IDERA® | SQL Security Whitepaper

THE SQL SERVER SECURITY THREAT... IT'S CLOSER THAN YOU THINK

BY KEVIN BEAVER, CISSP

INTRODUCTION

Today, business is about data. Database systems and the elements they store are arguably the most valuable assets in any given enterprise. Not only are business executives and IT leaders responsible for doing what's right to protect the business's best interest, they're obligated to comply with the seemingly endless list of industry and government-imposed regulations.

As we've seen for more than a decade, database-related security breaches can't be taken lightly. One of the greatest threats to databases is insiders with ill intent. Computer networks have become so complex that it's easy for database administrators and IT managers to overlook database security gaps that are easily exploited without anyone ever knowing about it. Security weaknesses that would've been considered obvious and relatively simple to fix not that long ago are now the Achilles heel of modern business.

These challenges have created an environment where not only can a lot go wrong but there's also so much to lose. This is especially true when you don't have the proper culture combined with the proper business and technical controls/tools to ensure database security and compliance are kept in check. All it takes is one oversight, misstep or bad choice by a malicious insider and you've got a database security breach on your hands that you and your business executives may not be prepared to take on.

WHAT YOUR BUSINESS IS UP AGAINST

Compliance is often seen in a negative light. It's not just big government agencies and industry bodies trying to tell executives how to run their businesses. The reality is that information security and privacy-related regulations have been put in place because so many business owners and managers ignored the generally accepted practices for keeping their information systems in check. In other words, they disregarded the security basics, which have been around for decades.

Despite all the compliance regulations and increased awareness, SQL Server systems are often wide open for attack. They're one of the biggest targets for the bad guys because, as a bank robber will tell you, that's where the money is. Today's business reality is showing us that you can be "compliant" with any set of regulations at any given time, yet a single misstep or exploit of a database system can take your entire business out of compliance.

Staying on top of all the known – and yet to be discovered – SQL Server weaknesses can be difficult enough. Throw in various regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), as well as the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act into the mix and you've got yourself some seemingly insurmountable business challenges. The directives and penalties included in the General Data Protection Regulation (GDPR) for protecting the Personally Identifiable Information (PII) of EU citizens only add more fuel to the fire.

Generally speaking, compliance is not as difficult as it appears. Look closely at each of these regulations. You'll see that they're nothing more than a set of security best practices designed to help minimize business risks. They help ensure systems availability and safeguard the confidentiality and integrity of sensitive information. In order to determine where you need to focus your compliance efforts you have to consider the specifics of each regulation including:

1. **What's the general goal of the regulation?**
2. **What unique policies and technical controls are required to achieve compliance?**
3. **What gaps currently exist between where you are and where you need to be?**
4. **What are the regulators and auditors ultimately going to expect of your business in terms of your information security and privacy programs?**

Going beyond these government and industry regulations, you also need to look at specific contracts and service level agreements that your business is bound to. These are not specific "compliance" requirements but they're still commitments the business has made to business partners, customers, and other interested parties to ensure information security and privacy.

Finally, it's people that are at the core of database compliance and information security. Understanding and cooperation on the part of your users, management, IT and information security staff and even business partners are critical. The last thing you need is for compliance and security to be mired in political problems. It can happen. So, you have to be savvy about balancing everything for the greater good of the business.

THE DBA'S ROLE IN COMPLIANCE

Database administrators (DBAs) play a critical role in ensuring that database security is kept in check and related business risks are minimized. If you're currently working in this role or managing someone who is, it's important to understand what's required to pull everything together for reasonable SQL Server security and compliance.

There are numerous factors that determine how you manage database-related compliance and security initiatives including: the size of your business, the number of database systems that fall within the scope, and your overall network complexity – both in-house and in the cloud. Even the industry in which your business operates can shape the challenges and necessary approaches. For example, DBAs working in the financial industry will likely have more of a compliance burden than DBAs working in manufacturing. Ditto for healthcare versus non-profits. Every industry is different and every business has its own unique needs.

All things considered, the time and effort required to manage database security and compliance can easily add up to be a full-time job. The problem is that time is the scarcest resource in IT and there seem to be fewer and fewer resources to take on these evolving challenges.

IT professionals are being pulled in multiple directions all the time. This can result in just the opposite of the desired outcome for database security and compliance. DBAs in particular are often putting out fires to "keep the joint running" and very little time is left for higher-level work such as addressing database security and compliance at the strategic level of the business.

Business managers that force more compliance-related job duties on existing DBAs who are already stretched thin will likely set everyone up for failure. It's a basic time management principle – if you're going to take on something new, you've got to be prepared to stop doing something else. What's that something else going to be?

Given what's at stake, as long as you can see the bigger picture of database security and overall information risk management and take the appropriate steps toward gaining control over time, you'll do fine. It's the managers and DBAs who choose to ignore the obvious that end up creating more problems for their businesses than they solve.

The key with compliance is that you have a choice in the matter. Compliance is not black-and-white. From initial risk assessment to ongoing visibility and control, there are infinite shades of gray and you get to choose how to approach each area in your business. The important thing is to have compliance on your radar and understand that every decision you make around SQL Server and database management will ultimately impact compliance and the overall security posture of your business.

UNDERSTANDING THE DATABASE SECURITY THREAT

In order to truly manage database-related risks, you've got to understand what you're up against. The media has portrayed the threat to be a young punk trying to crack into your network in the middle of the night. But that's not necessarily true, especially when it comes to database hacking. Instead, there are targeted attacks – often government supported – that are carried out via social engineering, namely email phishing. A few well-placed emails combined with some gullible users is all it takes for an outside entity to penetrate your network and ultimately access critical databases that were assumed to be locked down from external attack. This attack alone can negate all other security efforts and investments and, as I have discovered in my work, it's very simple to carry out, even in organizations with well-established security awareness and training programs. The same goes for unsecured Web applications that allow SQL injection – a vulnerability that's a top finding among information security studies year after year.

Looking at this pragmatically, there's just as much of a threat on the inside of your network. In fact, one of the greatest threats to your critical databases is likely a trusted insider working in your environment this very moment. According to the Ponemon Institute's 2016 Cost of Cyber Crime Study & the Risk of Business Innovation, malicious insiders contribute to the most costly cyber crimes. The study also found that insider attacks make up 41% of attacks, on average, and can take more than 52 days to contain, resulting in an annualized cost of $167,890 – a cost that has increased by over 50 percent in less than a decade.

But why would insiders raid your databases? Simply put: because they can. They may be curious. They may have a vendetta for someone in management. They may even be hurting financially at home and see it as an easy way out. Regardless, employees, contractors, and other users in your environment often have full, unfettered access to any database system they want and you may not even know about it. They have a network connection. They have privileged accounts. They even have your trust. People with ill intent know that the odds of getting caught are in their favor. They know that their "attacks" will likely go unnoticed. Even if something turns up, they know they'll be long gone and the business will have a hard time piecing together the steps that led up to the breach.

The real kicker is just how easy it is to exploit any given SQL Server environment. Many – arguably most – SQL Server security weaknesses are low-hanging fruit that require minimal technical skills to exploit. Turning seemingly benign weaknesses into serious compliance violations and business risks only takes a matter of minutes.

Improperly secured and managed SQL Server systems create enormous business risks – these are issues you might not discover until it's too late such as:

- Unsecured SQL Server systems (often the Express version) placed on the network by random employees that no one knows about or that have been around so long they've been forgotten – something easily discovered using commercial vulnerability scanners and even free tools such as SQLPing
- Weak or blank passwords on privileged accounts providing full database access to anyone that downloads, installs, and runs SQL Server Management Studio Express
- Orphaned and backdoor user accounts that aren't being monitored
- Missing SQL Server patches that can be scanned for and exploited using a free tool such as Metasploit to provide full remote access to anyone on the network
- Unsecured development databases that house – and expose – production data
- Database backups that aren't encrypted or are encrypted with the key stored directly on the backup media – something that exposes your databases to external parties when a backup tape is lost
- Data that's been extracted from the database and placed on unsecured network shares or unencrypted laptops or external hard drives – something that exposes your databases to external parties when a laptop or drive is stolen

In practically every internal network security assessment I perform, I find these database security weaknesses. An insider exploiting just one of these issues can lead to complete database exposure and compliance violations that will have a lasting impact on the business.

You have to ask yourself if your business is prepared to proactively handle these situations. How are you going to answer to your board, your shareholders, or even business partners and customers when one or more of these weaknesses is exploited and something goes awry in database land?

WHAT YOU CAN DO TO MINIMIZE DATABASE RISKS

There's an irrefutable law of information security: you cannot secure what you don't acknowledge. Yet, that's the mode of operation for many businesses when it comes to keeping their database environments in check. The assumption is that the four walls of the building will keep critical databases safe from harm. This is a dangerous mindset. If your databases are out of sight and out of mind, the same will likely hold true for the threats your business faces. That's when it's easiest to get bitten and most definitely when it will hurt the greatest.

You've got to understand the weaknesses and then take the appropriate steps to do something about them. The higher-level process goes like this:

1. **Know what you've got.**
2. **Understand how it's at risk.**
3. **Do something about it.**

Getting more specific, a detailed information risk management program consists of:

1. **An initial risk assessment to determine where you need to focus your efforts**
2. **Documenting the necessary policies, supporting procedures and contingency plans**
3. **Use of technical controls to help enforce your policies wherever possible**
4. **Open communication between IT and management on what's working and what's not**
5. **Setting users' expectations regarding what they should and should not do**
6. **Periodic and consistent checks for new threats, vulnerabilities and risks**

An important factor in minimizing database security risks is to not get caught up in all the regulatory minutiae and address every requirement in a standalone fashion. Instead, you can address most of the required regulations across the board at the same time. Again, the big regulations like GDPR, PCI DSS and HIPAA/HITECH are saying the same basic things. If you want to be more efficient, then it's important to address database security – and security overall – from a risk management perspective.

You can analyze each regulation and map all the requirements on your own or you can use third party resources such as the Unified Compliance Framework (http://www.unifiedcompliance.com) where other people have already taken the pain out of the process for you. The important thing is to make sure you're working towards addressing your database security risks at the highest level possible. Anything less and you're likely to just end up spinning your wheels and driving yourself crazy in the process.

IT is constantly in a state of flux. Being proactive with all the changes taking place in any given environment is one of the biggest challenges that businesses face. There's not a simple solution for getting your database environment under control other than the fact that you're going to have to be methodical and concise in your efforts. Simply putting this control or that control in place to merely please an auditor or check a checkbox and assuming all will be well moving forward won't cut it.

A key aspect of database security and compliance is having the proper visibility. You're going to have to get the proper insight needed to make good decisions. Insight into what's taking place at any given time will help you stay on top of the threats and allow you to respond in a more mature and professional manner when something goes awry. You'll also be able to prove your security or compliance status at any given time – something your auditors will love.

Good visibility requires good tools. I have yet to see any business that's able to effectively manage database security risks without the proper tools. Manual processes for managing database security are not only time-consuming; they're also highly inaccurate which can create more problems than are solved. Given your limited time and resources, you can't afford to assume that you have all the right information when you need it.

The final tie-in that will help bring database security and compliance full circle is reporting. Once the basic database controls are in place, your long-term success will depend on how well you stay on top of your security and compliance-related reporting. Some reporting will be for your own purposes such as access management, security standards, and system maintenance. Other reporting will be done for the benefit of your internal auditors, regulators, and executive management. Again, good tools play an important role.

In the end, you want to be able to prove where things stand at any given point. Being able to demonstrate the current security posture of your database environment will help you stay on top of compliance requirements, stay on good terms with your auditors, and most importantly, keep your database-related risks to a minimum.

There's an irrefutable law of information security:
you cannot secure what you don't acknowledge.

TO COMPLY OR NOT TO COMPLY, IS THAT THE QUESTION?

Compliance is not an option. Many business managers and IT staff often treat it that way but that's a risky approach. Like it or not, compliance as we know it isn't going away. In fact, given the transformation taking place in IT including the dependence on electronic information and insider threats looking to take things down, the traditional compliance requirements we've known will only grow more complex.

Today's auditors, regulators, and lawmakers have a unified voice and will go to great lengths to ensure that management understands the compliance requirements of the business. The same people are often quick to point out the consequences of security breaches and the resulting non-compliance such as business disruption, lost revenue, fines, negative media coverage, and damage to your brand.

As real as they are, I've found that management often takes these consequences with a grain of salt – sometimes as veiled threats – that don't really inspire action. Another way you can put it to management is to talk in terms of cost. As past studies have shown, the cost of non-compliance is often much greater than the cost of compliance. So, avoiding compliance can be a bad financial decision in and of itself. It's ultimately up to management to make this call, but it's your responsibility to get the message across that database security is not something to be taken lightly.

When communicating your message, focus on the business aspects of database security and compliance. For most businesses, information integrity and system availability are key drivers. Find out ways you can talk about those areas and demonstrate their value to the business's bottom line.

The mere act of working together with IT, compliance and security staff to come up with "how" things can be done rather than "No, that can't be done" is key.

Another important fact to keep in mind – something the regulators and auditors won't tell you – is that a security "incident" doesn't always translate to data exposure. The details come out in forensics investigations, which are often overlooked or dismissed. Also, it's important to remember that compliance is not all about protecting PII. Instead, it's about protecting all types of information that contribute to the business's fiduciary responsibilities including intellectual property, human resources records, and financial reporting information for SOX compliance. Obviously, intellectual property in the traditional sense is not covered by these regulations but it would certainly behoove you to bring all sensitive and valuable information under your risk management umbrella.

In the end, it pays to be proactive. Wait around to address security and compliance after an incident occurs and it'll be too little, too late. As Murphy's Law says, "There's never time to do it right but there's always time to do it over." Don't fall into this trap!

MOVING FORWARD

Focus on managing your information risks. It's as simple as that. Look at the entire picture. Think about everything you're doing today regarding SQL Server security. From database access controls to software patching to audit logging to backups, everything you do counts.

Database security and compliance can seem overwhelming. If you understand what you're up against along with what there is to lose, and then you proceed with getting the right people on board and acquiring good tools, you'll no doubt be ahead of the security curve. You'll minimize the threat and ultimately set yourself, your users, management, and your business up for success.

As the Chinese proverb goes: dig your well before you're thirsty. Thinking long term and preparing your business to ward off database security threats can have tremendous payoffs. It's up to you to make things happen.

IDERA SOLUTIONS FOR MICROSOFT SQL SERVER COMPLIANCE & SECURITY

IDERA offers award-winning solutions to help you meet your compliance and security needs, and each one offer a fully-functional free trail:

IDERA's award-winning SQL Compliance Manager provides low-impact SQL Server auditing of all user activity and data changes. **START FOR FREE**

IDERA SQL Secure helps you manage SQL Server security and permissions to find out who has access to what, and how permissions are granted. **START FOR FREE**

Extend your security to backups with IDERA SQL Safe Backup, which offers accelerated, compressed and encrypted database backups along with data recovery and restoration. **START FOR FREE**

REGULATIONS IMPACTING DATABASE SECURITY

Practically every IT-related regulation can be tied to database security in some way. From the internal control mandates of SOX to the vulnerability management requirements of PCI, all roads seem to lead back to the database. Let's use HIPAA as an example. Within the HIPAA Security Rule, there are numerous required Administrative Safeguards in section § 164.308 of the regulation that apply directly to SQL Server security as follows:

1. **Risk Analysis**
2. **Risk Management**
3. **Sanction Policy**
4. **Information System Activity Review**
5. **Assign a Security Official**
6. **Isolating Healthcare Clearinghouse Functions**
7. **Response and Reporting**
8. **Data Backup Plan**
9. **Disaster Recovery Plan**
10. **Emergency Mode Operation Plan**
11. **Security Evaluation**
12. **Written Contract or Other Arrangement**

There are also two required Technical Safeguards in section § 164.312 of the regulation that apply in the same manner:

1. **Access Control**
2. **Audit Controls**

Each regulation has a unique approach but they all encompass security best practices that have a direct tie-in with database management.

Don't let compliance regulations drive your database security needs. Step back and look at the bigger picture and manage risks instead. Compliance will come about as a result.

COMMON SQL SERVER SECURITY QUESTIONS

If you haven't had the pleasure of experiencing a database security or compliance audit, odds are that you will at some point. As with any major "test", understanding where your auditor or assessor is coming from and what you can expect is key. Every audit or assessment is different but here are some real-world questions you're likely to encounter:

1. **What sensitive data is stored in this database?**
2. **Which user accounts have full access?**
3. **Who has access to the 'sa' and other privileged accounts?**
4. **How are changes to database security controls being managed?**
5. **How are SQL Server logs acquired and retained?**
6. **What is the current patch status for SQL Server and Windows?**
7. **How are backups performed and protected?**
8. **Can I see the results of your latest database security assessment?**

LINKS TO POPULAR U.S. COMPLIANCE REGULATIONS

Gramm-Leach Bliley Act (GLBA) Safeguards Rule

Health Information Technology for Economic and Clinical Health (HITECH) Act

Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Payment Card Industry Data Security Standard (PCI DSS)

Sarbanes-Oxley Act (SOX)

State Breach Notification Laws

ABOUT THE AUTHOR

Kevin Beaver is an independent information security consultant, writer, professional speaker, and expert witness with Atlanta-based Principle Logic, LLC. With over 28 years of experience in the industry, Kevin specializes in performing independent security assessments to help his clients uncheck the boxes that keep creating a false sense of security. He has authored/co-authored 12 books on information security including the best-selling Hacking For Dummies and The Practical Guide to HIPAA Privacy and Security Compliance. In addition, he's the creator of the Security On Wheels information security audio books and blog providing security learning for IT professionals on the go. Kevin can be reached at through his website at www.principlelogic.com and you can follow him on Twitter at @kevinbeaver.