



Guru Interview: Richard Hunter & George Westerman

Are you exposing your business to IT risk and leaving profit opportunities on the table? You might be if you are managing your IT risk using more traditional approaches. Find out more in this interview with Richard Hunter & George Westerman.

Interview by Alistair Craven

Richard Hunter is Vice President and Research Director in Gartner Executive Programs (EXP), where his recent work has focused on information security, managing external business relationships and risk management.

Mr. Hunter is the author of the acclaimed book *World Without Secrets*, published in 2002, and he is in much demand as a speaker and advisor on issues of security and privacy. Mr. Hunter was appointed Vice President and Director of Research for Applications Development in 1998 and was also a Research Director in GartnerG2. He joined Gartner as a Research Director in the Applications Development and Management service.

George Westerman is a Research Scientist at the MIT Sloan School's Center for Information Systems Research. He studies two aspects of managing technology, namely risk and organizational change.

He is currently examining ways to identify and shape the enterprise's IT risk profile. This research, which combines quantitative survey findings with deep insights from a dozen case studies, identifies the drivers of IT risk and effective risk management practices.

Prior to earning his Doctorate at Harvard Business School, George gained over 12 years of experience in engineering and IT management. He regularly works with executives in a number of sectors, including financial services, technology, retail, and government.

According to Hunter & Westerman's new book *IT Risk: Turning Business Threats Into Competitive Advantage*, traditionally, managers have grouped technology risk and funding into silos. The authors set out to provide a new model for integrated risk management, which identifies three core areas you can develop to eliminate the problems that silo strategies create. The authors also offer specific ways to make the most of your newfound advantage.

You note that although IT is increasingly recognized as central to business success, many enterprises have failed to adjust their processes for IT decision making and risk management. Why is this so?

Hunter & Westerman:

We said that IT is increasingly central to business success, not that it was generally recognized as such. Management recognition of the importance of well-managed IT is less widespread than recognition of the importance of well-managed sales or marketing (for example). (Can you imagine anyone publishing an article in *Harvard Business Review* titled “Sales Doesn’t Matter”?) Besides that, many management teams have not realized that failure of their IT can have immediate and deadly consequences for the business. Nor have they realized that the limitations of their IT create important constraints on the business’s agility.

We believe that part of the reason they have not adjusted their processes is that they have not fully come to understand how important IT really has become to their businesses. We’re no longer in the days of the back-office mainframe. As firms have introduced each new innovation – from desktop PCs to business process reengineering to electronic commerce to integrated global supply chains – they have integrated IT more tightly into their core business processes. But they often still try to manage IT as something they can delegate to an IT unit. If the highly-publicized negative incidents, and the resulting regulatory responses, of the past few years have done anything, they’ve helped everyone wake up to the importance of IT in their enterprises, and to realize the need to start changing their IT decision-making and risk management processes.

In researching the book, what were some of your most surprising findings of all with regard to IT risk management?

Hunter & Westerman:

One very interesting finding is that notwithstanding the enormous attention devoted to security breaches in the popular and business press, the most important investments management can make in controlling IT risk – and the ones that pay off fastest in real dollars – are associated with the “foundation” of infrastructure, applications, and IT processes.

A second important finding is that controlling IT risks effectively requires strength in three disciplines: risk aware culture, risk governance process, and foundation. Most companies focus on one of these, but every company must achieve competency in all three.

A third important finding is that it is vulnerabilities, not threats, that create runaway risk situations. This is really good news, because an enterprise can’t control threats, but it has plenty of control over vulnerabilities.

What is probably our most important finding is that risk management doesn’t have to be just about paying money to make bad surprises go away. If we build risk management into everything we do with IT, risk management becomes a real source of value for the firm, in terms of both efficiency and agility. That’s why we named our book “...from business threats to competitive advantage.”

You highlight agility as one of four main types of IT risk. Can you elaborate?

Hunter & Westerman:

Agility is the ability of the enterprise to change course with controlled speed, risk, cost, and schedule. We show that IT decisions optimized for short-term gains often produce complex, poorly understood IT foundations that ultimately reduce the enterprise’s strategic options. In one of the cases we cite, that of Tektronix, a complex, poorly documented IT foundation actually balked the planned spin-off of a division.

Agility is an important requirement for firms in today’s dynamic competitive environments. What’s really interesting for us, though, is that doing the basics of risk management – fixing the foundation, building core risk disciplines – can actually eliminate many of the barriers to agility in firms. What’s usually seen as a negative cost of doing business – risk management – can actually provide positive upside for the firm.

In dealing with IT risk you suggest implementing a “risk register”. Can you tell us about this?

Hunter & Westerman:

A risk register is a document that records risk names, descriptions, and estimated importance, along with the enterprise’s plans for dealing with the risk (by ignoring it, mitigating it, transferring it, etc.). Our data shows that maintaining a risk register, even in very simple tools such as a spreadsheet or word processing document, improves the effectiveness of risk management.

According to the book, the “Foundation Discipline” is the most cost-effective way to reduce IT risk. Can you summarize the Foundation Discipline for us?

Hunter & Westerman:

The Foundation Discipline is about the enterprise’s technology infrastructure,

applications, and technology management practices. Our research shows that weaknesses in the foundation – such as excessive and undocumented infrastructure and application complexity, poorly maintained devices and software, and sloppy IT organizational practices – create myriad vulnerabilities that can lead to runaway IT risk. Our research also shows that attacking infrastructure complexity in particular produces rapid and substantial reductions in ongoing operating costs – as much as 15-20 per cent of annual IT budget.

“...it is vulnerabilities, not threats, that create runaway risk situations. This is really good news, because an enterprise can’t control threats, but it has plenty of control over vulnerabilities.”

We recommend a clear, staged, improvement path to fixing the foundation. Start by fixing the holes in the foundation, including conducting IT audits and fully implementing business continuity management. Then start improving and simplifying by starting with infrastructure and then moving to applications.

Many of your suggestions require buy-in from the very top of an organization. What are the best ways in which companies can go about instilling an IT-focused culture?

Hunter & Westerman:

First of all, we’re not talking about an “IT-focused culture” – we’re talking about a “risk aware culture,” meaning a culture in which open conversations about risk are the norm. The best way for executives to create such a culture is to make it clear, in word and especially in deed, that employees who raise issues related to risk get immediate help, and to make it clear that hiding one’s risks – such as by overbudgeting for ‘contingencies’ or by trying to play hero – is no longer an acceptable practice.

Are there any tell-tale early warning signs managers can look out for to indicate problems with an IT project?

Hunter & Westerman:

The most important warning signs occur even before the project is chartered and resourced. If an effective business sponsor (meaning an executive with a personal stake in the success of

the project and the necessary authority to command all resources necessary to success) can’t be identified; if a capable project manager with a history of success on similar projects is unavailable; if a convincing business case does not exist; and if business as well as IT resources are not available, then the project is already much more than halfway down the road to failure.

Then, during the course of a project, if requirements keep changing, if team members keep changing, or if key experts such as business process owners don’t find the time to play their role, somebody should start getting worried about the progress of the project.

Stories abound of companies stung by being persuaded into investing in the wrong kinds of applications and systems. What advice would you give to those in this predicament?

Hunter & Westerman:

I would advise companies to ask specifically what business capabilities and business performance improvements will be enabled by the investment. In other words, I would advise companies to make sure that a convincing business case for the investment is present, and that an effective sponsor is on board.

Too many business cases focus on the potential return, and avoid considering risk. The business cases should consider both project delivery risk – how likely is it that this project will actually deliver the value it promises – and operation risk – what will this project do to the risk profile of the firm? Buying a non-standard, standalone package may pay off for a specific measure in the short term, but if it means we need a new set of support skills, or if it increases risks by creating complexity, it may not be worth it. The business case should look at the whole elephant.

What are the main components of an effective business continuity plan?

Hunter & Westerman:

1. Understand IT assets and availability risks

- Conduct a business impact analysis, and use it to prioritize spending on the most critical business processes.
- Develop an inventory of IT and business assets, and link the inventory to business processes

2. Create a plan

- Build an incident management plan, team and process. Document preferred

communication channels and methods in the incident response plan.

- Establish a service-level classification and testing scheme (e.g. gold-, silver-, and bronze-level service) for availability and business continuity.
- Develop contingency plans for expanded scenarios, such as regional events, and plans to mitigate the risks of external events.

3. Implement and test the plan

- Build business continuity into the business and IT project life cycles to ensure recovery of people, technology, facilities, and business processes.
- Define standard and repeatable development, infrastructure, and operations architectures to meet the required service levels.
- Create an employee notification system for large events, and train employees.
- Test at least annually. If comprehensive testing is not practical, perform walk-through testing, and ensure that external dependencies are addressed.

Source: Gartner. Inc. research.

You suggest giving every employee in an organization appropriate awareness of the risks, vulnerabilities and policies that matter most to them. Can you give us an example of how this might be done in practice?

Hunter & Westerman:

Here's a recent example. A major defence contractor is experiencing a wave of targeted e-mails that reference company projects and personnel, and ask the intended victim click on a hyperlink that takes the victim to a website where the victim's machine is infected with malicious code. Such attacks can't be thwarted unless employees know about them, and know not to click on the hyperlink. One way to do this is to send out e-mails or other communications informing employees of the threat, but employees get lots of e-mails, and such warnings may not be read or thoroughly understood. Another way to do it is for the IT team to send out e-mails of their own containing hyperlinks that, when clicked, pop up a big message telling the employee that he or she has been scammed. No employee will forget that message.

In more general terms, management teams should engage employees at all levels in frequent

discussions of risk. This includes formal risk planning exercises, which our research says are most effective when they're conducted at least four times a year. It also includes frequent reviews of initiatives or projects that are considered high risk.

The risk awareness that is often toughest to provide is at the more senior levels of the firm – awareness of how managers' decisions and decision processes affect the risks facing the firm. IT people can improve this kind of awareness in formal governance meetings, but also through frequent gentle reminders during their conversations with business counterparts and each other.

Are there any closing comments you wish to make?

Hunter & Westerman:

IT risk is now too important to be delegated to IT management. In a large business, there are typically 50-75 enterprise-level risks, and 5-10 of those are likely to be IT risks. Business executives must take responsibility for overseeing the management of IT risk, just as they oversee the management of credit risk, market risk, and other enterprise-level risks. This means that IT risks must be managed according to their business consequences.

It is the duty of both IT and business executives to make sure that the business consequences of IT risks are discussed and understood, and that appropriate actions are taken to deal with those risks. Our book offers proven advice on how to do that. □

December 2007.