IT Risks

Linda Wilbanks, *US Department of Education*
Rick Kuhn, *US National Institute of Standards and Technology*
Wes Chou, *US Department of Defense*

"Risk management" is a common phrase when managing information, used by everyone from the chief information security officer to the programmer to explain how we identify, assess, and prioritize risks. It thus reflects how we manage uncertainty as we attempt to control the probability and effect of unfortunate events. Depending on your IT-related experience and area of work, your view of risks will differ. Perhaps you've experienced a risk-related project failure during development or post release, perhaps someone has stolen personally identifiable information, or perhaps a hardware or software failure resulted in a financial loss. These are some risks we've come to accept, and mitigation strategies are part of our development approaches and everyday work. Most IT professionals would agree that IT is good at identifying and managing the risks—but is this really the case? Or has risk management become simply buzz word for us?

Risk Management

Most organizations acknowledge cybersecurity risks, assuming we're constantly under attack. Some professionals don't think anything sent electronically is secure, so you must accept the risk of exposure for all electronic files—including everything from Facebook posts to the files on your office computer. Consequently, companies work hard to mitigate these risks, and parents tell their kids not to post anything on Facebook they don't want the world (or future employers) to see. This issue of *IT Pro*, however, aims to highlight risk areas that are often overlooked. As IT professionals, we talk about risk management mitigations, write risk management plans, and use these terms in our testing strategies, but we often overlook risks in areas outside of normal project development.

As the IT environment changes, new risks appear— some of which are new variations of old risks. For example, consider the integration of user-owned devices into the organizational environment, known as Bring Your Own Device (BYOD). As with laptops, there's a risk of loss of corporate data on the device, given that many users receive email, including documents, on the device, or use the device to store potentially sensitive information, such as client names and contact data. Also similar to laptop and even desktop devices, users might install risky apps of unknown provenance, or visit websites that install malicious code. The risks are confounded by the fact that, as a user-owned device, the enterprise might have little control over its use.

A less widely discussed new risk is the potential for misuse of built-in webcams in laptops. Software for remote control of webcams has become easily available, and numerous news reports have illustrated the potential for malicious use. While most reported incidents of remote administration tool programs, or RATs, as they are fittingly known, have involved invasions of privacy, the risks to virtually any enterprise should be considered. When it's possible for a remote user to control the microphone and camera on a corporate laptop, risks of unwanted disclosure of sensitive information are obvious, and managers might need to rethink current security practices. We hope that the articles in this issue can help to spur creative thinking for addressing new enterprise risks.

In this Issue

The terms "global software development," knowledge management," "analytics," and "big data" have different meanings in IT but represent new areas and approaches in terms of managing the vast amount of data we're compiling. We must identify, investigate, and mitigated the new risks created by the continual increase in global projects and the challenges presented owing to physical distance and cultural differences. "Managing Knowledge in Global Software Development Projects," by Torgeir Dingsøyr and

Darja Šmite, is a thought-provoking article on these challenges and their risks. In business, it's common for smaller companies to merge into a larger one, or sometimes a larger company will split into multiple companies. When these changes occur, the focus is how this affects the personnel, customers, and assets. In particular, "information" is an important asset to consider, along with hardware and software. How can a merger exploit IT to merge different systems, programs, and projects into a single system? The change presents a unique set of risks that, if not mitigated, could affect the success of the merger and of the new company. In "Managing Risks: Post-Merger Integration of Information Systems," Maria Alaranta and Lars Mathiassen discusses these risk areas, which aren't often investigated within IT.

The final article addresses something rarely considered a risk—IT professionals. Over the course of IT's growth and expansion, personnel have honed skills in new technical areas to meet various requirements. These new professional areas are often ad-hoc, with no defined skill set or professional qualifications. In "Architecting a Profession," Charlene Chuck Walrad, Mark Lane, Jeffrey Wallk, and Donald V. Hirst discuss the development of the IT professional enterprise architecture. However, the model they describe could be leveraged to minimize risks in new technical focus areas.

Risks are in every aspect of IT and must continually be identified and mitigated. As new applications of IT are developed, we must recognize and address the associated risks. As IT professionals, we can't become complacent toward risks, or we'll fail.

Acknowledgment

Certain products may be identified in this document, but such identification doesn't imply recommendation by the US National Institute of Standards and Technology or other agencies of the US Government, nor does it imply that the products identified are necessarily the best available for the purpose.

Linda Wilbanks *is the Chief Information Security Officer for Federal Student Aid, Department of Education. Contact her at linda.wilbanks@ed.gov.*
Rick Kuhn *is a computer scientist at the US National Institute of Standards and Technology. Contact him at kuhn@nist.gov.*
Wes Chou *is an Infrastructure Division Chief at the US Department of Defense. Contact him at wes_chou@yahoo.com.*