<https://securityintelligence.com/get-serious-about-data-protection-to-secure-mongodb/>

Attackers stole data from thousands upon thousands of misconfigured MongoDB databases and demanding ransom money to get it back. Cybercriminals are going after even more misconfigured systems on the internet. The IT community has known for some time that default settings can leave databases open for attack. MongoDB has made no attempt to hide these issues. A technical rep from MongoDB posted on Security Intelligence about the importance of hardening the MongoDB server and following security best practices. Unfortunately, these education efforts won’t be understand by everyone. Or maybe people just plain didn’t know one way or another whether they were at risk. Data security software was invented to fill in those gaps. Manuals and warnings are scattered all over the world, but people forget things, fail to follow process and awareness to adhere to security best practices. IBM enhanced its Guardium Data Protection Platform to support MongoDB and developed the software with input from the MongoDB security team.

<https://martinfowler.com/articles/web-security-basics.html>

Way down at the bottom of the list of requirements, behind, fast, cheap, and flexible is “secure”. That is, until something goes wrong, until the system you build is compromised, then suddenly security is, and always was, the most important thing. Security is a cross-functional concern. Our business owners often know they need Security, but aren’t always sure how to quantify it.

[**https://www.techopedia.com/definition/29841/database-security**](https://www.techopedia.com/definition/29841/database-security)

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks.

It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment

[**https://study.com/academy/lesson/database-administration-and-security-definition-and-purpose.html**](https://study.com/academy/lesson/database-administration-and-security-definition-and-purpose.html)

**Who is responsible for keeping all the data secure in an organization? That would be the database administrator, or DBA.**

**Controlling data security, including preventing unauthorized access to the data and protecting against other security threats.**

**Setting data privacy, which means that only authorized individuals are able to see certain data. For example, there is no need for everyone in the organization to be able to see all the personnel files of all the employees.**

**Controlling access to the data helps to implement data security and data privacy policies.**

[**http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-engineering/database-architecture-and-security/#gref**](http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-engineering/database-architecture-and-security/#gref)

**An essential but often missing element in an information security program is a well-defined and complete information security architecture that reflects the business decisions and the information security policy decisions of the organization. The purpose of enterprise information security architecture is to address the organization’s need for a holistic approach to IT security that will provide enterprise-wide guidance to ensure that information security is approached in a consistent manner and with a consistent level of risk.**

[**http://ieeexplore.ieee.org/document/7755135/?reload=true**](http://ieeexplore.ieee.org/document/7755135/?reload=true)

**The common people used to think that cloud is the best place to store and retrieve the values virtually, and 62% of business entrepreneurs used to think that cloud is the best place to store the content but the case about security from hackers. A user might want to protect the privacy of his search queries for a variety of reasons, including protection of commercial interests and personal privacy. In the current era of digital world, different organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. A feasible solution can be presented to enable the owner to enforce access control of the data stored on a remote un-trusted CSP. Through this solution, the data is encrypted under a certain key, which is shared only with the authorized users.**

[**https://www.sciencedirect.com/science/article/pii/S2212567114004651**](https://www.sciencedirect.com/science/article/pii/S2212567114004651)

**To reduce the risk of loss and destruction of information stored in a database, the management of an organization should use the implementation of various security methods. A comprehensive strategy to secure a database is more than data security. Usually, security events can be associated with the following action: illegal access to data confidentiality damage, damage to the integrity of data, loss of data availability.**

<https://www.checkmarx.com/2016/06/24/20160624the-importance-of-database-security-and-integrity/>

**Databases often hold the backbone of an organization; Its’ transactions, customers, employee info, financial data for both the company and its customers, and much more. are all held in databases, often left to the power of a database administrator with no security training. Database security and integrity are essential aspects of an organization’s security posture.**

<https://en.wikipedia.org/wiki/Database_security>

Database security concerns the use of a broad range of information security controls to protect databases against compromises of their confidentiality, integrity and availability. It involves technical, procedural/administrative and physical.

<https://www.datamation.com/big-data/big-data-security.html>

Big Data deployments are valuable targets to would-be intruders. A single ransomware attack might leave your big data deployment subject to ransom demands. Even worse, an unauthorized user may gain access to your big data to siphon off and sell valuable information. The losses can be severe. Your IP may be spread everywhere to unauthorized buyers, you may suffer fines and judgments from regulators, and you can have big reputational losses.

<https://ideas.repec.org/a/rom/bemann/v3y2013i2p5-15.html>

This study provides a short literature review in information systems security (ISS) approaches either technical or non-technical in nature. Although, the benefits and uses of the technical information systems security approaches are valuable, there is still a need to investigate the alternative non-technical approaches or at least, to find a way to combine them in a more appropriate and thus, successful way.

<https://caseclosedsoftware.com/leads/>

Case Closed provides software to manage Tips and Leads that come in from the general public. Tips are entered into a database which can be auto assigned to a law enforcement professional. Optionally, a Task can automatically be created for that officer or investigator. Tips can be assigned to a Case or Incident and reported on as needed. Tips and Leads are very time sensitive and getting these leads in front of the officers/investigators in real time for follow up is critical to criminal activity and cases.

**Software**

<https://www.publicsafety.gc.ca/cnt/cntrng-crm/plcng/cnmcs-plcng/ndx/dtls-en.aspx?n=35>

Evidence and Reports (E&R) is a software program developed exclusively by the Royal Canadian Mounted Police (RCMP) to meet the needs of major case investigations. A “major case” is defined as an event that exceeds a unit/police services’ normal resourcing requirements. The system is typically used in situations where numerous personnel are required and allows for the creation of tasks and assignment of those tasks to investigators.

---<https://www.arms.com/>

ARMS Records Management allows your agency to create, maintain, and retrieve your case data. Whether in the office or on a mobile device, ARMS allows for seamless data entry. RMS allows your officers to create and submit case reports while in the field, and allows your administrators to assign 'required fields' for each Incident Code - working to ensure that the first time the case is submitted for approval will be the last time.

---<http://nicherms.com/>

The NicheRMS™ Police Records Management System is an incident-centric tool that manages information in relation to the core policing entities: people, locations, vehicles, organizations incidents and property/evidence. Policing includes managing incidents and, irrespective of the incident type, there are common information requirements in relation to the location, people involved, vehicles involved or property relevant to the incident.