Six steps to increase cybersecurity in the age of innocence
By Ray Rothrock

Let's face it; we have a lot to learn about cybersecurity. For weeks, the FBI and Apple squared off in an epic and public battle over encryption, the holy grail of cybersecurity warriors. "Help us break the iPhone," said the FBI. "The risk is too great, too many will be harmed," argued Apple. But the battle was over before the parties fully engaged. The FBI found someone, somewhere to hack the iPhone; never mind, problem solved. Do you feel secure? With attacks launched every day, I don't think so.

This brief iPhone history captures the dilemma facing President Obama's new Commission on Enhancing Cybersecurity. The commission's charge is to make actionable recommendations for the public and private sectors that address cyber threats today and in the future. But every day we learn that solutions can have a short shelf life, and that hackers have managed to stay a few steps ahead of those trying to track them down.

As an early investor in cybersecurity startups and now CEO of a cybersecurity analytics company, I applaud the commission's goals. Billions of dollars are spent every year on cybersecurity products, yet breaches continue to happen; they have almost become routine. What gives? Last year, JP Morgan Chase said it planned to spend $500 million on cybersecurity. The company's general counsel for IP and data protection said they "still feel challenged." Does half a billion buy peace of mind; apparently not.

What can the commission do to keep us more cyber secure? Here's a modest six-step plan that will move us forward.

Step one is a change of perspective. All of our networks are regularly probed and penetrated by attackers looking for weaknesses. Given the complexity of our networks and the sophistication and persistence of attackers, some of these attacks will be successful. Rather than focusing solely on preventing the unpreventable, we should prepare for the inevitable and make networks resilient so they can operate through an attack and minimize business disruption.

Step two is to realize that digital resilience is no longer just the responsibility of an organization's IT department. It must be managed at the highest levels of an organization. Businesses and organizations should follow the example of New Orleans and appoint a *chief resilience officer* reporting to the CEO and board executive committee. This role is broader than that of chief information security officers (CISOs) who have traditionally focused on cybersecurity technology. A resilience officer would manage risks and tradeoffs, set priorities, and engage senior decision makers on what is really important for an organization's continuity. Corporate boards need to get involved, too. Every board should be required to include at least one member with cybersecurity experience.

Step three is to understand what each network looks like, how it is set up, and how it is constantly changing. Networks, even simple networks, are patchwork structures that grow over time; more end point devices, more storage, more computational power, and more administrative rules. As networks grow, mistakes are made and new attack vectors are opened. If you don't know what you really have, how can you manage it? When you know the extent of your network, you can verify you are complying with regulations, policies, and industry best practices. You can understand what part of your network might be at risk and respond quickly when any incident does happen.

Step four is to identify clear metrics for resilience and security preparedness. A key tenant of all management training is that you can't manage what you can't measure. Currently, there are many measures of how much activity is going on in a network, how many attacks have been launched, and how many successful defenses have been deployed. But we need to go beyond activity and measure the results of cybersecurity, examine how resilient a network is, and how prepared IT managers are to identify active threats and keep a network operational even during a successful attack.

Step five is relatively straightforward. We generally don't need to invent new standards and regulations. We have many thoughtful public and private sector policies in place from the Department of Homeland Security, the North American Electric Reliability Corporation, Common Weakness Enumeration group, and others. We need to implement and maintain them to minimize damage to our networks and stay resilient.

Step six may be the most challenging. Everyone in an organization uses the network. And networks are all interconnected. All it takes is one click on a phishing email and malware is launched. Malware is a door that hackers can open immediately or months or even years later. We need to develop a culture of cyber awareness, help people spot hacking techniques, and train them in good security practices. It starts with simple things like changing your passwords regularly. How do we make people cyber aware? President Obama's cybersecurity commission is filled with smart people. It needs someone to help the panel address the human factor.

My advice to the Commission on Enhancing Cybersecurity it to stay focused on short term solutions with a long term foundation. The cybersecurity battle will be fought in a changing digital landscape. Today's successful strategies and tactics will be tomorrow's battlefield blunders. With the threat landscape constantly changing, security is an elusive goal. But with a change in perspective, new leadership, and broad cyber awareness, we can be prepared and resilient so that networks that are critical to our economy and civil society can be sustained while the battle rages.

Ray Rothrock is chairman and chief executive officer at RedSeal. Prior to joining RedSeal, he was a general partner at Venrock, the venture capital firm founded by the Rockefeller family.