Mighty Guides®

7 Experts on
Database Security

Expert advice on effectively securing databases

Securing databases has become a serious challenge for many organizations. One reason for this is that the bad guys know some of the most sensitive and valuable data they can steal is stored in databases. Another is that in this world of cloud computing, mobility and easy data sharing, it is becoming very difficult to know exactly where your data is at all times.

So how do businesses secure their databases? How do they keep track of their data, and how do they know they are meeting compliance requirements? How can they be sure they are adequately patching database vulnerabilities? To answer these questions, we once again turned to the experts. With the generous support of Trustwave, we asked seven security experts the following question:

What advice, strategies and best practices would you give to a business to effectively secure their databases?

One interesting insight that comes from reading these essays is that although many traditional security controls, such as access management and data validation, remain central to database protection, how they are applied is in a state of transition. This is being driven in part by the decentralization of databases and the role of DevOps processes in deploying database functionality.

Like much that is happening in cybersecurity today, the practice of securing databases is evolving. I believe these essays provide an interesting snapshot of current database security practices.

All the best,

David Rogelberg
Publisher, Mighty Guides Inc.

ℳ Mighty Guides®

Mighty Guides make you stronger.
These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Most enterprises today are capturing a staggering amount of data produced every day by its customers, users, applications and devices. It is more difficult than ever to keep track of who has access to what sensitive data (or even where all the sensitive data lives!) Cyber criminals, hacktivists, and state actors recognize this data sprawl challenge and are constantly probing for ways to access or manipulate that data for financial, competitive or political gain. As the attack surface grows in the data center and the cloud, we are seeing an increase in the number of sophisticated and targeted attacks. As a result, it is becoming increasingly challenging for organizations to proactively secure their data stores, prioritize remediation efforts, reduce excessive user privileges, and respond to data breach attempts in a timely manner.

At the same time, organizations are being required to demonstrate that they meet a growing number of stringent security and privacy regulations, such as HIPAA, PCI-DSS, DISA-STIG, FISMA, GDPR, MTCS and many others. And to make matters worse, there is a widespread shortage of skills and resources that are needed to implement effective database security controls across their growing data store landscape.

Although databases and their contents are vulnerable to internal and external threats, there are many tried and tested database security best practices, tools and controls that can help you secure your data stores, mitigate risk, demonstrate compliance and significantly reduce the number of attack vectors keeping you up at night. We created this Mighty Guide so that security leaders can share their insights on how their organizations have successfully protected their data and databases in today's formidable threat environment.

Regards,
Andrew C. Herlands, CISSP
VP, Global Systems Engineering
Trustwave

Trustwave is a leading cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data, and reduce security risk. Offering a comprehensive portfolio of managed security services, security testing, consulting, technology solutions and cybersecurity education, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.

Trustwave®

There's a New Leader in Cybersecurity

A Leader
2018 Magic Quadrant
for Managed Security Services,
Worldwide

Gartner.

Cybercriminals are relentless. So are our security experts, ethical hackers and
researchers. Recognized as a leader by the top cybersecurity industry analysts and
media outlets, they protect data around the clock for businesses in 96 countries.
Transform the way your business manages security with cloud and
managed security services from Trustwave.

TABLE OF CONTENTS

CHRIS THOMPSON

**GLOBAL DIRECTOR, IT
SECURITY AND CONTROLS
BENTLEY SYSTEMS**

DANIEL SCHATZ

**CISO
PERFORM GROUP**

DAVID BILLETER

**CISO
CA TECHNOLOGIES**

DILIP PANJWANI

**CISO & IT CONTROLLER
LARSEN & TOUBRO
INFOTECH LTD (LTI)**

JONATHAN LEVINE

**CTO, CIO, CISO
INTERMEDIA**

LESTER GODSEY

**CISO
CITY OF MESA, ARIZONA**

RICHARD RUSHING

**CISO
MOTOROLA MOBILITY, LLC.**

CHRIS THOMPSON

Global Director, IT Security
and Controls
Bentley Systems

Chris Thompson is a global director of information security who works with commercial organizations to establish risk-based information-security programs. Thompson understands the challenges of a cost-effective program that can adapt to the rapidly evolving threat landscape. He has implemented strategies designed to meet the business requirements of securing information, while ensuring compliance with regulatory obligations. He is a CISSP, CISM, and GLEG with an MS in Security Management.

in
LinkedIn

When securing databases in the cloud, all the database-security strategies and techniques still apply. You still have to know what database assets you have, how you are managing access, how you are segregating duties, and how you are doing encryption and data validation. You also have to understand the controls in the environment, the systems that are coming in and out of your database environment, what's normal, and what is a deviation from normal. "I think all of those principles that are very traditional in the security mindset still apply," says Chris Thompson, global director, IT security and controls, at Bentley Systems. "The challenge comes in applying these common security principles when your database is now a service running in the cloud as opposed to a server in a data center. How do you ensure segregation of their environment? How do you ensure encryption within their environment? How do you ensure proper access?"

This practical reality means several things when you are doing an overall capabilities assessment to determine what you need to secure and how you are going to secure it. For example, one thing you need to know is where your databases are located, but using a cloud database may force you to define "location" differently. "If the database is in my business's data center, I can go to the server room and point to an array of hard drives and say that's where my data is. If I'm using Microsoft Azure, I can tell you that it's in the US East. I can't tell you what system or which drive," Thompson explains. The cloud provider may store redundant instances of your data as a reliability measure, and that could be anywhere. "You have to more loosely define the term 'knowing where your data is,' and then rely »

> " *I think all of those principles that are very traditional in the security mindset still apply.* "

on vendor controls to actually do more detail protection of the data in that environment," Thompson says.

These uncertainties make it more difficult to quantify the risk to your data. To offset that unpredictability, many people responsible for securing their cloud databases rely more on encryption and granular data controls. "You really have to drive the security controls down to the data level and the record level," Thompson says. "A lot of people are not there yet, but I believe the world is well on its way to encrypting every field and every record." ∎

> **"**
> You really have to drive the security controls down to the data level and the record level.
> **"**

KEY POINTS

1 When you move a database to the cloud, you still have to know what database assets you have, how you are managing access, how you are segregating duties, and how you are doing encryption and data validation.

2 To offset unpredictable risks associated with hosted databases, many people responsible for securing their cloud databases rely more on encryption and granular data controls.

DANIEL SCHATZ
CISO
Perform Group

Daniel Schatz is CISO at Perform Group's London office. Prior to this he led the global Threat and Vulnerability Management program for Thomson Reuters. He is a chartered security professional (CSyP) and a member of the International Systems Security Association (ISSA-UK), and he holds several qualifications including CISSP, CISM, CCSK, CVSE, MCITP-EA, ISO 27001 LA/LI, and MS Information Security and Computer Forensics.

Twitter I LinkedIn

One of the greatest challenges when securing databases is gaining adequate visibility to know what data you need to protect and where it is located. This is essential for building a manageable regime of access and governance controls. Daniel Schatz, chief information security officer (CISO) at Perform Group, believes the General Data Protection Regulation (GDPR) has been instrumental in helping businesses come to terms with their data. "GDPR's data-register requirement imposes a whole new consciousness about what kind of data we hold. This plays toward information security because we now have people collecting that information," he says. He also notes the impact this has had on the question of database visibility. "A year or so ago I had much less visibility into what kind of data we held and where we had it. GDPR brought that visibility for entirely unrelated reasons, but now I know which part of the business holds which data and how they process it. I can make use of this."

How does this kind of visibility help with data security? First, it enables you to classify data according to how it needs to be protected and the its value to the organization. "You have to separate out your most valuable data," Schatz explains. "The key is understanding what data you have and where you store it. Then you can segregate out what you really need to protect so you can focus your spending on that critical data. Similar to Payment Card industry [PCI] protection requirements. You don't want to protect your whole environment under PCI." Another example is the kind of data Schatz's »

> **GDPR's data-register requirement imposes a whole new consciousness about what kind of data we hold.**

company handles as part of its sports media operation. "We have data on player performance which can be sensitive, personal data," he says. "It does not fall under the healthcare data regime, but it is governed by GDPR. We would not put that in the same database environment as we have our usual sports statistics."

Once you have this level of visibility and understanding about your data, then you can make proper decisions about how to handle, process, and protect it. Schatz says that once again GDPR is helpful in making these decisions. "There are certain requirements dealing with sensitive data. For example you may need to encrypt it, you may need to manage it very closely, who has access to it and what is happening to that particular data set." He also points out that it's not just about regulatory compliance. There are practical security-management reasons for looking at data in this way. Schatz notes, "The more you can break that down into defined requirements, the more you can narrow down your controls. This is important, because database-security functions cost money, so you want to understand what you need to buy." ■

> " Database-security functions cost money, so you want to understand what you need to buy. "

KEY POINTS

1 Visibility into the types of data you have and how you process it helps you determine its value to the organization and how you need to protect it.

2 Classifying your data by defined requirements not only helps with regulatory compliance, it helps you make wise decisions when investing in database-security functions.

DAVID BILLETER

Chief Information Security
Officer
CA Technologies

David Billeter is chief information security officer for CA Technologies, where he is responsible for leading CA's global and diverse information security and IT risk strategy. Previously he led information security for Staples and the InterContinental Hotels Group. Outside of the office, David is an active member in the cyber security industry in the Boston area.

Website I Blog I LinkedIn

Many organizations cannot protect every piece of their data, and in most cases they would not want to go to that expense. David Billeter, chief information security officer (CISO) at CA Technologies, says you must focus on your most critical data. "You've got to figure out what you really care about and what the processes are for using that data, and make sure that when that particular data is being used, it's going through the kind of processes that protect everything."

So an important step in securing databases is knowing what data you have and where it is located. This includes knowing how your data is being shared and how third parties who use it manage the data. Additionally, you need to understand any regulatory requirements that apply to your data. Only by knowing all these things are you able to build and enforce database-protection policies. Key among those are:

- **How you encrypt.** Encrypting database data is very important, but many people have poor encryption implementations. Billeter says, "One thing people often overlook when they're implementing encryption is you have to be very, very careful about the kind of encryption you're using, and how you manage the encryption keys themselves. I've seen many cases where they used very substantial encryption on the data, but the keys were relatively easy to get."

- **Managing database administrator (DBA) access.** DBAs are going to have access to decrypted data. "You need to make sure that any privileged or administrative database access is carefully protected," Billeter explains. "This means using tools to create a privileged access-management regime around all DBA credentials so that it's much more difficult to get that kind of access." »

> " *I've seen many cases where they used very substantial encryption on the data, but the keys were relatively easy to get.* "

- **Processes that minimize the spread of database data.** This encompasses everything from what data you store, to who has access to it, to how you back it up. Managing these things can be difficult, yet new regulatory requirements such as the EU's General Data Protection Regulation (GDPR) are requiring many companies to strengthen their processes. Billeter cites examples. "It's a problem if someone asks to be removed from your list and a couple of weeks later they get an email from your company. They may not have received that message through your company's email. It might have come from the marketing company that you hired, and they ran the campaign from their data set. Or, if for some reason you do a backup and restore, you need to be able to recreate privacy or regulatory changes that you made in the meantime. A restoration can restore things to a previous status. These can be problems as companies that face stronger regulations around the data they store." ∎

> " You need to make sure that any privileged or administrative database access is carefully protected. "

KEY POINTS

1 An important step in securing databases is knowing what data you have and where it is located. This includes knowing how your data is being shared and how third parties who use it manage the data.

2 Processes that minimize the spread of database data encompass everything from what data you store, to who has access to it, to how you back it up.

DILIP PANJWANI

Chief Information Security
Officer & IT Controller
Larsen & Toubro
Infotech Ltd (LTI)

Dilip Panjwani is a hardcore professional with 18-plus years of experience in IT and IS. He is a seasoned, hands-on manager with a proven record of developing and implementing information technology systems and information security controls based on global best practices. Panjwani is the head CISO, chief data privacy officer, and IT Controller for Larsen & Toubro Infotech Ltd. Previously, he was the director of information security at FIS Global.

 Twitter | **Website** | **LinkedIn**

D ilip Panjwani, chief information security officer (CISO) and IT controller at Toubro Infotech, sees two principal areas that contribute to protecting databases. These include securing data that is in the database, and securing the database application.

Protecting data inside the database requires balancing a number of factors that maintain principles of confidentiality, integrity, and availability and comply with regulatory requirements — and do all that without undermining database performance. "Whenever you put a security control on the database, whether to harden access or have encryption, it impacts the performance of the application and the database," Panjwani points out. That's why it's necessary to consider the kinds of controls you are applying, who they are controlling, and the specific business security and compliance requirements they are serving. "The strategy has to consider first of all analyzing what is the data that the organization really wants to protect and what kinds of protection are needed from the perspective of compliance, business security, and users," he adds.

Securing the database applications themselves becomes part of your vulnerability-management strategy. "You need to take a look at your vulnerability-management processes at the organization level," Panjwani says. This requires classifying your various assets based on the data types that are hosted on the system. This classification may be something like a criticality index of high, medium, and low, and using that classification to determine how frequently you scan the systems for vulnerabilities and patching status. There are various ways of managing this process. "Many »

> " *Whenever you put a security control on the database, it impacts the performance of the application and the database.*

organizations look at outsourcing this activity to a third-party vendor," says Panjwani. "Some go into a cloud solution, or they choose a solution within the organization and perform the scans themselves. An organization needs to consider a healthy balance of compensating controls where risks cannot be mitigated directly due to application or business constraints." ■

> **"**
>
> **You need to take a look at your vulnerability-management processes at the organization level.**
>
> **"**

KEY POINTS

1 Protecting data inside the database requires balancing a number of factors that maintain principles of confidentiality, integrity, and availability and comply with regulatory requirements — and do all that without undermining database performance.

2 Securing the database applications themselves becomes part of your vulnerability-management strategy.

JONATHAN LEVINE

Chief Technology Officer,
Chief Information Officer,
Chief Information
Security Officer
Intermedia

As CTO, CIO, and CISO at Intermedia, Jonathan Levine manages and directs 200 matrixed staff members. He has more than 20 years of experience guiding technology operations through financial, operational, and key decision-making by identifying, quantifying, and managing risks and opportunities for organizations and clients. He leads all aspects of solutions delivery for significant global initiatives, from initial conception through delivery.

Jonathan Levine, chief technology officer, chief information officer, and chief information security officer (CTO/CIO/CISO) of Intermedia, says that securing databases requires using several tools specifically for that purpose, but also applying best practices that help keep database data safe. Here are his recommendations:

- **Scan for vulnerabilities.** IT environments are always changing, so scanning must be ongoing. "We have software that scans for the most obvious database vulnerabilities. And before we deploy major releases, we have a third party come in and audit our systems," Levine says.

- **Know where your data is.** Keeping track of data is difficult in a dynamic IT environment. Things grow organically, people come and people go, and it's often hard to know who's got what data. "We run script periodically that looks on people's laptops and checks for things that look like credit-card numbers," says Levine. "Sometimes people take shortcuts and put credit-card numbers in Excel or Notepad."

- **Minimize the data you put into databases.** Levine recommends not storing any more data than you have to. "Look at the data you are storing and make sure it's absolutely the minimum data set you need," he says. "If you don't put data in the database, it's not at risk." A recent incident in which a prominent airline lost a large number of credit-card numbers, including expiration dates and CVV codes, illustrates this point even though it was not caused by a »

> **" We have software that scans for the most obvious database vulnerabilities.** "

database penetration. Most payment processors now offer tokenization so that there is no need or reason to store credit-card data.

- **Encrypt database data.** Levine recommends encrypting all data stored in the database. "Data that you have to put in the database should be encrypted," he says. "If somebody gets access to the whole database, it's of no use to anyone without decryption keys."

- **Segment your network.** Levine explains, "You should know which systems will be accessing the database. Those systems should be the only ones allowed to talk to the database server. If another machine is doing that, then you know you have a problem."

- **Test software that accesses the database.** "Check software you are deploying that accesses the database to make sure it doesn't have simple bugs around information formatting," says Levine. One example is using web forms to execute database commands. "This is an old, well-understood, and well-exploited issue that people still struggle with," he notes. "You still find websites where you can execute a database command because the input isn't sanitized when somebody types something into a web form." »

> " Look at the data you are storing and make sure it's absolutely the minimum data set you need. "

Levine also emphasizes the importance of a culture that encourages security without being adversarial. You want people to learn from their mistakes. "If you fire somebody the first time, what you've taught everybody else is that if they make a mistake, they're fired," he says. "The incentive to them is don't let anybody know I've made a mistake." That attitude can be disastrous if you are trying to keep your data safe. ■

KEY POINTS

1 Only give database access to systems that need it. An unauthorized machine accessing the database is a clear indication of a problem.

2 Before deploying, you should check software that accesses the database to make sure it doesn't have simple bugs around information formatting, such as the ability to launch database commands from a web form.

LESTER GODSEY

Chief Information Security Officer
City of Mesa, Arizona

Lester Godsey is the CISO for the City of Mesa, Arizona. With over 24 years of public-sector IT experience, Godsey has presented at the local, state, and national levels on topics ranging from telecommunications to project management to cybersecurity. He has taught technology and project management at the collegiate level. A published author, he holds a BA in Music and an MS in Technology from Arizona State University.

in
LinkedIn

When it comes to protecting databases, Lester Godsey, chief information security officer (CISO) for the City of Mesa, notes the incredible variety of data a municipality manages. "Municipalities are like big conglomerates," he says. "We have development services where we do building inspections, permitting, and code enforcement. We have public safety. We have to deal with HIPAA [Health Insurance Portability and Accountability Act] and PCI [Payment Card Industry]. We have utilities. We have gas, wastewater, water, and electricity. We have economic development, so we have a lot of sensitive information from a business perspective. We have all these verticals similar to what you might see in larger organizations, but not as many resources. Still, we face the same constraints and challenges."

Godsey says the first step in protecting all the database assets associated with these activities is knowing what you have. "You have to have an inventory, because you can't protect your data if you don't know what you have and where it's located. It's amazing how many organizations don't have an authoritative and accurate inventory of all their data resources." Finding your data is not easy because in a complex IT environment, it can be in many places.

In addition to having a data inventory, Godsey also says that data classification is an essential part of a database security strategy. "We have a lot of data that we make public to residents and businesses. That's treated differently than data that needs to be confidential, for internal use only, and then »

> ❝ *It's amazing how many organizations don't have an authoritative and accurate inventory of all the data resources.* ❞

there's data some people in the organization can access and others cannot," he explains. "This can be a mix of classification based on compliance requirements and usage."

Finding data, classifying it, and enforcing rules around access and use requires tools and automation. These are tools that scan the environment, identify data and determine its classification and which controls should be applied to it. "I can't think of a better example for the need of automation and orchestration than data classification and data management as a whole," Godsey says. "You could put the best process in place, but if you rely on human beings to manage and adhere to those processes across all that data, it just won't happen."

Another challenge in securing databases is that code changes, sometimes frequently. Godsey says there needs to be a DevOps workflow in which security becomes part of an iterative process that is integral to the lifecycle of software development. "You need to carry out testing and scanning during code development," but he also notes that you still have to do regular vulnerability scanning in the production environment. "You still need to do your standard vulnerability scans to look at the databases and the applications they are built upon." Effectively securing databases requires a multipronged approach that includes data discovery, classification, access management, and code integrity. ∎

> " I can't think of a better example for the need of automation than data classification and data management as a whole. "

KEY POINTS

1 Finding data, classifying it, and enforcing rules around access and use requires tools and automation. These are tools that scan the environment, identify data, and determine its classification and which controls should be applied to it.

2 Effectively securing databases requires a multi-pronged approach that includes data discovery, classification, access management, and code integrity.

RICHARD RUSHING

Chief Information Security Officer
Motorola Mobility, LLC.

Richard Rushing participates in several corporate, community, private, and government security councils and working groups, setting standards, policies, and solutions to security issues. As CISO for Motorola Mobility, he has developed an international team to tackle the emerging threats of mobile devices, targeted attacks, and cyber-crime. A much-in-demand international speaker, Rushing has presented at many leading security conferences and seminars around the world.

Twitter I LinkedIn

Database security begins with understanding the importance of the data in the database. Richard Rushing, chief information security officer (CISO) at Motorola Mobility, puts it this way: "The security controls you use are determined by the most sensitive piece of data in the database," making the point that even in the largest databases, the most sensitive data becomes the common denominator that governs the security regime for the entire database. This security regime encompasses physical security of database servers and user access to the data in the database.

User-access controls include role-based rules and privileges given to users who require access to the database. Managing these controls in a constantly changing user environment is a major challenge in securing databases. In addition to rules that limit exactly what specific users are able to do in the database, there are a number of controls that regulate and recertify those privileges. For example, some organizations base their privilege review on access patterns. "Every 60 days I might want to take a look at who has access to the database to see if they still need access, or if they've moved on to another project and no longer need that level of access," Rushing explains. "Some people use logs to monitor access. If a user hasn't logged into the database in the past 30 days, their access is modified or dropped because they are not using or adding data to the database." These strategies limit database exposure.

In addition to user-access controls, the database itself can be hardened. One approach to database hardening is encrypting all data in the database. "If the data is encrypted, that's not going to »

> **The security controls you use are determined by the most sensitive piece of data in the database.**

prevent data theft, but it is going to prevent bad things happening as a result of stolen data," says Rushing. He notes there are a number of ways to implement data encryption, and the best way depends in part on the application. For example, encryption can add undesired processing overhead in a high-volume transactional database. In a case like that, hardware encryption can provide an advantage. "If I have encrypted drive capability, then I can use encrypted volumes on the database," Rushing says. "It's faster, and it just happens automatically." In fact, he favors applying the latest technology, such as hardware encryption, when setting up a new database.

One of the biggest challenges to security is database proliferation, in which users copy data for a project and then forget about it. It's now very easy to set up a temporary database and copy data into it for a specific purpose. "A lot of proliferation is just people doing the wrong thing," Rushing says. "They take a subset of data and copy it to someplace else. Now you've taken your data and replicated it in two places. There should be no reason to copy data. You really need to work with business teams to control that. If there's a problem of users not being able to do what they need in the secure database, let's figure out why."

Still, proliferation happens, and part of securing the database is making sure you know where all the data is located. There are a number of tools you can use to do this. "There are tools that help you search your environment, and they can be part of a vulnerability scan," suggests Rushing. "You can also look for certain kinds of traffic. For instance, if just one person is using a database, that's a one-person database that might indicate replicated data. You can »

> " There are tools that help you search your environment, and they can be part of a vulnerability scan. "

also get a lot of information just from the network tools. For example, looking at your top SQL connections allows you to spot unexpected things, such as a non-database server with an SQL tool set on it. You can also use endpoint tools, because endpoints connect to databases. Look for traffic and protocols that are actually used."

Being able to track and identify database data not only helps secure your data, but it is an essential part of regulatory compliance, whether that is complying with the General Data Protection Regulation (GDPR), or operating in China where rules require Chinese data to stay in China. Rushing emphasizes that it comes back to having controls to verify the data that you have, and to validate access to that data. "It also boils down to having really good auditing and good end-to-end logging on all the systems that connect to the database." ■

KEY POINTS

1   Being able to track, identify, and verify database data, and being able to validate access, not only helps secure your data, but it is an essential part of regulatory compliance.

2   There are various techniques for keeping track of database data, including monitoring network traffic and protocols that are actually used, and monitoring endpoints, because endpoints connect to databases.

DAVE WHITELEGG

Capita plc, Group Cyber Risk
and Intelligence Officer

Twitter | LinkedIn

" The foundation on which a sold data-center security strategy is built is information asset management. By identifying and then understanding the value of the databases (information assets) to the business and to threat actors, efficient security controls can be deployed which reflect both the business importance and the threats to each specific database or groups of databases. "