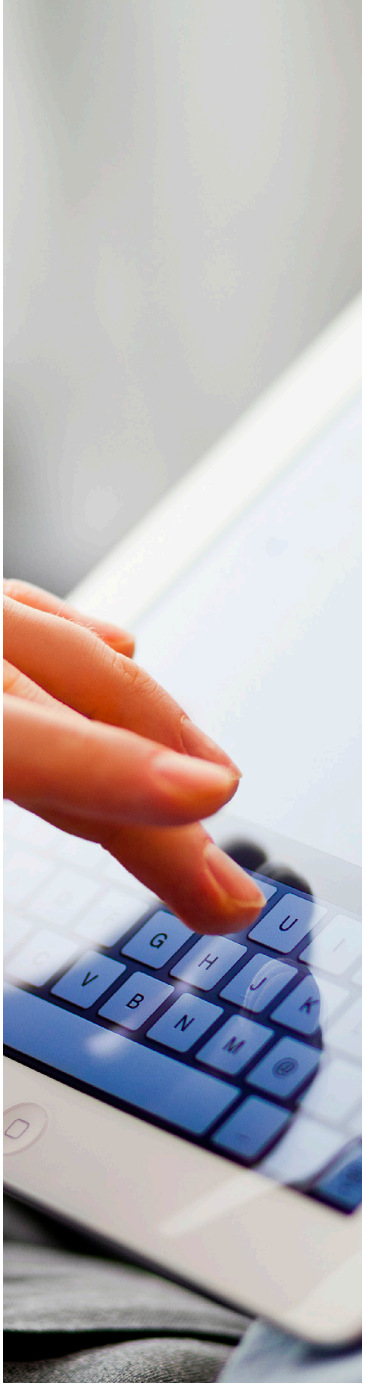


CareTech
An HTC Global Services Company

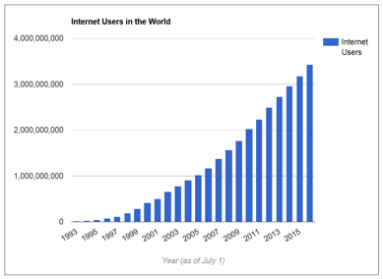
In Our Opinion

I heard an interesting stat the other day that surprised me – over 3 billion people now have access to the Internet. This means that over 40% of the world's population has the ability to go "online."

In 1995, that number was less than 1%.

Japan leads the way, with over 115 million people, or 91.1% of the population, currently connected.

The United States is 20th on the list, with a population penetration of 88.5%.



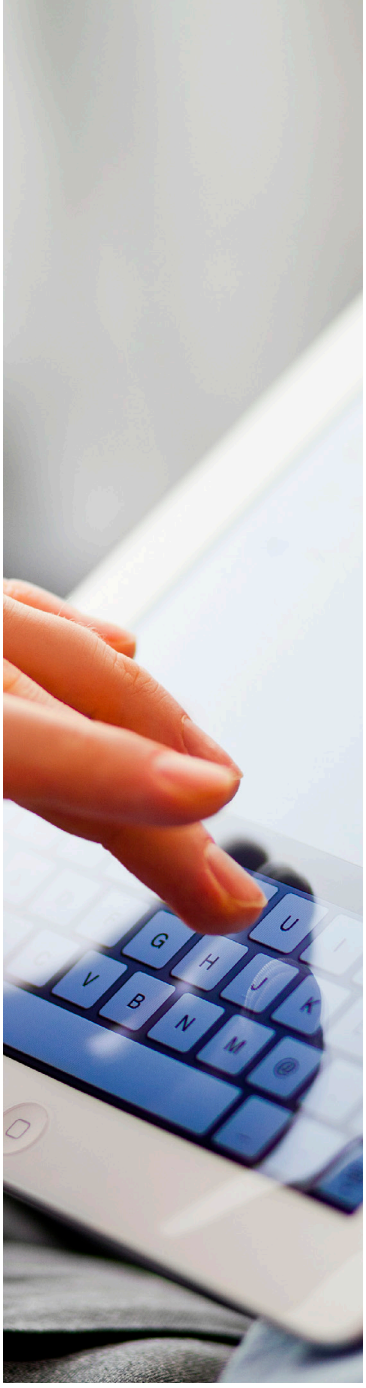
As you can see from the chart to your right, our appetite for information has grown exponentially with each passing year. This connectivity has provided greater access to data, improved efficiencies and given us the ability to interact with the rest of the world on a scale never imagined. It's also left us with myriad of security questions to accompany it.

Should we be concerned? What can we do?

While attending the AHA Annual Membership Meeting earlier this month, I had the pleasure of attending a panel discussion that Jane Holl Lute, CEO for the Center for Internet Security and former deputy secretary of Homeland Security, sat on. She posed several challenging questions that I think all of us should consider as we deploy IT in the healthcare space. I found her ideas compelling for the executive suite, and not just for the insight to be gleaned from the IT perspective. They were simple enough for everyone to understand and implement. By addressing the following questions, Jane believes we could help eliminate 85% of potential outside breaches from happening:

1. *Do you know what is connected to your network?*
2. *Do you know what is running or attempting to run on your network?*
3. *Who has administrative rights to your network and how do you know?*
4. *Do you have systems in place to patch it (your network)?*
5. *How can you demonstrate this to me?*

CareTech
An HTC Global Services Company



CareTech
An HTC Global Services Company

Understanding that there is someone who will attempt to infiltrate your systems at some point is the first step. Being able to respond and recover can be just as important as securing your systems. She challenged the audience to think about it from an enterprise perspective:

- *How do we architect systems we trust from components we can't?*
- *How do we insure the integrity of our information and identity in an open Internet?*
- *What will or should the role of government be in all this?*

The topic of security can be so broad and complex that it sometimes overwhelms us. My challenge to you today is to use some of the ideas from Jane's discussion and focus on the simple concepts and questions. Knowing who and how your network is being accessed is a necessary first step towards securing your systems in an open Internet and avoiding a breach.

Hospitals are viewed as easy or "soft" targets because they are considered relatively unprotected and vulnerable. They are also highly desirable because they contain a rich source of information and are connected to many different data sources, such as HIEs, physicians' offices, clinics, vendors, and even the home. Knowing who, why and how these entities are connected to your systems is vital to keeping your information safe.

As Jane said, "All known threats have known fixes." By working on the threats that we know, we can hopefully avoid some of the unknown ones coming our way as well.