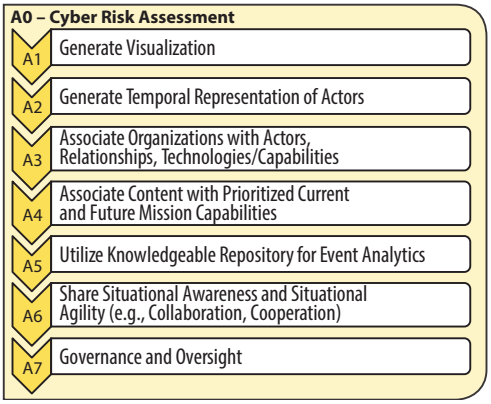
IDA | Research Insights

August 2016

Cyber Risk Response Framework*

Laura Odell, Institute for Defense Analyses (lodell@ida.org)

The Department of Defense is increasingly concerned that the loss of sensitive data to our adversaries is eroding our competitive advantage. This sensitive data includes business proprietary information on key programs of record and infrastructure, including government documents that describe gaps in and limitations of our national assets. This loss of data compromises the effectiveness of our readiness for defense of the nation, and it minimizes the investments we have made to build advantages into our offensive and defensive capabilities.



In lieu of a compliance-based cybersecurity model focused on the state of networks, malware, and patching, a risk-based cybersecurity decision model that enables a predictive capability to respond to impending cyber-attacks is needed. Operationalizing analysis of data, information, and intelligence from disparate sources across multiple service sectors to provide a common operating picture and decision framework must begin now. The framework below provides context and a common understanding for cyber decision-making to help Federal and State leaders operationalize intelligence and information:

1. **Generate visualization** – Geospatial representation is important to consider when dealing with actors—but it can be misleading. Hackers for hire and other third-party actors may be state-sponsored and not physically located at the origination point of the attack. Although the association of location to content may be manipulated, every actor has signatures that machines can identify.
2. **Generate temporal representation of actors** – In cyberspace, time is both relevant and irrelevant. It is irrelevant because incidents only occur when there is a congruence of sufficient intent and capability (Bash was a vulnerability for over 20 years but only became relevant when hackers sought to exploit it). However, domestic and international triggers/hooks (lifting sanctions puts more funding into play to hire third-party actors to commit cyber-attacks) may be an indicator (forcing function) in predicting an attack. The ability to anticipate/control the progression of events to maximize the opportunity to observe the adversary and know the time when they are most prepared to act is critical.
3. **Associate Organizations with Actors, Relationships, Technologies/Capabilities** – Not all cyber risk is high-impact. Intent and capabilities put these in the context of a wider knowledge of actors and relationships (i.e., nation–states, corporate states, and criminal organizations) to improve insight into the threat.
4. **Associate Content with Prioritized and Future Mission Capabilities** – National assets should be prioritized based on their potential impact on our nation. Responses to threats or data losses should be weighed in the context of their importance to the overall mission outcome.
5. **Utilize Knowledgebase Repository for Event Analytics** – Federal and State governments should expand their sources of information to include international actors, non-state actors, event histories, social media, and episodic behaviors. These sources could assist in contextualizing and filling gaps in knowledge. The United States should begin to leverage non-traditional data sources to better protect and defend against cyber intrusions and attacks.
6. **Share Situational Awareness and Situational Agility** – Awareness is important, but alone, it is not enough. The accelerated nature of many cyber-attacks requires a readiness to act and commitment to a rapid response with already established trusted systems and communities of interest.
7. **Governance and Oversight** – As Federal and State governments seek to develop and expand automated courses of actions and thresholds, the global community is a key resource in developing a better understanding of the cyber risk.

NS D-8148

* Based on IDA NS D-8094, *Data to Decisions—Terminate, Tolerate, Transfer, or Treat*, July 2016.

Research sponsored by the Office of the Secretary of Defense, Chief Information Officer.