

Eight Steps To Holistic Database Security
[Download here](#)

Sign up for Dark Reading's new Database Security Weekly newsletter.
[Click here now!](#)

Welcome Guest. | [Log In](#) | [Register](#) | [Membership Benefits](#)

- ATTACKS / BREACHES
- VULNERABILITIES
- APPLICATION SECURITY
- CLIENT SECURITY
- PERIMETER SECURITY
- SECURITY MANAGEMENT
- STORAGE SECURITY
- ENCRYPTION
- NAC
- ANTIVIRUS
- PRIVACY
- BLOGS

SEARCH

Tech Center: Database Security

E-mail this page | Print this page | BOOKMARK

Shell Employee Directory Leaked, Allegedly By Activist Workers

Oil company acknowledges leak, but says it isn't sure current employees did the deed

Feb 12, 2010 | 02:31 PM

By **Tim Wilson**
DarkReading

The names and phone numbers of more than 170,000 employees and contractors at Royal Dutch Shell have been emailed to environmental and human rights campaign groups, the oil company acknowledged today.

The database, from Shell's internal directory, gives names and telephone numbers for all of the company's workforce worldwide, including some home numbers, according to a story in the *Financial Times*. The e-mail was ostensibly sent by disaffected staff calling for a "peaceful corporate revolution" at the company.

The database was emailed with a 170-page cover note, explaining that it was being circulated by "116 concerned employees of Shell Oil dispersed throughout the USA, the UK, and the Netherlands" to highlight the harm allegedly done by the company's operations in Nigeria, according to the *Financial Times*.

Shell confirmed the database was genuine, but said it did not pose a security risk because it did not include home addresses, according to the news report. The company said it was investigating the security breach, but did not believe the claim it had been leaked by disaffected staff. So far, no Shell employee has admitted playing a role in the data theft.

The leaked information is about 6 months old, suggesting it could have been taken by a former employee, *Financial Times* said. Shell cut 5,000 jobs last year and recently announced a further 1,000 job losses for this year.

The e-mail was sent to a handful of campaign groups, including Greenpeace, and to www.royaldutchshellplc.com, a Website used to air grievances about Shell, the report said.

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, [send us a message](#).

[Discuss This](#)

Add Your Comment:

Please [login or register here](#) for a free Techweb account to post

[XML](#) [Subscribe to RSS](#)

- » [Write To Editor](#)
- » [Reprint This Article](#)
- » [Download Top Reports](#)

D Database Security Insider Threat Security Services on Assets

Vulnerability Management Monitoring: Emerging Technology Keeps Tabs

You can read about the consequences of not protecting critical data in the daily headlines. In response, security-conscious organizations are tackling the complexities involved in effectively monitoring their databases for potential leaks and compromises. Fortunately, an emerging class of software is stepping up to help. Here's what enterprises need to know about selecting, deploying, and managing DAM technology.

SQL Injection: A Major Threat to Data Security

Of all the attacks taking place on Web sites across the Internet today, SQL injection is the most popular for cybercriminals trying to hack their way into corporate data stores. But for such a pervasive threat, there is still little understanding within the development and database communities about what constitutes a SQL injection vulnerability, how attacks against a SQL injection bug work, and how to mitigate the risk. We examine how these exploits work and what you can do to stop them.

Protecting Your Databases From Careless End Users

While much attention is paid to outside attackers' efforts to crack enterprise databases, IT organizations often overlook an even greater threat: end users. Ignorance and disregard of company security policies may lead employees to expose their organizations' databases to compromise, often without even knowing that they're doing so. In this report, we offer advice on how to educate users on database security, and some common-sense recommendations on how to limit the damage.

A Database Administrator's Guide to Security

While most security pros have become painfully aware of the threats posed to their organizations' databases, many of those who create and maintain the databases still don't fully understand the danger. This "security primer" is designed to open the eyes of the DBA to the risks posed by poor database security - and to current "best practices" that can help prevent those risks from becoming reality.

Why Your Databases Are Vulnerable To Attack - And What You Can Do About It

Most of an enterprise's most sensitive and valuable information resides in databases. Yet, in many organizations, database security is often neglected, misunderstood, or even ignored. In this report, we discover why databases have become one of the most popular targets for hackers - and how everyday mistakes in database administration contribute to these attacks. We also offer some advice on what your organization can do to protect your most critical data - and to stop hackers in their tracks.

Related Content

Sponsored by: **Guardium**
SAFEGUARDING DATABASES - AN IBM COMPANY

HOWTO Secure and Audit Oracle 10g and 11g

Read the "Hardening Your Database" chapter from the 454-page book "HOWTO Secure and Audit Oracle 10g and 11g" and learn how to navigate the many security options within Oracle (authored by database security expert and Guardium CTO, Ron Ben Natan, Ph.D.)

HOWTO Monitor Database Activity

Read the "Database Activity Monitoring (DAM)" chapter from "HOWTO Secure and Audit Oracle 10g and 11g" (CRC Press, 2009) and learn how to leverage DAM to prevent cyberattacks, monitor privileged users and track access to sensitive data.

8 Steps to Holistic Database Security

Get the 8 essential best practices for a holistic approach to both safeguarding databases and achieving compliance with key regulations such as SOX, PCI-DSS, NIST 800-53 and data protection laws.

Essential Steps to Implementing Database Security and Auditing

Learn best practices and specific tips for effectively securing Oracle, SQL Server, DB2, MySQL and Sybase environments, including tracking security vulnerabilities, the anatomy of buffer overflow vulnerabilities and database auditing.

Databases at Risk: Current State of Database Security (ESG Research)

This recently published ESG report analyzes the current state of database security -- concluding it depends upon too many manual processes -- and also offers concrete steps to improve database security across the enterprise.





Are Your Sensitive Databases Secure?
 Rogue insider threats
 Cyberattacks
 Fraud


Database Security Newsfeed

- [PacketMotion Simplifies PCI DSS Compliance With New Virtual Segmentation Solution](#)
- [Dataquise Announces Dgmasker Application Templates](#)
- [Study: Server Virtualization Still Growing](#)
- [Secerno Debuts Data Protection At 230,000 Transactions Per Second](#)
- [Facebook Automates Sensitive Data Discovery](#)
- [Oracle Announces Latest Release Of Oracle Audit Vault](#)

[MORE NEWSFEED >>](#)



HOWTO Secure & Audit Oracle 10g/11g




The Global Leader in Technology Media

InformationWeek Business Technology Network

- [Advanced Trading](#)
- [Bank Systems & Technology](#)
- [Bank Systems & Technology Executive Summit](#)
- [bMighty.com](#)
- [Contentinople](#)
- [Dark Reading](#)
- [Dr. Dobbs](#)
- [InformationWeek](#)
- [InformationWeek 500](#)
- [InformationWeek 500 Conference](#)
- [InformationWeek Analytics](#)
- [InformationWeek Events](#)
- [InformationWeek Financial Services](#)
- [InformationWeek Global CIO](#)
- [InformationWeek Government](#)
- [InformationWeek Healthcare](#)
- [InformationWeek India](#)
- [InformationWeek Magazine](#)
- [Insurance & Technology](#)
- [Insurance & Technology Executive Summit](#)
- [Intelligent Enterprise](#)
- [Internet Evolution](#)
- [Network Computing](#)
- [No Jitter](#)
- [Plug into the Cloud](#)
- [Wall Street & Technology](#)

Light Reading Communications Network

- [Heavy Reading](#)
- [Light Reading](#)
- [Light Reading Asia](#)
- [Light Reading Insider](#)
- [Light Reading Live!](#)
- [Light Reading's Digital Cable News](#)
- [Light Reading's Ethernet Expo](#)
- [Pyramid Research](#)
- [TelcoTV](#)
- [Tower Technology Summit](#)
- [Unstrung](#)

TechWeb Events Network

- [Black Hat](#)
- [Cloud Connect](#)
- [Enterprise 2.0](#)
- [Gov 2.0 Expo](#)
- [Gov 2.0 Summit](#)
- [GTEC](#)
- [Interop](#)
- [VoiceCon](#)
- [Web 2.0 Expo](#)
- [Web 2.0 Summit](#)

Most Popular

- [ANTenna](#)
- [Bob Evan's Global CIO](#)
- [Cable Catchup](#)
- [David Berlind's Tech Radar](#)
- [Digital Life](#)
- [Enterprise 2.0 Blog](#)
- [Evil Bytes](#)
- [InformationWeek Analytics](#)
- [Interop Blog](#)
- [Jon Erickson's Blog](#)
- [Microsoft/Windows Blog](#)
- [Monkey Bidness](#)
- [Over the Air](#)
- [The Philter](#)
- [Valley Wonk](#)

[Web 2.0 Blog](#)
[Wolfe's Den](#)

[About TechWeb](#) | [Advertising Contacts](#) | [Become a Member / Membership Benefits](#) | [Contact Us](#)
[Feedback](#) | [Reprints](#) | [Technology Marketing Solutions](#) | [TechWeb Digital Library / White Papers](#) | [TechWeb.com](#)

[Dark Reading Home](#) [Attacks and breaches](#) [Vulnerabilities](#) [Application Security](#) [Client Security](#) [Perimeter Security](#) [Security Management](#)
[Storage Security](#) [Encryption](#) [NAC](#) [Antivirus](#) [Privacy](#) [Blogs](#) [Security discussions](#)
[Newsletters](#) [Video](#) [Webcasts](#) [Live events](#) [TechWeb Digital Library](#) [Registration/membership](#) [About us](#)
[Sales and marketing contacts](#) [Send us a tip or comments](#) [Site map](#) [Technology Marketing Solutions](#)

[Terms of Service](#) | [Privacy Statement](#) | [Copyright © 2010 United Business Media LLC. All rights reserved.](#)
