bcs The Chartered Institute for IT

Standards that create the outstanding

Securing big data

The challenges – malice, misuse and mistake

Introduction

Big data can create business value by solving emerging business challenges. However, big data also creates security challenges that need to be considered by organisations adopting or using big data techniques and technologies says Mike Small, FBCS CITP.

There is now an enormous quantity of data in a wide variety of forms that is being generated very quickly. However, the term big data is as much a reflection of the limitations of the current technology as it is a statement on the quantity, speed or variety of data.

The term big data needs to be understood as data that has greater volume, variety or velocity than can be comfortably processed using the technology that you already have. Big data comes from a number of sources both internal and external. Many organisations have accumulated large amounts of data that they are not exploiting. There is an even larger amount of data that is held in publicly available sources, like government databases, social media, as well as data that organisations would be willing to share.

In addition the inbuilt instrumentation of smart systems generates a massive amount of, as yet, untapped data. To realise its potential value big data needs to be transformed into smart information, which can then be used to improve planning and increase efficiency as well as to create new kinds of products.

Information security challenges

The underlying information security challenges of malice, misuse and mistake apply equally to big data. Big data techniques can also be used by criminals to improve their exploits, provide insights that facilitate security breaches and aggregate data to assist with identity theft.

Big data can be misused through abuse of privilege by those with access to the data and analysis tools; curiosity may lead to unauthorised access and information may be deliberately leaked. Mistakes can also cause problems where corner cutting could lead to disclosure or incorrect analysis. The Cloud Security Alliance has published a report on the top ten big data security and privacy challenges.

There are three major risk areas that need to be considered:

Information life cycle: big data turns the classical information life cycle on its head. There may be no obvious owner for the data to ensure its security. What will be discovered by analysis may not be known at the beginning. The provenance of the data may be doubtful, the ownership of the data may be subject to dispute and the classification of the information discovered may not be feasible until after analysis. For all of these reasons the compliance requirements and controls needed cannot easily be predetermined.

Data provenance: big data involves absorbing and analysing large amounts of data that may have originated outside of the organisation that is using it. If you don't control the data creation and collection process – how can you be sure of the data source and the integrity of the data? How do you know that you have the right to use the data in the way

that is being planned? These points are brought out very clearly in a UK report on the use of smart metering of power consumption by utility companies .

Technology unknowns: the technology that underlies the processing of big data was conceived to provide massively scalable processing rather than to enforce security controls. While this is not a new phenomenon in the IT industry there has not been sufficient time for the inherent vulnerabilities and security weaknesses to become manifest.

Information stewardship for big data

Taking care to look after property that is not your own is called stewardship. Information stewardship is not a new term; it has been in use since the 1990s and covers the wide range of challenges involved in managing information as a key organisational asset. These include the management of the whole information life cycle from ownership to deletion as well as aspects like business value, data architecture, information quality, compliance and security.

The basic objectives of information security for big data are the same as for normal data being to ensure its confidentiality, availability and integrity. To achieve these objectives certain processes and security elements must be in place. There is a large overlap with the normal information security management processes, however, specific attention is needed in the following areas:

Everyone is responsible

The unstructured nature of big data means that it is difficult to assign the responsibility to a single person. Everyone in an organisation needs to understand their responsibility for the security of all of the data they create or handle.

Verification of data source

Technical mechanisms are needed to verify the source of external data used; for example digital signatures.

Systems integrity

There needs to be good control over the integrity of the systems used for analysis including privilege management and change control. Be careful to validate conclusions, if you can't explain why the results make sense they probably don't.

Always build in a way to check, don't let big data lead you to stupid conclusions.

Secure processing

Measures to secure the data within the analysis infrastructure are needed to mitigate potential vulnerabilities and to secure against leakage. These could include disk level encryption and a high level of network isolation. Big data should be secured in transit preferably using encryption - at least using SSL/TLS. If the cloud is being used to process the big data understand how to verify that this
is secured.

Access management

Access to the analysis infrastructure, data being analysed and the results should be subject to proper IAM controls.

Audit

There should be logging and monitoring of activities on the analysis infrastructure to allow proper auditing. The key risk areas for big data are the changed information life cycle, the provenance of the big data and technology unknowns.

The basic objectives of information security for big data are the same as for normal data, however, special attention is needed to ensure controls for these key risk areas.

References

www.kuppingercole.com/report/advisorynote_bigdatasmartdata 70750140513

www.enisa.europa.eu/activities/risk-management/evolving-threat_environment/ENISA_Threat_Landscape/at_download/fullReport

https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Top_Ten_v1.pdf

www.energynetworks.org/modx/assets/files/electricity/futures/smart_meters/ENACR009_002_1.1-Control%20Points.pdf



About the author

Mike Small, FBCS CITP is is a senior analyst with KuppingerCole. Previously Mike worked for CA (now CA Technologies Inc) where he developed the strategy for identity and access management and was VP responsible for product development. He is a frequent speaker at IT security events around EMEA and contributor to the security press.

Mike is a member of the London Chapter of ISACA Security Advisory Group, a Chartered Engineer, a Chartered Information Technology Professional, a Fellow of the British Computer Society, and a Member of the Institution of Engineering and Technology.

About BCS

We help global enterprise align its IT resource with strategic business goals. We work with organisations to develop people, forge culture and create IT capabilities fit to not only lead business change but to meet companywide objectives and deliver competitive advantage. IT has been gaining momentum within global business for decades and we've been there from the beginning, nurturing talent and shaping the profession into the powerhouse that's now driving our digital world. Today organisations partner with us to exploit our unique insight and independent experience as we continue to set the standards of performance and professionalism in the industry.

Call us on +44 (0) 1793 417 755 or visit us at enterprise.bcs.org

BCS The Chartered Institute for IT
First Floor Block D North Star House North Star Avenue Swindon SN2 1FA
T +44 (0) 1793 417 755 **enterprise.bcs.org**

© BCS, The Chartered Institute for IT is the business name of The British Computer Society (Registered charity no. 292786) 2013

If you require this document in accessible format please call +44 (0) 1793 417 600

BC411/LD/ART/1013