# INNOVATIVE TECHNOLOGIES FOR A SECURE SOCIETY

**Saswati Soumya**
*Department of Education, St. Vincent Pallotti College,* saswati.soumya28@gmail.com

## ABSTRACT
Society owes its very existence to the basic human need for collective security. In this way, security and society are synonymous. Without one, the other ceases to be. But the relationship between security and society has grown increasingly complex and dynamic over the last two decades. Never before has the balance between the two been more in flux, as globalization, interdependence and digital technologies have literally reshaped the foundations of society, challenging every accepted approach to its security. Today, we are a truly global society, traveling freely and conducting business without borders over a communications network that connects virtually every person on the planet. The speed with which this change has taken hold has created unprecedented opportunity, both legitimate and otherwise. As business models and lifestyles have migrated from the physical world to the digital world, so too have criminal elements and other destabilizing forces.

## INTRODUCTION
It's all part of the inevitable security power struggle and the reason why truly complete security is not an attainable goal. Perhaps this is why many believe that security strategies should focus more on resiliency, or the ability to absorb and respond to attacks, rather than hardening perimeters and securing boundaries. Or that society needs to take a more distributed approach to security, empowering and enabling each of the world's security stakeholders to take more responsibility for the collective. On the following pages, you will find a more detailed description of the concept of distributed security, as well as further insights culled from a series of six brainstorming sessions, or "deep dives," that IBM convened around the world in 2008. These meetings brought together business leaders, government officials, entrepreneurs, academics and nonprofits to ask the hard questions about the future of security. The end result of this effort is not, of course, a solution to the world's security problems. This report is instead a collection of innovative security strategies for a globally connected world, strategies in which every government, business and citizen has a role to play."Society moves faster and is more complicated today than ever before. We expect access to communications and information anytime, anywhere, on any device. And security threats are constantly attempting to undermine these services. That's why it takes a monumental effort to secure the infrastructure that supports that capability. And why it's monumentally important that we do it well."

## THE NETWORK EFFECT
Globalization has supplied us with a new breed of security threat: those that know no geographical boundaries. Online attacks can emanate from anywhere, and target anyone. Geographical borders are easily crossed. And global communications are cheap and easy. In this new era of global interdependence, the amount of damage that one individual can do is far greater than at any time in history.

>Common Law
>Wireless Watchdogs
>The Secure Supply Chain

It is called the network effect, in which the harmfulness of a single threat is exponentially proportional to the number of people exposed to it. To date, the network effect has worked in favor of the bad guys. They have harnessed and exploited this new digital reality, and they themselves have become a network of formidable strength and speed. For example, 94 percent of all browser-related online exploits occur within 24 hours of a vulnerability being disclosed. These so-called "zero-day" attacks provide further evidence that the traditional centralized, command-and-control approaches to security are no longer sufficient in this fast-paced, constantly changing networked environment.

**Common Law**

Considering the Internet is only a few decades old, it's not surprising that the security systems that guard this digital realm are less evolved than those that govern the physical world. In fact, many of the terms used to describe Internet security are still borrowed from the lexicon of physical security: firewalls, backdoors, patches and so on. But for a medium as distributed and populist as the Internet, putting up walls hardly seems an appropriate response to the rapidly evolving security threats that plague it. That's why many GIO participants advocate the idea of community-based security, in which online groups that share a common interest police themselves, sensing and responding to threats as needed. "Could there be a time in the future when bad behavior is punished by the community?" asks Pat Conley, Senior Vice President of Product Development at VeriSign. "On a very small scale you see this in forums and other online communities already, and this kind of self-imposed punishment is a way in which the community lays down the law." For better or worse, the idea conjures up images of the puritanical village in Nathaniel Hawthorne's novel The Scarlet Letter. But these communities can take a variety of forms: a company; a political party; a social network. And in the digital world, communities are even more fluid and self-selecting. The only requirement is that the group share a common set of values.