a post that had sat idle for 14 months.

Even without its top cybercop, Homeland Security has made strides in meeting its mandate but has yet to fully succeed. The Government Accountability Office, the investigative arm of Congress, identified 13 key cybersecurity responsibilities for the department (see box for highlights), but none has been completely addressed, and some of the agency's efforts seem halffisted. GAO, for instance, cited working groups Homeland Security established with industry to practice responding to cyberevents, but judged those efforts as lacking synergy with other initiatives. A report from the Business Roundtable, an association of corporate CEOs, says the nation lacks the sort of coordinated response needed to fix Internet infrastructure in the event of a massive disruption.

Business' Role - Insofar as the government succeeds, business is going to play a big role. No single entity owns the Internet. Often, the companies that do own the Internet's infrastructure won't share information about their networks with the government. Some businesses gripe that the information the government wants is proprietary, and they believe that lax controls
could result in that data being leaked to competitors. David Powner, GAO's director of IT
management issues, says Homeland Security needs to better inform businesses about how
sensitive information will be used and protected. "Right now, with the folks we talk to in the
private sector, they don't see a lot of return from the Department of Homeland Security,"
Powner says. "There are real leadership issues there."

Foresman says his biggest challenge is getting cooperation from industry leaders, many of
whom don't trust the government. But he says the department is taking steps to coordinate its
efforts with the private sector. Homeland Security is working with the Business Roundtable to
develop specific actions regarding Internet recovery and reconstitution, Foresman says. The
Internet Disruption Working Group, which includes public- and private-sector members, was
formed to augment information-sharing among various levels of government and business.

**See You And Raise You** - The stakes of getting it right are high. Not only Americans have
become highly dependent on the Internet, but the entire world. Since the beginning of the
millennium, the number of Internet users has quadrupled to about 1 billion, according to
Internet world usage statistics. And it's not just the number of users that's relevant but how
they're using the Net for business and pleasure, employing Internet-enabled devices and apps
such as VoIP, wireless PDAs, and text messaging. Consider your own business' dependence on the
Net.

Internet users are more vulnerable to attacks than ever. According to the Internet Security
Alliance, a quarter of America's economic value--$3 trillion a day--moves across network
connections protected by a 30-year-old protocol that contains many known security flaws.
American businesses are already taking a hit from online attacks. As recently as 2004, the
economic impact of cyberattacks on business reached $226 billion, the nonpartisan
Congressional Research Service reports. The SANS Institute claims that financial losses for
banks from cyberattacks have soared 450% in the last year, and data-breach notifications
reached record levels this summer.

An attack on the Net needn't be massive to be overwhelmingly disruptive. Imagine terrorists
tampering with a minute portion of the Internet to corrupt key data, such as financial or
medical records, so as to compromise the integrity of other sets of data. "It doesn't have to be
all the data corrupted to lead to a loss of confidence of all information we look at on the
Internet," says Paul Kurtz, executive director of the Cyber Security Industry Alliance.

Before the Garcia appointment, critics freely attacked the federal government for not giving
cybersecurity its proper due. Now, with that position finally filled, we'll see how committed the
government is to getting the job done.

**Instructions.**

Read the Minicase article above and answer the following questions.

**Q1.** What is the job of the Department of Homeland Security for the United States
government as described in this article?

[5 points]

**Q2.** In order to fight cyberattacks and cyberterrorism, there must be cooperation
between the government and private businesses. However, it was said that
"the biggest challenge is getting cooperation from industry leaders, many of whom
don't trust the government". Why do you think that happens?

[5 points]
ANSWERS TO MiniCase for Quiz-No3

Q1. What is the job of the Department of Homeland Security for the United States government as described in this article? [5 points]

**ANSWER**

The exact job and responsibilities of the Department of Homeland Security for the United States government is gazetted in the document of the "Homeland Security Act of 2002". It is one of the many laws of the US government. However, some of the jobs we can gather from this article are:

- to take the lead in developing the mechanisms to prevent large-scale attacks and to prepare a process for reconstituting the internet if a major disaster occurs [line 31]
- to be in charge of orchestrating activities to support the IT systems that safeguard the nation's critical infrastructures. [line 33]
- to establish with all relevant agencies, institutions and industry players a coordinated response to fix Internet infrastructure in the event of a massive disruption. [line 47]

Q2. In order to fight cyberattacks and cyberterrorism, there must be cooperation between the government and private businesses. However, it was said that "the biggest challenge is getting cooperation from industry leaders, many of whom don't trust the government". Why do you think that happens? [5 points]

**ANSWER**

According to the article, I think private businesses and industry leaders do not trust the government and so do not give full cooperation in the fight against cyber-attacks and cyber-terrorism because:

- the information the government wants to prepare against those threats is proprietary, and they believe that the government’s lax in control procedures could result in their competitive advantage and sensitive data being leaked to competitors [line 56]
- the uneasiness in revealing information to the working groups which includes public- and private-sector members, and have their information shared among various levels of government and business. [line 67]
- The internal parties in the working groups may “misuse” the information provided – like businesses operating in an illegal manner, revealing trade secrets for profit, knowing previously “hidden” illegal practices, e.g. of over-charging customers, mischarging customers, avoiding taxes, avoiding tariffs etc. Who in the right mind wants to reveal these to the government? You are shooting your own foot by revealing that “hidden” information. For that the government can then bring you to court for contravening some other laws. So if you are in business - just keep quiet. Do not tell what is not necessary or not required by law to be declared to the government. This is the real reason for difficulty in getting full cooperation. Ha ha ha. No business is clean. Do you think Mr. Microsoft Corporation is clean? Please please. I will have to get another mini case for you to learn on this. Ha ha ha.