Contact: Daniel A. Morgan
damorgan@dbsecworx.com
+1 612-240-3538

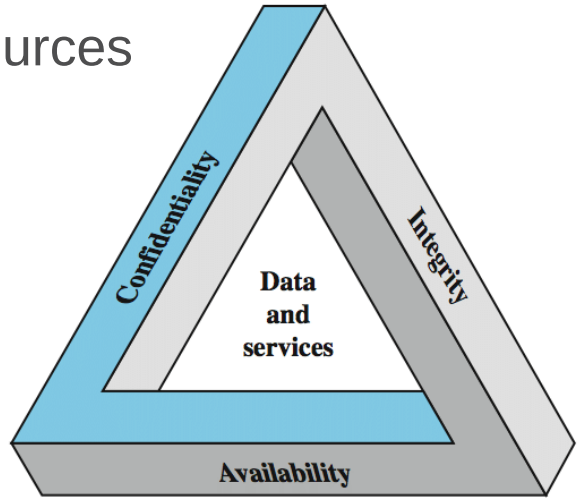
14 Jun 2019

Who

- Daniel Morgan, Managing Director
- Oracle ACE Director Alumnus
- Adjunct Professor, University of Washington, ret.
- Consultant, Harvard University
- Oracle Beta Tester
- Hands On with every Oracle Database version from 6.0 through 19.3
- International experience
  - Americas, Europe, Asia Pacific
- Industry expertise
  - Aerospace, Biomedical, Defense, Distribution, Education, Energy, Finance, Health Care, High Technology, Hospitality, Insurance, Manufacturing, Public Sector, Retail, Telecommunications, Travel & Entertainment

What

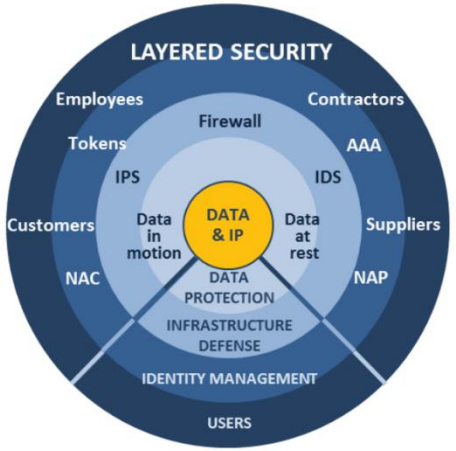
- **DBSecWorx** is our new name, reflecting our focus on Oracle database security, for a professional practice founded in 2004
- **Solving** business problems by providing the tools, services, and expertise required to extend "Defense in Depth" to data and databases
- **Targeting** all forms of data and databases misuse
  - Use of Privileged Database Tools to Attack Additional IT Resources
  - Data Theft, Misuse, Loss, and Corruption
  - Denial of Service
- **Producing** tangible, measurable, results
- **Investing** in the community and our customers

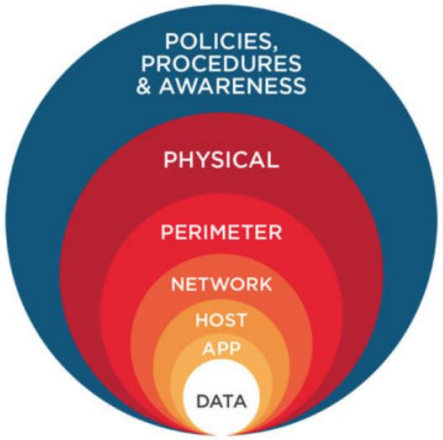


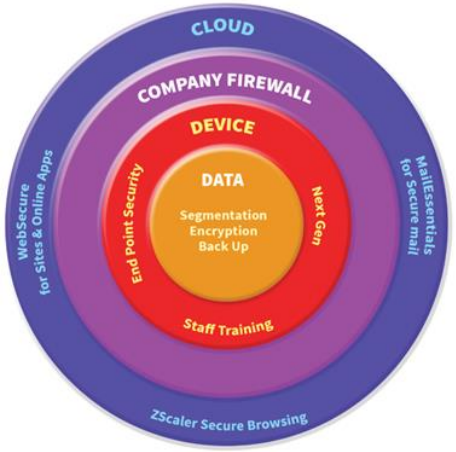
CIA Triangle

Why

- **Defense in Depth** is the only strategy proven to secure IT resources
- Every diagram published shows data at the core

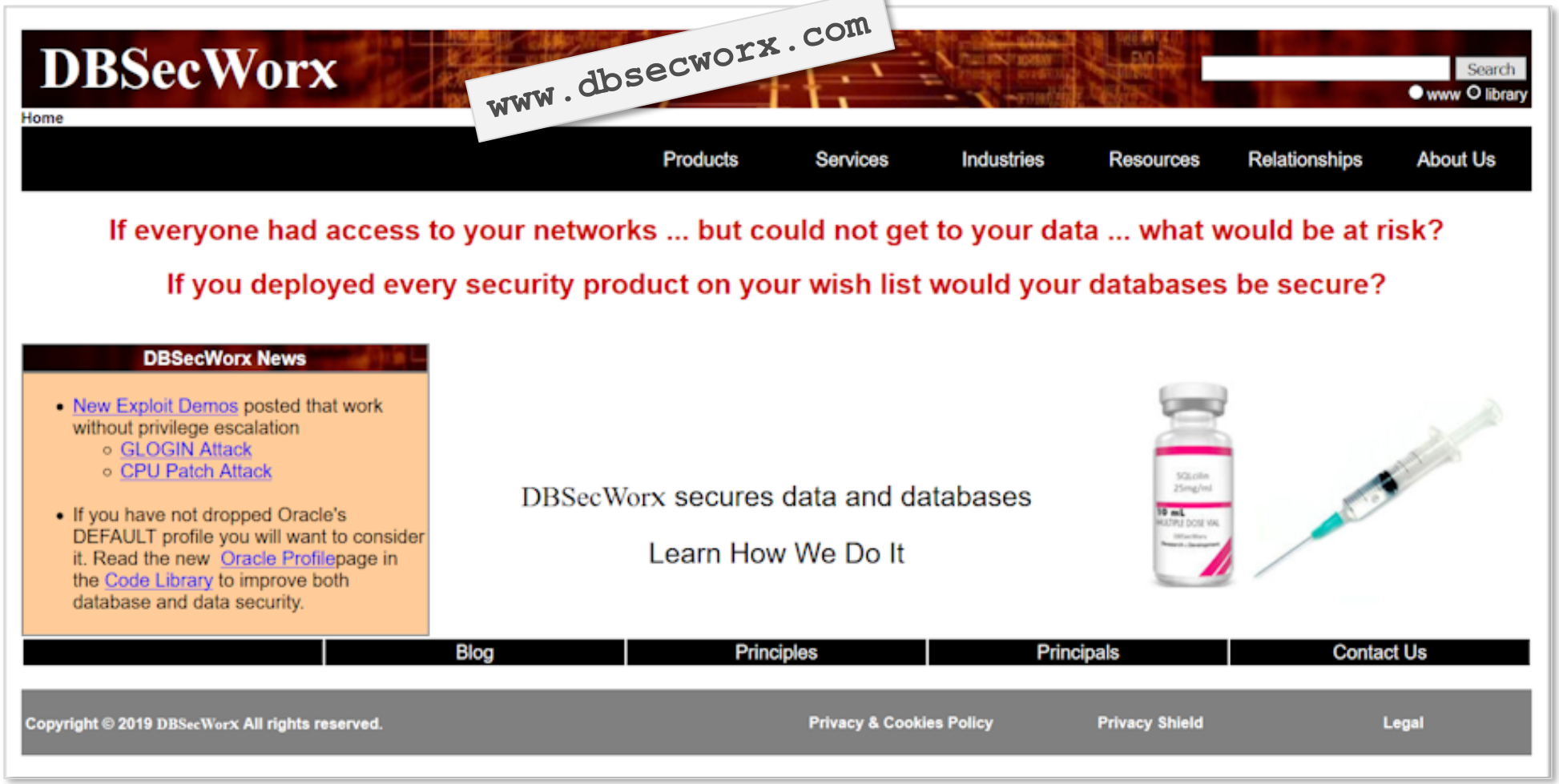






- Yet, we focus our effort and dollars almost exclusively on the perimeter
- When that perimeter is breached we are generally defenseless
- Audits tell us what happened but do not prevent it from happening

Where



SQLcillin GL

Contact: Daniel A. Morgan
damorgan@dbsecworx.com
+1 612-240-3538

09 May 2019

Business Problem

- We must have confidence in the integrity of our data
- We must proactively protect our data and databases from misuse
- Standards compliance is essential but attackers know what isn't covered
- Auditing records what happened but only after it has already happened
- The overwhelming majority of tools and assessments focus on the perimeter and end-points, not the ultimate target of the attack, the data

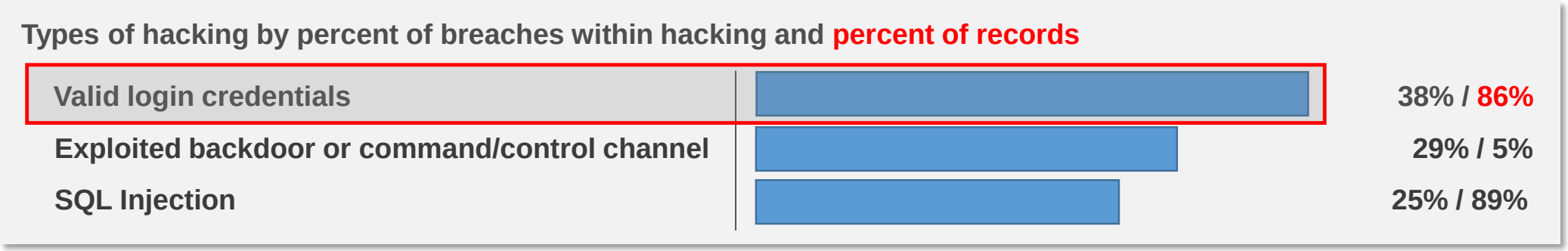
IT's Traditional Focus


History has proven that all perimeters can be breached

- Most IT security investment targets the perimeter and end-points
- Billions of dollars are spent every year
- The number of successful break-ins proves that this is insufficient

The Biggest Risk Is Credentialed Users

- How attackers gain access to data
  - 48% involve privilege misuse
  - 40% are the result of hacking
  - 38% utilize malware
  - 28% employ social engineering



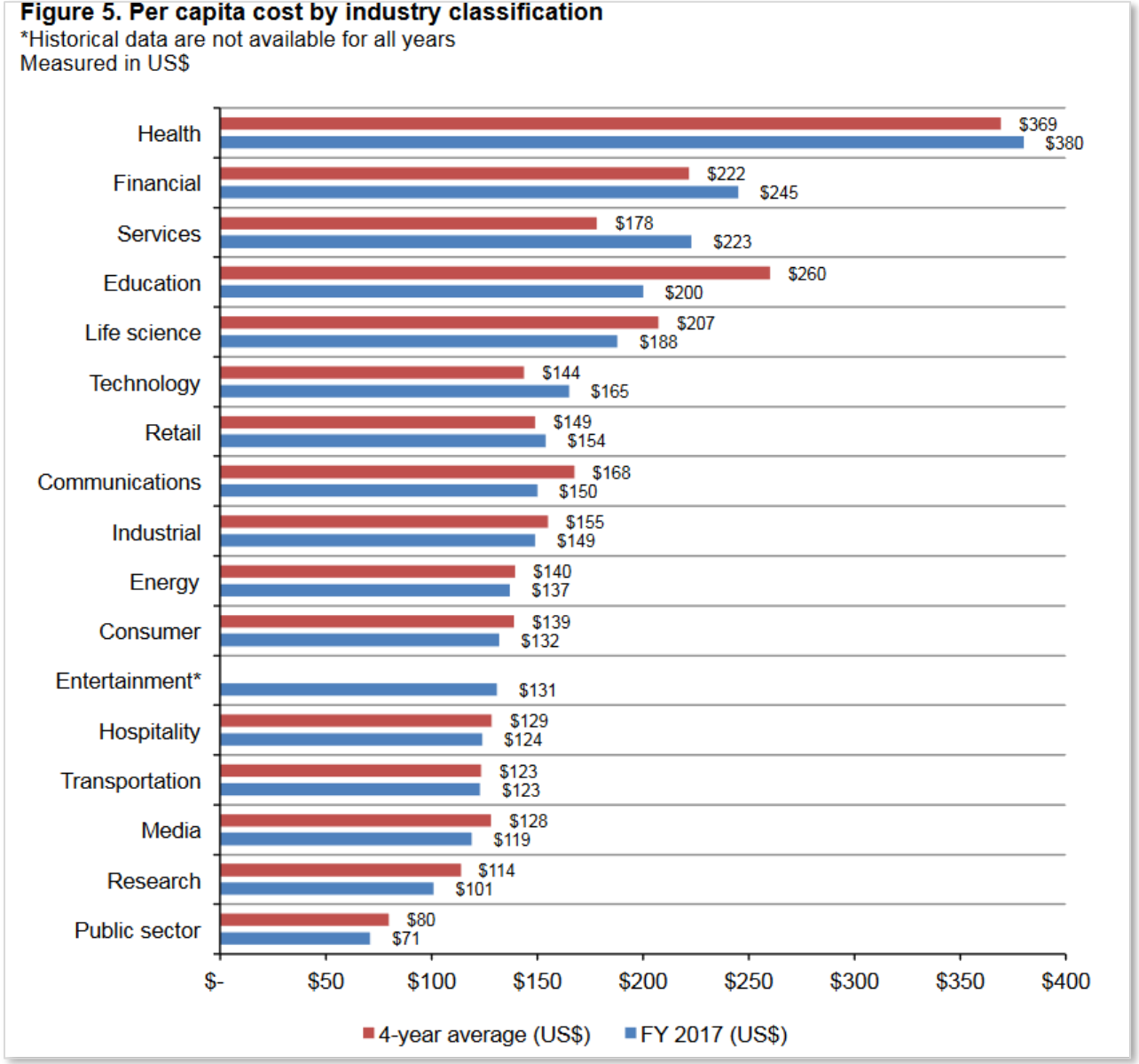
- The single biggest is that 86% of record compromises were executed by someone with a valid userid and password
- Perimeter protection will not stop someone with valid credentials
- Which is why there are so many failures to stop determined attacks

Breaches Are Far More Than Embarrassing

"Hackers and criminal insiders cause the most data breaches. Forty-seven percent of all breaches in this year's study were caused by malicious or criminal attacks.

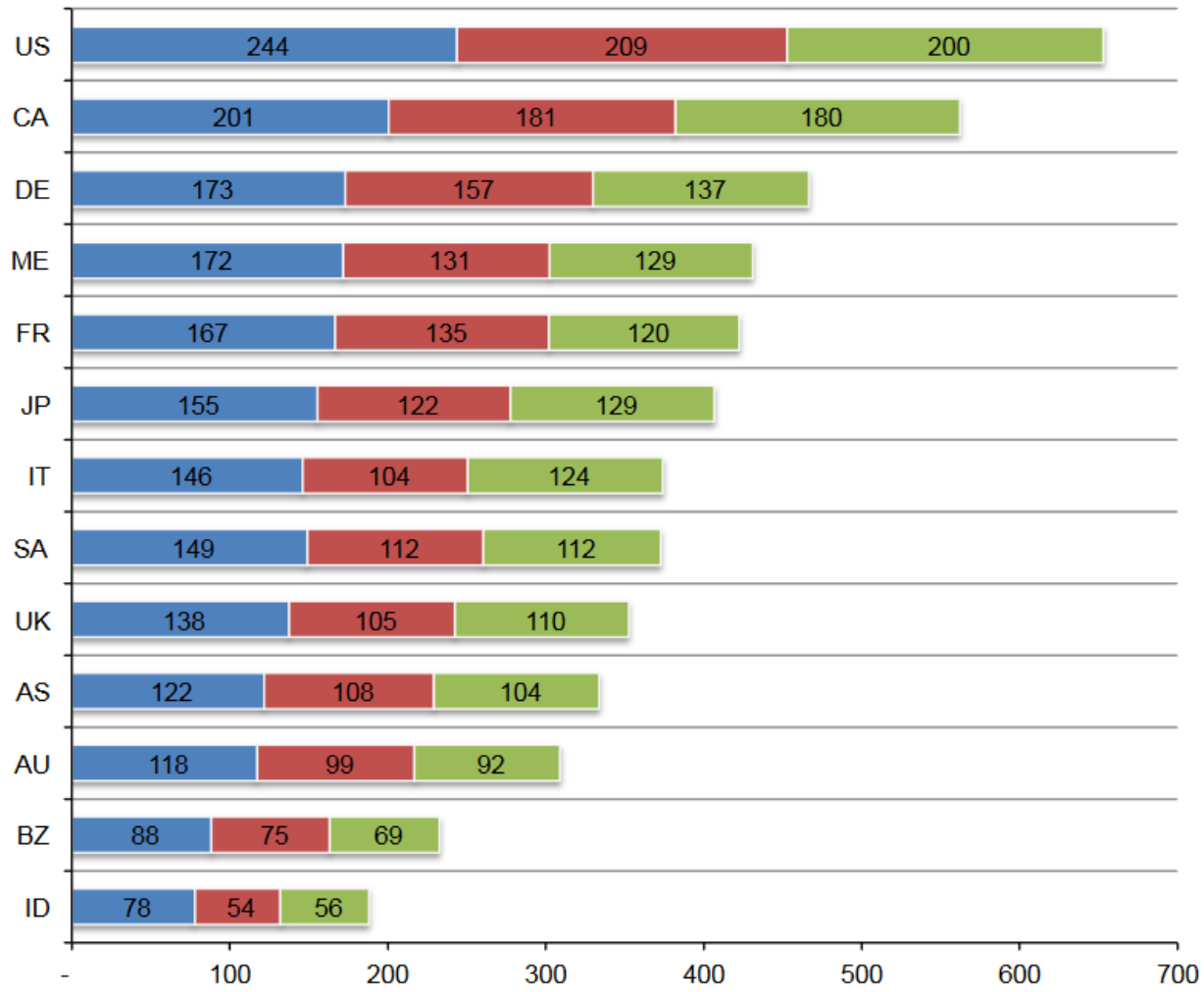
Data breaches are the most expensive in the United States and Canada and least expensive in Brazil and India. **The average per capita cost of [a] data breach was $225 [per record] in the United States** and $190 in Canada.

Breaches Are Expensive



Breaches Are Expensive

Figure 8. Per capita cost for three root causes of data breach by country and region
Measured in US$



Additional Challenges

- Database professionals are not trained in database security
- DBAs are unaware of vulnerabilities in the products they manage
- The media focuses on a single risk: data theft ... there are many others
- Security solutions must not interfere with work getting done
- A solution must be maintainable
- A solution must be affordable

The Ideal Solution

- Eliminates a high risk vulnerability
- Does not interfere with day-to-day operations
- Standards compatible
- Easy to install
- Easy to maintain
- Affordable

The GLOGIN Exploit

- Well known: First reported in 2002, detailed again in a 2014 book
- Creates users with any desired privileges for later exploitation
- Defeats any Oracle database of any version on any platform
- Exploited by network and system admins, contractors and vendors
- Executed transparently by orchestration tools like Ansible and Chef
- Requires no special database knowledge or technical expertise to perform
- Can be executed in less than 1 second

How The GLOGIN Exploit Works

- A global login file, glogin.sql, is part of every Oracle Database installation
- It is read and executed every time there is database login with Oracle's primary DBA tool
- Commands in the file execute automatically and transparently
- Database credentials are not required to utilize this exploit
- The attacker need only add three short lines to the file
- After the commands have been executed the attacker can take control

How Does SQLcillin GL Work?

- SQLcillin GL verifies the glogin file has not been altered, without authorization, every time a command is executed in Oracle's Data Control or Data Definition Language
- If an unauthorized change has been made, the command will not execute until the change to the glogin file is approved
- Messages are written to the database's alert log every time the product protects the database detailing the date, time, and actions taken

Will SQLcillin GL Work For Us?

- SQLcillin GL is compatible with every version of the Oracle Database*
- SQLcillin GL is compatible with every edition of the Oracle Database

- Can be installation by your DBA in less than 60 seconds per database
- SQLcillin GL resides entirely inside the database
  - No additional memory required
  - No additional database or file system space required
- Support is available 7 x 24 x 365

* under standard or extended support by Oracle Corp.

How Is SQLcillin GL Sold?

- Licensed by the database DBID
  - The first database is always free *
  - Licenses are available for 1, 2, and 5 years
- Support for included for no additional charge for all purchased licenses
- To place an order we only require a list of DBIDs
- Your customized copies of SQLcillin GL will be made available for download from a website personalized for your organization

* includes 30 days support

Next Steps

Daniel A. Morgan
email: damorgan@dbsecworx.com
mobile: +1 612-240-3538

What We Recommend

- It is much harder to dig yourself out of a hole after the sides have fallen in

- Request a free 100% technical Lunch & Learn for your team
- Request your first copy of SQLcillin GL, free, for evaluation
  - Protects one Oracle database, fully functional, never expires (includes 30 days support)
- 50% discount is available for all sales during 2020
- 25% additional discount if we can use you as a reference

There isn't a lot of room in IT for Conscientious Objectors

- Please join us in the fight against cyber crime

Daniel A. Morgan
email: damorgan@dbsecworx.com
mobile: +1 612-240-3538

09 May 2019