BDO NEWS

April 2020

www.bdo.com.hk

TECHNOLOGY UPDATES
April 2020 Issue

CONTENTS

- How to create competitive advantage with data?
- How IT vendor management mitigate the impact of data breach and cyber-attack risk
- How blockchain technology save $400m annually for air cargo industry
- How to manage the key of personal data protection after GDPR?
- How can BDO help?

Innovation and technology are drivers for organisation growth and the key to enhance competitiveness of different industries. Just as technology rapidly evolves, so does the sector. In every monthly issue of our 'Technology Updates', it will include the latest updates from cybersecurity, emerging technology & data privacy.

How to create competitive advantage with data?

An invincible competitive advantage has been a belief to be possible by leveraging customer-data capabilities. The more customer data we have, and that data, when analysed with machine-learning or deep learning tools, allows us to offer a better product that attracts more customers. Let us rethink this belief today.

Data-enabled learning indeed become much more powerful to deliver customer insights than the old school analysis in the past. The past data collection process, used to be slow and difficult to scale up has been changed dramatically with the advent of the cloud and new technologies that allow firms to quickly process and make sense of vast amounts of data. These 'digital exhaust' after machine-learning algorithms analysis, company's offerings can be hopefully adjusted to suit every customer needs.

However, these tremendous customer information gathering efforts contributed to design better products and services do not guarantee defensible barriers from other market entrants attack. To determine to what degree a competitive advantage or entry barriers is effective provided by data-enabled learning, companies could re-think from seven perspectives as suggested by Harvard Business Review:

1. **How much value is added by customer data relative to the stand-alone value of the offering?**

   Smart televisions, for instance, include software that can provide 'insights' with personalised recommendations for movies based on an individual's viewing habits.

However, consumers largely consider TV size and picture quality when making purchasing decisions. 'Insights from data are powerful, they don't guarantee defensible barriers.'

2. **How quickly does the marginal value of data-enabled learning drop off?**

   A counterexample is smart thermostats, which merely need a few days to learn users' temperature preference. Data-enabled learning cannot offer much competitive advantage.

3. **How fast does the relevance of the user data depreciate?**

   A rival can easily enter the market given depreciation rate of data is high. Casual social games market illustrate losing most of the user base given the value of learning from user data can decrease quickly.

4. **Is the data proprietary-meaning it can't be purchased from other sources, easily copied, or reverse-engineered?**

   Proprietary customer data with few or no substitutes is of course a key ingredients to creating a defensible barrier.

5. **How hard is it to imitate product improvement based on customer data? Copycat explains everything.**

6. **Does the data from one user help improve the product for the same user or for others?**

   Pandora was the first big player in digital music streaming but then fell behind Spotify and Apple Music. Whilst Pandora's main selling point is that it can tailor stations to each user's tastes, but it doesn't lead to the type of exponential growth that network effects produce.

7. **How fast can the insights from user data be incorporated into products**?

   Rapid learning cycles make it hard for competitors to catch up, especially if multiple product-improvement cycles occur during the average customer's contract.

   In the coming decades, using customer data to improve the product will be a prerequisite for staying in the game, and it may give incumbents the advantage over new entrants. But in most cases, it will not produce a winner-take-all dynamic. To create a successful competitive advantage from an effective entry barrier in the foreseeable future, wise data-enabled learning is the key.

Read more from the source:
https://hbr.org/2020/01/when-data-creates-competitive-advantage

How IT vendor management mitigate the impact of data breach and cyber-attack risk

On 7 April 2020, BlackBerry researchers have released a new report that examines how hackers have systematically targeted Linux servers while remaining undetected for nearly a decade. However, many companies and enterprises are using IT vendors' solutions and thereafter rely on Linux to run websites, proxy network traffic, business application and store valuable data. In fact, Linux runs nearly all of the top 1 million websites, 75% of all web servers, 98% of the world's supercomputers and 75% of major cloud service providers (Netcraft, 2019, Linux Foundation, 2020).

There are countless reasons why companies outsource IT activities ranging from infrastructure to software development, maintenance and support to IT vendors. And some of the most common reasons include: enhancing company's focus, access to world-class capabilities & controlling and decreasing the operational costs. However, when companies sign a bond with efficient and specialised IT service providers, companies also introduce third-party risks on data breach & cyber-attacks.

Why data breach & cyber-attacks still happen in third party providers?

Your company might outsource all of its data storage needs because it does not want to buy and maintain its own data storage devices. However, even though company has very solid cybersecurity & data privacy controls eg data security policies and cybersecurity procedures are formally documented and kept up-to-date, that does not necessarily implies IT solution provider follows your rules and/or with an obligation to enforce data protection as requested by industrial standards. Your IT providers may have limited resources on data privacy & IT security expertise that failed to always keep addressing cybersecurity threats & monitoring suspicious access of your data.

Vendor selection matters

Selecting a right vendor becomes crucial for IT vendor management. You can add data privacy and cybersecurity requirement in the service contract and establish a vendor management organisation that best fits the enterprise. You can also define reporting lines for any data breach & security incidents from IT vendors. Most importantly, the contract terms should enable independent assessor to conduct your data security and cybersecurity audit over your IT vendor solution. Unless you have contract terms to protect your data and IT services empowered by IT vendor, strong controls for data breach & cybersecurity are never guaranteed.

We have seen different business face varies challenges from IT vendor selection over core business operations, uncertainties

of data security compliance of their critical IT vendor, data breach incidents and so on. The longer your organisation waits, the more difficult to mitigate impacts. Don't wait and do data privacy impact assessment as well as cybersecurity review to protect from data breach and cyber-attacks.

Read more from the source:
https://blogs.blackberry.com/en/2020/04/decade-of-the-rats

How blockchain technology save $400m annually for air cargo industry

On 12 March 2020, a Canadian based trade association ULD Care and an air transport communications and information technology company announce that they are exploring possibility of using blockchain technology to save US$400m a year in the air cargo industry.

The proposed blockchain platform will also embed authentication and trust-based functions to reduce risk of tampering, cybercrime, trade-based money laundering, fraud, and illicit trade. Bob Rogers, vice president and treasurer of ULD Care, added that:

" A container travelling from Shanghai to Long Beach could take up to 30 days to finish its journey, but the true travel time on sea or road is only around 15 days, with the remaining time spent on back-office and paperwork. The use of blockchain could revolutionise that process."

Challenges of data verification

Different cargo companies monitoring and tracking the cargo for shipments by paper documents. This not only makes the process complicated and causes frequent trust, transparency issues and human error, but also a lot of times spent on data verification as well as waiting.

What is blockchain and how it can help

Blockchain can be used as solution to improve data integrity to the highest standards. A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. By design, blockchains are inherently resistent to change of data. Blockchain ledgers are indisputable such that if data addition or transaction has been made. In addition, blockchains are not only a data storage but a timekeeping data structure that it can provide proof of the history of data eg transportation records, sales records are easily reportable and maintained. Organisations facing different challenges from audit, regulatory compliance requirements, or legal can use blockchain technology to improve data integrity.

The cargo companies can use blockchain to record and track two stream of data: a digital cargo activity logs and a digital passport. The activity logs provides the real-time status, chain of custody and every trips track. The digital passport act as human passport, provides the immutable identity such as certification of airworthiness to prove ownership. Through accurate tracking and secure data sharing, shipping times could be saved.

We have seen different business face varies challenges from traditional business operation flows, outdated system design, lack of technology driven processes and so on. The longer your organisation waits, the more difficult to catch up industries. Don't wait and do gap analysis assessment as well as proof-of-concept works on emerging solution to meet new business needs.

Read more from the source:
https://www.logupdateafrica.com/sita-uld-care-to-develop-blockchain-for-uld-tracking-industry-to-save-400-mn-a-year-aviation

How to manage the key of personal data protection after GDPR?

Since the last adoption of the major European law on data protection (Data Protection Directive 95/46/EC) in 1995, there has been a dramatic change. For example, mobile devices are ubiquitous, and it is not uncommon to carry two or even three mobile devices at a time. At the same time, sensitive corporate data is about to go beyond the security of traditional corporate security boundaries. Employees can email documents to themselves, access information from their smartphones and tablets, and store them in the cloud. Today, major personal data breaches are common, exposing customers to the risk of identity theft and financial losses, while businesses are at risk of losing customer and investor loyalty and regulatory fines. We shall discuss the implications of the General Data Protection Rules (GDPR) for global organisations.

The GDPR imposes a number of requirements on organisations that collect or process personal data, including compliance with six key principles:

1. Ensure transparency, fairness, and legality in the processing and use of personal data.
2. Be clear about how personal data is used and process it 'in accordance with the law'.
3. Limit the processing of personal data to a specified.
4. Make sure your profile is correct and allow it to be cleared or corrected.
5. Ensure that only the personal data required to achieve the purposes of data collection is retained.
6. Ensure the security, integrity and confidentiality of your personal data. Your organisation must take steps to secure

your personal data through technical and organisational security measures.

There are some important articles related to keeping personal data safe, as well as the possible consequences of a violation. Article 32 describes the security of processing data:

Article 32 of EU GDPR 'Security of processing'

The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) Encryption of personal data;

(b) Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In short, this article requires organisations to implement appropriate security measures to protect personal data. This article specifically mentions 'personal data encryption' as one of the means to achieve this. The article also refers to 'the ability to ensure the continued confidentiality, integrity, availability and flexibility of processing systems and services that process personal data'. With regard to encryption, this means that in addition to encrypting data, there shall be a powerful key management program.

How painful is key management?

However, according to a global encryption trends study sixty percent of respondent's rate key management as very painful, which suggests respondents view managing keys as a very challenging activity. The highest percentage pain threshold of 67 percent occurs in Germany. At 38 percent, the lowest pain level occurs in France. No clear ownership and lack of skilled personnel are the primary reasons why key management is painful. Companies continue to use a variety of key management systems. The most commonly deployed systems are 1. formal key management infrastructure, 2. formal key management policy, and 3. manual processes.

Read more from the source:
https://www.ncipher.com/2020/global-encryption-trends-study

How can BDO help?

At BDO, our Risk Advisory Services (RAS) team, a group of dedicated IT professionals, is well equipped, qualified, experienced and well-prepared to assist your board or management to explore alternative options on digital transformation through application programming interface (API) and proof-of-concept (PoC). We are also experienced to perform IT security assessment, data protection review, vulnerability assessment as well as penetration test or any other IT matters relating to regulatory requirements. Please do not hesitate to contact us and talk to our consultants. We are pleased to provide further insight or assistance, if needed.

BDO'S SUPPORT AND ASSISTANCE

25th Floor, Wing On Centre
111 Connaught Road Central
Hong Kong
Tel: +852 2218 8288
Fax: +852 2815 2239
info@bdo.com.hk

RICKY CHENG
Director and Head of Risk Advisory
Tel: +852 2218 8266
rickycheng@bdo.com.hk