

BDO NEWS

February 2020

www.bdo.com.hk

TECHNOLOGY UPDATES February 2020 Issue



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 predictive analysis benefits your organisation

In the field of artificial intelligence, variety of analytical technologies are delivering more business efficiency. The fundamental descriptive analytics, providing business information and knowledge. Predictive analysis forecasts events and enables us to predict them. State-of-the-art prescriptive analysis allows company to make decisions automatically.

Predictive analytics provides information about what will happen to your company. By means of more complex machine learning and AI processes and algorithms, predictive analytics can tell you what will happen - how the product would be sold, who might buy it, and which marketing campaign would have the most impact.

Predictive analytic is another analytical technique that automates decision-making and evaluates the optimised solutions in complex environments. It deploys the information delivered by descriptive and predictive analytics.

Easier marketing by prescriptive analytics

Let's give an example. Time was, marketing teams drafted marketing campaigns and used descriptive analysis to target people they thought were the most willing to accept them. Customers in the 20-30 range may receive 'younger' information than customers in the 45-60 age group. They may be marketed for different products or services. This usually results in better overall performance of the sport. Let's be honest: many companies still sell in this way. But this type of marketing is still not ideal. There are still many assumptions that even results (high or low selling rates) do not

CONTENTS

- ▶ How predictive analysis benefits your organisation
- ▶ How end of life system increases security risks to organisation
- ▶ Mandatory IoT security in the offing with UK proposal
- ▶ How can BDO help?

provide insight into why marketing campaigns are under-performing or over-performing.

As we move into predictive analytics, things become clearer. AI and machine learning can tell us more specifically which customer groups to target and which products or discounts could be offered to maximise impact. They can even tell you when and what medium to contact in the day. However, the results of these movements are still descriptive. They won't tell you what you should do to further improve your grades.

Enter, prescriptive analytics. The prescriptive analysis takes three main forms: guiding marketing, guiding sales and guiding pricing. It uses AI and machine learning to guide buyers with less human interaction - deliver ingesting the right product for the right buyer at the right time, with the right content - tell the salesperson what words to use to deliver which product, and tell you what price at what time. This information allows you to maximise not only sales, but also overall price and profit.

In fact, the benefits of predictive and normative analytics go far beyond sales conversions. They could be translated into time savings, efficiency, human capital and transaction costs. Predictive analytics, when automated, allows you to make real-time decisions – such as, chemical and gasoline companies do, changing prices every day to maximise profits. The benefits of enabling data and, more specifically, prescriptive analysis are due to having the technology, systems, and processes to maximise available data.

Challenges of prescriptive analytics

The most obvious challenge in prescriptive analysis is governance. If you remove people from the decision-making process and your model is defective (either because the situation has changed or because you have an anomaly), you will not only make mistakes, but also make mistakes automatically and on a large-scale. In the realm of sensitive or human risk, it is common for people with the insight and benefits of normative analysis to make, but it is ultimately up to humans to make the final decision.

Let's start with a big question: What do you want to do? As mentioned above, prescriptive analytics is powerful, but not every company or every marketing campaign you push to your customers is required. They also need a lot of adjustment. For the first time no algorithms have been perfectly crafted. It takes time, effort, and focus to make prescriptive analytics work. However, if you are in a competitive market (from product to people, managing everything) prescriptive analysis can mean a huge increase in profits and productivity.

Companies can prepare for this by revamping the traditional framework for analysing problems. Companies need to think about new business questions they can ask, and not just thinking about how to get results to answer business questions. In other words, if you can look at historical patterns and predict

what might happen in the future, where will you apply them? Next, ask analysts to actually address these issues using tools that make it easy for them to develop models using machine learning techniques.

Read more from the sources:

<https://www.forbes.com/sites/danielnewman/2020/01/02/why-the-future-of-data-analytics-is-prescriptive-analytics/#3da6deae6598>

<https://www.techradar.com/news/the-path-from-predictive-to-prescriptive-analytics>

<https://decidesoluciones.es/en/prescriptive-analytics-in-artificial-intelligence/>

How end of life system increases security risks to organisation

On 14 January 2020, a software giant Microsoft terminated technical support for Windows 7 & Windows 2008 servers (strictly speaking Windows Server 2008 R2). According to the research of Net Applications, Windows 7 was so popular that it took Windows 10 nearly four years just to pass it in market share. However, even today, millions of workstations are still running on Windows 7 or even Windows XP after their discontinued status.

What happen if organisation continues using the obsolete and/or non-support system? The answer is clear: your system is still valid, but it is more vulnerable to security risks and bugs. Your PC or system will continue to up and running, but will no longer receive software updates, including security updates from IT vendor. As a matter of facts, Microsoft has released critical security updates after 14 January 2020 for NSACrypt whilst NSACrypt is a spoofing vulnerability that exists in the Windows CryptoAPI(Crypt32.dll, this DLL appeared in Windows family for more than 15 years old) cryptography certificates. Sadly, none of the systems running of Windows 7 and Windows 2008 servers can make this security updates and their systems are vulnerable for mysterious attacks. Historically, we have seen similar attacks take place in the 2017 WannaCry attack to target outdated systems.

Challenges in migrating obsolete systems

With reference to different IT governance framework like ISO 27001 or CIS Top 20, the best practice is to upgrade your system with new security patches. However, there are many challenges during migration process.

Whilst the direct challenges were around user acceptance of new systems, the big challenges are finding obsolete systems very difficult to upgrade. We have seen some companies relying heavily on outdated systems for critical business operations. Meanwhile, the company reserved budgets for upgrade. However, after performing number of proof-of-concept works on new system, they realised it was not only sort of 'Windows upgrade' matter, as the new system no longer supported the

technology they satisfied with for more than 10 years!

We have seen security threats coming from outdated operating systems, unpatched vulnerabilities and so on. The longer your organisation waits with updating their systems, the bigger the risk becomes of a potentially costly attack. Don't wait and do security assessment as well as proof-of-concept works on solution integration to extend your legacy system to meet new business needs.

Read more from the source:

<https://www.microsoft.com/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/>

Mandatory IoT security in the offing with UK proposal

Cybersecurity Law will come into force in late December in Internet of Things (IoT) is one of the hottest technologies in the era of digital transformation, connecting everything to Internet. According to the marking research conducted by Gartner, the enterprise and automotive Internet of Things (IoT) market will grow to 5.8 billion endpoints in 2020, a 21% increase from 2019.

What is IoT?

IoT is a term for devices used to share data and information in order to give added convenience and control to consumers and, in some cases, even allow users automate simple processes such as ordering supplies. Tens of billions of these IoT connected devices are already around the world and that number will only grow as internet connections begin to become a standard feature for a large number of electronics devices. Although heavily integrated into the consumer electronics market, IoT extends far beyond handheld devices and home appliances; IoT subsystems such as industrial internet and connected cities are designed to automate factories and urban areas, not just homes.

Security Issues with IoT devices & regulatory requirements

While IoT devices bring effective communication between devices, automate things, save time and cost and have many benefits, there is one thing still concerning the users—IOT security. With more IoT devices and connected Machine-to-machine(M2M) technologies coming into service, a

large scale security breaches expected to come into existence in near future due to sensitivity of the data being prone to hackers which has further led government to launch advanced security framework and compliance requirement.

Recently, UK government issues a consultation on regulatory proposals on consumer IoT security. "Our new law will hold firms manufacturing and selling internet-connected devices to account and stop hackers threatening people's privacy and safety," Matt Warman, U.K. Minister for Digital and Broadband, said in a statement. "It will mean robust security standards are built-in from the design stage and not bolted on as an afterthought." Having said that it takes times from IoT manufacturing to compile with the new rules, organisations should regularly conduct vulnerabilities assessment as well as network based penetration tests to prevent and detect potential cyber-attacks raised by IoT devices.

We have seen IoT security threats coming from factories, retail operations as well as enterprise businesses. The fewer health checks performed with IoT devices, the bigger the risk becomes of a potentially costly attack. Don't wait, do IT security health check to protect your critical infrastructure to sustain business operations.

Read more from the source:

<https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation>

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

BDO Limited, a Hong Kong limited company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO to discuss these matters in the context of your particular circumstances. BDO, its directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

© 2020 BDO