



**Guardium eNews: July/August 2008**

## **Contents**

[Guardium Expands International Reach with 29 New Partners and 5 New Regional Directors to Meet Growing Demand](#)

[Best Practices Seminar Featuring Forrester](#)

[Ex-Countrywide Employee Charged With Selling Customer Data \(Dark Reading\)](#)

[File Sharing's Threat to Agency Data is Growing \(NextGov\)](#)

[P2P File-Sharing Sinks Ships \(CRM Buyer\)](#)

[California Expands Identity Theft Prosecution \(InformationWeek\)](#)

[What's Behind the Rash of Employee Cybersnooping? \(Computerworld\)](#)

[Report Details Snooping in Celebrity Passport Files \(LA Times\)](#)

[Insider Threat Doubles \(Dark Reading\)](#)

[Upcoming Events](#)

[Quick Links](#)

## **Guardium Expands International Reach with 29 New Partners and 5 New Regional Directors to Meet Growing Demand**

Guardium, the database security company, is aggressively expanding its international presence to meet increasing demand for safeguarding enterprise data and automating compliance controls.

The company has formed new strategic partnerships with 29 international resellers and system integrators in the past 18 months, and expanded its global team to include five new regional directors responsible for managing and supporting Guardium's growing indirect channel. This expansion enables Guardium to align its worldwide sales organization and partners to strengthen the company's market leadership and ability to penetrate emerging markets.

[Click here to read the full release](#)

## **Best Practices Seminar Featuring Forrester**

Guardium is hosting an executive seminar on "Best Practices for Database Security & Compliance" on Tuesday, September 9th in San Francisco, featuring Forrester principal analyst Noel Yuhanna and database security expert Ron Bennatan, Ph.D., Guardium's CTO.

CTOs, CSOs and DB administrators will gain practical recommendations on the latest methods for protecting sensitive data stored in corporate databases - such as financial/ERP information, credit card data, personally identifiable information (PII) and intellectual property - and reducing compliance costs via automated and centralized controls for Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI-DSS) and data privacy laws.

[Register here](#)

## **Ex-Countrywide Employee Charged With Selling Customer Data**

Kelly Jackson Higgins, *Dark Reading*

The FBI has busted a former Countrywide Home Loan worker who is suspected of downloading the personal data of some 20,000 customers a week over a period of two years and selling it to third parties.

According to a published report, the data may have been sold to companies that wanted to offer their own loans to the Countrywide victims. Up to 2 million Countrywide customer names were "run and sold," according to the report.

Phil Neray, vice president at Guardium, says Countrywide's breach was caused in part by a lack of proper internal controls. "The lack of internal IT controls is perhaps indicative of a corporate culture that was less focused on internal controls than other objectives," Neray says.

[Click here to read full story](#)

## **File Sharing's Threat to Agency Data is Growing**

Gautham Nagesh, *NextGov*

The security breach that led to the loss of personal information for 800 clients of a Washington-area investment firm, including that of Supreme Court Justice Stephen Breyer, is becoming increasingly common in the federal government, according to a peer-to-peer intelligence company.

Justice Breyer was among those clients whose private information, including birth dates and Social Security numbers, was [exposed by a security breach](#) at Wagner Resource Group, an investment firm in McLean, Va. The breach occurred when an employee loaded the file-sharing program LimeWire onto his computer. Users download LimeWire and other peer-to-peer file-sharing programs to share files, most commonly music and

movies, with other computer users.

Phil Neray, vice president of marketing at database security company Guardium, said the best practice agencies can take is to establish policies regarding the use of file-sharing clients, instant messaging programs and other peer-to-peer technologies. You need three things: people, process and technology, Neray said. Educate the people about what's not acceptable, have a process and policies in place to deal with it, and technology to enforce the policies. If you only implement one of the three, you're not going to be effective in preventing unauthorized behavior.

[Click here to read full story](#)

## **P2P File-Sharing Sinks Ships**

Erika Morphy, *CRM Buyer*

"Data security" may soon rank right up there alongside "military intelligence" as an oxymoron of the high-tech era. If it's not lost or stolen laptops, it's hackers breaking into sloppy networks-or perhaps thousands of unwitting music lovers sharing sensitive corporate secrets along with the latest hot tracks.

Monitoring what employees are doing may be the most urgent piece that companies need to address, said Phil Neray, vice president of marketing at Guardium. Many companies have established some type of security policy, at least on paper, he told CRM Buyer. "What they haven't done is implement what Gartner calls 'content monitoring software'-products that examine network traffic and specific protocols to identify suspicious behavior," Neray said. "These products have been in the market for at least a few years, but it has only been recently that adoption has begun to take off."

This particular incident was bad, especially considering how long it took for the information to be taken down, he continued. "It could have been much worse though-too many people still don't realize the dangers of using P2P networks. Now, can you imagine if this employee had worked for a credit card company or a bank or insurance company? It wouldn't have been a couple of thousand names out there-but tens or hundreds of thousands."

[Click here to read full story](#)

## **California Expands Identity Theft Prosecution**

K.C. Jones, *InformationWeek*

Gov. Arnold Schwarzenegger recently signed Senate Bill 612 into law. It allows prosecutors to charge people with identity theft in the jurisdictions where the victims live. Without the bill, prosecutions could only take place where the crime occurred, which is usually in the perpetrators' towns or cities.

That may make sense if it's in an old-fashioned property crime like a burglary, or even an auto theft, said Sen. Joe Simitian, a Palo Alto Democrat who sponsored the bill. If an identity thief in Los Angeles goes online and steals the identity of a half dozen people in San Jose, the crime [had] to be prosecuted in L.A. That makes no sense at all, and, of course, it makes prosecution altogether unlikely.

Schwarzenegger said he's committed to protecting Californians' personal information and privacy. This commonsense legislation will lead to more prosecutions of this terrible crime, and anyone that commits or even thinks of committing identity theft should know that they will be prosecuted to the fullest extent of the law, he said.

[Click here to read article](#)

## **What's Behind the Rash of Employee Cybersnooping?**

Jay Cline, *Computerworld*

It seems like a month doesn't go by anymore without news of another celebrity's personal data being peeked at by some employee at some workplace where the files are kept. It's news when Britney Spears' hospital records or Barack Obama's passport files get perused. But is there truly more employee snooping, or just more reports of it?

The best control is the blocking and tackling we should have been doing all along -- logging and monitoring. Not necessarily monitoring all systems, but those known to contain the most sensitive information and information of high-wealth individuals. By developing this kind of targeted discipline around logging and monitoring of VIP accounts, you might just find that it doesn't take much to scale this for all of your customers.

*Guardium's [real-time database security](#) and monitoring solution protects sensitive corporate and customer data with a single, scalable solution for all major database platforms and enterprise applications. The system prevents unauthorized or suspicious activities -- without impacting database performance - via real-time policies that monitor all privileged user activities and/or all users accessing specific sensitive objects.*

[Read article here](#)

## **Report Details Snooping in Celebrity Passport Files**

Paul Richter, *Los Angeles Times*

A federal investigation of unauthorized snooping into government passport files has found evidence that such breaches may be far more common than previously disclosed, and the State Department inspector general is calling for an overhaul of the program's management after it was revealed that government and contract workers had snooped in the files of three presidential candidates, Senators Hillary Clinton, Barack Obama and John McCain.

To assess the extent of the problem, investigators assembled a sample of 150 famous Americans and examined how many times their files in a government database were viewed over a six-year period. The files of 127 people in the sample were accessed at least once; in total, these files were hit 4,418 times. Nine of the files were opened more than 100 times.

In the report, the inspector general found many control weaknesses in the department's administration program, including what investigators said was a lack of sound policies on training staff, accessing electronic records and disciplining workers who break privacy rules. Five people have been fired so far. Officials said they were investigating whether more workers had violated procedures or federal privacy laws and deserved punishment.

[Click here to read article](#)

## **Insider Threat Doubles**

Kelly Jackson Higgins, *Dark Reading*

Insider-borne attacks have doubled in the last year, according to a new report. The Identity Theft Resource Center recently reported that nearly 16 percent of breaches so far this year came from insiders, up from 6 percent in 2007, and 11.7 percent came from attackers outside the company -- down from 14.1 percent last year.

The ITRC's data is consistent with other reports that insider incidents are on the rise. However, many experts point out that disclosure of all incidents is also on the rise, thanks largely to the legal requirements put in place by many states over the last year.

*Guardium's approach: alert IT security teams to unauthorized insider activity based on corporate policies, plus pinpoint anomalous activity such as access to sensitive objects from unauthorized applications or subnets, and provide granular access controls that addresses the insider threat by preemptively blocking privileged users from unauthorized access to sensitive data through its new S-GATE offering.*

[Click here to read full story](#)

## **UPCOMING EVENTS**

Please visit us at the following upcoming events:

**On-Demand Webcast: Best Practices for Government Database Security & Compliance**

Co-sponsored by BMC, this informative Webcast outlines effective strategies for securing personally identifiable information (PII) and complying with OMB Directive M-06-16. [Register here](#)

**ArcSight Protect'08 User Conference**

September 7-9, 2008  
Hilton Alexandria Mark Center  
Alexandria, VA

*Guardium is a [member of the ArcSight Technology Partner Program](#)*

**Best Practices for Database Security & Compliance Seminar,**  
featuring Forrester principal analyst Noel Yuhanna

September 9, 2008, 9-12PM (breakfast at 8:15AM)  
Le Méridien San Francisco  
San Francisco, CA

**CSO Executive Seminar on PCI Compliance**

September 10, 2008  
Grand Hyatt New York  
New York, NY

**Oracle OpenWorld**

September 21 - 25, 2008  
Moscone Convention Center (Booth #3826)  
West Exhibit Hall  
San Francisco, CA

*Guardium is a [member of the Oracle PartnerNetwork](#) and [supports advanced Oracle security capabilities such as Oracle ASO](#)*

**Accenture Technology Consulting Workshops**

Business Partner Fair  
September 23 - 24, 2008 - London, UK  
September 30 - October 1, 2008 - Rome, Italy

*Presentations will be given by Ron Bennatan, CTO  
Topic: Protecting Your Most Critical Assets - Data  
September 24th - Infrastructure Security Track (London, UK)  
September 30th - Infrastructure Security Track (Rome, Italy)*

**BMC UserWorld 2008**

October 13-17, 2008  
Fontainebleau Resort  
Miami Beach, FL

*Guardium's CTO, Ron Bennatan, Ph.D., will be presenting a session entitled: Secure Your Data - Pass Your Audit.*

*Guardium is a BMC MarketZone partner and a member of BMC's Technology*

Alliance Program (TAP).

**McAfee FOCUS 2008**

October 20-23, 2008  
MGM Grand Las Vegas  
Las Vegas, NV

*Guardium is a founding member of the McAfee Security Innovation Alliance.*

**IBM Information on Demand**

October 26 - 31, 2008  
Mandalay Bay Resort & Convention Center (Booth #11)  
Las Vegas, NV

*Guardium is a member of IBM's Data Governance Council and has achieved Advanced Industry-Optimized status for the Financial Markets industry, within IBM's PartnerWorld Industry Networks.*

**2008 ISSA SoCal Security Symposium**

October 30, 2008  
Renaissance Long Beach Hotel  
Long Beach, CA

**STAY ON THE MAILING LIST**

[Please click here.](#)

And please let us know what you like (and don't like) about our newsletter - just send an email to [phil\\_neray@guardium.com](mailto:phil_neray@guardium.com).

***Quick Links***

[Auditing & Compliance](#)  
[Database Activity Monitoring](#)  
[Change Control](#)  
[Database Leak Prevention](#)  
[Lab Reviews, Case Studies & White Papers](#)  
[Media Coverage & Upcoming Events](#)

Copyright © Guardium 2008. All rights reserved.  
Guardium is a trademark of Guardium. All other trademarks and service marks are the property of their respective owners.