e-BUSINESS
ADVISOR® MAGAZINE

ADVISOR® INTERVIEW™

Tom Talleur

Cybercrime expert Talleur advocates "safe hex" when it comes to e-business security.

By Heather Leed, Managing Editor

Tom Talleur is a managing director in KPMG's Forensic & Litigation Services Practice and the U.S. practice leader for cyber forensic matters. He completed a 31-year federal civil service career in December 1999. Twenty-nine years of this service were as a federal law enforcement officer. He has extensive executive, law enforcement, intelligence community, and public policy-making experience and expertise in cyber, advanced technology crime and exploitation, and national infrastructure defense matters. Tom is a graduate of the U.S. Naval War College, Newport, Rhode Island, and the Federal Executive Institute, Charlottesville, Virginia. He's a seized computer evidence recovery specialist, certified fraud examiner, and a UNIX and network security specialist. He's the recipient of awards from President's Council for Integrity and Efficiency, and from the Attorney General for his work in the computer crime field.

Advisor: Tell me a little about your job, and what brought you to this position at KPMG's Forensic and Litigation Services Practice.

Talleur: I spent the past 31 years working for the government—the past eight-to-ten years specializing in cybercrime work because there was enough of it to specialize in. My last position was with NASA, where I created and ran the Network and Advanced Technology Crimes Division. When I retired from the government in December 1999, I came to KPMG to open up an anti-cybercrime practice.

A lot of businesses today know that e-commerce equals e-risk, and they understand that they're being exposed in cyberspace, but so much of the activity is on the security side of things, and not so much on the crime and the actual risks involved. I'm providing cyberforensic services to our clients.

What's a good example of a case you might consult on?

If an individual is extorting a company and leaving with their trade secrets, we look into that. If someone has their resources attacked across the Internet, and they lose their resources and intellectual property, we look into that. If there's trademark infringement, trade secret theft, or cybersquatting, we look into that, too. Basically, it's a spin-off of what I did for the government, but applied to the private sector.

Take, for example, the Microsoft case of October 2000. Microsoft lost intellectual property, but by standard property value insurance, they didn't sustain a loss, because their data is still there. This begs the issue of how we define cyberinsurance policies. Companies call me all the time and say they have their network security experts on staff, they do the assessments ... but how do they address problems once something has gone wrong and they have to litigate? What's the digital evidence? How do they deal with that? What are some of the issues once something goes wrong? In cyberspace, the issues are all a bit different.

How are e-business organizations falling short on their security strategies?

I think a lot of them are throwing their servers up and going into business because it's quick and easy and dirty. What they don't realize is that what they reach out for in cyberspace, also reaches back and touches them. This is what leaves many organizations open to risk. The problem is that there's this urgency to get to market that's so heavy, with such a burden, that most people don't think about the risks to come.

I always tell people to practice safe hex in cyberspace. The first major risk is provisioning services without understanding how they can be exploited. That's a basic security risk.

Historically, it takes lawyers two-to-three years to catch up with new litigation opportunities, but once they do, litigation breaks out everywhere. We can see it now in cyberspace litigation trends: Cybersquatters buying and registering domain names and then getting sued under the Federal Trademark Dilution Act; the use of trademarks in file metatags by web site operators to divert customers' traffic to their sites (example: Playboy Enterprises, Inc v. Asia-focus International, Inc.); infringing on copyrights or enabling others to infringe (Napster is the example here); general Web site advertising liability exposure; downstream civil liability (a company's exposure for its point of presence on the Internet being exploited by hackers or inside offenders); and the theft of business methods (taking a brick and mortar patented method and creating a cyber equivalent without the permission of the brick-and-mortar originator, or stealing a cyber business method (e.g., Amazon.com's "one-click" business method patent and its successful suit against Barnes & Noble).

There's just so much cyberlitigation today, through infringement of trademarks and copyrights, and it's a growing pattern. What it suggests to me is that e-commerce businesses are trying to set up and do business faster than they have time to think about what exactly they're getting themselves into.

How do businesses protect themselves? And how do you go about tracking down criminals after an attack?

When an incident occurs, companies must have guidelines in place to respond. These guidelines must have thresholds. If it's just a basic door rattling from outside, or even an inside offender, the organization must have guidelines that dictate what level of threat this is.

The standard blanch reaction is to remediate, put servers back online, and continue to do business because they don't want to lose revenue. This approach isn't always bad, but if a particular intrusion is pretty bad, intellectual property has been stolen, the bad guys now have root access control or trusted access control of that domain. The response has to be not an incident response for remediation, but an incident response for litigation. These response techniques are different.

Companies need to have a first-responder plan in place to preserve the digital evidence. It's so complicated that companies can't usually handle it themselves. They need to decide to give it to their attorneys or someone trained in digital evidence, so they can either defend themselves in litigation or launch litigation against someone for civil action.

What's desired in cybercrime cases is contiguity of offense. If you can have the victim's information on the victim's side of the intrusion—let's say it was a network intrusion—and if you can have any other intermediary materials, like information from ISPs or other conduit points of attack, then you have the evidence of a source point of where the criminal is launching the attack. If it's an insider, it's their machine, but it can just as easily be an offender from, say, Pakistan.

If you have this evidence, then you have a contiguity of offense, and you have a prima facie case to be proved.

This is true for civil or criminal litigation. What companies are lacking is integrated policies where privacy and forensic incident response, coupled with training and awareness, are tied to the core business mission of the company so they know how to respond. If they do have decent response procedures in place where they can identify and do a limited preservation of evidence, then they have what they need to take the criminals to court.

How can these organizations prevent it from happening in the first place?

You can't. You just can't stop cybercrime. There's no magic bullet, no technologies to stop it. None of these killer new applications with encryption are going to stop it.

So it's always about being reactive, rather than proactive?

Well, the proactive piece is if you prepare a front for how to deal with things when they do go wrong, your reaction is cleaner, better, and timelier. The problem most companies have is that they're putting up their business to make revenue now, to provision their services now, to go to market now without thinking through or understanding how they're at risk. Because they're so focused on getting to market and beating the competition, they're not thinking about the risks involved, and that's the problem.

What advice do you have for new e-commerce businesses, and the established e-businesses?

Setting up and operating an e-business impulsively could head businesses for an appointment with a bad disappointment in terms of cyberspace civil litigation. Doing business in cyberspace means more than opening up a Web site. Owners must consider their liability when relying upon Web site builders, outsourced service providers, and alliance partners, and themselves for content and the operation of these sites. And, if they're the harmed party, they must understand where the digital evidence is and how to get to it to either defend themselves or to launch an action..."

Advisor Interview is designed to share insights, perspectives, opinions, advice, and guidance from industry thought leaders and e-business implementers. Interviews are edited for clarity, length, and organization. While some of the speaking style is altered to be more readable, every effort is taken to preserve the speaker's meaning. Suggestions for candidates? Contact e-Business@Advisor.com.

Article reprinted with permission from **e-Business Advisor Magazine** February 2001, Vol.19, No.2.
Copyright © 2001 **ADVISOR MEDIA, Inc.** All Rights Reserved.
5675 Ruffin Road, San Diego, CA 92123. 858-278-5600, fax 858-278-0300, info@advisor.com, www.advisor.com.