MILKEN INSTITUTE

The Power of Ideas

2017 | Insights for Building Meaningful Lives

Ray Rothrock
Chairman and CEO, RedSeal

The Power of Resilience

Cybersecurity is no longer just the esoteric concern of very technical people; it is an important concern for us all. We read about major new breaches and compromised data at least once a week. And those are the ones that come to light. How many of us have gotten personal messages telling us to change our passwords or offers of free credit monitoring because our personal information is out there? You have to wonder what—if anything—is being done about this.

In fact, there are now more than 1,400 vendors focused on producing cybersecurity products. In 2016 alone, organizations spent $100 billion on information security. But the negative numbers are staggering. Billions of records have been compromised. Losses from cybersecurity attacks are on a trajectory to reach $2 trillion in 2018. And a major attack on our vulnerable utility grid—for example—would send even those figures skywards. Clearly, we need to do something different.

To date, cybersecurity focused on detecting the bad guys and how to keep them out. Yet the bad guys are still getting into the best companies with the best defenses, the best technology, and the best engineers.

The solution to this can be seen all around us—resilience. Organisms that can adapt and bend with issues, then snap quickly back, survive. The brittle ones break. This analogy works for organizations and networks too. We need to accept the reality that all our precautions and defenses can't stop every bad thing. It is no longer enough to ask "How can we prevent an attack?" Instead, we need to ask "What should we do when we're hacked to minimize damage and disruption?" We need digital resilience strategies.

Digital resilience does not assert that security can stop all attacks and breaches. Resilience is about surviving inevitable attacks and penetrations, about continuing to do business

Ray Rothrock

even when under attack; it is about discovering breaches and containing them, and about ultimately prevailing in spite of them.

It is more than just a technology issue; it is an organizational issue. Achieving and maintaining resilience must involve the whole organization, not just a security team. It begins with cyber teams working with executives and managers across the organization to prioritize all important data assets and know where they are. The objective is to analyze the value of data items as well as their accessibility to attack. Organizations can create a truly resilient strategy that provides differentiated protection for their most important data only when these insights are in hand. Critically important assets call for close control of access as well as high levels of encryption. Less sensitive data assets can be made more widely and readily accessible.

Resilience strategies need to be comprehensive, addressing all organizational

"Achieving and maintaining resilience must involve the whole organization, not just a security team."

processes, from product development, to marketing and sales, to human resources, and the supply chain. We know that building a firewall around the perimeter of a network, while important, will not make a network resilient. Threats can still come from the outside—often through connections you make—as well as from the inside, for example, from unwitting employees clicking on dangerous links. The fact is that your network is no more secure than the networks with which it connects.

Once you have a strategy set in place, you still cannot rest—you must remain aware and agile. Networks are always changing, and we need to understand the risks each change brings, and adapt. The safest automobiles, for example, are sophisticated, agile systems. In a collision, they crumple strategically, absorbing energy that would otherwise be transferred to driver and passengers. A digital resilience strategy gives you the agility to adjust to the attack, contain it, and operate despite it. It enables organizations to adapt to sudden impact.

Resilience is not a product. It is not a department. It is not the responsibility of one person. Resilience is a way of thinking, and—once committed to—it quickly becomes an essential part of how effective organizations operate, delivering confidence to customers and partners. Resilience begins with knowing your networks in real-time, all the time.