Cutter
IT Journal

The Journal of
Information Technology Management

Vol. 22, No. 4
April 2009

"The growing number of security and privacy incidents — accompanied by an increasing number of fines, penalties, and civil actions — emphasize the need for the information security and privacy areas to work together for effective management enterprise-wide."

— Rebecca Herold,
Guest Editor

The Convergence of Information Security, Privacy, and Compliance

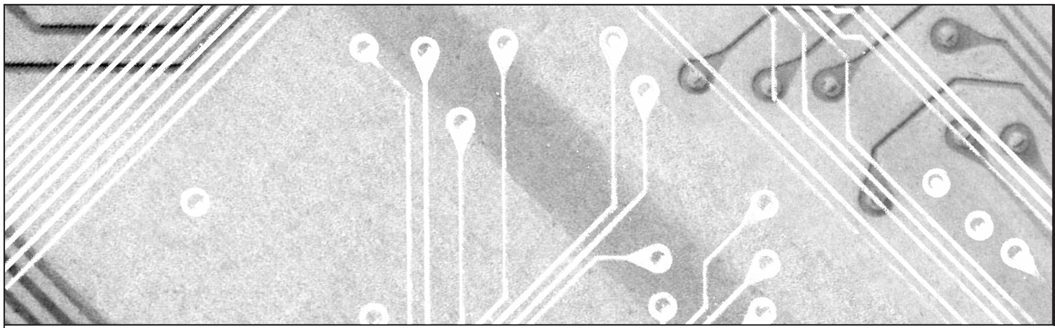
Convergence Is Bad for Business

Too many cooks in the information assurance kitchen spoil the information security and privacy compliance broth. It is more efficient to assign responsibilities to just one area, then let them get on with it!

Convergence Is Better for Business

If separate areas throughout the enterprise work together to address information security and privacy issues, the efforts are more successful and the resulting efficiencies save time, money, and headaches.

CUTTER
CONSORTIUM



Cutter IT Journal

About Cutter IT Journal

Part of Cutter Consortium's mission is to foster the debate of, and dialogue on, the business technology issues challenging enterprises today, to help organizations leverage IT for competitive advantage and business success. Cutter's philosophy is that most of the issues that managers face are complex enough to merit examination that goes beyond simple pronouncements. Founded in 1987 as *American Programmer* by Cutter Fellow Ed Yourdon, *Cutter IT Journal* is one of Cutter's key venues for debate.

The monthly *Cutter IT Journal* and its weekly companion *Cutter IT E-Mail Advisor* offer a variety of perspectives on the issues you're dealing with today. Armed with opinion, data, and advice, you'll be able to make the best decisions, employ the best practices, and choose the right strategies for your organization.

Unlike academic journals, *Cutter IT Journal* doesn't water down or delay its coverage of timely issues with lengthy peer reviews. Each month, our expert Guest Editor delivers articles by internationally known IT practitioners that include case studies, research findings, and experience-based opinion on the IT topics enterprises face today — not issues you were dealing with six months ago, or those that are so esoteric you might not ever need to learn from others' experiences. No other journal brings together so many cutting-edge thinkers or lets them speak so bluntly.

Cutter IT Journal subscribers consider the *Journal* a "consultancy in print" and liken each month's issue to the impassioned debates they participate in at the end of a day at a conference.

Every facet of IT — application integration, security, portfolio management, and testing, to name a few — plays a role in the success or failure of your organization's IT efforts. Only *Cutter IT Journal* and the *Cutter IT E-Mail Advisor* deliver a comprehensive treatment of these critical issues and help you make informed decisions about the strategies that can improve IT's performance.

Cutter IT Journal is unique in that it is written by IT professionals — people like you who face the same challenges and are under the same pressures to get the job done. The *Journal* brings you frank, honest accounts of what works, what doesn't, and why.

Put your IT concerns in a business context. Discover the best ways to pitch new ideas to executive management. Ensure the success of your IT organization in an economy that encourages outsourcing and intense international competition. Avoid the common pitfalls and work smarter while under tighter constraints. You'll learn how to do all this and more when you subscribe to *Cutter IT Journal*.

Cutter IT Journal®

Editor Emeritus: Ed Yourdon
Publisher: Karen Fine Coburn
Group Publisher: Chris Generali
Managing Editor: Karen Pasley
Production Editor: Linda M. Dias
Client Services: service@cutter.com

Cutter IT Journal® (ISSN 1522-7383) is published 12 times a year by Cutter Information LLC, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA (Tel: +1 781 648 8700; Fax: +1 781 648 8707; E-mail: citjeditorial@cutter.com; Web site: www.cutter.com).

Subscription rates are US $485 a year in North America, US $585 elsewhere, payable to Cutter Information LLC. Reprints, bulk purchases, past issues, and multiple subscription and site license rates are available on request.

☐ Start my print subscription to *Cutter IT Journal* ($485/year; US $585 outside North America)

Name ____________________ Title ____________________

Company ____________________ Address ____________________

City ____________________ State/Province ____________________ ZIP/Postal Code ____________________

E-Mail (Be sure to include for weekly *Cutter IT E-Mail Advisor*) ____________________

Fax to +1 781 648 8707, call +1 781 648 8700, or send e-mail to service@cutter.com. Mail to Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA.

SUBSCRIBE TODAY

Request Online License Subscription Rates

For subscription rates for online licenses, contact us at **sales@cutter.com** or **+1 781 648 8700.**

Opening Statement

by Rebecca Herold

There has been much talk recently regarding a convergence of information security and privacy. However, this convergence has actually existed ever since privacy became a concern. After all, privacy requires the implementation of information security controls and appropriate safeguards.

I experienced this relationship firsthand during the early 1990s before the passage of the Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) in the US. At that time, although bills addressing privacy had been considered in the US and around the world, the Organisation for Economic Co-operation and Development (OECD) privacy principles were the basis for most privacy requirements. While establishing the security requirements for one of the very first online banks, I recognized the need for a privacy policy based not simply upon legislation, but also on the need to obtain and maintain customer trust. This policy, based predominantly upon the OECD privacy principles, brought the need for security controls clearly into focus.

Over time, I've identified more than 20 business areas where information security and privacy responsibilities and activities converge, and this number continues to grow as technology, laws, and business evolve. Today enterprises must understand and comply with the multiple requirements of at least 47 US state-level privacy breach notice laws[1] and an increasing number of new US state laws, US federal laws, and international laws. In addition, the growing number of security and privacy incidents — accompanied by an increasing number of fines, penalties, and civil actions — emphasize the need for the information security and privacy areas to work together for effective management enterprise-wide. At the core of compliance for these hundreds of laws and regulations is understanding:

- What constitutes personally identifiable information (PII) within the organization
- Where this PII is collected, stored, and leaves the organization
- That effective safeguards must be established to protect this PII throughout the entire information lifecycle

Privacy is not a strictly legal issue, and information security is certainly not a strictly technical issue; they intersect in many ways. There are compliance responsibilities for both, and while these frequently overlap, they are often handled separately within most organizations. This results in both compliance gaps and conflicting compliance activities, each counterproductive to business in multiple ways. Here are just a few of the issues in which information security and privacy governance converge:

- Clear-text PII on mobile computers and mobile storage devices (e.g., hard drives, backup media, USB drives)
- Disposal of PII on paper as well as digital media
- Employee errors in handling PII
- Entrusting PII to business partners, such as vendors, managed service providers, and other outsourced service companies
- Improper retention and inventory practices for PII

Basically, whenever PII is involved, information security and privacy converge.

So how can companies work effectively to ensure information security, privacy, and compliance areas collaborate to make initiatives most successful? The authors in this issue attempt to answer that question, addressing a wide range of information security and privacy convergence issues in the process. In fact, we had more than 20 folks who offered to write articles on this topic! Because of the overwhelming response, we are going to dedicate two issues — this one and another later in the year — to information security and privacy convergence.

REAL LIFE: STRANGER, AND OFTEN MORE THREAT-FILLED, THAN FICTION

Many information security and privacy practitioners spend a lot of time thinking up hypothetical situations to use within information security and privacy training content and awareness communications. What a waste of valuable time! All you need to do is scan the headlines for a few minutes, and you're sure to find many security and privacy incidents that have occurred throughout the world. What kinds of incidents are you likely to read about? Consider the following:

- **Insider threats.** Personnel and others with access to PII either don't want to take the time to — or don't know they are supposed to — encrypt the PII they load onto mobile devices. When these devices get lost or stolen, the organization's data is at risk.
- **Insider threats.** Personnel who lack sufficient awareness of information security and privacy issues perform activities on behalf of the business for all the right reasons, but end up with all the wrong results, including legal violations.
- **Insider threats.** Personnel and others with access to PII, for any number of reasons, use their company's systems and/or PII in malicious ways. For example, after receiving a bad performance review, a computer network engineer for a consortium of community health clinics retaliated by disabling the systems backups of patient information and deleting patient data on many of the consortium's servers. This not only resulted in financial losses to the consortium and its member clinics, but also caused patient care to suffer.[2]
- **Insider threats.** When personnel lose their jobs, especially during hard economic times, many take trade secrets or employee and customer PII with them in the hope that this valuable information will secure them a new job more quickly or give them something to sell for a profit. According to a survey by IT security data experts Cyber-Ark, more than half of the workers surveyed (in the US, the UK, and the Netherlands) had downloaded competitive corporate data with the intention of using it as a negotiating chip to land their next job. 58% of US workers surveyed had already downloaded business data, including customer PII, to take with them if they lost their jobs.[3]

Oh, and did I happen to mention the threats that insiders pose to the business?

IT'S A LEGAL MATTER, BABY

In the first article in this issue, attorney William Zucker and his colleagues provide four fascinating case studies that cover exactly the types of incidents described above. Whether the organization's sensitive data is imperiled by criminal employees, a careless vendor, or an overly forthcoming Web presence, the result is the same — costly security and privacy breaches that could likely have been prevented. Together, these case studies provide an excellent demonstration of why information security, privacy, and legal areas must collaborate to have a successful program.

PERSONNEL DON'T KNOW WHAT YOU DON'T TELL THEM — DUH!

As I noted above, sometimes information security and privacy breaches are the result of nothing more insidious than a lack of awareness on the part of employees. In our next article, Ilene Switalski Klein tells us how the information security and privacy areas can work together to build security and privacy awareness. Klein provides a step-by-step plan for developing a comprehensive awareness program that, by coordinating its messages, can cut through the "noise" employees hear daily. Partnering on such education efforts not only makes them more effective; it also is more cost-efficient than having each area tackle such activities alone.

CAN YOU MEASURE INFORMATION SECURITY AND PRIVACY? YOU BETCHA!

We've all heard the quote from Wharton professor Morris A. Cohen, "You can't manage what you can't measure." The truth of this adage is demonstrated in our next article, by Nandita Jain Mahajan, chief privacy officer and VP – information security of IBM Daksh. Mahajan discusses how security and privacy professionals can use information security and privacy posture measurements, particularly in the form of dashboards, to help business management understand and take ownership of these vital issues. While Mahajan approaches her topic from a vendor's point of view, her sage advice on incident reporting, remediation, and prevention is sure to be useful for many of our readers.

YOU DON'T KNOW WHAT YOU DON'T KNOW, WHICH IS RISKY

Too many organizations try to establish information security and privacy policies and procedures without first knowing what their risks are, and without talking with business leaders throughout the enterprise. Not knowing your business and its risks and requirements leaves the business open to noncompliance fines, privacy breaches, and information security incidents. Ron Woerner, our next author, walks us through a process he calls "collaborative risk management," in which the information security and privacy areas work together with the business to "identify, assess, and properly respond to risks." He also lists a wealth of resources for you to use in developing your own internal collaborative risk management procedures.

YOU AREN'T IN KANSAS ANYMORE — YOU'RE IN VIRTUAL KANSAS!

As if the real-world problems we've been discussing weren't enough, our final author, Yesha Sivan, tells us about the security and privacy challenges posed by virtual worlds. Chances are you have personnel who are participating in virtual worlds from their work computers, or your company may already be using virtual worlds for collaboration, product design and feedback, product marketing, and/or participation in virtual exhibitions. Sivan surveys the security and privacy risks that virtual worlds present and calls for a systemic approach to "identity" as a means of addressing them. He concludes with a number of tips to help IT "monitor and support [the] enterprise's exploration into virtual worlds."

THE NEED FOR ENTERPRISE COLLABORATION

It is critical to address information security, privacy, and compliance issues in a thoughtful and collaborative manner throughout the entire organization. It is also vital for personnel at all levels to have the knowledge relevant to their jobs so they use information resources securely and in a manner that protects privacy and conforms with law as well as policy. Because people are the weakest link in information security and privacy assurance, collaboration among governance programs — along with providing effective, targeted training coupled with ongoing awareness communications — is key to ensuring successful convergence of information security and privacy responsibilities. I am confident you will find the articles in this issue helpful in improving your business information security and privacy posture.

ENDNOTES

[1] See a listing of the US state-level privacy breach notice laws at www.privacyguidance.com/files/USStateandTerritoriesBreachNotificationLaws032209.pdf.

[2] "News Release." Office of the United States Attorney, Southern District of California, 9 June 2008 (www.usdoj.gov/criminal/cybercrime/osonSent.pdf).

[3] "The Global Recession and its Effect on Work Ethics." Cyber-Ark Software, December 2008.

Rebecca Herold, CISSP, CISA, CISM, FLMI, CIPP, is a Senior Consultant with Cutter Consortium's Enterprise Risk Management & Governance practice and a contributor to that advisory service. She has been an information privacy, security, and compliance consultant, author, and instructor with her own company, Rebecca Herold & Associates, LLC, since 2003. Ms. Herold has more than two decades of privacy and information security experience and has provided information security, privacy, and compliance services to organizations in a wide range of industries throughout the world. In 2008, her blog was named one of the "Top 50 Internet Security Blogs" by the Daily Netizen*. In both 2008 and 2007, Ms. Herold was named one of the "Best Privacy Advisers" as well as "Best Privacy Firm" by* Computerworld*, and in 2007 she was named one of the "Top 59 Influencers in IT Security" by* IT Security*. She is also an adjunct professor for the Norwich University Master of Science in Information Assurance program and the author of 12 books. Ms. Herold can be reached at rherold@cutter.com.*

FOREWARNED IS FOREARMED

Cautionary Tales About Information Security, Privacy, and Compliance: From the Archives of McCarter & English, LLP

by William A. Zucker, with William J. Heller, Scott S. Christie, and John M. McKelway, Jr.

It is a delight for me to be joined in these cautionary tales by three of my colleagues at McCarter & English, LLP. While I, Bill Zucker, have been honored to be one of the few lawyers on Cutter's consultant roster for many years and have heard more than my fair share of lawyer jokes, on this subject we lawyers have the advantage of seeing all the mistakes that clients do not like to admit to the world.

One of the true advantages of being a lawyer is that you can be the best Monday quarterback in the world. Hindsight is always 20/20. Foresight, of course, is the key, and one of the benefits of being an active practitioner in issues of privacy is the accumulation of all of the experiences of one's clients.

This particular article could easily have become a book, as it is simply four real-life tales drawn from many more (with the names changed to protect the guilty), written by four active practitioners in the area of privacy and security at our law firm. We wanted to share with you some of our experiences in the hope that from these cautionary tales, you, like us, will develop good judgment from experience — with the understanding that, unfortunately, experience comes from bad judgment.

1. BEWARE THE GRAVEYARD SHIFT — IT CAN BURY YOU

by William J. Heller

Personally identifiable information (PII) stolen during a graveyard shift proved costly to one major US company, whom we will call Victimco. Victimco is a nationwide company whose outlets are found in almost every airport in the country. Without warning, it started receiving complaints from its customers throughout the country — their credit card numbers and other PII had been stolen. To its credit, Victimco used computer analysis to determine that all of these customers had conducted business with the company's location at one particular airport, and always between the hours of 11 pm to 7 am — the graveyard shift. With that focus, further investigation revealed that several employees assigned to that location and shift were relatively recent hires. With the assistance of the FBI, Victimco learned that its recent hires were connected as part of a gang of conspirators who had targeted Victimco by seeking employment on the graveyard shift in order to obtain access to customer credit cards and other PII, which they promptly transmitted and sold to drug dealers for a handsome sum per record.

As a result of the data breach, Victimco had to comply with the many state laws governing consumer notifications of data breach, had to supply customers with free credit reporting services, and otherwise sustained a "hit" to its goodwill. The costs of compliance and cure far exceeded the company's estimates, and it had no insurance to cover the losses.

Over 50% of data breaches in 2007 were internal, having been traced back to employees, service providers, and contractors.[1] Victimco now knows that these are high odds, meriting attention to the employment relationship and technological security. No recommendations can eliminate the risk of data breach, whether through the accidental loss of a laptop or the organized theft of personal data. But savvy companies can reduce the risks.

The obligation to safeguard personal data is growing in importance. Apart from the huge losses that follow on discovery of a data breach, the courts are starting to decide cases in this field, and there is a growing consensus that corporate directors and officers have an obligation to take reasonable security measures to protect PII. Corporate officers and directors have a fiduciary duty to the company and its shareholders to safeguard data.[2] One court recently held that financial institutions have a common law duty to ferret out impostors seeking or using PII.[3]

Victimco learned that data security starts with the employment relationship. For employees with access to PII, background checks using outside vendors are de rigeur. Computerized checks today are relatively inexpensive and can plumb databases and sources not available to most employers or their human resources departments. Had it performed background checks, Victimco may have learned of prior arrests or convictions that would have given it pause before it hired new employees who would have access to PII. And background checks should go further than past criminal tendencies; they also should address marital status and financial condition. Employees with marital difficulties or in financial distress are easily tempted, and have the motivation, to seek and sell PII to those all too willing and able to buy records for use in criminal enterprises.

Background checks most often begin and end at the inception of the employment relationship. Employers generally do not renew the investigations to learn of changed circumstances. That is a mistake. The annual review of each employee who handles PII should be expanded to consider data security issues and the company's policies on protecting PII. It should also include a renewed background check to detect changed circumstances that can reveal temptations to commit data breach for personal gain. Those who have had a data breach understand that the financial and reputational risks of such breaches are so much more significant than the costs of these additional precautions.

Victimco also learned that data entry and storage are areas ripe for risk reduction. Once data is entered into a company's computer systems, it should be encrypted so that access is rendered difficult except to the most sophisticated hackers using decryption techniques not generally known or available to most data thieves. Computer systems should include audit trails that allow easy detection of who accessed data, when, and for what purpose. Simple procedures such as password-protecting unattended computers, or requiring all systems to be shut down each day, also reduce the risk of unauthorized access to and loss of PII. Think of the cleaning people who have access to computer terminals — still logged into company systems — in the dark of night.

What is the takeaway from this cautionary tale? Employees and contractors represent the greatest risk of data breach, whether by design or mere accident. The obligation to protect PII and to secure data begins internally. Finally, beware the graveyard shift!

2. SECURITY IS ONLY AS GOOD AS THE WEAKEST LINK

by Scott S. Christie

It started innocently enough. A US educational institution (which we shall call WhoU) was looking to update and standardize the PII of current and former students in its electronic database and upgrade its software to automate much of this process on a going-forward basis.

WhoU had good reason to do so. With alarming frequency, tuition bills, calendars, and school newsletters were not reaching their intended recipients. Attendance at school-sponsored events had suffered because many did not receive timely notice. Not surprisingly, alumni monetary contributions were also on a downward spiral and collection goals were not being met. Shaming alumni into increasing their financial commitments and dangling the prospect of legacy admissions for their children only carried WhoU so far. It concluded that it couldn't extract cash from alumni it couldn't reach out and touch.

However, revamping the database and data collection process was a tall order for WhoU, requiring thousands of hours of work by already overtaxed employees. Hundreds upon thousands of lines of software code would have to be written, revised, debugged, tested, and integrated into the existing system. Students and alumni would have to be contacted and recontacted in order to confirm the accuracy of existing PII, modify the PII that was inaccurate, and supplement PII that was missing. Then, all the updated data would have to be entered into the electronic database using the new software.

WhoU decided that it was more cost-effective to outsource this effort and decided upon Vendodrama, a purported leader in the field that had been recommended by word of mouth from other school administrators. Vendodrama had its own form service contract that it presented to WhoU on a take-it-or-leave-it basis. WhoU, eager to get the project started and without outside assistance, signed on the dotted line. With the transfer of the existing electronic database of PII and a check, WhoU could turn its attention to the impending strike by unionized, nonsalary employees and an escalating student protest over the school's investment in China, which the students deemed counterproductive to the self-determination of ethnic Tibetans. After all, WhoU thought the project was in good hands. But was it?

For reasons that may never be entirely clear, soon after the contract was signed, a Vendodrama employee took a business trip (unrelated to WhoU) to a country with a gross domestic product equivalent to that of Rhode Island, a large majority of which is spent to supply government leaders with the finer things in life and to combat a revolutionary insurgent movement. And this individual brought his laptop computer with him. You can guess what happened next. In a moment of inattention, the laptop was liberated from the Vendodrama employee by a local resident. Gone not only was the computer, but also the WhoU database of alumni and student PII that was stored on the hard drive.

Vendodrama didn't exactly break any land speed records in informing WhoU of the data loss. WhoU learned the fate of the PII about two weeks after the theft, and only then because it had inquired about the security of the information. WhoU was prompted to ask about the PII because several alumni had notified the university after receiving solicitations from the widow of an African dictator who was looking for a reputable businessperson with a Western bank account to assist in the transfer of $20 million from that country's national bank to avoid its falling into the hands of corrupt government officials. A few of these alumni recalled communicating with a Vendodrama employee not long before receiving this business proposition.

Now in full crisis mode, WhoU began to fathom the enormity and complexity of the problem. There was a breach of security of the alumni and student PII in the WhoU electronic database, right? Well, maybe. Vendodrama swore that the hard drive on the laptop was fully encrypted. If so, then there would be no legal obligation to report the loss of the PII under most state data breach laws due to the lack of a reasonable belief that the security of the PII had been compromised. Could the messages out of Africa really have been a mere coincidence? WhoU wouldn't know for certain unless the laptop was recovered, and that did not seem likely.

That begged the question, which data breach laws applied to this situation? Technically, the state data breach law that corresponds to the state of residence of each victim dictates legal obligations in the event of the breach of security of that victim's PII. Yet when, as here, a security breach involves residents of all 50 states, the District of Columbia, Guam, and Puerto Rico, how can anyone possibly meet all the legal obligations under the dozens of inconsistent statutes?

How about law enforcement notification? Most state data breach laws require that law enforcement, usually the state police or the state attorney general's office, be notified of the breach of security of state resident PII before the actual resident victims to allow for the possibility of a viable criminal investigation. Did that mean WhoU needed to burn up the line to each and every state capitol?

Furthermore, law enforcement notification does not obviate direct victim notification; it only delays the inevitable. Even though Vendodrama was responsible for the arguable data breach, it was acting as an agent of the holder of the PII. Accordingly, the obligation for complying with the data breach laws — if there was a data breach — rested on WhoU. From a public relations standpoint, it would be preferable to pass the buck — that is, make the vendor send out the victim notification letters on its letterhead. Then you can supplement this letter after the fact with one of your own in which you not-so-subtly reinforce as often as possible the idea that the vendor is to blame for the problem and (hint, hint) can be served with a lawsuit at its business address. Alas, when it signed its contract with Vendodrama, WhoU had not considered the potential PR issues.

And let's not forget the unique issues posed by data theft victims who are not flag-waving Americans. A reunion of WhoU alumni could be mistaken for a model United Nations. If you think the state data breach laws are draconian, just wait until you get a load of the corresponding laws of other countries. The UK, Canada, and the member states of the European Union are especially rabid about the protection of their citizens' PII. Any effective response to a data privacy breach must take into account legal obligations under the national laws of countries whose citizens have been victimized.

So, what did WhoU choose to do? Although it may not have had a legal obligation to do so, it elected to comply with the data breach obligations of its state of residence. WhoU concluded that the long-term interests of its students and alumni and its ongoing relationship with them were better served through disclosure and notification rather than avoidance and obfuscation. Through counsel, it notified its home state law enforcement, and that officer gave WhoU dispensation from having to notify law enforcement in any other state.

When it came time to notify WhoU students and alumni, Vendodrama refused to participate in sending out notification letters. Unfortunately, WhoU had no legal recourse to force Vendodrama to take on any such responsibility. With some trepidation, WhoU ended up sending out thousands of letters internationally to all affected students and alumni. Luckily, the feared backlash never materialized. There were a small number of letter recipients who followed up with and complained to WhoU, but for the most part their anger was directed at Vendodrama, and they appreciated WhoU's candor. Nevertheless, it will come as no surprise that WhoU didn't break any alumni fund-raising records that year.

What is the takeaway from this cautionary tale? WhoU learned the hard way that vendors can be a weak link in the chain of data privacy. If you decide to share employee and/or customer PII with an outside third party, it behooves you to insist upon contractual terms that adequately protect your legal and reputational interests. Among other things, the contract should specify that:

- PII will be encrypted at all times during storage and transmission.
- PII will be stored in a secure manner that is at least as robust as the manner in which the vendor stores its own PII, and certainly never on a laptop computer.
- PII will be accessed only by vendor employees for whom such access is a job necessity.
- PII will not be taken or transmitted outside the country without express written approval in advance.
- The vendor will provide immediate notification of any significant threat to the security of the PII, whether or not the data itself has been compromised.
- The vendor will provide full indemnification and assume legal liability for any and all data breach obligations with your oversight, guidance, and approval.

In short, avoid the WhoU ballyhoo. It's your vendor they should pursue. Too true.

3. EVIL ROBOTS STOLE MY BRAIN … ER, DATABASE

by William A. Zucker

You are an Internet consultant. One of your specialties is doing intelligence on competitors. A newly minted travel company approaches you. It wants to mimic and underprice all of the trip programs that are being done by a market leader. The data is actually available on the market leader's Web site in the sense that a prospective customer can select a trip, dates, accommodations, and add-ons and get pricing. However, the variations are many, and manually gleaning intelligence about the competitor's trip programs through repeated trip schedule/price inquiries is a daunting task. You decide to devise a robot or spider that will query the Web site repeatedly. You are concerned that the robot you create will, in its requests for the data, appear to be a denial-of-service attack. So, you slow the robot down to more closely mimic repeated requests from a customer. In addition, you use the robot at night, when fewer people are likely to be accessing the Web site.

The robot is extremely successful. Using tour codes that are obtainable from the Web site but that can be puzzled out only by members of the trade, the robot repeatedly accesses the site, sending over 30,000 inquiries and downloading 60,000 lines of data, the equivalent of eight telephone directories. The information is then collated into a spreadsheet and used by the new travel company to systematically undercut the market leader's prices and to generate a competing travel program. The rival mirror-image programs do serious damage to the market leader's business.

The market leader wonders how its database was penetrated and begins to examine its computer system. The 30,000 queries from one IP address come to light. The market leader then hires a forensic expert to evaluate what information was taken and by whom. A year and a half later, the market leader files a lawsuit alleging that the Internet consultant and the new travel company violated the US Copyright Act and the US Computer Fraud and Abuse Act (CFAA), which prohibits certain access to computers. The lawsuit seeks an injunction and the return of the allegedly purloined information. The linchpins of the argument rest on the provision in the CFAA that defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter" and on a claim that accessing the database violated copyright law.

The federal district court had no problem concluding that the database was not protected under US law. But it did grant an injunction under the CFAA. It imposed a "reasonable expectations test," finding that the robot bypassed technical restrictions on the Web site that permitted only one page at a time to be displayed and that whatever expectations there may have been with regard to access, it was not reasonable for a competitor to think that it could bombard the Web site with requests to obtain information for competitive use.

This commonsense rationale for the injunction, however, did not stand up on appeal. The appellate court applied a different commonsense approach, observing first that any company would presumably dislike a competitor's constructing a database to undercut pricing whether it were done by a scraper or manually, and then ruled that:

> The public Web site provider can easily spell out explicitly what is forbidden and, consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like "reasonable expectations."

In short, without a clear prohibition, the consultant's access of the market leader's Web site was not unauthorized access under the CFAA because it used a public portal to gain access to the database even though the market leader viewed the database as containing the heart of its competitive information.

What is the takeaway from this cautionary tale? One obvious point is that you need to post "no trespassing" signs on any public portal as part of your terms of use (think of the computer equivalent of no hunting, camping, walking, etc. signs), and better yet would be to implement true technical restrictions. If your Web site generates any public data that can be used as entry points (in this case, the tour codes), that public data should be encrypted. Overkill is a good thing. Think as well of protecting the information through confidentiality agreements with anyone who would understand the significance of the public data and with whom you have a contractual relationship. Finally, think about copyright protection before, not after, the fact. It may be the location of the database that will determine whether the information in the database can be protected. Europe, for example, affords a greater standard of protection to databases than the US. Had this database been located in Europe, there would be additional arguments in favor of protection.

4. REMEMBER THE COBBLER'S CHILDREN: BEWARE OF SELF-HELP

by John M. McKelway, Jr.

A sophisticated US IT firm ("the Company") with 350 employees, including international operations, maintained a regional sales force. The regional sales manager ("Jack") operated out of his home, traveling extensively and working remotely via a Company laptop. The Company had regular sales meetings at the home office in the Boston area, but for the most part, Jack operated independently without direct supervision.

All members of the sales force were required to execute standard nondisclosure and nonsolicitation agreements with the Company as a condition of their employment. These agreements prohibited the sales force, including Jack, from (1) disclosing or misusing trade secrets or confidential or proprietary information, and (2) wrongfully soliciting the Company's clients and accounts. Standard policies were also in place restricting access to confidential information, and highly sensitive data was stored separately.

One fall day, Jack made an unusual demand: he wanted a substantial raise in compensation, which he insisted must become effective in 30 days. Jack's boss was surprised that he would make a request of this sort — he was ordinarily very passive in such matters — and increases of this magnitude were typically awarded in the spring, during performance evaluations. Nor did Jack's sales numbers justify a raise. In fact, his biggest customers were strangely inactive at that moment. Jack's request, of course, was denied.

In December, Jack gave notice of his resignation, effective at the end of the year. Jack further disclosed that he was leaving to join one of the Company's biggest competitors ("the Competitor"). The Company initiated standard security protocols, terminating his access to the computer system, requesting that all confidential materials be returned, and demanding return of all Company property, including the laptop.

Jack's last day at work was 31 December, and although he was very cooperative in the exit process, the laptop was not immediately returned. Jack kept making excuses for the delays but finally sent the laptop back in early February. In the interim, the Company did a search of Jack's recent e-mail communications but came up empty. When Jack's customers started leaving to join the Competitor, the Company consulted a lawyer.

The evaluation of the situation disclosed some difficulties in bringing a lawsuit against Jack. First, there was no evidence that he took or misused confidential information or trade secrets. And even though some of Jack's customers were now doing business with the Competitor, there was no evidence of wrongful solicitation by Jack. Finally, the law in Jack's home state was not favorable to employers in these circumstances. The Company was reluctant to spend considerable time and expense in litigation, only to come up short, even though they were highly suspicious of Jack's behavior. What, they asked, should be done?

The Company's lawyer suggested sending the laptop out to a seasoned forensic expert to see if any incriminating information could be recovered. The Company balked at this proposal. After all, they were the computer-savvy IT professionals, and Jack's e-mail communications had previously been searched! Although skeptical about their prospects, the Company decided to let an established forensic expert take a look.

At first, the forensic review came up dry. However, a thorough examination of the hard drive revealed stunning information. While still employed at the Company in the fall, Jack was communicating directly with the Competitor, setting up job interviews. Shocking evidence followed. An e-mail trail was pieced together that demonstrated Jack had improperly accessed a proprietary Company presentation to a client and forwarded it to the Competitor's software engineers!

Evidently, Jack used the laptop to access his personal, Web-based e-mail account to forward the trade secrets, never imagining that it could somehow be recovered. A classic "smoking gun" e-mail from Jack sealed his fate:

> If my employer learns about this, they will haul my rear end into Court so fast that our heads will spin!

Jack was prophetic in that regard. Armed with this incriminating evidence, the Company launched an immediate lawsuit and request for injunctive relief. Claims against Jack included theft of trade secrets, breach of contract, breach of fiduciary duties, and violations of CFAA. The Competitor was also named a defendant. The court issued an immediate injunction requiring the defendants to freeze all computers containing the pilfered trade secrets and requiring their return to the Company. Jack and the Competitor were also enjoined from doing business with the Company's former clients.

The case resolved within a few months. As part of a comprehensive settlement agreement, the Competitor was required to:

- Pay for the costs to inspect the "infected" computers and remove all information related to the Company
- Agree to refrain from doing business with the Company's clients for the period of Jack's non-solicitation agreement
- Pay damages to the Company
- Pay the Company's legal fees

The disruption to the Competitor's business was enormous and represented a public relations nightmare.

What is the takeaway from this cautionary tale? Do not assume you know what you do not know. A do-it-yourself approach is not always the best approach where the subtleties of data theft are concerned. Even worse, self-help efforts may destroy or compromise valuable electronic evidence. Finally, the subtle signals from Jack warranted immediate followup. As the saying goes, "Where there's smoke, there's fire." And nobody likes to get burned.

CONCLUSION

The one thing that we can be certain of in the world of data security is the inventiveness of the attacks on our data. But we should not focus simply on preventing the unexpected. We need to protect against the mundane as well as the unexpected, because it is most often the known that is responsible for our data leaks. In American football, they call it going back to the fundamentals and "blocking and tackling." It is what every team needs to do. The same approach is necessary in the world of data security. We hope that these cautionary tales give you food for thought and some ideas to make your security programs more thorough and less subject to attack.

ENDNOTES

[1] PwC Advisory Services. *The Global State of Information Security 2007*. PricewaterhouseCoopers, 11 September 2007.

[2] See Caremark International, Inc., Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).

[3] See Brunson v. Affinity Fed. Credit, NJ App. Div. 9 Sept. 2008.

The writing of this article exemplifies the team approach that the lawyers at McCarter & English, LLP bring to issues and the wealth of knowledge and experience they can bring to a problem. William J. Heller, Scott S. Christie, and William A. Zucker are partners in the IP/IT Group at McCarter & English, LLP. All three are trial lawyers who are actively involved in counseling of clients and in trial work regarding all fields of intellectual property, information technology, data privacy, and licensing. John M. McKelway, Jr., is a partner in the Labor and Employment Group at McCarter & English, LLP and also a trial lawyer. Mr. McKelway is heavily involved in counseling clients on and litigating matters relating to data protection and privacy regarding employees, executives, and employment contracts. William J. Heller is Chair of the IP/IT Group and is instrumental in the negotiation of technology and life sciences agreements. He regularly advises clients in corporate-wide IP protection programs. Scott S. Christie, in the data privacy area, instructs companies on protecting personally identifiable information of customers and employees, investigates breaches of security of such information, provides guidance to clients concerning their obligations in response to such breaches of security, assists clients in satisfying these obligations, and defends companies sued for data security breaches. William A. Zucker is a longtime senior consultant for Cutter Consortium on intellectual property and technology issues that include outsourcing, data security, and privacy. He has written the International Institute of Conflict Prevention and Resolution's rules for fast-track technology arbitrations and mediations. He is also coauthor of a chapter on intellectual property issues in the Computer Security Handbook, *5th edition.*

Mssrs. Zucker, Heller, Christie, and McKelway can be reached at wzucker@mccarter.com, wheller@mccarter.com, schristie@mccarter.com, and jmckelway@mccarter.com, respectively.

All Together Now: Converging to Build Information Security and Privacy Awareness

by Ilene Switalski Klein

It’s 7:05 am at Marc’s local coffeehouse, and he’s frantically trying to finish his employees’ annual performance appraisals before they’re due to HR. Marc’s a finance director at a global consumer products company. He’s much better at analyzing pending mergers than trying to describe what tasks his people accomplished, to say nothing of the company values they embodied to do them. He sighs and gets a refill, hoping that more coffee will improve his day. It doesn’t. When he returns to his table, Marc’s laptop is gone.

News of Marc’s laptop theft gets reported up the management chain, and the VPs agree that the company must increase user awareness of information security and privacy. In a flurry of responses to the VPs’ decree:

- *Global Security sends an e-mail to all employees telling them how to protect laptops and instructing them to call Global Security to report any cases of laptop theft.*
- *Legal sends an e-mail to all employees reminding them of the company’s “Data Classification Policy” and that they should not store confidential information on laptops.*
- *HR sends an e-mail to all managers reminding them not to store performance appraisals containing employees’ personally identifiable information on laptops.*
- *The SOX Program Management Office sends an e-mail to all employees reminding them that the integrity of materially relevant financial information must always be protected and that they should not store it on laptops.*
- *Records Management sends an e-mail to all employees reminding them of the “Records Management Policy” and telling them to store company records on servers, not on laptops.*
- *The Privacy Office sends an e-mail to all employees reminding them of the “Privacy Policy” and telling them not to store personally identifiable information on laptops.*
- *IT Security sends an e-mail to all employees reminding them of key points in the “Acceptable Use Policy,” telling them how to protect laptops, and instructing them to call the Help Desk to report a laptop theft.*

Around the world, the company’s employees glance at the messages flooding their in-boxes and spend more time gossiping about the incident that must have precipitated the communications than absorbing the key messages. Within days, the communications and gossip die down ... until the next major incident.

GET YOUR STORY STRAIGHT

We all know that information security and privacy awareness is important. It’s a strong preventive control that’s considered the first line of defense against security’s weakest link.

The above example shows what happens when you have an uncoordinated awareness program with different business areas competing for employees’ attention. You often end up with overlapping, inconsistent, and conflicting messages (e.g., to whom to report a lost laptop). With limited communications channels (e-mail, face-to-face, intranet, posters), your message competes with all the other “noise” an employee hears daily. And speaking of employees, they’re too busy doing more with less that they simply don’t have the time or energy to handle communications they consider useless. That is, provided you even have the budget this year for your program.

So where does that leave you?

It leaves you with major business drivers to build information security and privacy awareness through convergence. Convergence allows you to share limited resources — including people, time, and budget — to develop and deliver an awareness program. Together, you can coordinate key messages and present a single “face” to employees by branding all communications. When you deliver consistent communications, your employees know what to expect and are more apt to pay attention.

Here’s how to get started.

BUILD YOUR TEAM

At a minimum, your awareness team should include people from the following areas:

- IT security
- Legal/compliance (ethics, records management)
- Physical security
- Privacy

In some organizations and countries, communications that may impact employees' jobs must be approved by HR, unions, and/or works councils. If so, then include them as team members.

Does the corporate or internal communications department "own" the internal communications channels in your organization? Do all e-mails or intranet postings have to go through them? If so, then invite them to join your team. Even if they decline to join the team, make sure you discuss available communications channels, their processes, approval requirements, and lead time for publication/dissemination.

You may also consider including your audit or controls (SOX) organization. This helps remind employees that auditors really do perform a needed service for the organization and that the terms "auditor" and "enemy" aren't synonymous.

DEFINE YOUR PURPOSE

Once your team is established, gain agreement on and document your purpose. For example, the purpose of the awareness team is to:

- Build a comprehensive awareness program to transform YourCompany into an information security– and privacy-conscious organization where employees incorporate security and privacy best practices into their workday
- Inform key stakeholders of new regulatory requirements, information security and privacy trends, and emerging threats and countermeasures directly related to YourCompany's applications, systems, and business
- Reduce the risk of business impact due to employees' failure to employ security and privacy best practices
- Support YourCompany's growth, organizational effectiveness, and financial goals by delivering security- and privacy-related information to reduce information risk and to increase organizational resiliency.

Why is a mission statement necessary? So you can rein in the privacy and IT security folks when they start arguing about which encryption algorithm the company should use and refocus the team on what employees need to know about protecting information.

When organizations rotate responsibility, competing priorities often interfere, causing missed deadlines and lower-quality communications.

DEFINE GROUND RULES

Defining the ground rules for how the awareness team will work together and then complying with those rules will be critical to your success. For example, will team members take turns leading the communications efforts each month, or will one person be tasked with developing all communications that the team reviews? Here are the key rules to develop:

- Meeting frequency, length, and method (in person, teleconference)
- Roles and responsibilities, deadlines, and deliverables
- Review process, approval gates, and number of review cycles
- Cost sharing
- Ultimate decision maker

I recommend that the information security and privacy awareness team meet monthly to validate upcoming topics and plans. The first meeting each quarter should be face-to-face where feasible; otherwise, teleconferences are fine. Allow one hour for the quarterly planning sessions, while a half hour should be sufficient for the other months' "topic validation" teleconferences.

When establishing roles and responsibilities, determine who is actually going to write and publish the communications. One option is for each team member to take responsibility for each quarter's deliverables. This option helps spread the work and costs so that no one organization is burdened with them. Another option is to simply dedicate one full-time employee to awareness efforts. This option helps ensure all communications have the same "voice." In my experience, a dedicated (skilled, knowledgeable, creative) full-time person tends to work better. When organizations rotate responsibility, competing priorities often interfere, causing missed deadlines and lower-quality communications.

Defining your review process is critical to avoiding churn. Not to be confused with "analysis paralysis," churn is when you continuously go back and forth over the same topic — as when you review a document, make small changes, request a new version, make more small changes, and request yet another new version, ad nauseam. To eliminate churn, I recommend two review cycles such that:

- The writer submits a draft.
- Reviewers/approvers have one to two weeks to review and return comments.
- The writer submits a final draft.
- Reviewers/approvers have one to two weeks to review and return comments.
- The writer publishes the communication.

Determine how decisions will be made and who your ultimate decision maker will be. In some corporate cultures, all decisions are made by (often time-consuming and compromise-filled) consensus. Be careful if you go that route, as writing by committee rarely works. I recommend the "benevolent dictator" model, in which the team leader listens to all opinions, weighs them against his or her own judgment, and makes the decision.

> **It's a sad truth that, in most organizations, communications that come from IT are generally ignored by the business units.**

ESTABLISH YOUR BRAND

Develop an identifiable logo and brand for your team and all communications. An information security and privacy awareness program is a marketing campaign that has to gain your employees' attention and overcome their barriers, such as their impression of security, privacy, and legal requirements. Branding your communications designates them as "official" and makes it more likely that employees will actually read them. Branding also helps employees identify fraudulent messages, such as fake virus warnings.

If you have a marketing or graphics department, I strongly recommend you consult with them on best ways to brand your team and all its communications. You may even consider adding them as part of your team. And make sure your brand and logo fit your company culture.

Another key consideration for naming your team is recognizing who has the "power" in your organization. It's a sad truth that, in most organizations, communications that come from IT are generally ignored by the business units, while communications that come from the legal department garner attention and respect. When naming your team and creating your logo, use that fact to your advantage and make sure that "legal" is referenced in the name.

BUILD YOUR PROGRAM

By now you have your stakeholders, a good idea of what you want to do, and a logo and brand that resonate with your employees. Now it's time to actually plan and build your program. Remember, information security and privacy awareness is not a one-time event! You should include:

- Scheduled communications, including awareness articles, policy announcements, and project/initiative news
- Unscheduled communications, such as virus/threat alerts based on template messages
- Direct communications from employees, such as e-mail questions to an awareness mailbox and an "Ask the Security/Privacy Expert" link from the intranet site
- Surveys to gauge employee knowledge and attitudes before and after training and awareness program implementation
- An information security and privacy awareness intranet site that provides awareness articles and links to online presentations and training
- Information security and privacy awareness training, including both annual training and new employee orientation
- Face-to-face communications, such as staff/organizational meetings, events, technical fairs, and security/privacy awareness road shows
- Promotional items that act as awareness reminders

As you build your program, consider using champions to help spread your message. Information security and privacy awareness champions are generally volunteers from different business areas or geographic locations. Not only is this approach generally inexpensive, but it's also very effective. People are more apt to pay attention to and engage in information when they receive it from someone they know.

To solicit volunteers, determine their role and how much time they'll spend, get their managers' approval, and emphasize what's in it for them. For example:

The Champion's Role

- Host one event per quarter
  - *Presentations:* lunch-and-learn sessions, staff meetings
  - *Movies:* show information security and privacy videos and facilitate discussion
- Distribute materials
  - One e-mail message per month
  - Posters
  - Trinkets
- Collect feedback and answer questions
  - Submit topic suggestions and other feedback
- Estimated time commitment: six hours/quarter
  - *Two hours:* getting and reviewing materials
  - *One hour:* event setup and teardown
  - *One hour:* hosting event
  - *One hour:* marketing and miscellaneous e-mail
  - *One hour:* collecting and reporting feedback

Benefits to Champions

- Increased knowledge
  - Information security and privacy
  - Your local site and people
  - Your business and employees
- Career benefits
  - Demonstrates leadership qualities
  - Offers opportunities for networking and extending one's influence
  - Hones presentation skills

COMMUNICATE

Figure 1 shows the basic communications process. No matter what type of communicating you're doing for the awareness program, you should always follow this process.

There are a few ways to select your key messages. If you're one of the lucky few who have budget dollars, you can always hire a consultant to conduct a formal needs analysis. Those of us who are living in today's economy can chat with peers to find their problem areas (and collect metrics if possible). For example, talk to:

- **Help desk personnel.** What kinds of calls are they getting (password resets, virus infections, users receiving strange phone calls, etc.)?
- **Desktop support staff.** What kinds of trouble are users having (virus and spyware infections, unapproved downloads, spam, etc.)?
- **Managers.** What do they observe, and what keeps them up at night (excessive Web surfing, anti-harassment policy violations, privacy data breach, regulatory compliance)?
- **Users.** What is their current level of knowledge, and what would they like to know more about (where to learn about company policies, what to do about identity theft, how to request new accounts for contractors, how to protect home PCs)?

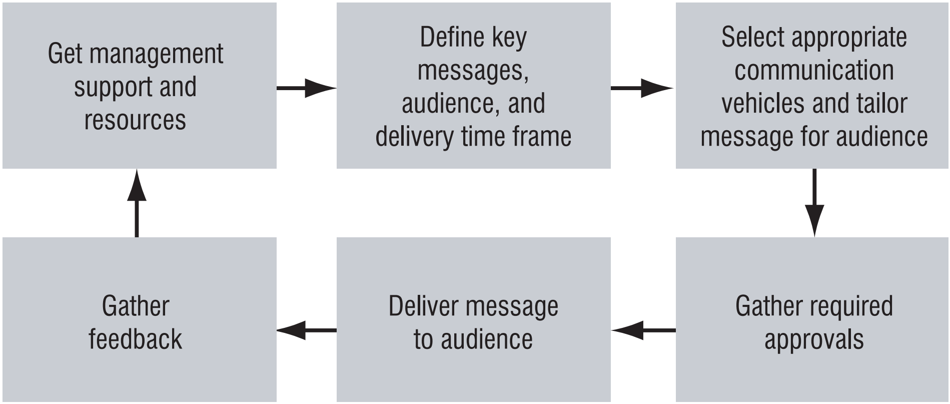

Get management support and resources
Define key messages, audience, and delivery time frame
Select appropriate communication vehicles and tailor message for audience
Gather required approvals
Deliver message to audience
Gather feedback

Figure 1 — Basic information security and privacy awareness communications process.

Once you know your key messages, I recommend developing an annual information security and privacy awareness calendar. This allows your team to plan the year's major topics. Make sure you include information that is personally relevant to employees, such as how to protect their families from cyberpredators.

Table 1 shows sample quarterly topics with monthly subtopics. Each month, the awareness team meets to review next month's subtopics and tailor key messages to what's going on in the industry and within the organization. Remember, building your communications on shared information is a key advantage of convergence. For example, you may learn in your monthly meetings that employees were recently fired for violating the company's Acceptable Use Policy or that updates to HIPAA require more stringent controls around personal health information. You can then use this information to add a timely cautionary tale to your communications or to pick "protecting privacy" as your next communications topic.

In Table 1, the quarterly deliverables consist of:

- A 15- to 20-minute PowerPoint presentation on the quarterly topic, with the presentation's script in the Notes pages. The presentation is posted on the awareness intranet and team members send it to managers throughout the organization to present.
- A one- to two-page article each month on the monthly subtopics. The article is posted on the awareness intranet, and the corporate communications department includes a link in their monthly "all hands" e-mail message.
- A one- to two-paragraph tip each month on the monthly subtopics. The tip is posted on the awareness intranet, and corporate communications includes a link in their monthly "all hands" e-mail message.

Together, the deliverables form a library of information security and privacy awareness articles, tips, and training.

Another scheduled communication vehicle is a monthly newsletter. If your corporate communications group does not allow individual organizations to e-mail monthly newsletters to all employees, make the

Table 1 — Sample Information Security and Privacy Awareness Topics by Quarter

Topic	Subtopics
Q1 Information Protection	Confidentiality, integrity, and availability (CIA) terms and importance
	User responsibility, policies, and records management
	Controls, regulatory requirements, and audit (SOX, HIPAA, etc.)
Q2 Internet Threats and Safeguards	Threats (viruses, worms, spam, phishing, etc.)
	Wireless security (coffeehouse surfing, basic laptop protection, rogue access points, etc.)
	Home PC protection
Q3 Preparedness	Risk management
	Incident response
	Disaster recovery/business continuity planning
Q4 Defense in Depth	The human element (social engineering, shoulder surfing, public conversations)
	Physical security (laptop protection, door piggy-backing)
	Putting it all together (layers of security, importance of each employee)

newsletter opt-in and advertise it on every communication that you publish. Figure 2 shows an example of a newsletter that contains “snippets” of information security and privacy information. Newsletter contents could include:

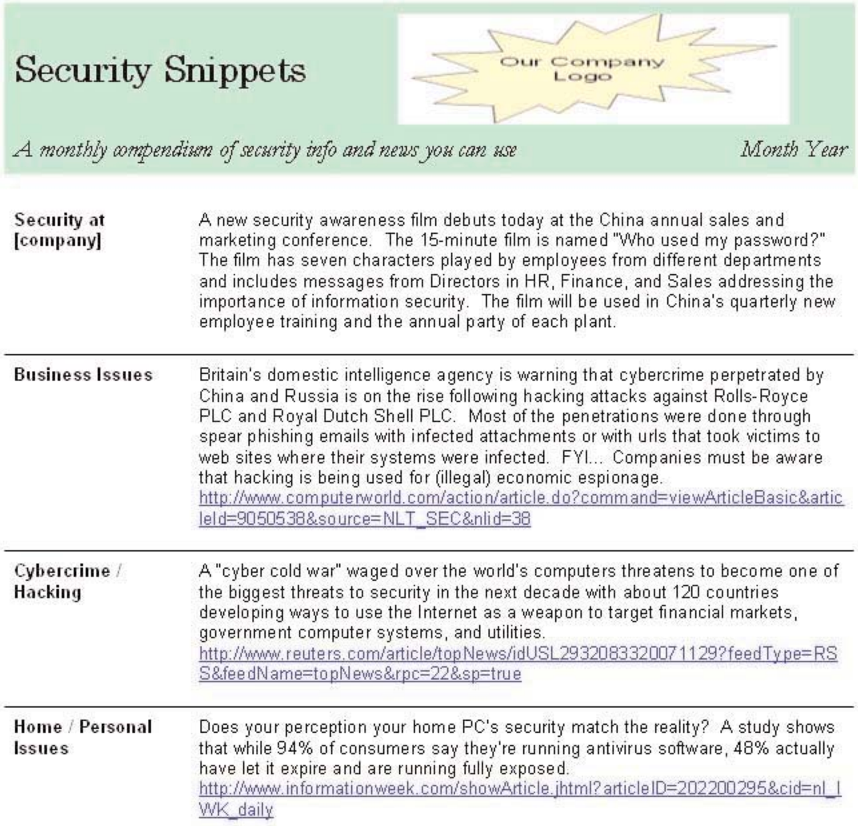
- Information security and privacy at YourCompany
- Business issues
- Cybercrime/hacking
- Home/personal information security issues
- Law/politics/legislation
- Privacy
- ID theft
- Best practices/risk management
- Security/privacy quote of the month
- Links to the awareness intranet and current publications
- Subscription information and reader feedback

CONVERGE FOR EVENTS

Plan an annual information security and privacy awareness event with your stakeholders. Solicit your CEO or another executive to sponsor it and give an introduction. This not only demonstrates your organization’s commitment to information security and privacy, but also helps drive attendance.

At the event, give each stakeholder group a booth to staff with their employees to answer questions and to hand out brochures and trinkets to attendees. Choose a theme, such as:

- **It’s always time to do the right thing.** Team members give presentations themed to times of the day, such as selecting a strong password for morning computer login at work and protecting your PC for the night at home.
- **CSI: Computer.** Attendees interview suspects, including a hacker, business traveler, and office employee to determine who killed the computer.
- **Survivor: Compliance.** Attendees compete to demonstrate they know the right thing to do to avoid being “voted off the island.”



Security Snippets

Our Company Logo

A monthly compendium of security info and news you can use *Month Year*

Security at [company]	A new security awareness film debuts today at the China annual sales and marketing conference. The 15-minute film is named "Who used my password?" The film has seven characters played by employees from different departments and includes messages from Directors in HR, Finance, and Sales addressing the importance of information security. The film will be used in China's quarterly new employee training and the annual party of each plant.
Business Issues	Britain's domestic intelligence agency is warning that cybercrime perpetrated by China and Russia is on the rise following hacking attacks against Rolls-Royce PLC and Royal Dutch Shell PLC. Most of the penetrations were done through spear phishing emails with infected attachments or with urls that took victims to web sites where their systems were infected. FYI... Companies must be aware that hacking is being used for (illegal) economic espionage. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9050538&source=NLT_SEC&nlid=38
Cybercrime / Hacking	A "cyber cold war" waged over the world's computers threatens to become one of the biggest threats to security in the next decade with about 120 countries developing ways to use the Internet as a weapon to target financial markets, government computer systems, and utilities. http://www.reuters.com/article/topNews/idUSL2932083320071129?feedType=RSS&feedName=topNews&rpc=22&sp=true
Home / Personal Issues	Does your perception your home PC's security match the reality? A study shows that while 94% of consumers say they're running antivirus software, 48% actually have let it expire and are running fully exposed. http://www.informationweek.com/showArticle.jhtml?articleID=202200295&cid=nl_IWK_daily

Figure 2 — A newsletter is another good vehicle for promoting information security and privacy awareness.

- **Clean Sweep.** Desk/office "event" where employees comply with records management policies, clean out old records, and dispose of them properly.

Another option is to tie your event to sponsored one, such as:

- 28 January: Global Data Privacy Day (www.intel.com/policy/dataprivacy.htm)
- 31 July: System Administrator Appreciation Day (www.sysadminday.com)
- September: National Preparedness Month (www.ready.gov)
- September (varies): Global Security Week (www.globalsecurityweek.com)
- October: National Cyber Security Awareness Month (www.educause.edu/SecurityResourceKit/7479)
- November (varies): National Fraud Awareness Week (www.fraudweek.com)
- 30 November: Global Computer Security Day (www.computersecurityday.org)

As you define your program, determine how you'll measure success.

USE AVAILABLE RESOURCES

If you have limited inhouse resources, help developing your awareness materials is literally a click away. All of the sponsored events listed above offer communications and educational materials, such as posters and presentations. Most major computer vendors, such as Microsoft and Symantec, have extensive information security and privacy awareness pages on the Internet. There are also many vendors and industry leaders that specialize in security and/or privacy awareness and offer free articles and materials for download. A sampling of these includes:

- NoticeBored (www.noticebored.com/html/freebies.html)
- Security Awareness Incorporated (www.securityawareness.com/free.htm)
- Scott Granneman's Security Analogies (www.granneman.com/techinfo/security/securityanalogies)
- Rebecca Herold's training and information security and privacy awareness articles (www.privacyguidance.com)
- Gideon Rasmussen's awareness articles and a link to his information security resources site (www.gideonrasmussen.com/security-awareness.html)
- Bruce Schneier's newsletter and articles (www.schneier.com/index.html)

I think government, educational institutions, and training and nonprofit organizations provide some of the best free information security and privacy awareness materials. For example, at the US Federal Trade Commission's (FTC) Web site, you can download a comprehensive toolkit to host a Protect Your Identity Day. The kit includes information and sample materials on a CD-ROM and videos on a DVD. You can also order 500 free Laptop Security Tips Bookmarks to distribute to your employees.

Listed below are some of my favorite government and organization awareness sites:

- Federal Information Systems Security Educators' Association: winning materials contest entries (http://csrc.nist.gov/organizations/fissea/FISSEA-contest/previous-winners.shtml)
- FTC (www.ftc.gov; http://bulkorder.ftc.gov)
- National Institute of Standards and Technology (NIST) Special Publication 800-50: Building an Information Technology Security Awareness and Training Program (http://csrc.nist.gov/publications/nistpubs/index.html)
- NIST awareness materials/activities (http://csrc.nist.gov/ATE/materials.html)
- OnGuard Online: informational materials, quizzes, videos (http://onguardonline.gov/index.html)
- University of Georgia (US) Security Awareness Training and Education: presentations and links (www.infosec.uga.edu/sate/index.php)
- SANS Awareness Training: *OUCH!* newsletter, training, tips, and reading room (www.sans.org/free_resources.php)
- Stay Safe Online: lesson plans and materials (www.staysafeonline.info)
- US Security Awareness: list of resources (www.ussecurityawareness.org/highres/security-awareness.html)

Note: This list includes just a few of the countless sites that offer information security and privacy awareness resources. As always, before downloading and using any materials, always comply with all copyright and licensing requirements.

MEASURE YOUR SUCCESS

As you define your program, determine how you'll measure success. Make sure you collect metrics before starting your awareness program so that you have a baseline with which to compare. Some common metrics include:

- **Help desk calls.** Your calls may actually increase for a while as employees become more information security and privacy conscious.
- **Incidents.** These include viruses, breaches, inappropriate usage, and policy violations. They should decrease after you implement your information security and privacy awareness program.
- **User involvement.** This includes numbers of e-mail questions, survey responses, Web page hits, and training/event attendees.
- **Feedback.** This includes survey responses, water cooler chat, contest entries, and e-mail.

As you can see, these measures are more behavior focused than the typical "numbers of awareness articles published" metric.

OPTIMIZE YOUR PROGRAM

You've followed these recommendations and built an information security and privacy awareness program through convergence. Now it's time to assess and grow your program's maturity based on an awareness capability maturity model:

- **Initial** (chaotic, ad hoc, heroic) — intermittent, inconsistent communications from different stakeholders
- **Repeatable** (project management, process discipline) — consistent, scheduled communications from the awareness team
- **Defined** (institutionalized) — defined, documented, and managed awareness program from the awareness team
- **Managed** (quantified) — defined, documented, and managed awareness program from the awareness team, with metrics showing the program's reach and effectiveness, such as intranet site hits, numbers of employees taking awareness training and participating in events, survey results, numbers and types of employee-submitted questions and policy violations, and employee feedback
- **Optimized** (continuously improved) — ongoing process to improve the awareness program based on metrics, employee feedback, and industry best practices

It's 7:05 am at Marc's local coffeehouse. With practiced ease, he uses the local Wi-Fi to VPN into his company's network and access data stored on a server. A year has gone by and once again it's time to finish his employees' annual performance appraisals. With a resigned sigh, he signals the waitress to bring him another cup of coffee and then gets to work.

Ilene Switalski Klein has more than 20 years of experience in information systems, starting as an electronics instructor at Commonwealth College in Virginia. She traveled from Honolulu to Heidelberg as a systems engineer installing proprietary software for the US Army and resolving system crashes. In the past 10 years, Ms. Klein has been directly involved in information security. As an Information Security Manager for Kraft Foods, she built and led the company's global information security awareness program, and while at Philip Morris (PM) USA, she established and led PM USA's Virus Response Team and Vulnerability Assessment Team. Along the way, Ms. Klein has written scores of security policies, processes, strategies, and white papers, and she has given dynamic presentations to all levels of internal and external audiences ranging in size from 10 to 250, including one at the Computer Security Institute's NetSec 2007 *conference. Ms. Klein can be reached at iswitalski@yahoo.com.*

Driving the Point Home: Using Privacy Dashboards to Implement Secure Work Practices

by Nandita Jain Mahajan

The current business environment is vastly different from what it was a few years ago. The globally integrated enterprise is rife with challenges that threaten the security of data as well as the privacy of customers. CXOs across the globe would agree with the following as their topmost security/privacy concerns:

- Leakage of information, mainly sensitive personal information
- Fraud committed by an employee
- Accepting and acquiring unknown liability
- Contractual noncompliance
- Vendor risks — you can outsource a process, but not risks
- People don't know what they don't know and are the weakest link in the chain

Most business process outsourcing (BPO) organizations have created specialist security and privacy functions headed by a chief information security officer (CISO) and/or a chief privacy officer (CPO). While these specialist functions have streamlined processes, advocated good work practices, and greatly improved the corporate security and privacy posture, they have also led to a false sense of comfort. In some BPO firms, the responsibility and entire accountability relating to data security and privacy issues have shifted to these functions rather than line management. This is potentially hazardous and a recipe for failure.

The speed with which an organization's senior leaders become sensitized to seemingly "technical" areas like security and privacy is largely driven by the CISO/CPO's ability to provide them with visibility of issues and incidents. This must be done promptly and accurately, and such incident notices must include an assessment of the impact and suggested remedial measures. Simple yet effective dashboards supported by a strong business case provide compelling justification for line management to take ownership of information security and privacy issues. They also assist CFOs and CEOs in understanding the situation and taking decisions on approvals for security and privacy spending. Business leaders can use dashboards to initiate a dialogue with their clients and convince them to improve their own security and privacy posture. This will result in lowering the risk for the integrated enterprise.

This article discusses the challenges faced by service providers, the effect of culture on security and privacy, levers for a security and privacy framework in a BPO organization, and the importance of an incident response process. It also elaborates on how information from comprehensive and well-prepared incident reports may be used to create compelling dashboards, which will lead to correct business decisions.

THE THIRD-PARTY BPO ORGANIZATION: A GLOBALLY INTEGRATED ENTERPRISE

Businesses have been sourcing, and will continue to source, services from third parties located in distant countries to meet their organizational objectives of reduced cost, improved efficiencies, and higher quality of services. Yet the interconnectedness of enterprises increases operational complexity and adds to the burden on each entity to comply with strict privacy legislation and data security requirements. This in turn forces entities joined in business not only to have acceptable and compatible work practices, but also to conform to each other's culture and work ethics. This is important from a privacy perspective, because privacy, as we are well aware, is not just an issue of IT and secure work practices but also of behavior. Behavior is a function of organizational culture, existing norms in the society, the family atmosphere, and an individual's value system. All these have significant bearing when an individual is faced with making a difficult choice.

One of the most difficult problems to solve is one of resolving differences in the understanding and appreciation of privacy in two very diverse entities. In some cultures, for example, it is common practice for a family member to be given access to a patient’s medical test results. This may not be a common practice in other countries. When a process involving queries on medical tests is offshored, there is a possibility that sensitive information may be disclosed to patients’ relatives. Though done with good intent and according to prevailing practices in the agent’s own environment, this would be completely unacceptable elsewhere.

The differences in understanding of what is private and how sensitive information needs to be handled must be understood by the employees of the vendor organization. A single breach caused by inadequate understanding or an employee’s poor judgment may be enough to lose a valuable client, cause an irreparable dent in the company’s reputation, and/or result in high financial liabilities.

KEY STAKEHOLDERS THAT INFLUENCE THE PRIVACY POSTURE

A majority of large third-party BPO organizations have several thousand employees and delivery centers that are located in multiple countries and several cities. Clients are large multinationals in the areas of finance, insurance, healthcare, retail, telecom, banking, air transport, and so on.

The third-party BPO firm services end customers through its large population of technical customer support agents, who provide assistance via phone, mail, chat, or remote desktop services. While fulfilling a support request, an agent may handle personal information (PI) such as name, address, and phone number, and sensitive personal information (SPI) such as bank account numbers, healthcare records, credit card details, Social Security number, an individual’s marital status, and/or other personal details. These customers may be residents of any country, and their privacy must be protected under the existing laws of their respective state and country, cross-border laws, and the privacy commitment of the service provider. The responsibility of the agent in ensuring compliance with applicable privacy policies is therefore critical. Experience shows that inadequate awareness and understanding, as well as irresponsible handling of SPI, leads to unintentional disclosures and breaches.

In a third-party BPO firm, the complexity in IT security arises due to the diversity of clients and their business processing platforms. Each client may have its own extended networks, specific security and privacy frameworks, and legacy IT platforms. This complexity is aggravated further if the baseline security measures of the BPO firm are more stringent than those of its client. An open Internet client environment with mobile or home agents poses several challenges to the BPO firm’s IT and security organizations. Thus, while the role of agents is crucial, it is equally important for the IT security team to identify and implement tools and technologies that will ensure adequate security for the data at rest, in motion, and while being handled.

For business process executives (BPEs), the primary consideration is meeting the contractual agreement with the client. In most BPO contracts today, security and privacy breaches are linked to stiff liability clauses, hence a BPE’s understanding of security and privacy commitments plays a vital role in contractual compliance.

Responsibility of the CXOs centers primarily on driving down business risks while improving the top and bottom line. Therefore, in a BPO organization, there are four distinct groups that the CISO/CPO must target:

1. Agents
2. IT and security staff
3. BPEs
4. The CEO, CFO, and other CXOs

A simple diagram (see Figure 1) shows the issues third-party BPO organizations must consider as they build a security and privacy framework.

TYPICAL CONTROLS IN A THIRD-PARTY BPO FIRM

In order to meet client requirements, most BPO firms have implemented secure and dedicated work areas for sensitive client processes and have stringent measures on the operational floor (see Figure 2). Notable amongst these are:

- Security personnel at the entry and exit points who may frisk personnel for mobile storage devices, mobile phones, cameras, and writing materials such as paper and pen
- Surveillance cameras and digital video recorders
- Restricted access to the outbound calling facility, faxes, printers, e-mail, collaboration tools, and the Internet
- Hardened desktops with USB ports disabled, no storage of data on hard drives, no use of copy-and-paste functions allowed
- Hardened IT infrastructure devices and servers, secure applications complemented by strong processes such as ID/access management, patch

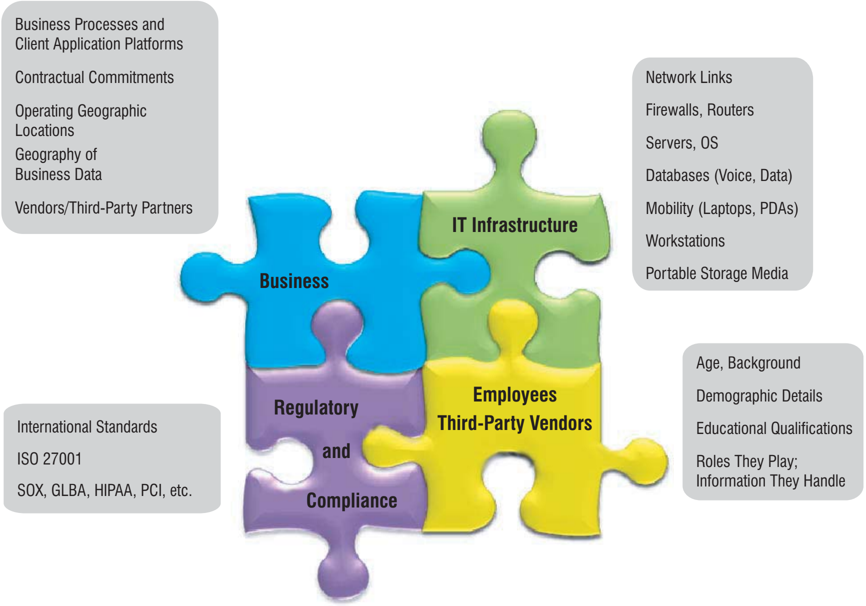

Business Processes and Client Application Platforms
Contractual Commitments
Operating Geographic Locations
Geography of Business Data
Vendors/Third-Party Partners
Network Links
Firewalls, Routers
Servers, OS
Databases (Voice, Data)
Mobility (Laptops, PDAs)
Workstations
Portable Storage Media
IT Infrastructure
Business
Regulatory and Compliance
Employees Third-Party Vendors
International Standards
ISO 27001
SOX, GLBA, HIPAA, PCI, etc.
Age, Background
Demographic Details
Educational Qualifications
Roles They Play; Information They Handle

Figure 1 — Key drivers for security and privacy.

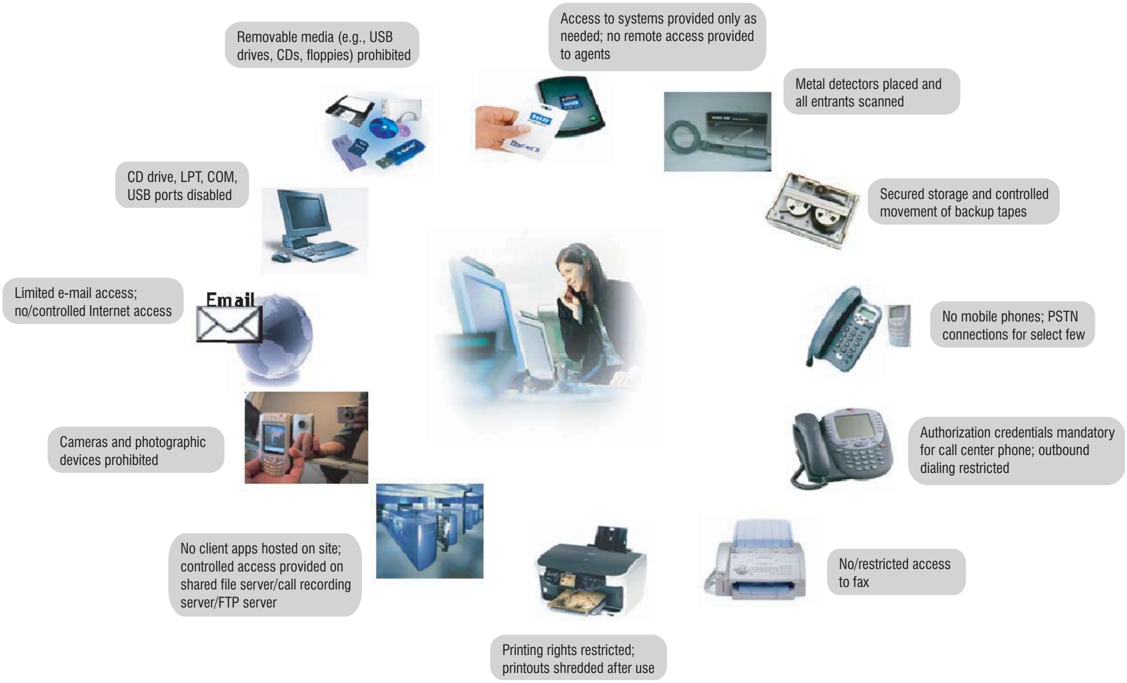

Removable media (e.g., USB drives, CDs, floppies) prohibited
Access to systems provided only as needed; no remote access provided to agents
Metal detectors placed and all entrants scanned
CD drive, LPT, COM, USB ports disabled
Secured storage and controlled movement of backup tapes
Limited e-mail access; no/controlled Internet access
Email
No mobile phones; PSTN connections for select few
Cameras and photographic devices prohibited
Authorization credentials mandatory for call center phone; outbound dialing restricted
No client apps hosted on site; controlled access provided on shared file server/call recording server/FTP server
No/restricted access to fax
Printing rights restricted; printouts shredded after use

Figure 2 — Typical controls in a BPO organization.

management, vulnerability scanning, and periodic penetration tests

INCIDENT MANAGEMENT

In spite of a robust security and privacy framework, strong governance, and effective detection and prevention mechanisms, security and privacy incidents will occur. A good incident management process supported by tools and procedures is invaluable, as it helps in:

- Ensuring standardization and consistency in handling incidents
- Maintaining and enhancing a knowledge base of root causes, exploitable vulnerabilities, and corrective and preventive measures

- Ensuring comprehensive incident investigation reports, which can be:
  - Shared with clients to convince them of weaknesses in their internal applications and operational processes
  - Shared with the BPO firm's line management, HR function, and IT to spur implementation of secure work practices and applicable tools
- Providing evidence acceptable in a court of law
- Maintaining details of all incidents and allowing for analysis, thus leading to better controls

Traditionally, a privacy incident was considered a lapse of IT security and was typically handled by security specialists. Though privacy rests on good security, it is also behavior driven. People will find ways of exploiting the system for personal gain or may divulge information due to lack of awareness.

Teams comprising purely technical staff may not be able to determine the exact sequence of events or understand their key motivators and root cause. Our experience at IBM Daksh shows that a cross-functional team must handle privacy incidents. Some of the best practices for investigating an incident are:

1. **Form the right team.** Assign an investigation team leader and assemble relevant experts from IT, forensics, IT security, line/operations, business controls, HR, physical security, and legal after a quick review of the incident. As the investigation progresses, change the team composition as required or leverage experts available elsewhere in the company or from third parties.
2. **Treat all incidents with a sense of urgency.** An incident must be investigated almost as soon as it is reported and the first draft report published within 48 hours. Privacy requirements — especially in terms of notifications to the client, privacy commissioner (in certain countries), and individuals — have become very stringent. A quick assessment is essential for identifying next steps.
3. **Implement corrective actions at the earliest moment.** To stop further exposure, plug all loopholes immediately. If there is action required from the client, inform their executives appropriately.
4. **Publish periodic reports to senior management.** For high-severity incidents, senior management of both the client organization and the BPO firm will be eager to know what progress is being made. Provide them with a summarized view at frequent intervals.
5. **Have a checklist ready.** Before starting a detailed investigation, acquire as much background information as possible (e.g., client contract, existing security and privacy controls, physical access records, shift roster, voice and screen recordings, privileges provided, functions performed, performance records, personnel file records). If required, read reports of similar incidents and prepare a list of all supporting artifacts that you will need to collect.
6. **Take custody of equipment as required.** Remove the equipment from the network and take custody of the hard disk or other equipment, as appropriate. Make sure that any forensic tools or utilities are run on a copy and not on the system under investigation.
7. **Involve the manager(s) of the suspect(s).** In case the investigation narrows in on a few suspects, take the managers of each in confidence and draw on their knowledge of the individual's past performance and behavior. Lifestyle changes in the recent past can provide significant clues to the motive that led to the incident.
8. **Complete all interviews on the same day.** A suspect may have to undergo several interviews. To the extent possible, close all interviews while the suspect is on company premises. If the person is allowed to leave, there is always the chance that he or she will get scared and not report to work ever again.
9. **Prepare the incident report and publish it to relevant stakeholders.** Use the latest version of the incident report template, get the report reviewed and signed off appropriately, and publish it promptly.
10. **Track recommendations to closure.** Your work does not end after you have published a good, comprehensive incident report. The effectiveness of the process lies in being able to close the recommendations in a timely manner. Multiple stakeholders will need to be pushed into closure. Raise the visibility by publishing the status of incident closure to senior management.

COMPONENTS OF AN INCIDENT REPORT

A comprehensive incident report is used for multiple purposes and forms the basis on which critical decisions are made and actions taken. Besides a step-by-step chronology of events leading to the incident along with all supporting artifacts, the components shown in Table 1 must be recorded for future reference and subsequent analysis.

Table 1 — Incident Report Components and Their Uses

Component	**How Can This Information Be Used?**
Date/time of occurrence of the incident	
Date/time when the incident was reported	If an incident is reported a long time after its occurrence, it indicates weak detection controls.
Short description of the incident	Keywords should be tagged for a faster search.
Incident reported by	If the reporter is in the client organization, it indicates weak detection controls in the service organization.
Location	Analysis by location will provide vital inputs into issues that are specific to this area.
Business unit (BU)	Analysis by business unit will provide vital inputs into issues relevant to the BU/client process.
Client name	This is useful for determining the number of incidents/issues for a particular client and determining whether the weakness is on the BPO firm's end or the client's end — or both.
Type of incident (e.g., unauthorized access, inappropriate usage)	Categorization will help in creating trends over a period of time.
Current status of the incident (legal, HR, business unit, client, security, privacy, business controls)	Noting status is useful for determining closure timelines and indicating with whom an action is pending.
Repository of incident artifacts	This indicates the repository in which all artifacts are stored.
Root cause — human factors (personal gain, carelessness, lack of awareness, lack of understanding)	The root cause offers insights into why an individual performed an action.
Immediate action taken	Implementation of immediate controls helps in arresting the issue and will assist teams in determining the effectiveness of the solutions offered.
Incident reported to (individuals/ distribution lists)	This component identifies the closed group of individuals who know about this incident. This should be a predetermined list.
Is this a repeat incident?	If so, it indicates that the previous incident did not result in total lockdown of the exposures. A red flag needs to be raised to senior management.
Possibility of occurrence in another location	This indicates the need for tighter controls across the organization, as the problem is not localized.
Tools used for investigation	Such tools help in calculating the ROI of the tool used. It is not sufficient to seek budgetary approvals with a cost-benefit case. It is equally important to demonstrate the value of the investment on a periodic basis.
Members of the investigating team	Listing team members is useful for seeking guidance on this case at a later date.
Severity (high, medium, low)	This will depend on each organization and the treatment of risk and impact.
Other organizations/agencies contacted	This is useful when specialized forensic investigators or legal counsel is needed.
Recommendations — Corrective (BPO)	These are corrective actions that the BPO firm must take (e.g., tightening lapses in the implementation of agreed controls).
Recommendations — Detective (BPO)	These are detective controls that the BPO firm must implement (e.g., cameras, digital recorders).
Recommendations — Preventive (BPO)	These are preventive controls that the BPO firm must implement (e.g., content filtering tools to block Internet access).
Recommendations — Corrective (Client)	These are corrective actions that the client must take (e.g., strengthening the ID management process).
Recommendations — Detective (Client)	These are detective controls that the client must implement (e.g., audit trails and alerts).
Recommendations — Preventive (Client)	These are preventive controls that the client must implement (e.g., data leakage prevention tools, anonymization of sensitive information).
Impact • Financial • Human resources • Customer satisfaction • Adverse press • Investigation and closure effort (hours)	Quantified impact is essential for creating dashboards.
Impact on compliance with contractual clauses and applicable frameworks	This indicates whether any contractual clauses, if applicable, were breached. It also mentions any violations to standards such as PCI, HIPAA, etc.

USING APPROPRIATE DASHBOARDS TO DRIVE CORRECT DECISIONS

Comprehensive reports and accurate data add tremendous value to decision-making individuals and teams. Storing this information in a database that allows slicing and dicing of data in multiple ways is equally important. Presenting the analysis in the right forums will ensure adequate attention and action. Let us now take a look at a few representative dashboards that have proven to be effective in driving a better privacy posture across organizations. (*Note:* The data depicted in the dashboards and charts is fictitious and used for illustrative purpose only.)

Enterprise Dashboards

A quick glance at the dashboard in Figure 3 would be enough for a top body such as a Security and Privacy Council (comprising the CEO, CFO, HR leader, and other business leaders) to determine the impact of the issues. The high-high, medium-high, and high-medium quadrants deserve the most attention. The size of the bubbles represents the number of incidents in a given period and can be drilled further to obtain insights into repeat instances and unaddressed vulnerabilities. CISOs/CPOs can generate reports, based on several fields captured in the incident reports, to drive decisions on policy matters and organization-wide special initiatives.

Adoption of a framework such as ISO 27001 (Information Technology – Security Techniques – Information Security Management Systems – Requirements),[1] over and above company-mandated security standards, assists in adopting industry best practices as the internal team engages with external consultants. Client-mandated compliance to such frameworks as HIPAA and the PCI data security standard helps the BPO organization focus on specific vulnerabilities. Certification to PCI, for example, provides a financial safe harbor in case of a breach.

While issues of awareness and understanding are addressed through education within the BUs and disciplinary actions meted out by HR, instances in which employees deliberately beat the system are cause for concern. Bringing these incidents before a top forum can help drive policy changes in the enterprise. For example, widespread instances of disclosure of sensitive information via open Internet mail or chat tools could result in restricting Internet access and availability of collaboration tools.

If implementation of preventive controls is not possible, then behavior needs to be molded so that employees do not perform activities that result in breaches. It is

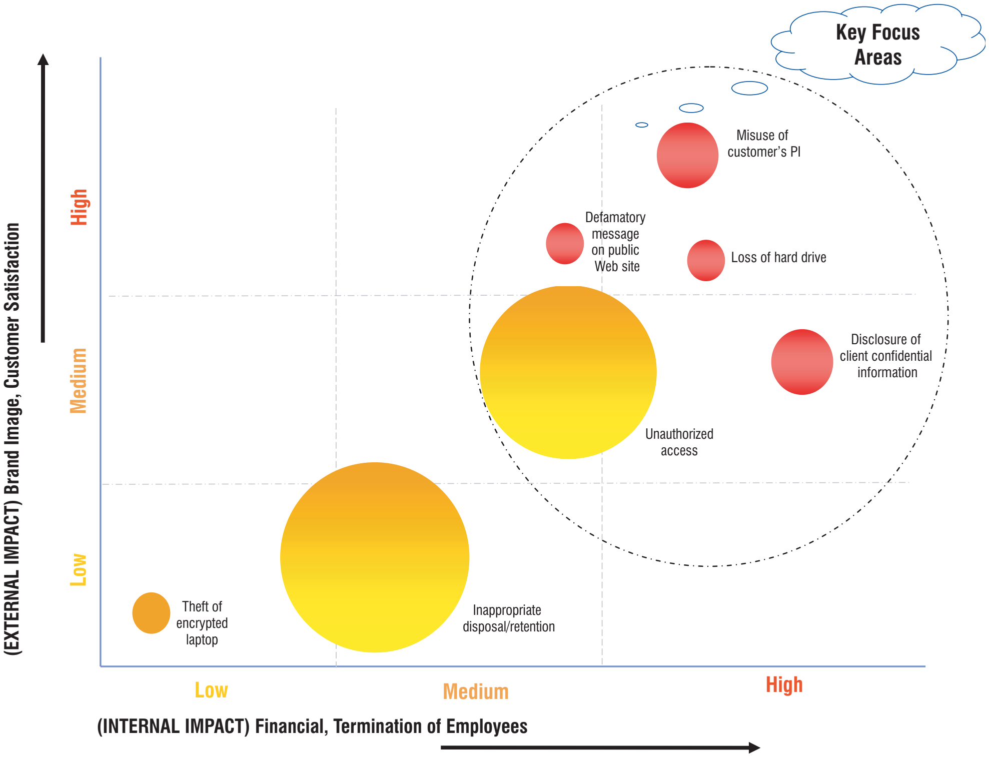


Figure 3 — Impact of incidents measured as external and internal to the organization.

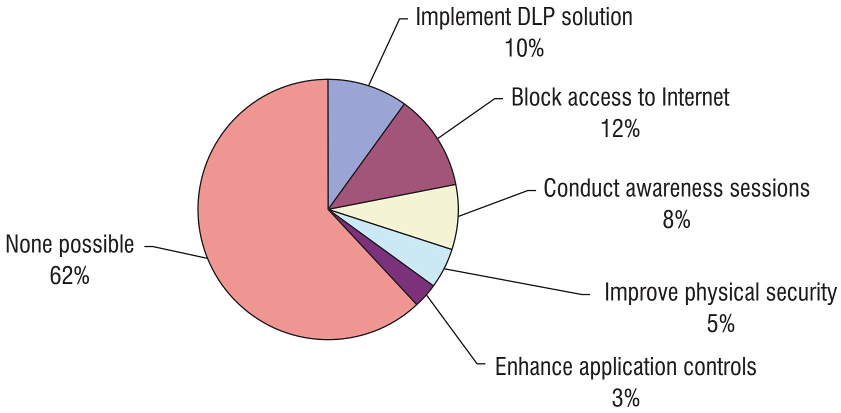


Figure 4 — Percentage of incidents that may be prevented by implementation of internal controls.

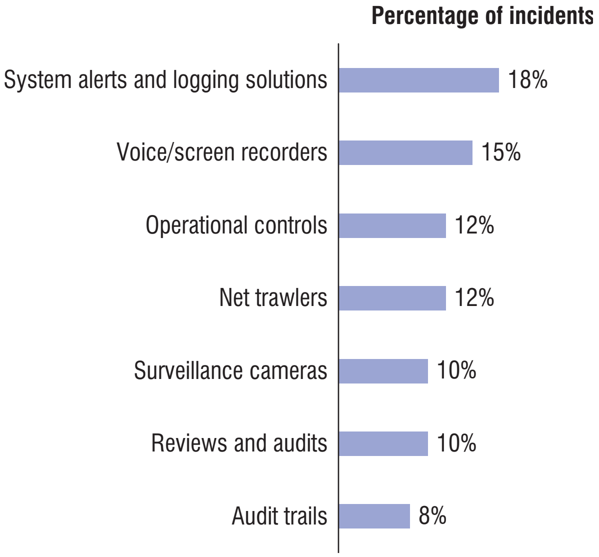


Figure 5 — Percentage of incidents that may be detected by implementation of specific controls.

well known that behavior is driven by motivation. Motivation to perform unacceptable activities must be reduced or offset by disciplinary actions that act as inhibitors and deterrents. Disciplinary actions and communication campaigns can be tailored based on incidents and root cause findings. For example, if open Internet is required for agents to perform their daily tasks, then awareness and training must be imparted on a regular basis. Dos and don'ts must be emphasized, along with disciplinary actions in case of a nonconformance to acceptable practices.

The CISO/CPO can obtain buy-in for special initiatives, such as implementation of content filtering or data leakage prevention (DLP) tools, by performing a what-if analysis on the incidents (see Figure 4). The enterprise dashboard shown in Figure 3 could look very different if these tools had been implemented. Comparing the cost of these tools with the cost of a security or privacy breach and extrapolating it over three to five years presents a solid case for the tools' ROI.

The cost of a security breach can be computed by summing the:

- Cost of resources used to investigate the incident, take actions, and track to closure
- Expenses and financial penalties, if any
- Cost of losing skilled resources (in the case of termination)[2]

While it is true that preventive measures are better than detective ones, there are times when prevention is not possible, either because of high cost or due to constraints in technology or environment. Detective controls then assume importance, as they provide early warning signals and could prevent wide-scale damage. Investment in appropriate tools, such as enterprise logging solutions and voice/screen recorders, can facilitate investigation and forensics (see Figure 5).

Business Unit (BU) Dashboards

Some incidents and issues are more significant at the BU level than at the enterprise level. Specific kinds of issues may be observed in a particular BU and not in others.

While the dashboard in Figure 6 compares two BUs in an enterprise, the one in Figure 7 provides an insight into the root cause (human factors) for one of the BUs. A large percentage of incidents occur due to lack of awareness or understanding. Education and sensitization can reduce such incidents to a large extent. Presenting these statistics to the business leaders in monthly review forums encourages adequate action.

Establishing a culture of sensitivity to security and privacy is easier when line management takes ownership of this issue. One of the most effective means of fostering such a culture is a hub-and-spoke model. The central specialist team creates the content of an awareness program based on organization-wide learning. Line management can then tailor it to suit specific needs within their own areas.

Using Dashboards to Improve Controls in the Client Environment

While a BPO firm can take some measures across the enterprise, and BPEs can take measures within their areas of influence, sometimes it becomes important to involve the client, as their environment and operational processes may have weak controls. In many third-party BPO firms, agents work on an extended client network and access the client's applications using Citrix. These are typically legacy applications and not designed for outsourced processes. Consequently, they may disclose more information than necessary. For example, a screen may show the entire credit card number even though it is not required by the agent for the services he or she provides. In addition, more privileges may be provided than required, the process of ID/access management may be weak, and daily operational reports may be insufficient to track sensitive transactions. There may also be limited audit trails. An open Internet environment compounds the risks further. Lack of awareness of security and privacy requirements may lead to unauthorized disclosure.

Interesting observations will be revealed when data for a particular client is extracted from the incident database. These will be particularly significant in processes where agents work on the client's environment, leaving the third-party BPO firm with little flexibility in implementing preventive mechanisms at their end.

It goes without saying that in order to do any analysis, the data fields must be accurately populated by the investigation team's findings. If a client environment has been exploited multiple times, a chart such as the one in Figure 8 will highlight incidents that may have been prevented had the client implemented appropriate controls. The field "Recommendations — Preventive (Client)" (from the incident report) can be mined for this purpose. The chart in Figure 8 is based on an example in which 40 incidents were reported for a client in a given period. Out of these 40 incidents, five would have been prevented if the Internet had been blocked, six if a DLP solution had been implemented, four if applications had been strengthened, and 10 if ID and access

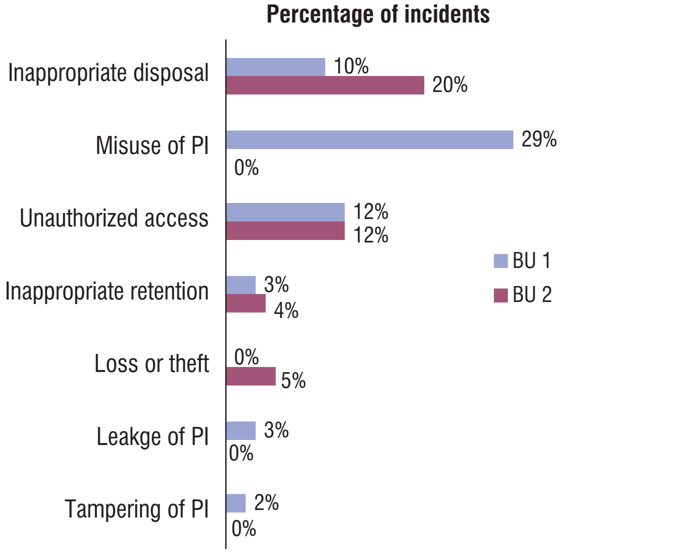


Figure 6 — Distribution of the types of privacy incidents by BU.

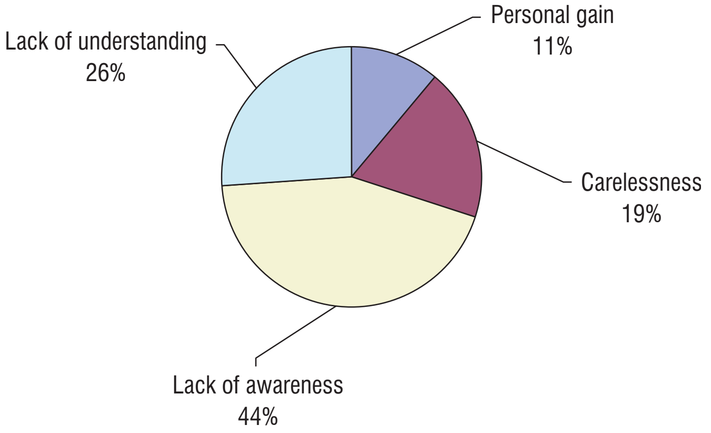


Figure 7 — Reason why incidents occurred in a BU (human factors).

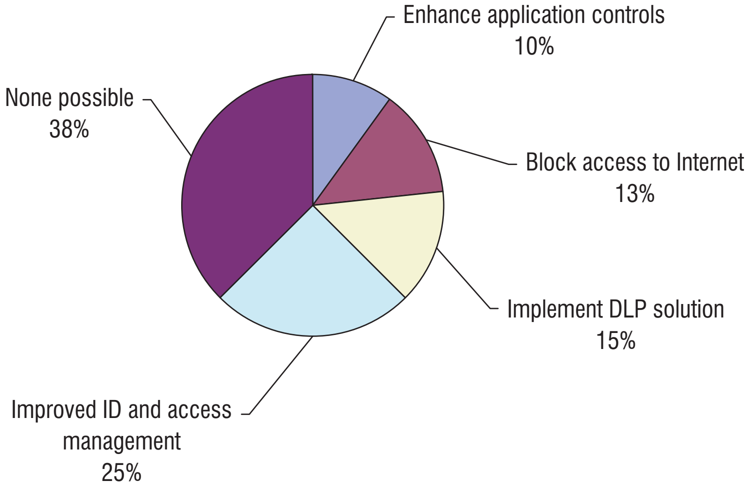


Figure 8 — Percentage of incidents that may have been prevented by implementing preventive controls on the client end.

management procedures had been improved. That leaves 15 incidents that could not have been prevented by implementing any control at the client end.

A chart such as the one in Figure 8, coupled with financial data on the cost of each incident, helps justify the need for tighter controls on the client end. If the client accepts the data and implements the recommended controls, it will drive down the risk not only for the client but for the entire integrated enterprise (i.e., for the client and all the vendors to which the process has been outsourced).

CONCLUSION

The approach that a CISO/CPO adopts with senior executives largely determines the success in adopting secure work practices as well as securing budgetary approvals for security tools, enterprise policies, and special initiatives. Dashboards derived from incidents are most compelling, as they are based on concrete historical data, leaders can relate to them, and the costs cannot be disputed or challenged.

If BPO organizations hope to meet the security and privacy challenges they face, business units must go from being reactive to being responsive, and ultimately proactive. A responsive BU will take actions based on the results of internal reviews and external audits to improve their controls posture. The executives in these units will work with their internal teams as well as client executives to strengthen controls, promote awareness, and actively drive policy changes. As BPEs improve their understanding of the sensitive data handled by their agents, vulnerabilities in their own processes, and exposures in client platforms, they should be encouraged to conduct security and privacy self-assessments. This transition will be gradual but very rewarding. BPEs will be seen to drive changes in their own spheres of influence through a bottom-up approach. This truly epitomizes a proactive organization, in which practitioners themselves uncover flaws, identify solutions, and implement the most viable controls. Changes across the enterprise will still require a discussion at the top level; however, localized issues will get addressed faster in a proactive organization.

The need of the hour is for organizations that are fully geared to handle sensitive information. To have a meaningful and a long-term relationship with their clients, BPO firms must become the "trusted" partner of choice.

ACKNOWLEDGMENTS

Working with my team and colleagues in IBM/IBM Daksh has provided me with tremendous insights into information security and privacy issues. I am particularly glad to have had a tech-savvy CEO who backed my numerous budget requests and gave me a free hand to implement security controls and shape the posture of the organization. My team humored most of my whims, believed in me, executed very aggressive projects, and made me proud of their individual, as well as collective, achievements. Nivedita Malhotra and Rishi Rajpal have been my strength and support as we built this function literally from scratch in IBM Daksh.

ENDNOTES

[1] See www.iso.org/iso/catalogue_detail?csnumber=42103.

[2] A breach will also likely have a negative impact on the BPO firm's brand and customer satisfaction. Yet such losses are intangible, and it is difficult to put a value to them.

Nandita Jain Mahajan is Chief Privacy Officer and VP – Information Security, Compliance & Business Continuity of IBM Daksh. Her responsibilities include formulating privacy, information security, and business continuity strategies; seeing to their execution; operationalizing processes; and driving down organizational risks. Ms. Mahajan began her career at the University of California–Berkeley, USA. Over a career spanning 23 years, she has played various IT leadership roles. She worked with organizations such as Tata Consultancy Services (TCS), American Express, GE, and Fidelity Investments before moving to IBM. Her experience in business process outsourcing started with American Express in India in 1997. Working in IBM Daksh has given her exposure to a large third-party BPO firm that provides services to many Fortune *100 clients.*

Ms. Mahajan holds a BSc degree from St. Stephen's College in New Delhi. She also holds MS and MBA degrees from Ohio University (Athens, Ohio, USA). Ms. Mahajan is a Certified Quality Analyst, having led two organizations to CMMi Level 5, as well as a Certified Information Security Manager. She is the coinventor of IBM's Voice Masking technology and has been the recipient of the Microsoft Security Strategist Award for displaying excellence in security leadership in the IT/IT enabled service (ITeS) area. Ms. Mahajan can be reached at nandita.jain.mahajan@dc.ibm.com.

Advancing Security and Privacy Through Collaborative Risk Management

by Ron Woerner

One of the basic human needs is to feel secure. This need is subjective, based on perception and intuition. How do we judge if we're safe and secure? Through basic, instinctive risk management principles. We weigh without thinking the probabilities and impact of an event, determine ways to reduce the risk, and then base our decision on that quick calculation. Animals do it all the time. Risk management is one of the basic learning principles developed at an early age. With weightier decisions, we will ask others for their opinion to gain further insight and detail before making our decision. This is collaborative risk management (CoRM), a process that links people in the identification, assessment, analysis, and mitigation of events that affect our world.

CoRM establishes a trusted environment built on a set of principles, processes, methods, and tools that enable the customer (the business) and supplier (the security and privacy groups) to work together cooperatively, continually managing risks throughout the lifecycle of a project, technology, or system. It's built on a foundation of the age-old principles of risk management and the philosophy of collaborative teams. It is critical that these teams work together to ensure that personally identifiable information (PII) and other critical or sensitive data are properly protected. The end result is the appropriate reduction of risks to ensure compliance and continual improvement at all levels of the organization. This is a requirement whether you're in the IT, security, privacy, or compliance area.

Common security and privacy problems occur when we lack the information necessary to make a decision, or when we believe that the risk is less than it is. These situations cause organizational managers to make business decisions that may increase the probability of a breach of sensitive data or exposure of PII. The low risk-intelligence level of many in our organizations increases the impact, probability, and costs of security and privacy breaches. In turn, this damages the reputation and revenue of the organizations in question or puts them in regulatory jeopardy.

The only way to ensure the security and privacy of PII is to develop a risk management approach among the information security, privacy, and IT groups and their customer: the organization or business. CoRM is such an approach, and it leverages positive collaboration and communication, focusing its actions on risks to the business. In this article, I will show you how to use CoRM in your organization to identify, assess, and properly respond to risks.

IN A NUTSHELL: RISK = IMPACT x PROBABILITY

In its most basic form, risk management is simply the impact of an event combined with its likelihood weighed against the costs of mitigation:

RISK = IMPACT x PROBABILITY | COSTS

In viewing the relationship of risks to costs, I used ratio (|) rather than "divided by" (/) on purpose. The statement above is not a true mathematical equation, but rather a weighing of risks against potential costs. This is the equation our brain uses unconsciously and naturally. Rather than complicating things with a difficult risk equation, I believe simplicity brings acceptance.

As I've said, humans and all animals use this equation instinctively in their decision making. It's a basic ROI formula used to understand the repercussions of actions or inactions. When I asked an HR VP about a privacy risk affecting our employees, she instinctively used this formula without any prodding from me. She asked:

- "What are the repercussions?"
- "How likely is it to occur?"
- "What's the cost to mitigate the risk?"

With the answers to those questions, she was able to quickly make a decision and set a course of action that was best for the business.

Impact is the effect on the organization should the risk occur. It answers the question, "How bad is the result of the risk?" Consider the dollar cost, the reputation cost, and the people cost when determining the impact level of the risk. While you can use actual dollar values for impact, I do not recommend it, because it adds complexity. It's best to estimate the damage felt by the organization both during and after the risk event. I recommend using a 1-5 scale where 1 is low and 5 is high.

Probability is the likelihood the risk could occur within a given time frame; it's the prediction of the risk event's odds based on previous experiences. This element becomes complicated when you add in the mitigations already in place that reduce the likelihood of the risk event. Base your judgment on the current state (i.e., "How likely is the risk event to occur today?") rather than on an anticipated future. Like impact, probability should be estimated using a 1-5 scale.

The cost element is the amount of dollars and time it takes to mitigate the risk (i.e., reduce the risk to an acceptable level) through risk reduction, insurance, or transfer. The costs are what you plan to do, not what has already occurred to reduce the risk impact or probability. Costs are often the balance point that helps you determine how to handle the risk.

Although this calculation is seen as a mathematical equation, it's really a qualitative measure. In most security and privacy cases, impact, probability, and costs are subjectively based on a 1-5 scale where, again, 1 is low and 5 is high. In the interest of simplicity, it's best to use this approach rather than force the user to develop actual impact amounts, probability percentages, or dollar costs. Most experienced professionals will be able to accurately rate impacts, probabilities, and costs using a 1-5 scale. This approach also helps when discussing these issues with business leaders and IT administrators. Rather than waste time debating a specific dollar impact, cost amount, or probability percentage, it's easier to come to a consensus when using a simpler scale.

Risk leaders should use the risk equation (RISK = IMPACT x PROBABILITY | COSTS) for each individual risk in order to develop the organization's complete risk picture. Once this is done, it's easy to prioritize risks based on the rank. You can also chart the risks as shown in Figure 1.

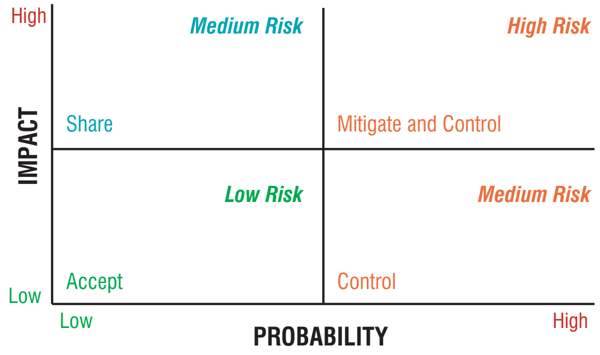


Figure 1 — Impact and probability chart.

CoRM STEPS

Security and privacy leaders can achieve collaborative risk management by following the steps outlined below.

1. Be a Leader

Like security and privacy initiatives, CoRM can't be pushed from behind. It takes someone willing to get out in front and take charge of the program. This person must have the authority to call out the risks, assess them, have decisions made, and take actions. This person doesn't have to be an expert in security and privacy, but he or she should have an understanding of the relevant philosophies and concepts.

For the sake of argument, let's say you are the designated leader of collaborative risk management in your organization. As CoRM leader, you need to be able to facilitate discussions so risks can be honestly addressed. This means bringing different groups together from around the enterprise. Obviously, this also means that you need the authority to make these conversations happen. Without it, as security experts Simson Garfinkel and Gene Spafford have observed, "You're just there to take the blame when something goes wrong."[1] The other danger posed by lack of authority or interest by business units or IT groups is that the risk picture will be incomplete. Risks associated with areas or groups that don't participate will be missed, thus increasing the overall risk to the organization.

It also takes leadership to make decisions. As Rush frontman Geddy Lee put it, "If you choose not to decide, you still have made a choice." It's often the decisions that aren't made that are the greatest organizational risks. In CoRM, all types of risks must be on the table. This is not to pick on one group or another, but to ensure the organization can thrive with its risks identified, assessed, and mitigated.

The CoRM leader is also responsible for determining and understanding the organization's risk management maturity level. To reach the vision and benefits of CoRM, the organization's current risk management activities must be understood. You do this by answering the following questions:

- How does the organization address different risks?

- Who or what areas use risk management in their decision making?
- What risks have already been identified, assessed, and/or mitigated?
- Are there any formal processes within the organization for risk management?
- How are risks identified, measured, or documented?

The answers to these questions allow you to map the course of action from where you are in terms of risk management to where you want to be.

Last, you need to define roles and responsibilities. Who will be responsible and accountable for the different risk areas, including security and privacy? This requires a thorough grasp of the organizational structure, not recreating the wheel.

2. Know Your Assets

You can't protect the things you don't know about. In this step, you as CoRM leader will identify and classify the assets. You should gauge the value of each asset to the organization and document it. Answering the following questions will help you evaluate the risks to each asset:

- How important is the asset to the organization?
- Who uses the asset (internally and/or externally)?
- How is this asset used by the organization, its associates, and/or its customers?
- Is there a cost if the asset is compromised or unavailable?
- What are the threats to the asset?

You should initiate this activity by identifying the assets that are the most critical to your organization — the one or two applications or systems that the organization cannot live without. That will give you a baseline for developing your process for asset discovery and provide a quick win. Once the first few are complete, move to others based on priority to the organization or top decision makers. The information gathered should be captured in a configuration management database or asset list. This information is dynamic, so schedule periodic reviews or have it automatically updated.

Rarely will a CoRM leader be able to gather this information for all assets in the organization without assistance. This step requires collaboration with all of the business units in order to develop the complete asset picture. Once an asset is initially identified, you should talk with all interested parties to discover their perspectives on the asset, its value, and its potential risks.

3. Assess Risks

This step is the start of traditional risk management. It's the point where you determine the risks, threats, vulnerabilities, and exposure points for each asset. Here you will use the risk equation stated above to classify the risks not only to the assets, but also to the organization.

To identify the security and privacy risks at a high level, I like to ask two questions:

1. What are the two or three events with the highest impact to the organization?
2. What two or three events are most likely to occur?

This information provides a starting point for risk identification by providing a small number of high-risk events. This approach is not perfect, as it depends on the experience, knowledge, and perspectives of the assessor. It also permits the introduction of "pet" risks. However, it's meant to serve as a foundation on which to base future CoRM activities.

Threats and vulnerabilities are risks and therefore should be treated as such in this process. Don't rely on your own knowledge to capture all the threats and vulnerabilities that could affect assets. Talk with others with a vested interest in protecting the security or privacy of the various assets. The output of this step is the creation of a list of threats and vulnerabilities either to a single asset or groups of assets. The risk management resources shown in the sidebar (see p. 32) contain common threats and vulnerabilities that can get you started in creating your own list.

Identifying existing security and privacy controls is the next step in the risk assessment. These are systems, programs, or processes that limit the impact or likelihood of a security or privacy breach. Controls may also provide a protection mechanism for assets against threats or vulnerabilities. Examples include firewalls/IDS/IPS, access controls or permissions, encryption, logging and monitoring, antivirus applications, and data leakage protection (DLP). Controls may also be nontechnical, including policies, procedures, and user awareness training. All controls should be listed for reference during the risk classification.

With the threat, vulnerability, and control lists, you can begin to populate your risk matrix. Table 1 provides an example. You can use a risk matrix or a governance, risk management, and compliance (GRC) application to document each risk; its impact, probability, and cost; the

RISK MANAGEMENT RESOURCES

Alberts, Christopher, and Audrey Dorofee. "An Introduction to the OCTAVE Method." Software Engineering Institute (SEI)/Carnegie Mellon University, 30 January 2001 (http://www.cert.org/octave/methodintro.html).

Bernstein, Peter L. *Against the Gods: The Remarkable Story of Risk*. John Wiley & Sons, 1998.

Enterprise Risk Management — Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission (COSO), September 2004.

"General Security Risk Assessment Guideline." ASIS International, 2003 (www.asisonline.org/guidelines/guidelinesgsra.pdf).

IT Risk Management Report, Volume 1, Trends through December 2006. Symantec, February 2007 (http://eval.symantec.com/mktginfo/enterprise/other_resources/ent-it_risk_management_report_02-2007.en-us.pdf).

IT Risk Management Report 2: Myths and Realities, Trends through December 2007. Symantec, January 2008 (www.symantec.com/business/theme.jsp?themeid=itrisk_report).

Kissel, Richard, Kevin Stine, Matthew Scholl, Hart Rossman, Jim Fahlsing, and Jessica Gulick. *Special Publication 800-64: Security Considerations in the Information System Development Life Cycle*. National Institute of Standards and Technology (NIST), October 2008.

Macaulay, Tyson. "Operational Risk and Resiliency Frameworks." *CSO*, 30 October 2006 (www.csoonline.com/article/221063/Operational_Risk_and_Resiliency_Frameworks?page=6).

"Risk Management FAQ." SEI/Carnegie Mellon University, 2009 (www.sei.cmu.edu/risk/risk.faq.html).

Risk Management Handbook, Risk Analysis Guide, and Repository. Security Officers Management and Analysis Project (SOMAP) (www.somap.org).

"A Risk Management Standard." AIRMIC, ALARM, and IRM, 2002 (www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf).

Ross, Ron, Marianne Swanson, Gary Stoneburner, Stu Katzke, and Arnold Johnson. *Special Publication 800-37: Guide for Security Certification and Accreditation of Federal Information Systems*. National Institute of Standards and Technology (NIST), May 2004.

"The Security Risk Management Guide." Microsoft, 15 October 2004 (www.microsoft.com/technet/security/guidance/secrisk/default.mspx).

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Special Publication 800-30: Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology (NIST), October 2001 (http://csrc.nist.gov/publications/nistpubs/index.html).

USAF Software Technology Support Center. "Risk Management." *CrossTalk: The Journal of Defense Software Engineering*, February 2005 (www.stsc.hill.af.mil/crosstalk/2005/02/index.html).

Table 1 — Risk Matrix

Risk Name	**Risk Description**	**Impact** (1-5)	**Probability** (1-5)	**Cost** (1-5)	**Overall Risk** (Impact x Probability | Cost)	**Risk Decision**	**Risk Owner**

overall risk score; the decision on how to handle the risk; and the person responsible for owning the risk. This table's simple design increases both its usefulness and usability. You can use a risk matrix to capture risks associated with individual assets or risks that affect multiple assets, systems, data sets, or processes.

Start populating the risk matrix by listing a general name for each risk along with a brief description. Use the threat and vulnerability list as well as the answers to the two risk assessment questions above to populate your list of risks. The idea here isn't to list every single possible risk, but just the ones that concern you or others in your organization. For example, a tsunami isn't a risk in the midwestern US, but it is in Pacific Rim countries.

For each risk, you need to estimate the asset exposure and the likelihood of occurrence. This requires collaboration and should not be done in a security or privacy vacuum. You can use the list of controls developed earlier to better define the risk's impact and probability score, as such controls will most likely provide a reduction factor. Perfection in developing the matrix is not required; refinement is always possible in future reviews. In CoRM, consensus is more important than exactness.

At this point, you can assign the risk owner. This is the person who is responsible for the risk or has a vested interest in its mitigation. If you have trouble identifying the risk owner, ask, "Who owns the headache" if this risk were to materialize? This will pinpoint the person who has the largest interest in determining the mitigation course for the risk. As CoRM leader, you should ask the risk owner's opinion as to how to rank the impact and probability for each risk.

A common risk today concerns regulatory compliance. While many don't see compliance (or rather, the lack thereof) as a risk, it is. A business can choose not to be compliant with a regulation, law, or standard, but it does so at the risk of fines and/or lawsuits. Therefore, compliance-related risks should be mapped in the risk matrix just like any other risk.

Continue this process for each identified risk. Don't work on any of the other elements in the risk matrix. It's more important to complete the list of risks, their impact and probability, and their owner. If you move ahead too quickly, you're in danger of missing risks or focusing on pet risks. It's better that the list be too big than too small. The risks I worry about the most are the ones that I miss.

4. Conduct Decision Support

Once you identify the risks and categorize their impact and probability, you need to work with the risk owners and other decision makers on what to do about them. This step takes the information collected and processes it to determine the appropriate course of action for the organization. Talk with the risk owner and any other affected business groups to determine whether to avoid, reduce, transfer, or accept each risk. Each option has a cost.

The risk mitigation cost is ranked on a scale of 1 to 5, because even cost can be relative. You need to address the cost in terms of dollars, time, and opportunity lost. Any accepted risk has a low or zero cost and is therefore listed as a 1. Other costs should be rated based on the cost to the business. When using this scale, it's critical that you develop a standard that's right for your business and consistent across the risks.

The overall risk is written as a ratio with the value of the impact times the probability on the left side and the cost on the right. For example, if the risk impact and probability are both moderate (3x3) and the cost is low (1), then the final overall risk would be listed as 9|1. You can also list multiple risk mitigation costs in order to assist in deciding risk mitigation or reduction steps.

Decision makers can use the overall risk score to assist in prioritizing the risks and deciding on appropriate mitigation techniques. High risks with low costs will stand out as "low-hanging fruit" that can be easily fixed. Low risks with high costs may be ones you want to accept rather than incurring the costs to mitigate them. You can also use the impact and probability chart (see Figure 1) to map each risk in order to determine the appropriate course of action.

Last, it's critical to note that risk decisions are usually not for the CoRM leader but for a business leader to make. Often security and privacy personnel are asked to accept risks. It's not your call unless you own the asset or are the owner of the risk. Risk decisions are business decisions based on the needs of the business versus the costs of risk mitigation or acceptance.

5. Implement Controls

Once the decisions are made, they need to be acted upon. It is the risk owner's responsibility, but he or she may collaborate with the security or privacy group. This can be done in a phased approach, based on the cost of the risk. As the leader of the CoRM effort, you should address those risks that are easiest or least costly to mitigate in order to get some quick wins.

Risks are rarely mitigated overnight. Security is a journey. You never reach the destination of being "100% secure," but you should still journey toward the goal.

6. Measure Program Effectiveness

Metrics and measurements are an important part of any security and privacy CoRM program. They allow leaders to view the program's effectiveness and efficiency. The risk matrices are beneficial for creating metrics charts of risks within systems or applications (local risks) as well as between them (global risks). You can leverage these metrics to show progress toward your goals and the value of your security and privacy program.

7. Rinse and Repeat

Risk management is an ongoing program, not a project. It has no definite end because risks never cease. In our ever-changing world, there are always new ones. Risk matrices are dynamic and should be updated as new risks arise or as new mitigations are put in place. Adjustments and reevaluations of the risks and costs should occur whenever changes occur to applications, systems, or business processes. A new threat or a vulnerability announcement is another cause to readdress a risk.

PRACTICING COLLABORATIVE RISK MANAGEMENT

Collaborative risk management is new territory for IT, security, and privacy professionals. In its implementation, you may encounter the following challenges:

- **No leadership support.** In order for any cross-organizational endeavor to be successful, you need support from upper management.
- **Lack of universal participation.** IT groups and business units may not see the value of CoRM and may not want to partake in the risk assessment.
- **"Not-my-job" mentality.** Some people think that security and privacy are only the job of those groups and that they have no part in it.
- **"Throw-it-over-the-wall" communications.** Successful CoRM implementation requires you to meet either face-to-face or on the phone with decision makers. You can't rely on e-mail or other methods to throw issues over the wall.
- **Started, but not maintained.** The CoRM program must be sustained. It's not a short-term fix. The list of risks needs to be periodically reviewed and updated.

To be successful with CoRM, you should leverage the following techniques:

- **Engage the whole organization.** Align risk management fully with objectives in all policies, plans, and operations affecting security and privacy. Aim for universal participation, in which everyone is engaged in security and privacy.
- **Enable people with processes, tools, techniques, and authority.** Don't just tell them to "be secure" or "protect personal data." Show them how and give them the tools to make it happen.
- **Consult and communicate with all stakeholders** throughout the process and the organization. It's better to overcommunicate than undercommunicate. Every meeting should be a coaching opportunity for security and privacy.
- **Sustain the initiative by building a supportive culture and processes** that develop participation, trust, and swift action on issues. Once you get it started, you need to keep the initiative going with constant care and feeding.

CONCLUSION

> You can either take action, or you can hang back and hope for a miracle. Miracles are great, but they are so unpredictable.
>
> — Peter F. Drucker

No organization is 100% secure or compliant, and personal information can never be kept 100% private. Perfection in those areas is impossible, but it isn't required as long as the risks are identified, weighed, judged, and acted upon to the level that's best for the organization. The key is finding the right balance of security, privacy, and compliance for your organization and having the right amount of protection when, where, and how it is needed. This balance cannot be found in a security, privacy, or business unit silo. These groups need to work together to find that protection "sweet spot." Too much is restrictive, while too little puts the organization in jeopardy. The way to ensure the right risks are addressed is through collaborative risk management.

Collaborative risk management is a simple way to positively protect the security and privacy of your organization, its customers, and its critical data. It provides a technique for identifying, documenting, and analyzing conditions that can put your organization in jeopardy by bringing together groups with a vested interest in protecting their assets. While it's not perfect, it doesn't need to be. Security and privacy endeavors are journeys, not a destination. We won't ever get there, but I hope you'll see that CoRM gets us a step closer.

ENDNOTE

[1] Garfinkel, Simson, and Gene Spafford. *Practical Unix and Internet Security*. O'Reilly & Associates, 1996.

Ron Woerner is a noted speaker and writer in the security industry. He is currently a Security Manager at a well-known online brokerage. He has 20 years of experience in IT and security and has worked for ConAgra Foods, Mutual of Omaha, CSG Systems, and the US State of Nebraska. Mr. Woerner earned a BS from Michigan State University and an MS from Syracuse University. He was awarded the CISSP, Certified Ethical Hacker (CEH), and Toastmasters Advanced Communicator and Leader designations. He loves to talk to others who are passionate about security and privacy. Mr. Woerner can be reached at ronw2007@gmail.com.

Identity 3D3C: Confronting the Security and Privacy Challenges in Virtual Worlds

by Yesha Sivan

Virtual worlds are an emerging medium that is constantly creeping into the enterprise.[1] Following the huge success of such gaming worlds as World of Warcraft, The Sims, and others, terms like 3D, avatars, chat, and real money are rising from the marketing department, operations, and product development. The drive to save travel costs and the need to gain new customers and retain current ones push this trend even further.

Before I go any further, I should explain what I mean when I write about virtual worlds. To distance virtual worlds from the gaming worlds, I use the adjective "real," which hints at a much more far-reaching potential. I've also coined the term "3D3C" to indicate that a real virtual world is an aggregate of four factors:[2]

1. **A 3D world.** A virtual world is a dynamic world, where viewers see such objects as avatars, houses, and cars. The world has land, a sky, a sun (or maybe more than one), wind, gravity, water, and fire. Avatars move around freely, and the user can examine the world from different points of view.

2. **Community.** Virtual worlds allow users (via their avatars) to meet, chat, shop, watch performances, hang out with friends, team up to fight bad guys, go clubbing ... or in other words, to interact in countless ways. Within "community," I include related concepts such as groups, permissions, rights, and roles.

3. **Creation.** The greatest technological achievement of Second Life (SL) was giving users the capability to develop their own objects. Users can simply move preconstructed objects from one place to another (say, to furnish a home or set up a nightclub), or they may assemble an object (e.g., a house) from basic components such as walls and ceilings and then "paint" them with various textures. SL's programming language, Linden Script Language, even allows users to program behavioral attributes for their objects, so that fish can swim in schools, golf balls can arc through the air, guns can shoot, and people can dance.

4. **Commerce.** SL's maker, Linden Lab, has created the Linden Dollar (L$), which has a defined exchange rate with the US dollar (one US $ fluctuates around L$260). The economics of the SL world is based on this currency. Within the Linden Dollar Exchange, you can exchange L$ to US $ immediately and at any time. For instance, if you earn L$2,600 from tips, you could exchange them for about US $10, which would be immediately transferred to your real PayPal or bank account. Going the other way, if you need L$6,000 for a new car, you could immediately buy them for about US $20. Nor is SL the only virtual world with a thriving "real" economy. The Entropia Universe also has a cash-based economy (with a fixed rate of 10 "PED" to one US $), and its maker, MindArk PE AB, has even received preliminary approval for an actual banking license by the Swedish Finance Supervisory. This would allow its users to conduct real-world banking transactions from within the Entropia Universe.[3]

IDENTITY IS THE KEY

Initial enterprise uses of virtual worlds include collaboration (internally and externally), product design and feedback, marketing of products, participation in virtual shows and exhibitions, and — with growing intensity — general experimentation. But while virtual worlds present new business opportunities, they also pose new IT threats:

- For faster access, virtual worlds use different ports and protocols than Web sites and thus present firewall issues.
- Some worlds allow code to run in them, which raises the risks of malicious code.
- When customers "chat" with an enterprise rep, they may reveal private information. Who stores this information, and how?

- Some worlds allow video to be broadcast inside the world. Cameras left on can transmit to the outside world.
- Your brand and corporate image can spread virtually. Who will protect it?

The security and privacy issues raised by virtual worlds revolve around one key factor: identity. Over the last few years, I have been fortunate enough to initiate and participate in several efforts to develop standards for 3D3C virtual worlds.[4] Repeatedly during these efforts, such terms as privacy, authentication, trust, rights, tracking, security, and other related terms came up as a necessary core to virtual worlds. For the sake of brevity, my colleagues and I chose "identity" as the term to mark these related terms.

I want to share my own excitement about the societal value of well-governed identity.

As we started to survey these identity-related terms, we looked at the current state of IT in general and the Internet industry in particular. For example, the Internet Society's *Trust and the Future of the Internet* report[5] defined trust as a combination of reliability, security, privacy, and liberty, while the Center for Democracy & Technology outlined several privacy principles for identity in the digital age.[6] The goal of this article is to motivate IT professionals to elevate the thinking and action about identity to a higher level. Such identity thinking is relevant to both IT departments and IT research labs, to customers and suppliers, to senior and junior personnel. The promise of identity is simple: much better, safer, more adaptable, and cheaper service to clients. In this article, I want to share my own excitement about the societal value of well-governed identity.

There is good news and bad news on the identity front. First, the good news. There is a lot of research, work, analysis, ideas, and even standards regarding identity. Now the bad news: in most cases, we are still struggling with competing nonstandard systems in this field. Or, to put it more bluntly, as users we still have too many passwords, our data is lost from time to time, and we are besieged with spam (although less of it lately, thanks to smart social antispam managers, such as the ones Gmail employs). The current combined IT and Internet system lacks a comprehensive system of identity.

In the remainder of the article, I will discuss some of the challenges that call for a systemic approach to identity. My goal is to expose some of the problems we face with respect to identity and, I hope, to drive people to action. I do not claim to present a complete or even a balanced approach to identity, but I do claim — emphatically — that we need to think about identity and build it into the next set of Internet standards. Future virtual worlds (when they arrive) and worlds that are based on current Internet and IT technologies will benefit from such a systemic approach to identity.

IDENTITY CHALLENGES IN VIRTUAL WORLDS

Security of Audience

One of the common things you do in virtual worlds is talk with other avatars. Talking ranges from simple instant messages (IMs), much like the ones we are familiar with in such services as Yahoo Messenger, ICQ, and Microsoft Messenger. Chat is an extension of IM. With chat, many avatars can gather around the fire, in a classroom, or in a meeting room and talk together about their favorite topic. Some virtual worlds also add voice, so several avatars can sit in a meeting room and talk to each other in both text and voice. With some advance setup, video can be added.

These meetings are touted as the next collaborative environment. Note that in SL, after you rent a US $5-a-month parcel of land, such conversations are free to as many as 40 avatars — in theory, anyhow. In practice, more than 25 avatars often stall the system. Still, having audio conferences with projection of 2D and 3D models for such low cost seems valuable.

The problem is, such discussions are far from secure. Today, if an avatar wants to sneak in and listen to the discussion (text or voice), he can simply do this. Let's assume that the authentication is solved and each avatar has an authenticated person behind it. Nevertheless, it is possible to view public chats with relative ease (even if they take place in a closed meeting room), to listen to public voice chats, and to peek behind walls (you can act as a peeping Tom). The physical space gives you the illusion of privacy, which is often not the case. Only with a relatively complex setup may you block other users from your meeting place — and in most cases, you will need a larger landmass to do it (which will cost you around US $300/month).

Even if you block the interlopers from the area (called "red tape" in SL lingo), other avatars can still hear or see. This is a classic case where the links between permissions, authentication, and services were not built into the system. A better design (or perhaps simply paying attention to identity) would build a solution into the communication stack of the platform. I do believe Wonderland, Sun's supported open virtual world, does solve this by linking chat and voice protocols directly to identity.

Anonymity

One of the key drivers of virtual worlds today — and I emphasize *today* — is the ability to act anonymously. Since most worlds currently are used for entertainment, such worlds really act as an extension of games. Until recently, SL's makers glorified anonymity with such statements as "life beyond reality, where imagination knows no bounds ... tempt fate without inhibition and court danger without fear."

Yet at times we need to cross into the real. In May 2008, federal prosecutors in Los Angeles charged a Missouri mother with fraudulently creating a MySpace account and using it to "cyberbully" a 13-year-old girl who later committed suicide. The girl, Megan Meier, hanged herself in her upstairs bedroom two years ago, shortly after being jilted by an Internet suitor she thought was a 16-year-old boy. The case caused a furor in the US when it was alleged that the "boy" was actually Lori Drew, the mother of one of Megan's former friends. As this case shows, virtual worlds can be painfully real.[7] As more of these worlds become part of our lives, we need to educate ourselves about the dark sides of anonymity. Real virtual worlds are not a game — they are yet another part of life with all the good and the bad.

Another angle to the matter involves actual work, training, support, and medical treatment in virtual worlds. All have legal ramifications that call for identity. Teaching a course in SL, taking a test, and doing a joint project mean course credit and grades. Treating someone with Parkinson's or a stroke in the virtual world calls for insurance billing and medical records (which in turn means that personal information, medical records, and US HIPAA regulations are added to the IT headache).

Another side of anonymity is money laundering. Say you gained US $100 illegally. Now you give it to 10 avatars. These avatars buy from you a virtual car for US $10 each. You report an income of $100. It's that simple. You can even script the entire process and use programmable avatars to save you time.

We must also remember that some countries are not as free as others. If we kill anonymity, we kill the very limited freedom people in such countries may have. Virtual worlds affect the real world, and the real world affects virtual worlds. The famous case of Google altering search results to satisfy Chinese authorities is an example.[8] The challenge is determining how to preserve the value of anonymity while preventing its perils.

Virtual Goods

The gaming industry has had virtual goods for ages — all those swords, potions, ships, and houses you gain in the game and store in your inventory. Then we were able to put money into the game and buy even more goods, yet the flow of money was always from the real world into the virtual worlds. With the advent of SL (and later worlds like IMVU and Entropia), we can now take the money out. Say Dera creates a nice pirate ship (see Figure 1). He puts it up for sale. Jane likes it. She charges her credit card US $1 and gets about L$260.

CONVERTIBLE CURRENCY OR FUNNY MONEY?

While many consider the Linden Dollar real money, Linden Lab's Terms of Service tell another story:

> **1.4 Second Life "currency" is a limited license right available for purchase or free distribution at Linden Lab's discretion, and is not redeemable for monetary value from Linden Lab.**
>
> You acknowledge that the Service presently includes a component of in-world fictional currency ("Currency" or "Linden Dollars" or "L$"), which constitutes a limited license right to use a feature of our product when, as, and if allowed by Linden Lab. Linden Lab may charge fees for the right to use Linden Dollars, or may distribute Linden Dollars without charge, in its sole discretion. Regardless of terminology used, Linden Dollars represent a limited license right governed solely under the terms of this Agreement, and are not redeemable for any sum of money or monetary value from Linden Lab at any time. **You agree that Linden Lab has the absolute right to manage, regulate, control, modify and/or eliminate such Currency as it sees fit in its sole discretion, in any general or specific case, and that Linden Lab will have no liability to you based on its exercise of such right** [emphasis added].

So far, Linden has treated the Linden Dollar as a fully exchangeable currency, and I see no sign that it won't continue to do so. Nevertheless, *caveat emptor*.

Figure 1 — A sample pirate ship (©2008 by Dera Carter).

She transfers the money by selecting "buy" on the ship. The money is transferred to Dera. Dera asks to pull the money out, and it is transferred to his bank account in a matter of days.

Today, in SL each object has an owner and a creator. The creator selects a few parameters for each object: Copy (allow owner to create copies), Transfer (allow owner to transfer ownership), Modify (allow owner to change the object). But in fact the story is more complex, as each object may contain several objects that have their own parameters. For example, a modifiable object can include a scripted object that is not modifiable.

I distinctly remember one of my students submitting an amazing virtual motorcycle as a final project. This was a masterpiece — so much so that I suspected it was copied. Because SL stores both the creator of the objects (which can never change) and the owner of the object (which changes when you sell or give the objects), my teaching assistant and I were able to look at the creator field and discover that the student was indeed the creator. But after few weeks, we reflected further — could we *really* be sure he created the motorcycle? He could have given his password to another user. He could have used SL to add one more object (which he indeed created) to an existing motorcycle, then linked it again to "stamp" his name in the creator field. Now we were entering the field of copyright and ownership.

Rights (and more specifically, copyrights) of virtual goods are a hot topic. Hackers have circumvented SL's internal client to make illegal copies of objects and textures. One virtual goods merchant, Stroker Serpentine (Kevin Alderman in real life), decided to act and sued a thief (Leatherwood) who was appropriating his objects. Here's what Stroker says in one blog post in March 2008:[9]

> When Leatherwood was first confronted and served a cease and desist, he made it very clear that he was not going to stop because he felt that his anonymity would protect him. It was also painfully apparent that Linden Lab's policies would not halt his activities. Given the fact that he cherry picked our most popular and profitable product, we had to make a decision. Ignore it or address it legally.
>
> Leatherwood made mention in a well-publicized interview that he would never be found. He tried to throw us off his trail by giving false accounts. When he was confronted with the cease and desist in real life, he denied knowing anything about the matter. However, his real life friends were willing to testify to the contrary, since he had run to their home and used their IP addresses to continue his activities when the story broke. They were [angry].
>
> This issue came to light by the various IP addresses he had used to connect to Second Life. These friends were also willing to testify that Leatherwood carried a notebook of dozens of credit card numbers with him everywhere and used them to make online purchases.
>
> When Leatherwood refused to answer the claims against him, we were faced with the decision to mount a full case in federal court. A case that included transaction histories, both real life and Second Life eyewitnesses (many Second Life residents who were willing to testify in person btw). The statement of the Private Investigator would also have been included, where in one conversation he denied being Catteneo [his Second Life identity] and retracted it in another. Leatherwood's computer would have been impounded by the FBI and a subsequent examination would have been done by a forensic examiner.

This case, which was settled in US District Court, involved two important issues: (1) protecting the rights of owners of virtual goods, and (2) making Linden Lab lift the anonymity shield.[10]

Protecting rights becomes even a bigger issue when we think about moving the pirate ship Jane purchased from Dera from one world to another: Can Jane store the ship in her local machine or on another machine? How can this be done while not allowing multiple copies of the same ship? To protect the creator's rights, can we store a user "token" in the ship (with expiration)? Can we demand "always-on" operation to enforce digital rights management? Is this another parameter creators need to worry about?

Let's extend the realm of virtual goods to the area of multilayered marketing. In my opinion, one of the potential key features of future virtual worlds is allowing people to resell derivatives of virtual goods. In fact, IMVU has a structure for that. For example, you can buy mesh for a dress, then color it and resell it. The revenues from the sale will be split between you and the manufacturer of the mesh.

Finally, dealing with virtual money is a new challenge to the enterprise. Imagine doing a purchase order for virtual land (Are we in the real estate business?), renting models as salespersons (Should HR be involved in this?), or buying skins (Why do you need to pay for a skin?). Clearly, virtual world commerce will raise a host of issues for the enterprise to consider. Virtual goods propel identity into a new domain that mixes anonymity, rights, ownership, and freedom to move objects from one place to another.

Scams

SL avatar Prad Prathivi[11] has demonstrated how a classic scam can work in virtual worlds:

> [10:39] Imas Cammer: Hey baby! How was your day today?
>
> [10:40] Gull Libel: It was tiring, sweetie ... but I'm glad to be home and on Second Life with you :)
>
> [10:40] Gull Libel: And how are you, sweets?
>
> [10:41] Imas Cammer: Hmmm ... I have an RL problem. :(
>
> [10:42] Gull Libel: Oh, what's up?
>
> [10:42] Imas Cammer: You remember how I told you a few months back that my father died a few years ago, and that my mom still lives in Nigeria?
>
> [10:43] Gull Libel: I remember, baby. You've had it rough :(
>
> [10:44] Imas Cammer: Yeah :(Well, you remember when you told me how it's good for people to help people less fortunate than themselves?
>
> [10:45] Gull Libel: I remember baby ... and I'd do anything to help you :)
>
> [10:46] Imas Cammer: :)
>
> [10:46] Imas Cammer: When my dad left the bank he ran, he left quite a lot of money in a bank account in Nigeria, but my mom says she can't touch it unless she gets some help ... we'd be happy to share some of it with you if you can....

In SL, instead of some suspect e-mail landing straight in your junk folder, the scam presents itself in the form of an avatar. Someone has put work into making the avatar look pretty, and she starts up a relationship with a potential victim, grooming him over several weeks or months until a trust develops between them. The intensity of the interaction in virtual worlds enables users to build reputation. One truly sees the person, her house, and her actions. One is temped to trust.

And the scammers aren't always after your money. Sometimes, information is just as valuable to them:

> [07:21] Imas Cammer: I really feel a strong connection with you, baby — I'd love to call you sometime. What's your phone number?
>
> [21:32] Imas Cammer: Your Second Life name is nice, but I was wondering today what's your real name, baby?
>
> [16:01] Imas Cammer: I found something beautiful in a store today, and I'd love to send it you for your birthday, baby! What's your address?

How does this apply to the enterprise? For starters, people tend to be nice in virtual worlds, and often they encourage real-life courtesy. Imagine a bank teller getting some personal information from an avatar that is being escorted by another avatar — his or her friend. That's one potential leak. Or consider an avatar that keeps his bag in the office — a bag that was given as a present by a friend. Yet the bag is really a listener that can hear everything that is being said in the virtual office.

THE VALUE OF A SYSTEMIC APPROACH TO IDENTITY

Virtual worlds are gradually entering the enterprise scene. They serve as a place for collaborating inside the enterprise or with outside suppliers and customers, a place to try out new designs, a place to market goods and services, and even a place to sell them. Banks can start to offer services, hospitals can start to treat people, and firms may present their products and allow users to try them.

We are in the initial phase of virtual worlds, and the following identity-related issues need attention *now*, because they may have regulatory, technical, and/or legal ramifications:

- **Networks.** Currently, such worlds as SL call for nonstandard network ports. Often, SL does not work behind the firewall. (Some people overcome this block with tools that allow limited Web-based access to SL for presence and messages.)
- **Code.** Advanced virtual worlds allow code to run, and code that can run also means viruses, bots, and other hazards.
- **Group identity.** Is the fact that you are a member of a group considered private or not? Can other members of the group know about your membership? What about people who are not in the group or people that left or were kicked out? Since many firms start to manage virtual groups, personal information needs to be managed.

- **Tracking.** Imagine you have a virtual bank with a virtual semihuman/semiautomatic teller. It is in contact with a well-authenticated client avatar. Now you need to be able to get instructions from this avatar. She may chat in these instructions, she may send you an IM message, she may voice these instructions. The teller avatar (or avatars) will need to store and track these instructions.
- **Doing business.** Even more issues emerge when we consider business relations in virtual worlds. Identity is necessary when it comes to common business requirements such as contract enforcement,

ENTERPRISE IT TIPS FOR DEALING WITH IDENTITY IN VIRTUAL WORLDS

Here are some concrete tips for IT managers as they monitor and support their enterprise's exploration into virtual worlds. These tips relate to both needed general infrastructure and identities governance.

TO START:

- **Professional avatar vs. personal avatar.** Make sure employees make a distinction between what they do as employees or subcontractors and their private personal actions. Avatars collect goods, spend, and gain money; their actions are logged and stored. Make certain everyone knows that.
- **Any initial activity in virtual worlds should be logged.** Ask all employees to send you a short e-mail if they start using a new world. This has an effect on networks, and you'd better know about it in advance.
- **Get the needed individual infrastructure.** Running a virtual world on a relatively weak computer misses the entire point. Make sure your experiments are done with sufficiently robust computers (which usually means lots of CPU power, memory, and, most important, graphics cards).
- **Know your rights.** Educate people about the rights of the organization itself and of other organizations. Explain the nature of virtual goods and the Digital Millennium Copyright Act (DMCA).
- **Conduct periodic meetings to educate and gain insight.** Arrange for quarterly, monthly, or weekly meetings to collect ideas, notions, and lessons about virtual worlds and the needed organizational infrastructure.

WITH MORE ACTIVITY:

- **Users should log their actions.** Many of the chats and IMs can be stored for future reference in the user's local machine.[1] Such local logs should be duplicated to a central place for future reference and traceability.
- **Get the needed enterprise infrastructure.** With more activity, you will need to invest in and then manage infrastructure. In SL, for example, you will need to buy your own land, set up groups, and open merchant accounts in places such as XstreetSL (which is now an integral part of the Second Life system).
- **Follow unusual activity.** Is a computer running a script all night? It could be a legitimate store in a virtual world — or it could be a bot sending messages over HTTP. Delving into such anomalies will allow you to spot emerging troubles. Note that today firewalls and various security systems are not aware of such exploits.
- **Consider how virtual world activity affects other systems.** Consider how various regulations may relate to virtual worlds and how your customer relationship management (CRM) or supply chain management (SCM) system may need to include virtual worlds data.
- **Ask the organization how virtual worlds affect business functions.** Share ideas and insights with HR, sales, marketing, and product development about ways virtual worlds can/should affect their actions.

[1] SL has a simple feature to log user actions, and duplicating this log can be done with a simple script. Other worlds may need further tools to do this.

IBM GUIDELINES FOR EMPLOYEES

In 2007, IBM published a set of employee guidelines for virtual worlds.[1] They represent a good set of general and identity considerations:

> These Virtual Worlds Guidelines for IBM employees have been created … to address the some of the choices that individual IBMers may face in virtual worlds. These guidelines are not intended to address every situation you may encounter through use of a digital persona or personas. But reflecting as they do the input and expertise of a global team of experts — IBM's Virtual Universe Community — the guidelines are a good start at informing our collective engagement and exploration.
>
> 1. **Engage.** IBM encourages its employees to explore responsibly — indeed, to further the development of — new spaces of relationship-building, learning, and collaboration.
> 2. **Use your good judgment.** As in physical communities, good and bad will be found in virtual worlds. You will need to exercise good judgment as to how to react in these situations — including whether to opt out or proceed.
> 3. **Protect your — and IBM's — good name.** At this point in time, assume that activities in virtual worlds and/or the 3D Internet are public — much as is participation in public chat rooms or blogs. Be mindful that your actions may be visible for a long time. If you conduct business for IBM in a virtual world or if you are or may appear to be speaking for or on behalf of IBM, make sure you are explicitly authorized to do so by your management.
> 4. **Protect others' privacy.** It is inappropriate to disclose or use IBM's or our clients' confidential or proprietary information — or any personal information of any other person or company (including their real name) — within a virtual world.
> 5. **Make the right impression.** Your avatar's appearance should be reasonable and fitting for the activities in which you engage (especially if conducting IBM business). If you are engaged in a virtual world primarily for IBM business purposes, we strongly encourage you to identify your avatar as affiliated with IBM. If you are engaged primarily for personal uses, consider using a different avatar.
> 6. **Protect IBM's and others' intellectual property.** IBM has a long-established policy of respecting the intellectual property of others, and of protecting its own intellectual property. Just as we take care in our physical-world activities to avoid infringement of intellectual property rights and to provide proper attribution of such rights, so we must in our activities in virtual worlds — in particular with regard to the creation of rich content.
> 7. **IBM business should be conducted in virtual environments only with authorization.** You should not make commitments or engage in activities on behalf of IBM unless you are explicitly authorized to do so and have management approval and delegations. If you are authorized, you may be asked by IBM management to conduct IBM business through a separate avatar or persona reserved for business use. You should certainly decide to use a separate avatar or persona if you think your use of an existing one might compromise your ability to represent IBM appropriately.
> 8. **Be truthful and consistent.** Building a reputation of trust within a virtual world represents a commitment to be truthful and accountable with fellow digital citizens. You may be violating such trust by dramatically altering your digital persona's behavior or abandoning your digital persona to another operator who changes its behavior. If you are the original creator or launcher of a digital persona, you have a higher level of responsibility for its behavior.
> 9. **Dealing with inappropriate behavior.** IBM strives to create a workplace that is free from discrimination or harassment, and the company takes steps to remedy any problems. However, IBM cannot control and is not responsible for the activity inside virtual worlds. If you are in a virtual environment in conjunction with your work at IBM and you encounter behavior that would not be acceptable inside IBM, you should "walk away" or even sign out of the virtual world. You should report abuse to the service provider. And as always, if you encounter an inappropriate situation in a virtual world that you believe to be work-related, you should bring this to the attention of IBM, either through your manager or through an IBM internal appeal channel.
> 10. **Be a good 3D Netizen.** IBMers should be thoughtful, collaborative, and innovative in their participation in virtual world communities — including in deliberations over behavioral/social norms and rules of thumb.
> 11. **Live our values and follow IBM's Business Conduct Guidelines.** As a general rule, your private life is your own. You must, however, be sensitive to avoid activities in a virtual world that reflect negatively on IBM. Therefore, you must follow and be guided by IBM's values and Business Conduct Guidelines in virtual worlds just as in the physical world, including by complying with the Agreement Regarding Confidentiality and Intellectual Property that you signed when you became an IBM employee. It is obviously most important to do so whenever you identify yourself as an IBMer and engage in any discussions or activities that relate to IBM or its business, or use any of IBM's communications systems or other assets to participate in a virtual world.

[1] "IBM Virtual World Guidelines." IBM, 2007 (http://domino.research.ibm.com/comm/research_projects.nsf/pages/virtualworlds.IBMVirtualWorldGuidelines.html).

insufficient tax documentation, copyright/IP prosecution and defense, and nondisclosure.[12]

As we think about virtual worlds and their future uses, it becomes ever clearer that we need a systemic approach to identity. This is hard work and a moving target. However, such an approach *is* possible — large-scale systems like the Internet, credit cards, and the GSM system for mobile phones have proved that. A systemic approach to identity will also facilitate many new products and services, as innovators will be able to focus on innovation and "outsource" the complex issue of identity. As a result, enormous social and monetary value will be created for both users and service providers.

ACKNOWLEDGMENTS

I would like to thank the members of the Metaverse1 European team and IETF MMOX group (especially Prokofy Neva). Their thinking helped shape this paper.

ENDNOTES

[1] For further discussion of enterprise virtual worlds, see the September 2008 issue of *Cutter IT Journal* (Vol. 21, No. 9).

[2] Sivan, Yesha. "3D3C Real Virtual Worlds Defined: The Immense Potential of Merging 3D, Community, Creation, and Commerce." *Journal of Virtual Worlds Research*, Vol. 1, No. 1, 2008.

[3] Thompson, Michael. "Real Banking Coming to Virtual Worlds." *Ars Technica*, 20 March 2009 (http://arstechnica.com/gaming/news/2009/03/real-banking-coming-to-virtual-worlds.ars).

[4] Sivan, Yesha. "The Birth of MPEG-V (MPEG for Virtual Worlds)." *Metaverse1*, 16 February 2008 (www.metaverse1.org/2008/02/birth-of-mpeg-v-mpeg-for-virtual-worlds.html).

[5] "Trust and the Future of the Internet." The Internet Society (ISOC), August 2008 (www.isoc.org/isoc/mission/initiative/docs/trust-report-2008.pdf).

[6] "Privacy Principles for Identity in the Digital Age (Draft for Comment, Version 1.2). Center for Democracy & Technology (CDT), March 2007 (www.cdt.org/security/20070327idprinciples.pdf).

[7] Glover, Scott. "Alleged MySpace 'Cyber-Bully' Indicted in Teen's Suicide." *Los Angeles Times*, 16 May 2008 (www.latimes.com/news/local/la-me-myspace16-2008may16,0,3642392.story).

[8] Martin, Kirsten E. *Google Inc., in China* (Case BRI-1004). Business Roundtable Institute for Corporate Ethics, 2006 (www.darden.virginia.edu/corporate-ethics/pdf/BRI-1004.pdf).

[9] Heslop, Heidi. "Stroker Serpentine Wins Moral Victory." SLNN.com, 25 March 2008. (The article is no longer available at the original URL, but it can be viewed in Google's cache at http://74.125.77.132/search?q=cache:LtEIrPPlM38J:www.slnn.com/article/serpentine-wins-moral-victory.)

[10] Silvestrini, Elaine. "Virtual Sex Toy Suit Settled." *Tampa Tribune*, 21 March 2008 (www2.tbo.com/content/2008/mar/21/virtual-sex-toy-suit-settled).

[11] Prathivi, Prad. "The 419." *The SL Revolution*, 3 February 2009 (http://theslrevolution.wordpress.com/2009/02/03/the-419).

[12] "The Importance of Identity When Doing Business in Virtual Worlds." *The SL Revolution*, 4 February 2009 (http://theslrevolution.wordpress.com/2009/02/04/identity-in-virtual-worlds).

Yesha Sivan is a senior lecturer at the Department of Software Engineering at the Shenkar College of Engineering and Design. Dr. Sivan is also the founder of Metaverse Labs (MVL), a leading think tank focusing on linking virtual and real worlds. His professional experience includes developing and deploying innovative solutions for corporate, high-tech, government, and defense environments (e.g., the Harvard 9 Keys for Knowledge Infrastructure). He has published numerous papers in the areas of knowledge, 3D3C virtual worlds, and standards. Dr. Sivan received his PhD from Harvard University. His avatar is Dera Kit, and his blog is www.dryesha.com. He can be reached at yesha@metaverse-labs.com.

ABOUT CUTTER CONSORTIUM

Access to the Experts

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, groundbreaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and agile project management, enterprise architecture, business technology trends and strategies, innovation, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you *Access to the Experts*. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts — experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including print and online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products, training, and consulting services, you get the solutions you need while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

Expert Consultants

Cutter Consortium products and services are provided by the top thinkers in IT today — a distinguished group of internationally recognized experts committed to providing top-level, critical, objective advice. They create all the written deliverables and perform all the consulting. That's why we say Cutter Consortium gives you *Access to the Experts*.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

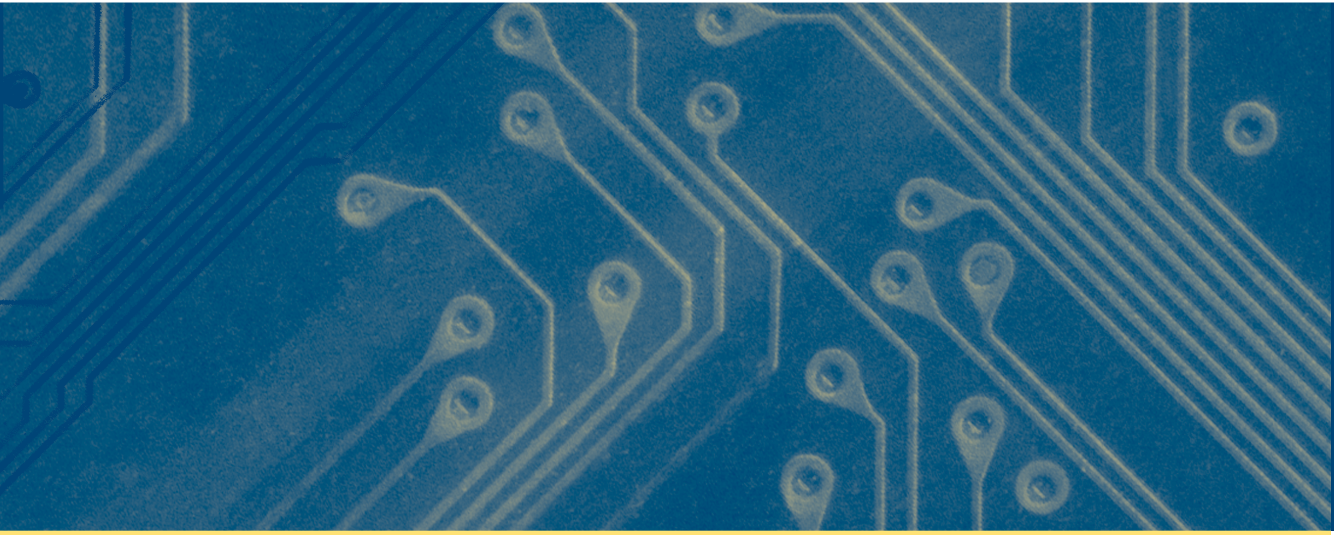
Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA. Client Services: Tel: +1 781 641 9876; Fax: +1 781 648 1950; E-mail: service@cutter.com; Web site: www.cutter.com.

Reprints make an excellent training tool. For more information about reprints and/or back issues of Cutter Consortium publications, call +1 781 648 8700 or e-mail service@cutter.com.

Rob Austin Ron Blitstein Christine Davis Tom DeMarco Lynne Ellyn Tim Lister Lou Mazzucchelli Ken Orr Mark Seiden Ed Yourdon

Cutter Business Technology Council

Cutter
IT Journal



About Cutter Consortium

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, groundbreaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and agile project management, enterprise architecture, business technology trends and strategies, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you Access to the Experts. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts, experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including content via online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products and training/consulting services, you get the solutions you need, while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

The Cutter Business Technology Council

The Cutter Business Technology Council was established by Cutter Consortium to help spot emerging trends in IT, digital technology, and the marketplace. Its members are IT specialists whose ideas have become important building blocks of today's wide-band, digitally connected, global economy. This brain trust includes:

- Rob Austin
- Ron Blitstein
- Christine Davis
- Tom DeMarco
- Lynne Ellyn
- Tim Lister
- Lou Mazzucchelli
- Ken Orr
- Mark Seiden
- Ed Yourdon