CTO Challenge: Building a New Internet to Protect People and Data

Today's Internet is a complex global system of technical protocols, physical infrastructure, information resources, users, and a governance model based largely on just "getting along with each other". Its technical roots date to the post-WWII era when American and European researchers began connecting large mainframe computers via telephone networks. From the 1960s through the 1980s government funded projects like the ARPANET and the NSFNET built much of the foundation for what became the public Internet in the 1990s.

Commercial Internet Service Providers (ISPs) began to emerge in the early 1990s and by 1995 the government had removed funding for the backbone networks. The emergence of the Internet browser, along with Microsoft's inclusion of the TCP/IP networking stack in Windows 95 made the Internet available to billions of consumers worldwide via the ISPs. As the Internet grew through the 1990s, the 2000s, and the 2010s it transitioned from an experimental network to a critical infrastructure depended on by nearly every person, business, and government around the planet. But unfortunately, the technical foundations have largely remained unchanged since the 1970s and 80s.

Security and privacy on today's Internet depends, at a technical level, on a trust model developed in the early 1970s. At that time, the users of the ARPANET were few, and most knew each other as members of the university research community. When designing one of the most fundamental protocols - TCP/IP - the "trust anchor" of the system was placed in the user. The network itself, largely run by the phone companies, was not trusted. This was a fair decision, since the researchers typically would not harm what they were building, and phone networks were designed for communication by analog human voices rather than digital computers.

Two other critical protocols - DNS (the Internet's directory service) and BGP (routing) - were developed in the 1980s and are relatively unchanged. DNS and BGP also trust the user to behave properly and were not designed to counter malicious behavior. Other protocols such as SMTP (email) and HTTP (web browsing) were likewise designed during a time when users could be trusted. Today, the trust model is inverted. The networks are highly reliable and very trustworthy while the users (now every human on the planet rather than a small group of computer researchers) cannot be trusted. But the soul of the Internet still believes in the old model and believes that people can be trusted.

As can be expected, an open system like the Internet attracts both good and bad users. The first exploitations of connected systems started in the 1980s and has grown exponentially since the late 1990s. Today, most users just accept that the Internet is full of criminals and corruption. "Fake news" and targeting of Internet users to influence their political views infect social media sites. Ransomware attacks lock a victim's data until a Bitcoin payment is made to a shadowy group. Botnets and DDoS attacks knock websites offline for hours or days. Data breaches expose the private information of millions of victims. Spam, phishing, and misleading emails overwhelm inboxes. Countries like Russia and Iran are building their own networks that will not connect to the public version. China built their "Great Firewall" to keep citizens from visiting websites in other countries. Tools such as anti-virus software, user education, and expensive corporate security teams seem to be unable to stop the growing malicious behavior and resulting damage to users, systems, and data.

In Washington, the term "admiring the problem" is frequently used to describe the various efforts across multiple administrations to secure the Internet and make it a safer place for all users. From the Clinton to the Trump administrations, all have tried to address the problem via working groups, agency

proposals, laws, and regulations, but no effort has made a significant difference. The White House recently challenged a group of CEOs to propose a way forward. In response, they developed a "Cyber Moonshot" plan that was warmly received, but like most of these research reports it now sits on a shelf collecting dust. We cannot continue to admire the problem. We really do need to determine how to reengineer the global Internet in a way that protects investments but also seeks to eliminate many of the technical weaknesses that underpin the system.

Here is the challenge to the CTOs:

Build a new Internet that will protect people and data, and will

- Provide privacy and security for Internet users (people, organizations, and machines)
- Provide personal anonymity when appropriate; likewise provide full attribution of users, machines, and code when appropriate
- Deter use of the Internet for criminal, terrorist, or offensive military actions
- Optimize the Internet for social good, economic prosperity, and political/religious diversity
- Preserve the "open" concept of the Internet via a suitable governance model