VOLUME VII, NUMBER 1

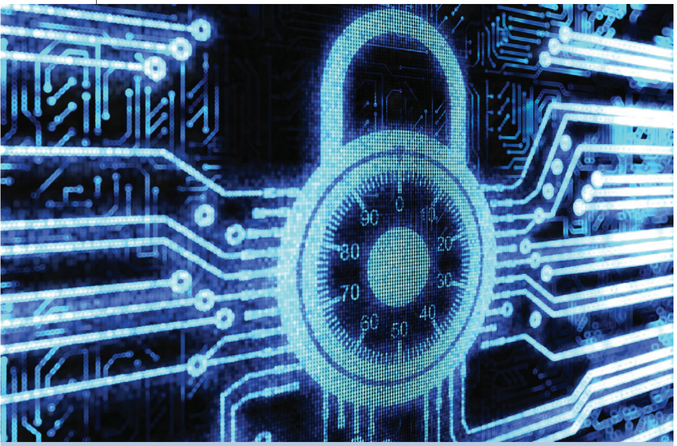
Quest® STRATEGIC ADVISOR

www.questsys.com

Quest® | CAPABILITY ADVISORY

Why Every Company Needs Data Loss Prevention

Your organization is spawning data — and duplicates of data — at an astonishing pace. But do you know how much of that data is sensitive? Do you have a clue about where your data and all the duplicates of it reside or who has access?



THE BOTTOM LINE

How can you prevent sensitive data from leaking to attackers, competitors, and wayward insiders? By identifying it and tagging it, then tracking and regulating its use — in short, data loss prevention.

Your business at risk

In the wrong hands, sensitive data becomes a weapon that works against your business rather than for it.

Risky behaviors are common among employees. These include accessing sensitive corporate data from mobile devices and storing it there without safeguards.

Too often, employees also use personal email accounts to send data to coworkers, customers, or prospects. They leave devices unattended in public places, use (and even hijack) unsecured wireless hotspots, neglect to change passwords, and more.

For too many employees, security policies don't exist, aren't enforced, or are too inconvenient to abide by — so they expose sensitive data to theft and corporate IT infrastructure to malicious attack.

Intellectual property as low-hanging fruit

Absconding with sensitive data tempts some employees because it's so easy to do. Consider these numbers about insider data theft from a recent Symantec study*:

- 75% stole material they had authorized access to,
- 65% had accepted positions with a competitor or started their own firm at the time of the theft,
- 54% used a network — email, a remote network access channel, or network file transfer — to send out stolen data, and
- A majority had signed intellectual property agreements (showing that policy is toothless without monitoring and enforcement).

Toward securing your sensitive data

Protecting sensitive data even from those who create it and use it poses an interesting security challenge — one that more and more compliance mandates demand be addressed.

"Obviously, you can't squirrel away sensitive data from employees who need to work with it," says Tim Burke, Quest President and CEO. "But you can do things that help prevent its unauthorized distribution. The trick is to identify sensitive data, tag it, then monitor and regulate its use in networks, at endpoints, and in data stores. That's what we call data loss prevention."

WHY DATA LOSS PREVENTION *(Cont. on p. 2)*

IN THIS ISSUE

* http://www.symantec.com/about/news/release/article.jsp?prid=20111207_01

WHY DATA LOSS PREVENTION *(Cont. from p. 1)*

What DLP can do

Data loss prevention (DLP) solutions can:

Discover where sensitive data is kept. The right DLP capability can sift through file servers, databases, documents, email, and Web content to discover sensitive data wherever it resides and tag it so it can be tracked wherever it goes.

Advanced DLP detection technologies can accurately analyze both the content and context of data, making data leakage prevention truly affordable.

> "You can't squirrel away sensitive data from employees who need to work with it. But you can do things that help prevent its unauthorized distribution."

Manage and enforce security policies. DLP makes it possible to manage and apply security policies across the enterprise, reducing burdens on IT staff while boosting compliance.

This ability to manage not just security policy but also security enforcement is especially important, given the proliferation of employee communication venues (e.g., email, IM, the Web, social media), work locations, and devices, some of which are employee-owned and inevitably used for personal activities.

Monitor and regulate how sensitive data gets used. With DLP, you'll not only gain visibility into policy violations, you'll be able to automatically enforce policies and compliance (and get employees to behave when it comes to data use).

DLP enables you to secure data proactively via automatic quarantine, relocation, and support for policy-based encryption. You can enable active blocking at the network and endpoints to prevent data from inappropriately leaving the organization. And you'll know who attempted what and when.

Strategy first

"Here's where I say 'don't bite off more than you can chew'," notes Tim. "The temptation to do too much can be really strong when you start to understand what DLP is capable of."

Aim initially for basic DLP capabilities. You can do this by focusing on just one kind of DLP coverage — i.e., network, endpoint, or discovery (storage) — and just one policy (to avoid being overwhelmed with alerts). Once this first DLP capability is deployed and optimized, tackle the next one.

"Glitchy DLP implementations are generally a result of glitchy business processes — not the technology," says Tim. "So before you deploy DLP capability, ask and answer 'What do we hope to achieve?'"

A trusted security services advisor can help you answer those questions and map your objectives to what's possible with DLP.

FROM TIM BURKE...

Curing Those Security Blues

Are you suffering from security fatigue? Find yourself getting irritated when your IT folks bring up yet another security issue? You're not alone. Lately I've been witnessing a good deal of security fatigue in the executive suite, and I'm not surprised.

Truth is, security remains a never-ending process. The easier we make it to move data, the more vulnerable it is to loss or theft. In fact, our Page 1 story this issue on Data Loss Prevention is all about how easy it is for too many employees to make off with sensitive, proprietary information.

But you're sick of hearing about it all, right? Well, maybe it's not security you're tired of, but the endless stream of checks you've been writing to buy security products that leave you less than secure.

As readers of this blog know, I've long been an advocate of buying capability rather than product. Want to be sure Salesman Bob, who's just resigned to go to work for a competitor, doesn't walk away with all your customer data to help him in his new job? Don't just buy a product. Look for a way to get the capability to protect your data.

You can't escape spending on security, but you can make each dollar work to deliver the functionality you need.

CHECK OUT MORE OF TIM'S THINKING AT
www.questsys.com/ceoCorner

Quest's Security Services:

Getting the Most from Your IT Security Spend

While absolute, 100%-guaranteed security is never possible, you can do three things to greatly reduce your organization's exposure and vulnerability to malicious attack:

1. Understand that attackers, whether internal or external, have limited time and resources, which means they focus on easy targets rather than difficult targets. Your goal is to always be a difficult target.
2. Because each security measure protects a portion of your IT resources in specific and limited ways, you need layers of security measures that cover the gaps in each other's protective capabilities.
3. To be effective, your security measures need to work together in awareness of each other — so, as much as possible, your security solutions and capabilities should be integrated, either via automation or expert management or both.

How Quest can help

Quest offers a full range of security capabilities and services that can be customized, integrated, and fine-tuned to precisely fit the needs of your organization.

Quest's Managed Security Services

We offer the latest technology protection without the investment and uncertainty of doing it yourself.

Working with your team, we can design, implement, and manage a comprehensive security plan that covers your networks, servers, databases, and applications. Full 24/7 management can occur at your site or from our remote Network Operations Centers.

Our Managed Security Services include:

- > Security Posture Assessment
- > Managed Unified Threat Management Services
- > Enterprise Firewall Design/Management
- > Intrusion Detection/Prevention
- > Vulnerability Scanning
- > Managed Antivirus Services
- > Email Virus Protection/Spam Detection
- > Managed Web Filtering
- > Data Loss Prevention Solutions and Services
- > Wireless Security
- > Quest's Security Response Team (SRT)
- > Computer Security Incident Response Planning and Management
- > Computer Forensic Data Collection and Analysis
- > Managed Network Services
- > Client VPN Design
- > Managed Site-to-Site VPN Service

Quest's security-related Professional Services

Our team of expert security professionals is ready to tackle any of your security challenges, including:

- > Security Policy Development, Forensic and Auditing
- > Infrastructure Security
- > Security Project Management
- > HIPAA Gap Analysis
- > MasterCard/VISA Certification Process
- > Vulnerability Testing/Assessments
- > Implementation of security related projects: Intrusion detection/protection systems, correlation analysis, log monitoring

Quest can meet your needs with a broad range of leading-edge, state-of-the-art capabilities that make more effective use of the security controls you already have and require no capital expenditure, so you pay only for what you use.

DID-YOU-KNOW?

How Much of *Your* Data Needs Security?

Every organization is different, of course. And many have no notion how much sensitive data they harbor or what security it does or doesn't have.

We can, however, get a glimpse of data in the world as a whole. Last year, says research outfit IDC*, the amount of data created (and replicated) globally exceeded 1.8 zettabytes — that's 1.8 trillion gigabytes — and worldwide data volume is more than doubling every two years.

Three-quarters of that data — documents, images, music, email, texts, etc., and the files that contain it all — is created by individuals. But along the way, enterprises have some sort of liability for 80% of it.

So how much of that data is sensitive enough that it should be secured?

IDC delineates five categories of security — privacy only, compliance-driven, custodial, confidential, and lockdown — and concluded that in 2010, 28% of all the data in the world needed some level of security. By 2015, that percent will grow to more than one third.

So there's the wider context.

And here's the question: How much of *your* data needs security?

* IDC, *Extracting Value from Chaos*, June 2011 (http://idcdocserv.com/1142)

Coming in the next issue of *Quest Strategic Advisor:*

Case Study of BAYGROUP INTERNATIONAL

What's New...

Insider data theft: What's stolen and how

Check out these findings from a 2011 study* of 50 insider thefts of intellectual property conducted by Carnegie Mellon University's CERT Program for the Department of Defense:

Type of intellectual property stolen	% of the 50 thefts studied	Leading theft methods used (in relative order of use)
Trade secrets	52%	Removable media, email, remote network access
Internal business information	30%	Email, remote network access, removable media, laptop
Source code	20%	Removable media, remote network access, file data transfer, laptop download
Proprietary software	14%	Laptop download, email, remote network access
Customer data	12%	Email, remote network access, laptop download
Business plans	6%	Remote network access, email

And who did the stealing? 44% were engineers or scientists, 18% were managers, 14% were salespeople, and 10% were programmers.

* Carnegie Mellon University, *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases*, February 2011 (http://www.cert.org/archive/pdf/11tn006.pdf)

Quest STRATEGIC ADVISOR

Publisher: Tim Burke
Editor: Barbara Klide

Contact the editor at
barbara_klide@questsys.com

FRIEND, FOLLOW, FIND QUEST

f	facebook.com/QuesTechUSA
twitter	twitter.com/QuesTechUSA
YouTube	youtube.com/QuesTechUSA

IN THE MEDIA ROOM

Visit http://www.questsys.com/media.aspx for

VIDEOS

NEW VIDEO! Service Delivery Centers: Find out about Quest's global Service Delivery Centers — and watch as we focus in particular on Quest's Business Resumption Center, strategically located at one of California's most seismically stable and secure locations. We'll show you why you can count on Quest when you're looking for the ultimate in disaster preparedness.

Who We Are: Colleagues describe achieving business systems success with Quest's help.

Data Security Video: Hear direct from the FBI, security experts, and your peers about the in-depth security issues and how Quest can help protect your company.

Business Continuity Planning/Disaster Recovery: More than 25% of businesses damaged from natural and/or man-made disasters never recover. Ensure your future.

Video overview of our Infrastructure Services: Wireless, Broadband, Fiber-optics, Fiber Splicing, Infrastructure Cabling, and more.

PODCASTS

QUEST ON THE RADIO: Download the podcast on Quest's Threat Review Process.

PCI Compliance podcast: Join (Co-Hosts) Scott Draughon (My Technology Lawyer) and Oliver Rist (InfoWorld) as they interview Mike Dillon (Quest CTO) and Jon Bolden (Quest Director of Professional Services) about PCI (Payment Card Industry) compliance.

NEWSLETTERS

Get current and back issues of our popular newsletter.

Manage your Newsletter subscription.
Let us know how you want your newsletter sent at http://www.questsys.com/SANpreference.aspx
Choose hard copy via USPS or the electronic version through your email.

FROM THE QuestCatalog.com

Discover where the HOT DEALS are and which PRODUCTS are TOP SELLERS.

Check it out at www.Questcatalog.com

THIS WEEK I SOLD COMPANY SECRETS, DID SOME INSIDER TRADING, AND TOOK KICKBACKS FROM VENDORS.
scottadams@aol.com
www.dilbert.com
I'LL GIVE YOU A TASTE IF YOU LOOK THE OTHER WAY.
© 2009 Scott Adams, Inc./Dist. by UFS, Inc.
5-14-09
ZIP!
THAT'S UNSETTLING.

DILBERT: © Scott Adams. Used by permission of Universal Uclick. All rights reserved.