TOLMAN & WIKER INSURANCE SERVICES, LLC
INNOVATIVE RISK ADVICE SINCE 1923™
VENTURA | LOS ANGELES | SALINAS | SANTA MARIA | BAKERSFIELD

Feds Publish Guidelines for Cybersecurity Framework

February, 2014

Property Casualty 360

One year after the White House directed the development of cyber standards by executive order, the National Institute of Standards and Technology (NIST) last week released voluntary industry standards and best practices to prevent cyber attacks in its publication "Framework for Improving Critical Infrastructure Cybersecurity."

In a statement, President Barack Obama says "Cyber threats pose one of the gravest national security dangers that the United States faces." He calls the Framework a turning point, but also notes that there is still work to be done against cyber threats.

NIST also released a Roadmap for future versions of the framework, which details cybersecurity development, alignment and collaboration.

The Framework was created through collaboration between the government and private sector. The government notes that the Framework should be used to complement an organization's risk management and cybersecurity program.

The government says that these guidelines are ideal for the country's critical infrastructure, which includes the energy grid and financial sector, but any organization—located within or outside the United States—may use the guidelines to strengthen cybersecurity efforts.

It is divided into three components: core, tiers and profiles.

The **core** provides a set of activities that achieve specific cybersecurity outcomes. The five functions can be performed concurrently to address risk.

1. **Identify**: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. Outcomes include asset management; business environment; governance; risk assessment; and risk management strategy.
2. **Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Outcomes include access control; awareness and training; data security; information protection processes and procedures; maintenance; and protective technology.
3. **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. Outcomes include: anomalies and events; security continuous monitoring; and detection processes.
4. **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Outcomes include recovery planning, improvements and communications.

The **tiers** provide context on how an organization views cybersecurity risk and the processes in place to manage risk.

1. **Partial:** Cybersecurity risk management practices are not formalized.
2. **Risk Informed:** Risk management practices are approved by management but may not be established as company policy. Cybersecurity priorities are determined by organizational risk objectives, threat environment or business requirements.
3. **Repeatable:** Risk management practices are formally approved and expressed as policy. Practices are regularly updated based on changing threats and technology.

4. **Adaptive:** The organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.

Profiles align functions, tiers, risk tolerance and resources of the organization. Profiles can be used to state current or meet desired cybersecurity practices.

7 steps to establish or improve a cybersecurity program

1. **Prioritize and Scope**
   Identify business/mission objectives and high-level organizational priorities. Make strategic decisions regarding cybersecurity implementations and determine the scope of systems and assets that support the selected business line or process. Adapt the Framework to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.
2. **Orient**
   Identify related systems and assets, regulatory requirements and overall risk approach. Then identify threats to, and vulnerabilities of, those systems and assets.
3. **Create a Current Profile**
   Develop a current profile by indicating which outcomes from the framework core are currently being achieved.
4. **Conduct a Risk Assessment**
   This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.
5. **Create a Target Profile**
   Create a target profile that corresponds to desired cybersecurity outcomes. Consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a target profile.
6. **Determine, Analyze and Prioritize Gaps**
   Compare the current and target profiles. Create a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis and understanding of risk to achieve the outcomes in the target profile.
7. **Implement Action Plan**
   Determine which actions to take in regards to the gaps, if any, identified in the previous step. Monitor current cybersecurity practices against the target profile.

Return to Article Index

Forward this article to a colleague

Address To | Recipient Name

Subject

Message

Send | Reset