Tony Sager
March 28, 2013

The Critical Security Controls: The Foundation For An Enterprise Risk Management Framework

The Top 20 Critical Security Controls (http://www.sans.org/critical-security-controls/) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive attacks. They were developed and are maintained by a consortium of hundreds of security experts from across the public and private sectors. An underlying theme of the Controls is support for large-scale, standards-based security automation for the management of cyber defenses.

By themselves, the Critical Security Controls have no official standing. So how can an informal, grass-roots movement like the Critical Security Controls be a complement to the comprehensive, formal enterprise Risk Management Framework published by NIST? The US Government's Risk Management Framework is defined by NIST publication SP 800-37, which specifies a risk management process for all federal information systems.[1] There are a series of additional documents that complement SP 800-37. For example, NIST SP 800-53 is the "catalog" from where controls are selected as part of the risk management process. NIST SP 800-53A describes how the controls are assessed, or verified to meet the organization's security objectives in the context of the Risk Management Framework.

The actions defined by the Critical Security Controls are demonstrably a subset of the comprehensive catalog defined by NIST SP 800-53. The Critical Security Controls do not attempt to replace the NIST comprehensive Risk Management Framework. The Critical Security Controls instead prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Critical Security Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action.

The Critical Security Controls (CSC) process takes a community- approach based (as opposed to specific enterprise-based) to the notion of a risk assessment. Instead of starting from the viewpoint of a specific enterprise (e.g., an agency or a facility), the CSC process was created using a consensus risk assessment process. This consensus risk assessment integrates the judgment of a large group of experts from government, industry, and academia regarding the common and pervasive threats and vulnerabilities that are typically found in large enterprises.

[1] The word "control" in the Critical Security Controls is used differently than in the NIST Framework. One of the Top 20 Critical Security Controls is more like a "control category", mapping to one or more of the controls in NIST SP 800-53.

This collective, or community, assessment of risk followed by a choice of action is not the ultimate or final answer to the cybersecurity problem for an enterprise. It might be more accurate to refer to the Critical Security Controls instead as a "foundational risk assessment" – one that can be used by an individual enterprise as a starting point for immediate, high-value action, and can also provide a basis for common action across an entire community. This foundational risk assessment can be augmented by implementation of the NIST Risk Management Framework as enterprises make progress on implementing the foundational controls that comprise the Critical Security Controls.

Why does the notion of a "foundational risk assessment" make sense?

We now live in a world where: everyone is using the same technology (with its associated vulnerabilities); the network is shared by Good Guys and Bad Guys alike; we are all engaged in complex interlocking business relationships that are reflected in commonly-used information technologies; and the threats are rapidly shifting (today you are the possible jump point or botnet node, tomorrow you might be the target). This common problem implies common action, at least a common starting point for all cyber defense implementations and as the expected baseline behavior for all organizations. This idea is consistent with the NIST-defined, Enterprise-centric approach, and in fact could be seen as a natural application of that Risk Management Framework to a community or critical sector level.[2]

Many of today's government and private sector enterprises simply do not have the access to the information, expertise, or time that would allow them to independently work through a meaningful risk management process following the NIST guidelines. A community approach gives every enterprise access to recommendations by some of the best minds in the business. An enterprise can use the Critical Security Controls to rapidly define the starting point for their defenses, direct their scarce resources on actions with immediate and high-value payoff, and then focus their attention and resources on additional risk issues that are unique to their business or mission. In fact, for many "low risk" organizations, this "foundational risk assessment" could prove to be adequate based on the specific risks they face.

Implementation of the Critical Security Controls can also play an additional role in managing dynamic risks in an enterprise. Assessment of risk for today's complex computing and network environments must be a continuous cycle of activity, not "events" that occur every 3 years. New information (e.g., threats, system vulnerabilities, sensitive data) affecting an enterprise's risk constantly enters the environment. Concepts like "Continuous Monitoring" have become the way that we describe and think about security management. But what should we be monitoring?

[2] Several industry groups have already mapped the Critical Security Controls against existing regulatory/compliance schemes of specific critical sectors of the economy (e.g., telecomm, power generation, Industrial Control Systems), and have found that the CSCs map very well to, and provide a specific, high-priority subset of existing formal requirements.

The Critical Security Controls provide a focus on the most important actions to be monitored because many of the controls include a primary emphasis on automation and continuous assessment. As such, their implementation provides a natural "lens" through which to focus the challenge of Continuous Monitoring. In short, a subset of the Critical Security Controls is a natural candidate to be the basis for the ongoing measurement, remediation, and reporting that Continuous Monitoring is intended to provide. This is the approach recently adopted by DHS, in particular for four sub-controls of the Critical Security Controls (which also map to the "Top 4" Mitigations identified by the Australian Defence Signals Directorate). DHS is now putting into place the contract vehicles for government agencies to acquire technology that would allow implementation of Continuous Monitoring across all US government agencies. They see this as a starting point for FISMA compliance, not a replacement.

In summary, the Critical Security Controls can be a powerful complement to a formal Risk Management Framework by providing a community-vetted "foundational risk assessment" which allows all enterprises to rapidly identify and focus their attention on high-payoff defensive actions, especially when they lack the resources to do so on their own. The CSC also provides a high-value, community-vetted foundation of expected behavior for implementation, management, reciprocity, and auditing or assessment. They can be best seen as a way for an enterprise to move through a first cycle of risk management (as defined by Frameworks like NIST SP 800-37, for example) much more rapidly, and with better information than they could generate on their own.

In an age of constant new information that affects risks, the Critical Security Controls play a vital role by defining the set of things that are worth monitoring continuously – information created by the highest priority defensive actions. They can be foundational for any effort at a cybersecurity framework.