Data Security Audit

Increasing security by understanding where your data resides and who has access to it

Highlights

- Reduce risk by identifying **where** sensitive data is stored and how it is protected
- Improve security controls by identifying **who** has access to your important data
- Ensure compliance with data security requirements

Every day, school districts generate and store vast quantities of data on district servers and networks. Data volumes are growing at 50% per year with unprotected sensitive data growing nearly twice as fast. A district firewall prevents unauthorized access to this data from external threats, but what about the internal threats?

30% of security incidents list human error as a contributing factor, and with thousands of district staff working with potentially sensitive information, what assurances does a district have regarding the security of sensitive data such as student records, human resources information, and district financials?

In the last year, over 27% of all security incidents and 77 million records breached occurred in the Canadian Education Industry. At an average cost of $188 per lost or stolen record, data security is a serious concern and financial risk that school districts should take steps to identify and manage. Organizations are also required to report certain privacy incidents to the Canadian federal privacy regulator and to the individuals affected by a breach, failure of which could trigger heavy fines. It is critical that school districts assess the security of their data to prevent privacy incidents resulting from the data being lost, misused, stolen, disclosed or accessed inappropriately, as a result of a cybersecurity incident, human error, or for any other reasons.

Take a data centric approach to security

Do you know exactly what data you should be protecting? Do you have a clear picture of where your most sensitive data exists in the organization, who has access and how it is used in the business processes?

- Have you recently assessed how securely your critical data is protected and where points of leakage could exist?
- Do you have a strategy for data protection, and how well is it aligned to your organization's risk management objectives?
- What industry regulatory requirements for protecting data most concern you, and to what extent do you feel you are compliant with these regulations today?

Districts are required to protect sensitive district, staff and student data; however, many districts are unaware of where their "crown jewels" exist and how to best protect them.

Our Data Security Audit solution can help you discover where your sensitive data resides and provide recommendations that can improve management of compliance with internal and external data security requirements.

Successful data protection relies on a comprehensive program with:

- Visibility into where the sensitive data resides,
- Awareness of how that data is used and by whom, and
- Knowing which data protection tools provide maximum protection

Solution Offering:

IBM's Data Security Audit service provides a comprehensive view into a district's sanctioned and unsanctioned data locations to provide insight into what data exists, where it is stored and who has access.

IBM can help your district discover data that has been inappropriately stored and validate your security controls to audit file shares and identify data security/access issues.

The IBM K-12 Data Security Audit service includes:

- A kickoff meeting to describe the audit process and information and credential requirements.
- Up to 3 days of on-site interviews with IT staff members and key stakeholders.
- Audit of file shares and key information systems such as SIS, HR, Financial, and Database servers
- Report to document data security/access issues and recommendations
- Presentation of the final report with executive summary and strategic recommendations

Typical Length of Engagement: 6-10 days

Why IBM?

By understanding the uniqueness of security in the K-12 Education Industry, IBM can help your district improve its security posture. IBM's security portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures.

For more information

To learn more about IBM K-12 **Data Security Audit**, please contact your IBM Marketing Representative. For more information on all our IBM K-12 Consulting and Professional Services, visit:
https://www.ibm.com/industries/education/canada-k-12-service-briefs

IBM Corporation
3600 Steeles Ave. East
Markham, ON L3R 9Z7 Canada
March 2018