REDSEAL

September 8, 2016

Comments to the Commission on Enhancing National Cybersecurity
Submitted by RedSeal, Inc., Sunnyvale, California

To start simply: You can't repave a cobbled street and call it a super-highway.

As a critical first step toward our country's cyber resiliency, the federal government needs to address its aging legacy systems – some systems are now more than 50 years old and running on eight-inch floppy disks – and it needs to do it now. To help solve the problem, the Obama administration wants to establish a $3.1 billion fund that will enable agencies to transition away from legacy IT toward more modern options.

While technologists are offering recommendations about what the government needs to focus on – from encryption to updating operating systems, and new hardware that can run the latest applications – I encourage you to address the underlying problem.

Our nation's legacy systems were never built for security. They are old, their applications are not compatible with new technology and they are riddled with misconfigurations that allow unintended access to high value assets and mission critical components.

Please resist attempts to further resuscitate the federal IT infrastructure and instead invest in next-generation networks, which are built from the ground up with security and performance in mind. This new network will be resilient from the get-go, so that when an attack comes the network can easily withstand it and prevent a breach of critical systems and data.

A New Approach to Cybersecurity

The reality, as Dr. Ron Ross of the National Institute of Standards and Technology recently told the President's Commission on Enhancing National Cybersecurity, is that we need a new approach to computer architecture to successfully address the nation's cybersecurity crisis. Our current IT infrastructure is insecure, and no amount of security software, firewalls or anomaly detection systems can truly protect it.

The only solution is, "to build more trustworthy secure components and systems," said Ross. He added that current approaches to the problem "fail to address the fundamental weaknesses in system architecture and design." In other words, many of the proposed "solutions" are unworkable in today's legacy environment. They are long-term solutions to an immediate problem.

To understand a network and its vulnerabilities, you have to understand all of its interactions. However, we have reached a point where systems and networks have multiplied in complexity, creating a reality that is nearly impossible to fully comprehend.

Networks, and the devices that are connected to them, are evolving targets and it is very difficult—if not impossible—to assure that they will be safe from cyber threats as they move and change. Compounding

the complexity is the fact that cybercriminals are always evolving as well, always finding new avenues of attack. “Our appetite for advanced technology is rapidly exceeding our ability to protect it,” said Ross.

That’s why we need advanced software to analyze the risk and create visual cues to prioritize the truly relevant threats. We need to start with a thorough assessment of an organization’s network-wide risk. Once an organization has assessed the risk, it can then make truly informed security decisions. It can make changes to reduce risk, insure against risk or simply decide that it can live with a certain level of risk.

Actionable recommendations to achieve digital resiliency: *A Matter of National Security*

To move us toward to an era of cyber best practices, and digital resilience, please consider the following modest, actionable recommendations:

- **Change perspective** from prevention to inevitability. Our networks are constantly probed and penetrated by attackers looking for weaknesses. Rather than focusing 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.
- **Appoint new officers**. Digital resilience is no longer just the responsibility of an organization’s IT department; it must be elevated to, and fully considered by the highest levels of an organization. Following the example of New Orleans, organizations should appoint a chief resilience officer who reports to its executive committee. Corporate boards need to get involved, too. Every board should be required to include at least one member with cybersecurity experience.
- **Understand the network landscape**. Networks, even simple ones, 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. When you know the extent of your network, you can verify that 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.
- **Manage through measurement**. Identify clear metrics for resilience and security preparedness. A central tenant of management is that you can only manage what you can measure. Currently, measurement is focused on activity in a network, such as how many attacks have been launched, and how many successful defenses have been deployed. However, to identify active threats and keep a network operational even during a successful attack, we need to go beyond activity and measure the results of cybersecurity, examine how resilient a network is, and how prepared IT managers are.
- **Implement not reinvent**. We generally don’t need to invent new standards and regulations. We have many thoughtful public and private sector policies in place from NIST, 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.
- **Address the human factor**. Networks are interconnected. All it takes is one click on a phishing email and malware is launched, leaving an open door for hackers to enter immediately, in a few

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.

My advice is to stay focused on short-term solutions with a long-term foundation.

Today's successful strategies and tactics will be tomorrow's battlefield blunders. 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.

Sincerely,

Ray Rothrock
Chairman and CEO, RedSeal
https://redseal.co/