

Guardium e-Newsletter.



June 2009

- [Podcast: Beyond the Perimeter with Guardium CTO, Ron Ben Natan, Ph.D.](#)
- [On-Demand Webcast: Best Practices for Data Privacy & Protection](#)
- [Cybersecurity Seminar on Best Practices for Data Security, Privacy & Compliance](#)
- [Security Industry Veteran to Lead Strategic Practice for Government Markets](#)
- [Hackers Hit U.S. Army Websites, SC Magazine](#)
- [Guardium on Twitter](#)
- [Upcoming Events](#)

Podcast: *Beyond the Perimeter* with Ron Ben Natan, Ph.D., Guardium CTO

Hear Ron Ben Natan on *Beyond the Perimeter*, a well-known security blog moderated by former Gartner security analyst, Amrit Williams, CTO of BigFix.

As security attacks increasingly emphasize theft of financially valuable data, this puts databases in hackers' cross hairs. Since many databases can trace their lineages back 20 years or more, this often presents the technical and cultural conundrum of how to protect 20th century assets against 21st century attacks. This podcast also mentions Ben Natan's new book "HOWTO Secure and Audit Oracle 10g and 11g," with more information on this work at <http://tinyurl.com/pgzbvj>.

The podcast focuses on database security and the importance of protecting information at the source. Amrit highlights how Guardium addresses these areas and also mentions Ron's book. Amrit comments that the book is comprehensive and its format makes it very easy to understand.

Amrit also posted the following Tweet: "Amrit and Guardium's Ron Ben Natan mull the need for 21st century security for 20th century databases."

<http://blogs.bigfix.com/beyondtheperimeter/2009/06/02/episode-24-20th-century-databases-need-21st-century-security/>.

On-Demand Webcast: Best Practices for Data Privacy & Protection

[Register](#) to view this on-demand webcast to learn best practices for protecting Personally Identifiable Information (PII) and other sensitive data against new and emerging threats such as SQL injection and rogue insiders. Protecting against cyber attacks, breaches, fraud and insider threats has heightened the need for organizations to carefully review their security programs for securing PII and other sensitive data against regulations and directives they must comply with including:

- EU e-privacy and personal data-protection rules
- UK Data Protection Act, or
- NIST 800-53 and OMB M-06-16 directive ("Protection of Sensitive Agency Information")

To replay the webcast, go to: <http://www.guardium.com/index.php/landing/722>

Guardium Hosted Cybersecurity Seminar on Best Practices for Data Security, Privacy & Compliance

Leading Data Protection Experts Highlight Pressing Government Issues Including Cybersecurity and Emerging Threats



On June 16, Guardium hosted a “Best Practices for Data Security, Privacy & Compliance” seminar at The Ritz-Carlton, Pentagon City in Arlington, VA. The seminar generated over 180 registrations from civilian, military and intelligence agencies, as well as private sector organizations. Featured speakers included:

- **John Pescatore, Gartner VP and Research Fellow**, who discussed the federal government's role in stimulating progress towards higher levels of cybersecurity; new and emerging threats such as SQL injection and privileged insider breaches; best practices for improving vulnerability management to reduce risks; and the security implications of cloud computing.
- **Andy Singer, Principal at Booz Allen Hamilton**, who described why traditional "fortress approaches" (such as firewalls and IDS/IPS systems) are no longer sufficient to protect against 21st-century attackers who can easily bypass perimeter defenses.
- **Ron Ben Natan, Ph.D. and Guardium CTO**, who discussed best practices for database security and compliance; how to leverage the latest technologies for database activity monitoring (DAM) and logging, vulnerability assessment, data discovery and configuration change control; and how to reduce the cost and complexity of compliance with automated controls and workflow processes.

Guardium Appoints Security Industry Veteran to Lead Strategic Practice for Government Markets

Key Hire with 20+ Years of Federal Technology Experience Will Continue Guardium's Rapid Growth Safeguarding Data for Government Sector

Guardium announced the appointment of Craig Marr as director of sales for government markets. Craig will be responsible for continuing Guardium's rapid growth in the government sector. The company's real-time database security and monitoring platform is currently deployed in numerous government organizations including:

- Federal agencies such as the Federal Trade Commission (FTC),
- Independent federal agencies,
- Government-sponsored enterprises (GSEs),
- The Washington Metropolitan Area Transit Authority (Metro), which transports more than a third of

the federal government to work every day.

Marr brings more than 20 years of federal technology sales experience, including more than 13 years focusing on security. As director of federal sales for IBM/ISS (Internet Security Systems), the trusted security advisor to thousands of government organizations and businesses, his team generated over \$200 million in cumulative revenue to civilian agencies, DoD departments and intelligence agencies. At ISS, he also teamed on federal programs with major system integrators such as CSC, Lockheed Martin, Northrop Grumman, SRA, General Dynamics, Unisys, IBM and Boeing.

Craig holds a Bachelor of Science Degree in Computer Science and started his career as a systems engineer developing enterprise databases for EDS.

Hackers hit U.S. Army websites

by Chuck Miller, *SC Magazine*

A group of computer hackers based in Turkey breached the sites of two U.S. Army facilities, leveraging SQL injection attacks, according to reports.

The group, which calls itself "m0sted," defaced the page and redirected users to pages that included anti-American and anti-Israeli statements, *Information Week* reported last week.

The hacker group is not new to these kinds of attacks, according to reports. In August 2007, m0sted hacked a United Nations website. And the group also carried out attacks against Kaspersky Lab. In September 2007, the hackers broke into Army Corps of Engineers' servers.

"The question of vulnerability to SQL injection attacks has come up frequently," Phil Neray, vice president of security strategy for Guardium, told SCMagazineUS.com. "The number is rising dramatically. SQL injection is a serious threat. Not enough organizations are paying attention to it."

[Click here to read this article](#)

Guardium on Twitter

Now you can follow Guardium on Twitter.com at <http://twitter.com/guardium>. The goal of Guardium Tweets is to post short, educational nuggets and tips about data security as well as breaking news regarding data breaches.

UPCOMING EVENTS

Please visit us at the following upcoming events:

UNITED STATES

[Gartner IT Security Summit](#)

June 29-July 1, 2009

Gaylord National Resort & Convention Center
National Harbor, MD

Booth #9

[ArcSight Protect 09](#)

Sept. 14-15, 2009

Gaylord National Resort & Convention Center
National Harbor, MD

2009 San Francisco [ISACA Fall Conference](#)

Sept. 21-22, 2009

Hotel Nikko
San Francisco, CA

EMEA

[UKOUG DBMS Special Interest Group Meeting](#)

July 1, 2009

Royal Institute of British Architects (RIBA)
London, UK

ISACA [Information Security and Risk Management Conference: Europe](#)

November 9-11, 2009

NH Grand Hotel Krasnapolsky
Amsterdam, The Netherlands

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.

QUICK LINKS

[Auditing & Compliance](#)

[Privileged User Monitoring](#)

[Application Monitoring: Fraud Prevention](#)

[Change Control](#)

[Database Leak Prevention](#)

[Lab Reviews, Case Studies & White Papers](#)

[Media Coverage & Upcoming Events](#)