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 MISTAKES TO AVOID IN RISK MANAGEMENT AND SECURITY

MISTAKES TO AVOID WHEN MANAGING RISK AND SECURITY

1. Focus on Securing Technology Instead of Business Processes and Data
2. Develop Metrics and Measures Without Thresholds and Actions
3. Use the Word "Risk" When You Actually Mean "Threat" or "Vulnerability"
4. Trust, but Fail to Verify
5. Fear the Auditor More than the Attacker

Taking advantage of the lessons learned by others can help you succeed by repeating what worked and avoiding what didn't. Information Risk Management and Security (IRMS) is a rapidly evolving capability and concept within many organizations. The pace in which organizations are implementing these capabilities and programs creates the opportunity for even the most seasoned CISOs to make mistakes as they try to meet the expectations of their leadership and stakeholders. Learn about five of the most common key IRMS mistakes that you should avoid.

1. FOCUS ON SECURING TECHNOLOGY INSTEAD OF BUSINESS PROCESSES AND DATA

Information security professionals often focus on protecting technology instead of the business processes and data that it supports. Why? Because it is easier. Technology is only a vessel with limited value (the cost of acquisition and implementation) until it's leveraged in a business process and/or has data introduced to it.

By focusing on business processes and data first, you can ensure appropriate risk and security considerations are in place no matter what technology it interacts with. Putting the emphasis on business processes and data also encourages cross-functional understanding—and in some cases, buy-in—which increases the likelihood you'll succeed in your mission.

2. DEVELOP METRICS AND MEASURES WITHOUT THRESHOLDS AND ACTIONS

CISOs are finally getting their wish that IRMS is treated as a business function instead of an information technology specialty. However CISOs need to be careful about what they wish for because they now have the same reporting requirements and scrutiny as other business functions.

Many CISOs are actively and aggressively implementing comprehensive metrics and measurement capabilities in an effort to regularly demonstrate the value of their programs and capabilities to their organizations. To be effective, these metrics need to have thresholds (both positive and negative) associated with them. This helps ensure that the intended audience has context about the information they are being provided so that they can interpret it appropriately.

It is also important to execute predefined, agreed upon, and clearly understood actions when a metric crosses a threshold. These actions can range from something as simple as an informational notification to the asset or business process owner, or as complex as incident response or incident escalation.

3. USE THE WORD "RISK" WHEN YOU ACTUALLY MEAN "THREAT" OR "VULNERABILITY"

Information security professionals often abuse and incorrectly use the word "risk" in their analysis and communications. They assume that they can evaluate the information risks to an organization based on their visibility into business activities. In many cases their visibility is actually limited to technology and infrastructure considerations. It frequently fails to include business insights such as business strategy and direction, enterprise risk or financial information. Often security professionals use the word "risk" when they actually mean to say "threat" or "vulnerability."

Risk management within your organization should use these data points as a key component in their enterprise risk assessments and calculations. This can help them determine the actual overall risk associated and business impact to your organization if they were realized, but not misrepresent them as a risk indicator.

4. TRUST, BUT FAIL TO VERIFY

It is hard to believe that your employees may not have your best interests in mind. Many organizations are unwilling to accept the possibility that trusted employees with privileged access to sensitive systems could be intentionally stealing data or carrying out malicious activities.

Without following a "Trust but Verify" philosophy and approach to monitor the activities of these users, you may not realize a problematic situation exists until you realize a material business impact. By using this method, trusted employees with privileged access to sensitive assets and systems can be assured that they will not be wrongfully or accidentally accused of inappropriate activities or actions. At the same time you, as a company executive, can take comfort in knowing that you have implemented effective controls to assist in mitigating the risk and impact of insider attacks.

TRUST WITHOUT VERIFICATION

In a well-publicized 2009 incident, a large, US mortgage company was the victim of a "logic bomb," malicious code placed by a disgruntled employee. According to the Wall Street Journal[1],

The bomb would have "detonated" on Jan. 31. It was programmed to disable access to the server on which it was running, block any network monitoring software, systematically and irretrievably erase everything—and then replicate itself on all 4,000 Fannie Mae servers. Luckily—and it does seem it was pure luck—another programmer discovered the script a week later, and disabled it.

Had this gone unnoticed, the company would have suffered huge negative impacts financially and to its reputation. In this case, the logic bomb was discovered before it caused any damage. Things could have been far worse.

As the old saying goes, "Trust is not a control." Ensure that you invest in processes and technologies that help you monitor and validate what your trusted employees are doing, particularly if they have elevated privileges within your applications and infrastructure.

5. FEAR THE AUDITOR MORE THAN THE ATTACKER

Compliance has been the driving force of many IRMS activities. In many cases, organizations and security professionals alike fear the auditor more then they fear the attacker. The typical reasoning is that the attacker may cause a material business impact if they are successful in their activities, but a failed audit has a known, defined business impact. If you follow a compliance-focused approach you may be forced to focus your efforts on areas that may not effectively mitigate your risks. In fact, some may actually increase your exposure to threats and vulnerabilities. This is due to the lack of focus and attention to key areas and assets that may not be covered by compliance requirements but have significant value and benefit to your organization's business activities. Compliance requirements will always evolve more slowly than the attackers, and should be considered a starting point for risk and security, not the endgame.

FEARING THE AUDITOR MORE THAN THE ATTACKER

.: One very dangerous trend is companies trying to optimize their security strategy to make the auditor happy, and going no further. For example, PCI publishes the "Digital Dozen," which is a list of 12 specific requirements for PCI compliance. Focusing only on these 12 can certainly help you prepare for an audit, but they can lure you into a false sense of safety. This could cause you to neglect security in other areas.

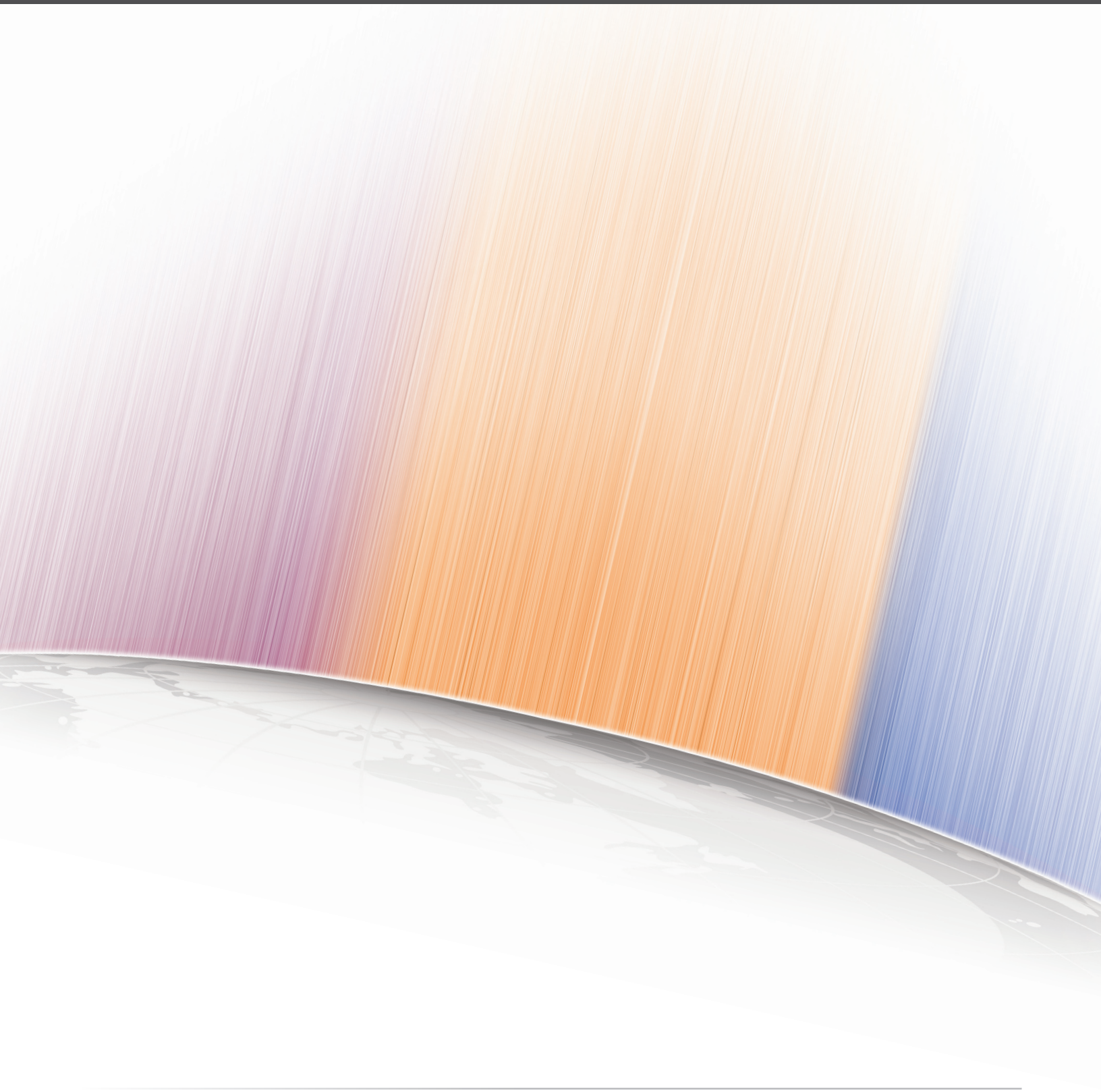
Compliance short lists are by no means comprehensive, and do not prepare you with well-rounded, adaptive security capabilities. Furthermore, if attackers know you're doing the bare minimum to satisfy your auditors, they know that anything beyond the minimum requirements for compliance is fair game. They'll use this knowledge to compromise your infrastructure and access your precious data. :.

FINAL THOUGHTS

If you are a CISO, you can easily make mistakes that have far reaching and long lasting negative business impacts if you are not careful. Learning from the mistakes of others can help you quickly improve your program and its capabilities—all with much less pain than the "school of hard knocks" approach.

The recognition and understanding of common mistakes that others have made when faced with similar situations can help you be more successful in your IRMS efforts. It will help both you and your program be recognized as a benefit to your organization instead of an obstacle to its success.

1 http://professional.wsj.com/article/SB123447990459779609.html?mod=rss_Technology&mg=reno64-wsj



tripwire®

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.

EBFMIRM1n 201206