tripwire®
TAKE CONTROL.

EXECUTIVE BRIEF

JOHN P. PIRONTI
CGEIT, CISA, CISM, CISSP, CRISC, ISSAP, ISSMP
PRESIDENT, IP ARCHITECTS, LLC.

DWAYNE MELANCON
CHIEF TECHNOLOGY OFFICER, TRIPWIRE, INC.

FIVE TIPS FOR OUTSMARTING THE INFORMATION AGE ADVERSARY

The concept of "Adapt or Die" has new meaning in the information age. Staying ahead of threats, vulnerabilities and their associated risks is a daunting task in even the best-funded and most mature information risk management and security (IRMS) programs.

As risks increase and become a more critical factor in your business, you need to prepare appropriately to meet the challenges they create. If you don't, you risk becoming a victim of ever evolving, highly motivated, and extremely capable adversaries who vigilantly wait for you to make a mistake before they strike. At the same time, you must meet the expectations and requirements of your Board of Directors, business leaders and key stakeholders.

If the situation described above sounds familiar, these five actions enhance your approach to information risk management and security and help you stay one step ahead of the information age adversary.

1. USE RISK MANAGEMENT TO REMOVE THE FEAR OF SECURITY

Consider the psychology associated with the words "security" and "risk." When a business person thinks of the term "security," words that often first come to their minds are "prevention," "obstacle," and "disempowerment." This reaction is typically based on frustrating past encounters with information security organizations. Unfortunately, these experiences have negatively influenced their perception of the positive impact and capabilities that security can provide.

When the same individual hears the word "risk," typically words like "understanding," "management," "opportunity," and "empowerment" come to mind for them.

Given the potential impact of the language you use, choose words that create a strong connection to risk in your interactions with others. You may find that this approach leads to greater acceptance—in both terminology and approach—than if you focus only on security.

FIVE WAYS TO OUTSMART YOUR ADVERSARY

1. **Use Risk Management to Remove the Fear of Security**
2. **Teach Decision-Makers How to Fish**
3. **Link Metrics and Measures Directly to Business Value or Impact**
4. **Interact and Share Information with a Community of Peers**
5. **Gain Capabilities Without Expanding Your Budget**

2. TEACH DECISION-MAKERS HOW TO FISH

Many business leaders and stakeholders resist or ignore security requirements because they view them as more of a burden than a benefit. By adopting an advisory and consultative approach rather than an authoritative one, you can help these individuals make well-informed, risk-conscious decisions with less resistance. The key is to help them better understand the threats, vulnerabilities, and potential business impacts that they should consider in their decision making process. Most importantly, you should help them recognize how these factors could impact their own success.

By taking this approach, stakeholders will no longer feel as though they are being "forced into" a security requirement. Instead, they will be more supportive of security, since they will now appreciate security's role in supporting their own business requirements, activities and goals.

3. LINK METRICS AND MEASURES DIRECTLY TO BUSINESS VALUE OR IMPACT

A common challenge for CISOs is effectively communicating the value of their activities and services to the Board of Directors, other business leaders and key stakeholders. One of the most effective ways CISOs can overcome this challenge is by developing metrics and measures that are directly linked to business value or impact. These must also be articulated in a way that resonates with other executives.

The best way to identify which metrics, measurements and associated reporting are most valuable to business leaders is through ongoing collaboration with them. Work with them to understand their priorities, what they are being measured against, and how you can help them be more successful. Pay attention to the words they use, and then describe your efforts using terms they recognize as compatible with their own.

Collaborating with key stakeholders ensures that the business will find your work relevant, measurable and actionable. It also provides an opportunity for you to embed security into the day-to-day operations of your company.

4. INTERACT AND SHARE INFORMATION WITH A COMMUNITY OF PEERS

To paraphrase an old saying: "No information risk management and security program is an island." Many other organizations are attempting to—or have already—overcome the same challenges that your organization faces. If you're not doing it already, establish relationships with a community of peers in which you can share information freely and openly. Connecting with the larger community will help you identify industry-leading practices, learn useful methods and insights, and allow for intelligence development and sharing.

You can also benefit from identifying and engaging with a small set of trusted external advisors who are knowledgeable about your industry and have your best interests in mind. This small "advisory team" can help you advance your career more quickly by learning from others who have walked the path before you. The lessons these individuals have learned can also be a great source of best practices for creating an effective IRMS program.

Using both of these approaches can accelerate the maturation of your IRMS program and your personal success. Working with and learning from the experience of others also greatly simplifies problem solving and builds a feeling of camaraderie.

5. GAIN CAPABILITIES WITHOUT EXPANDING YOUR BUDGET

Budget shortfalls and limited funding are always a challenge for IRMS leaders and their programs. One way to overcome these limitations is to "attach" your project to a better-funded program in another group.

We've already discussed the value of continuous collaboration with stakeholders (see "Teach Decision Makers How to Fish," above). This kind of cross-functional collaboration can also help you identify and communicate the value of your project in a way that positions it as vital to the success of the other person's project. When you do that, you can often convince another stakeholder to fund all or some of your project.

An example of this is configuration and system state monitoring, which is often viewed as "something security wants to implement to keep an eye on us." However, savvy IRMS leaders have successfully shown how these projects deliver benefits far beyond security. They've done that by demonstrating how infrastructure and IT Operations functions can benefit from mining configuration and system state data to gain vital insights into availability and performance problems and shorten recovery time from system-impacting events.

By making these benefits clear and connecting them to something that is important to IT Operations, these savvy leaders have been able to secure funding from Operations' budgets. In short, showing how your activities tie into the success of others' initiatives can often help you fund your project without directly bearing the costs or operational overhead.

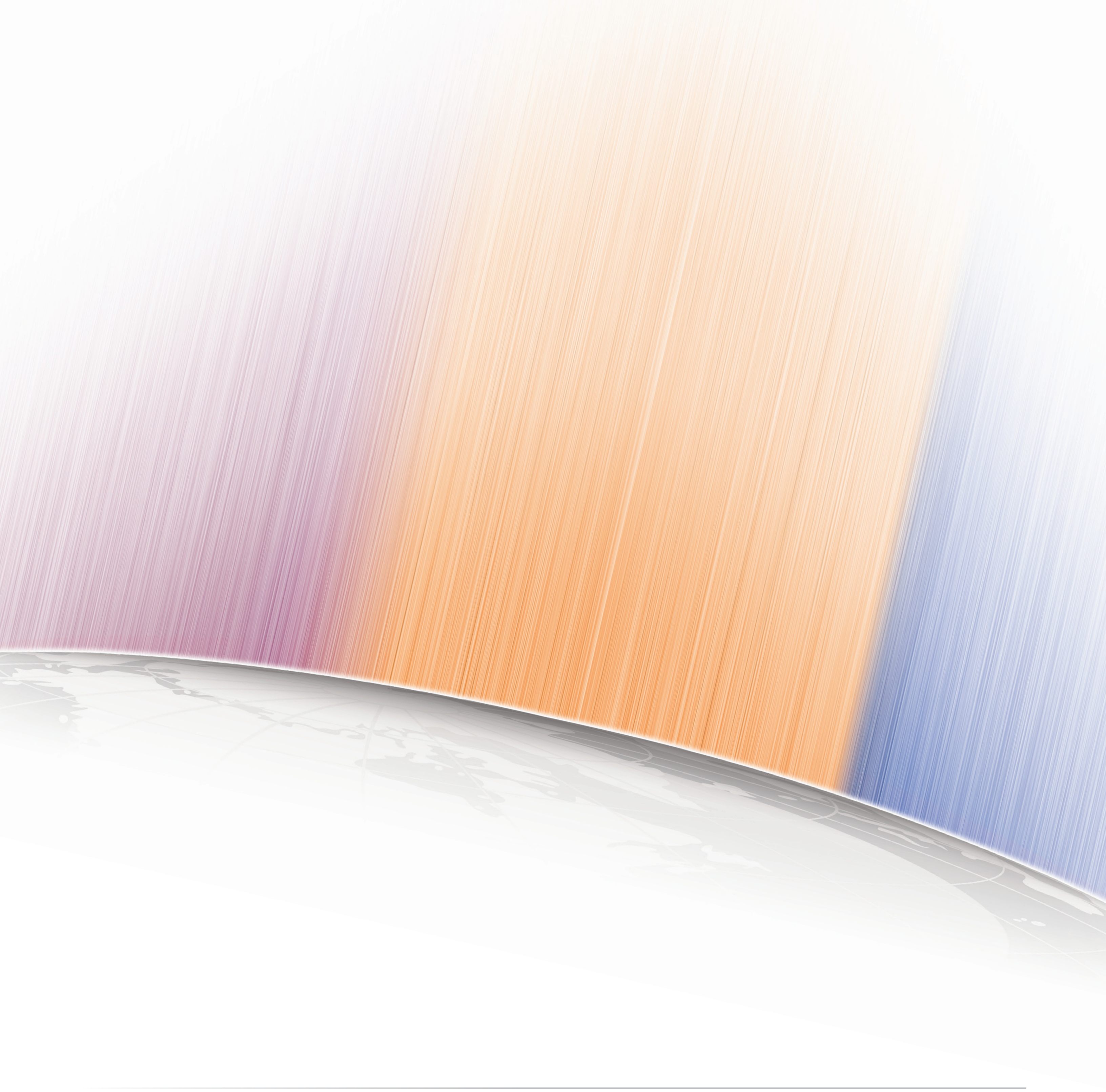
FINAL THOUGHTS

The information age adversary is better equipped and more highly motivated than ever before. He or she also has a much lower barrier to entry than ever before. With automated attack tools, online "cookbooks," and open markets for illicit information no more than a Google search away, these adversaries are becoming harder to fight by the day.

IRMS is now an essential component of many organizations' security strategy, as enterprise risk management emerges as the best way to stand up to these adversaries. The programs, capabilities, and individuals who support IRMS functions and capabilities must evolve beyond simply managing information risk and providing effective security. IRMS leaders must take bold steps to engage with the rest of the business in a way that demonstrates that they provide an essential business advantage. By taking this approach, they will embraced as a valued asset by their organization.

If you try to fight the battle alone, you will be overwhelmed and most likely defeated. In contrast, creating force multipliers in your organizations by adapting a risk-centric approach lets you to fight the battle more effectively, but also offers a greater chance of winning the war. Remember, there's no need to fight this fight alone.

The suggestions offered in this article represent key concepts and capabilities that you can employ immediately to accelerate your IRMS program's evolution and prepare to take on today's adversaries and challenges.



TAKE CONTROL.

.: Tripwire is a leading global provider of IT security and compliance solutions for enterprises, government agencies and service providers who need to protect their sensitive data on critical infrastructure from breaches, vulnerabilities, and threats. Thousands of customers rely on Tripwire's critical security controls like security configuration management, file integrity monitoring, log and event management. The Tripwire® VIA™ platform of integrated controls provides unprecedented visibility and intelligence into business risk while automating complex and manual tasks, enabling organizations to better achieve continuous compliance, mitigate business risk and help ensure operational control. :.

LEARN MORE AT WWW.TRIPWIRE.COM OR FOLLOW US @TRIPWIREINC ON TWITTER.