REDSEAL

EXECUTIVE GUIDE:

6 STEPS TO INCREASE CYBERSECURITY

IN THE ERA OF CONSTANT CYBER THREAT

By Ray Rothrock, RedSeal CEO

Let's face it – we have a lot to learn about cybersecurity.

We read about new network breaches every few days. They've almost become routine. Oracle, Yahoo, Wendy's, universities, healthcare providers of all sizes, state and federal government agencies – including the NSA – make the headlines. And these are just from this year. You can make yourself crazy reviewing a long list at the Identity Theft Resource Center.

We spend billions of dollars annually on cybersecurity products, but do you feel more secure? I don't think so. What gives? Last year, J.P. Morgan Chase and Co. said it planned to spend $500 million on cybersecurity. The company's general counsel for IP and data protection said they "still feel challenged," according to Forbes Magazine. I guess half a billion does not buy peace of mind. Every day, we learn solutions have a short shelf life and that hackers have managed to stay a few steps ahead of those trying to track them down.

This is the dilemma facing President Barack Obama's Commission on Enhancing National Cybersecurity, charged with making actionable recommendations for the public and private sectors that address cyberthreats today and in the future.

As an early investor in cybersecurity startups and now CEO of a cybersecurity analytics company, I applaud these goals. What can the commission – and all executives – do to keep us more cyber secure? Here are six steps we can take to move us forward.

1. Change of perspective. Networks regularly are probed and penetrated by attackers looking for weaknesses. Given the complexity of networks coupled with the sophistication and persistence of attackers, some of these hacks will be successful. Rather than focusing solely on preventing the unpreventable, we should prepare for the inevitable and make networks resilient to operate through attacks and minimize disruption.

2. Realize digital resilience belongs to all. No longer is it the responsibility of an organization's IT department. Businesses and organizations should follow the example of the city of New Orleans and appoint a chief resiliency officer. The role is broader than that of chief information security officers (CISOs), who traditionally focus on cybersecurity technology. A resiliency officer would manage risks and tradeoffs, set priorities and engage senior decision makers on what is paramount. Corporate boards need to get involved also. Every board should be required to include at least one member with cybersecurity experience.

3. Truly understand networks. Know what they look like, how they were set up and how they constantly change. Networks are patchwork structures that grow over time; more endpoint devices, more storage, more computational power and more administrative rules. As networks grow, managers can make mistakes, opening new attack vectors. If you don't know what you really have, how can you manage it?

6 STEPS TO INCREASE CYBERSECURITY

4. Identify clear resilience metrics 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. We must go beyond activity and measure the results of cybersecurity, examine a network's resiliency and how prepared IT managers are to identify active threats and keep a network operational – even during a successful attack.

5. Don't invent new standards and regulations. We have many thoughtful public and private policies in place from the National Institute of Standards and Technology, Department of Homeland Security, the North American Electric Reliability Corporation, Common Weakness Enumeration project and others. We must implement and maintain them to minimize network damage and stay resilient.

6. Everyone in an organization uses the network. This step might be the most challenging. Because networks are interconnected, all it takes is one click on a phishing email to launch malware and give hackers access. We must develop a culture of cyber awareness, help people spot hacking techniques and provide good training.

A word of advice to the members of the commission and all of us: Stay focused on short-term solutions with a long-term foundation. We are fighting the cybersecurity battle in a changing digital landscape. Today's successful strategies will be tomorrow's battlefield blunders, making 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 critical to our economy and civil society can be sustained while the battle rages.

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