Highlights from a recent Webcast on Security Strategy

SECURITY STRATEGY DEPENDS ON RISK-MANAGEMENT

NASA expert explains the steps to formulating a strong information security strategy.

RISK FRAMING TO INFORM DECISIONS

Risk framing is an essential aspect of formulating a security strategy. It establishes the boundary and scope of the environment in which risk-based decisions are made. "We need to make risk-based decisions: What do I protect first? Where am I most vulnerable?" says Willie Crenshaw, service executive for governance, risk and compliance at NASA.

A risk framing strategy must also define how to govern the agency's risk assessment, risk response and real-time risk monitoring. Agencies must have:

- Risk assumptions regarding threats, vulnerabilities, consequences, impact and likelihood of occurrence.
- Risk constraints regarding risk response and/or monitoring.
- Risk tolerance, meaning the degree of acceptable risk uncertainty.
- Prioritization and tradeoffs, because inevitably a control added to a given environment may take it down.

With the record-breaking data breaches of 2015 fresh in everyone's memory, information security remains a top priority for government agencies in the New Year. Until there's some sort of silver bullet available, officials are looking for ways to protect data in any and all locations.

The best starting place is to create a risk-management strategy, says Willie Crenshaw, service executive for governance, risk and compliance at NASA, during a March 17, 2015, Webcast entitled "Risk Management: Getting Ahead of the Cyber Crisis."

"The risks continually increase as the landscape for cyber and cyberattacks increases," says Crenshaw. "One of the first things that we look at as far as an overall risk strategy is risk-management strategy ... What are you going to protect on the network and also to assess and frame and respond?"

Create a Risk-Management Strategy

To create its risk management strategy, NASA adapted the National Institute of Standards and Technology's SP 800-39. This is a guideline for creating an enterprise-wide program for managing information security risks resulting from operating federal information systems. It also covers the four-pronged approach of the evolving risk-management process: frame, assess, respond to and monitor, says Crenshaw.

Risk Framing: Conduct holistic risk management to address risk from the strategic level to the tactical level. "You need to know what are your crown jewels, what's out there in your environment," says Crenshaw. NASA outlines this in three tiers:

- **Tier 1:** information technology security service areas and programs within the agency.
- **Tier 2:** centers, departments and divisions of the agency.
- **Tier 3:** information systems themselves.

This framework is the heart of the risk assessment strategy. Officials need to know what to protect and how to prioritize protection. To better spot vulnerabilities, NASA officials are considering a dashboard that will help everyone involved in security assess

> "Cyber is becoming more of a front for war and also propaganda. You need to be able to have a strong risk-management strategy."
>
> *—Willie Crenshaw, service executive for governance, risk and compliance at NASA*

what's happening in the environment.

"Are we looking at the right things? Are we detecting what's going on?" says Crenshaw. "As we know, the world climate is changing. There are a lot of things going on. We have wars over in other countries. That affects us because now cyber is becoming more of a front for war and also propaganda. You need to be able to have a strong risk-management strategy."

Risk Assessment: At Tier 1, risk assessment takes a holistic agency-level view to identify threats to an organization, internal and external vulnerabilities, the harm or impact a malicious exploit can have, and the likelihood of that happening. At Tier 2, the assessment focuses on those same areas as they relate to departments, centers, offices and programs within the agency. Tier 3 assesses threats specific to information systems.

"Everything may not be a threat to the organization or to the center or the department, but it may be a risk to that individual system," says Crenshaw.

To carry out these assessments, he recommends three things:

- Use existing capabilities and the Homeland Security Department's Continuous Diagnostics and Mitigation program.
- Set policies on how to conduct risk assessments, including defined procedures to ensure standardization throughout the organization.
- Use an organizational dashboard to see not only the data, but who's responsible for accepting and remediating risks to that data.

Risk Response: Risk response refers to the speed at which an organization can maneuver to mitigate risk. Sometimes an intruder can sit on a network for months without being detected. Once detected though, the response must be swift to minimize damage to the environment and your agency's public perception.

The fastest approach is to transfer the risk, which does not mean passing the buck, says Crenshaw. It means moving the risk to less-critical systems, components or organizations. Officials must identify tools, techniques and methodologies as part of their response plan and specify how to evaluate each and how to communicate responses to internal and external stakeholders.

"These tools and these things find a lot of vulnerabilities," says Crenshaw. "So you have to be able to go through and prioritize those vulnerabilities and elevate the proper ones up the chain so they can be remediated."

Risk Monitoring: Besides using CDM, agencies should conduct risk monitoring to verify response measures are in place and security requirements set by the agency, legislation, directives, regulations, policies and standards are met in a thorough fashion.

Monitoring also helps determine the ongoing effectiveness of risk response measures following implementation. It will help when making changes to the three tiers that might affect risk.

A round-the-clock security operations center is a key part of monitoring, says Crenshaw. What's more, agencies should develop metrics to measure risk and identify trends. "If we're going to get in front of the cyber threat, these are some of the things we need to do," he says.

Establish Governance

One more tool in the risk-management box is a well-defined governance structure that meshes with the agency's strategic goals and objectives. At NASA, IT Security Division service areas:

- Maintain the organization's risk-management strategy in accordance with evolving risk and emerging technologies.
- Define risk tolerance from the organization's perspective.
- Develop and execute enterprise-wide investment strategies for information resources and security.

"There are certainly changing things going on, so you have to be flexible in this space and you have to be diligent, if you will, on how you respond to risk, how you monitor, how you assess your systems, because the climate is getting more and more dangerous," says Crenshaw. "Making sure you have a strong risk management program and strategy in place will help minimize some of these attacks or the possibilities of these attacks. At the very least, it will give you a greater education on what's out there."

> "Attacks are one place to look, however knowing what is normal in your organization and monitoring it end-to-end for anomalies is critical for success."
>
> —*Sean Applegate, director of tech strategy and advanced solutions, Riverbed*

Apply the Right Solution

Risk management isn't just a consideration for federal entities operating in Washington, D.C. Many agencies have offices nationwide and overseas, and their data needs to be secure wherever it may reside.

Riverbed, a $1 billion data monitoring and optimization company, focuses on three pillars when it comes to its solutions: visibility, control, and optimization. Riverbed takes an end-to-end look at enterprise architecture and integrates with open application programming interfaces. Like NASA, it has adapted NIST SP 800-39 to create solutions for network planning, configuration management and modeling; network monitoring; application monitoring; and protection and response.

To handle network planning, configuration management and modeling, Riverbed offers NetCollector, a regionally-based solution with several modules. One is NetAduitor, which maps the network; audits configurations and changes; and reports on NIST and DISA STIG compliance, risk and many other factors. It provides daily operational insights and reports for collaborative risk management.

NetPlanner is another component. This handles survivability analysis and threat modeling so users can see how far attacks penetrate into their infrastructure. The final piece is Provisioner, which automates complex change processes at scale so they can be easily planned, approved, logged, deployed and rolled back should they not work. This means the system not only finds where changes are needed, but makes them as well.

Flow and packet-based network `monitoring offers a dashboard for broad situational awareness. Security teams can also drill down into locations or specific sites. A right-click provides access to metrics, alerts or reports on specific systems. Analytics automatically investigate and score events to help prioritize responses. The dashboard can also direct teams exactly where to look for the problem. For example, in a worm attack, this would find the host and everything the worm touched.

The perimeter is not the only vulnerable spot anymore. Teams must also monitor and track applications so officials know how they connect and what they do. Riverbed also provides an applications monitoring dashboard that can dig deeper into the details. By integrating with big data analytics, the solution can drill down into each transaction. If an SQL attack occurs, it can list any SQL transaction that matched the attacker's signature and determine when it came in and what query was made. Perhaps most importantly, a thoroughly instrumented monitoring solution can show you the exact data that was taken.

Riverbed also provides solutions for wide-area network optimization for branch and remote sites. Its solution can deduplicate data, or compress it by removing duplications. This makes it harder to decrypt and analyze in transit. It also optimizes the TCP, which connects the two hosts that exchange data. This helps agencies rapidly move data across constrained wide area networks. For example, agencies can perform disaster recovery four to 10 times faster with optimization. It can also detect events, look for specified Secure Sockets Layer signatures and more than 1,000 applications, and encrypt data at rest and in transit.

Some branches need physical servers onsite, using backup as one protection method. However, that can be less reliable and increases the your exposure to risk due to a high recovery point objective. Riverbed converts physical servers into virtual servers in what the company calls a Zero branch IT. All the information sits in the datacenter, and is projected out to the branch. It feels and acts local, which helps agencies get rid of tape backup, which increases security and decreases costs.

"Use a holistic thought process," says Sean Applegate, director of tech strategy and advanced solutions at Riverbed. "Let's work end-to-end across the tiers, let's look across all of your operations. Attacks are one place to look, but there is a lot of the organization we have to be aware of and [for which] we have to account. Leverage, integrate and automate your information solutions."