Ingredients for Risk Management: People Foremost, Plus Processes and Technology

By John N. Stewart, Vice President and Chief Security Officer, Cisco

Decisions about information security cannot be based on the answer to the question, “Are we secure?”, because the only truthful answer is no. Instead, it is far more relevant to ask, “Are we secure enough within our risk tolerance?” The answer to this question varies from agency to agency, and interestingly enough, from person to person.

What Influences Risk Tolerance?

Risk tolerance is how much risk is acceptable to an organization based on the benefits and consequences of doing or not doing something. In both the public and private sectors, risk tolerance is what the organization requires, the culture allows, and the individual does—although these three factors are not always in harmony. For example, many federal government agencies explicitly forbid cutting and pasting information, copying files onto USB drives, or bringing home laptops. Yet, these can and will occur if the agency culture does not hold individuals accountable when they take these actions.

Risk tolerance is also temporal as it must change with the times. Taking the same risk might be the right decision in some circumstances and wrong in others. Therefore, an agency needs to reevaluate its risk-management policy—to test and retest it—as the people and environment change.

The Triumvirate: People, Processes, and Technology

Effective risk management has three elements: people, processes, and technology. People have the greatest influence in risk management because, depending on their role, they either decide what is at risk, determine the agency’s risk tolerance, or make daily decisions that affect risk, such as whether to copy files onto USB drives or share passwords for expediency’s sake. Accordingly, agencies must embed awareness about the consequences of taking risks throughout the organization—from executives to individual contributors—so that people develop the habit of balancing outcomes against risk as they make daily decisions. This is not to say that people should never take risks. Rather, they need to be held accountable for their risk-taking, whether the outcome is positive or negative.

Processes need to balance risk and productivity. For example, taking a new project through a risk review may well slow it down. However, conducting the review will validate initial thoughts on how risky the project is and contribute to a better decision on whether to undertake it. Additionally, good processes are repeatable, which provides consistency and, therefore, lowers overall risk.

Technology, if used correctly, can aid risk-management decisions by providing objective data. This avoids subjective risk-management practices like those that can occur when an agency understands its vulnerabilities as “everything is a mess,” and begins investing in technology without first establishing priorities. Better decisions result when agencies can make data-driven decisions

about technology investments, based on how important the vulnerability is to the agency's ability to achieve its mission. Cisco® Security Monitoring, Analysis, and Response System (MARS) helps teams make data-driven decisions by identifying specific, active vulnerabilities—including those attributable to lapses in processes that the agency thought were in place, such as regular patching.

The Myth of Delegated Risk Management

A common misperception about risk management is that it can be delegated to a risk-management group. In fact, risk management needs to be an embedded practice at all levels of an organization. For example, all new Cisco employees view a video of Chief Executive Officer John Chambers stressing that information security is everybody's responsibility, and that it is now their responsibility, as well. The message comes from the top. Similarly, all federal government employees need to realize that they take risks every day, generally for the right reasons, and are accountable for their decisions.

Delegated risk management takes another form when something goes wrong, underscoring the importance of knowing the risks that were taken and who decided to take them. When things go right, too often people volunteer to take credit. When things go wrong, risk amnesia can occur, as can the likelihood for blame. Again, agencies can avoid this by holding all individuals accountable for the risks they take.

Action Items

Following are steps federal government agencies can take to develop or strengthen a risk-management strategy:

1. Obtain a commitment to information security from all levels of agency management. Agency managers should communicate the importance of individual risk management to their employees and model the desired behavior.
2. Assign and clarify roles and responsibilities.
3. Create an action plan with a budget. Establish budget priorities based on the consequences of specific vulnerabilities to the agency's mission.
4. Update information-security policies.
5. Develop an agencywide security awareness program, measure its progress, and continually adjust it based on feedback.
6. Develop an information-security incident response team and plan.

Ultimately, security is based on risk tolerance, an individual's actions, and applied technology. Agencies manage risk most effectively when they foster an awareness of risk management in employees, embed security in all of their processes, and regularly review security data to make data-driven decisions about technology investments.

To hear a podcast of John N. Stewart discussing risk management, or interviews with government chief information security officers discussing risk management and other security topics, visit www.federalnewsradio.com/?nid=350

To read case studies on Cisco's internal security practices, visit www.cisco.com/web/about/ciscoitatwork/case_studies/security.html

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-442870-00 11/07