Extra 12/9/2009 7:44 PM ET

What if the Internet breaks?

The 40 year old system might be vulnerable to technical collapse or cyberattack, which could cause widespread chaos in fields from banking to health care to government

By Katherine Reynolds Lewis
MSN Money

When your Internet service goes down, it's at best an inconvenience. If you rely on it for business, it can quickly cost you money.

So imagine: What happens if the Internet breaks?

Picture people wandering the streets lost without GPS or maps on their iPhones, unable to pay for food or other goods with a simple swipe of a card.

Companies would have to resort to faxes and phone calls instead of e-mail; they'd quickly reach capacity and be unable to function. Credit cards wouldn't work; stores and hospitals would run short of supplies. Even electrical power to our homes could be disrupted.

"It would be a mess," said Dave Marcus, the director of security research for McAfee (MFE, news, msgs). "You would be taking businesses that were designed to do all their point-of-sale and financial transactions through the Internet and going back to pen and paper and taking checks in a car to the bank. People would lose their minds."

On the 40th anniversary of the first transmission over the earliest version of the Internet, it's more than an idle question to examine the network's fragility. It's been more than 20 years since the last systemwide overhaul, and Internet infrastructure is still based on 1970s ideas about computer networks.

Headline-making outages of popular Web sites such as YouTube and Twitter merely hint at the damage a fullblown failure could wreak. The Internet protocols that allow computers to communicate in networks have infiltrated every sector of our economy.

"The Internet has moved from being a toy or ornament to something that's central to our economy," said James Lewis, a senior fellow at CSIS, a nonprofit think tank in Washington, D.C. "We've automated all these processes, which makes our economy much more efficient, which means cheap. But it also means we're now dependent."

How could the Internet break?

The obvious question is, could it happen? In fact, parts of the Internet go down quite frequently.

The outages that make headlines usually involve a large segment going down, either cutting service to a geographical area or taking down a given Web site. For instance, Michael Jackson's death sent people flooding to sites such as Google News and Twitter, rendering each temporarily inaccessible. A few years ago, Pakistan's attempt to block access to YouTube in that country resulted in a two-hour outage of YouTube across the world. And early this year, hackers kicked the entire nation of Kyrgyzstan off the Internet.

Those examples highlight the two main risks: an attack or a technical collapse.

A systemwide outage is hard to envision, though. The Internet is a decentralized system of routers and networks owned by a variety of governmental and private organizations. That makes it resilient: If one section breaks, the network calculates a route around the disruption.

The Internet opened for business in 1969, when a government project connected scientists, researchers and military officials by networking giant mainframes. In the early 1990s, the government opened the Internet to commercial development. In 1994, Netscape launched its browser, the first of an ever-increasing cascade of user-friendly software and applications for public consumption.

To bring down the entire Internet, something or someone would probably have to disrupt the core Internet protocols -- the rules that computers follow when trying to communicate with other computers. That would not only break the World Wide Web but also private IP networks that companies maintain for greater security.

One possible avenue would be to attack the domain name system, or DNS, that identifies the address of each computer or device attached to an IP network. Currently, just more than a dozen computers scattered around the world contain the DNS addressing information for the entire Internet, Lewis said.

If someone were able to erase or scramble that information, your computer wouldn't know where to find the information on a given Web page or where to deliver an e-mail. But all that information is duplicated on each of the central servers.

That redundancy is probably the Internet's best defense. The Internet was designed on the premise that computers are smart but the network is fallible, even when the computer operators attached to it were all highly educated academics. These days, of course, those 30,000 experts have been succeeded by 1.5 billion untrained people connecting computers, iPods, BlackBerrys, televisions and other devices.

Simply staying ahead of the demand for DNS addresses and server capacity is a challenge. VeriSign receives 50 billion queries each day from computers looking for DNS data and expects that to rise to 4 trillion by 2020, according to Ken Silva, the company's chief technology officer.

Part of the debate in Washington over so-called net neutrality involves who would pay for billions in upgrades to enable the Internet to handle the demand of uses such as high-definition video. Experts at AT&T and elsewhere have suggested the Net could run out of capacity next year. The point is hotly debated, and it's not clear what would happen if it did.

The doomsday scenario

If the Internet did break, the impact would ripple through to:

- **Communications.** You wouldn't be able to get information from e-mail or the Web. Phone and television services that rely on IP networking would go dark. News organizations would be unable to communicate internally or to use the Web to gather and disseminate news. Governments would have trouble communicating internally and broadcasting emergency information.
- **Financial transactions.** Banks process payments electronically over IP networks, whether by the swipe of a credit card or the check you send from your bank's Web site. They do have backup systems, relying on physical checks and phone networks, but those require human staffing and would struggle to keep up with demand.
- **Transportation.** Airplanes, trains and even some roads rely on IP networks to ensure smooth transportation. Much travel would grind to a near standstill, disrupting the movement of people and goods around the country.
- **Retail supply chain.** Even those trucks and shipping avenues that work would be taken back to the dark ages, since retail stores wouldn't be able to use automated inventory systems. At Wal-Mart, for instance, when an item is swiped for sale, the cashier's machine sends a signal to a central computer database that a new product is needed in that location. A Wal-Mart Stores (WMT, news, msgs) spokeswoman declined to comment.
- **Health care.** Many of our medical records are stored on computer databases. With networks down, a health care provider would have to be standing in front of the relevant computer in order to access a record. Pharmacies, hospitals and clinics would have trouble accessing records and keeping supplies in stock.
- **Electricity grid.** You wouldn't lose power automatically if the Internet broke, but energy companies would be unable to send control signals around the grid. "That network becomes a potential point of failure," VeriSign's Silva said.

"If the Internet stopped working, every major corporation and government agency would not be able to function," said Tom Kellermann, a vice president at Core Security Technologies.

Don't run off to stock the fallout shelter, though. Many measures are in place to prevent a catastrophic failure.

"There are so many redundancies built into the Internet protocol and the architecture," McAfee's Marcus said. "The actual root servers of the DNS are not approachable by most computers."

At VeriSign, which oversees Web sites ending in ".com," 75 duplicate servers contain the same answers for computers that query the database for DNS data. VeriSign uses multiple operating systems, computers from different manufacturers and redundant routers to ensure that a bad chip or operating system vulnerability doesn't become a single point of failure. The master database also checks data before sending it out on the network to make sure any corruption isn't propagated.

"We attempt to make sure we are over-provisioned enough to not only deal with the demand in load but the demand in threats," Silva said. "If companies don't invest in infrastructure, they will pay a price for it eventually."

The government requires financial companies to maintain backup systems to ensure the smooth functioning of the system, said Scott Talbott, a senior vice president at The Financial Services Roundtable, which represents banks, insurance companies, mutual funds and securities firms.

"Financial institutions, like all major users of the Net, maintain and test contingency plans for a wide range of scenarios, including Net capacity issues, outages, routing complications and browser problems," Talbott said. "These plans are designed to keep all critical functions up and running, and to keep service levels as high as possible.

"If computer systems shut down, banks would have backup systems, and those legacy systems would cut in. Depending on the length of delay, there may be an inconvenience to the customer and a slowing of the transactions."

But while the lack of a central Internet authority deprives bad actors of a single target to bring down the Net, it also means there's no single organization that can order new security or protocols.

"The people who are managing the system work really hard to keep it stable. Our problem is that these Internet protocols are from the '70s," said Lewis, of the CSIS think tank. "You can polish it and keep it tuned up, but it's still a 1970s car. We know there are people in the world who are trying to figure out, 'How can I bring this thing down?'"

Even criminals need the Net

Perhaps the most reassuring argument against the threat of attack is that even the people who have the skill and motivation to carry one out -- rogue governments, terrorists or criminals -- are dependent on it.

"The bad guys really have no interest," said Marcus Sachs, the director of the SANS Internet Storm Center, an all-volunteer Internet early-warning organization. "It's not to their benefit to monkey around with the wires and the switches because they too are reliant on the Internet for communication and to steal things. It's kind of like a bank robber who would blow up the bridge next to the bank."

The major crime syndicates of the world derive 60% of their revenue from cybercrime, and each has a business unit solely devoted to hacking. "They don't want to burn down the castle; they want to take it over. They want to pillage it slowly," Core Security Technologies' Kellermann said. "It's not about breaking the Internet; it's about controlling the Internet. It's about maintaining a consistent, clandestine presence."

Likewise, terrorists use the Internet to recruit new members, disseminate propaganda, move money and communicate. Moreover, McAfee's Marcus noted: "How can you see the terror you're supposed to be inspiring in others if you can't access the Internet?"

Click on one of the stars below to rate this article from 1
(lowest) to 5 (highest).
Low High

View all top-rated articles
E-mail us your comments on this article
Discuss in a message board
Rate this Article
Sort by ∫ Oldest first 1 10 of 135 Next