HealthManagement.org
Promoting Management and Leadership

Top Big Data and Security Trends for 2017

In today's digital age, organisations are relying more on technology to enhance their competitive advantage. Artificial intelligence, predictive analytics and ransomware security are among the emerging technology trends that will make an impact on organisations in 2017 and beyond, according to IT experts.

1. Predictive analytics and the power of the data scientist

Biopharma and med device manufacturers are among those companies turning to data analytics to achieve business advantage. Predictive analytics tools help companies to not only measure the past but effectively create a roadmap for future choices by learning from previous situations. "The role of the data analysts and data scientists designing the algorithms and mining the data will grow in importance," says Christian Gonzalez, CEO and co-founder of Wovenware.

2. Business users will drive more decisions on data management

Cleansing rules, integration processes and so on are used by organisations to get data into the shape they want. These rules are frequently used once and then thrown away. "Those are intellectual resources that shouldn't be wasted," explains Jake Freivald, vice president of marketing at Information Builders. "Think of a data scientist creating data cleansing rules for an analytical process that leverages a data lake — the knowledge that goes into her processes can be captured, stored and applied to downstream feeds, data governance processes that correct source systems, and integrated views of the data for others."

3. Control and ownership of data and metadata

Ettienne Reinecke, chief technology officer at Dimension Data, says that in the year ahead, control and ownership of data and metadata will emerge as a point of discussion — and contention. Moreover, organisations want to use the data to perform analytics. "We expect that this will trigger some interesting discussions between organisations and their cloud providers, for example, where are the boundaries with respect to ownership, especially around metadata," Reinecke adds.

4. Security, easy access drives adoption of hosted desktops apps

Although full adoption of hosted desktop apps may still be 2-3 years away, a spike in adoption rates in 2017 is expected, says Chanel Chambers, director of product marketing at Citrix. "Concerns about security are top of

mind for every size business this year, and organisations will seek out ways to keep data safe without investing hundreds of thousands of dollars. In addition, hosted desktop apps provide ease of access to company data, allowing employees to access their files from anywhere and any device."

5. The chief data officer position will gain momentum

The CDO's job is to extract maximum value from data. That can be done in many ways, including customer-facing portals, large-scale analytical apps, data feeds that stem from unified views of business entities, embedded BI inside other enterprise applications, and so on, says Jake Freivald, vice president of marketing at Information Builders. The CDO should work to ensure information is managed and shared across divisional and even organisational boundaries, leading to better data monetisation and lower per-user cost of data.

6. The security community will utilise big data more effectively

2016 was the year of "big data" and the data clutter that comes with it makes informed security decisions as difficult as ever, says Matt Rodgers, head of security Strategy at E8 Security. "In 2017, companies will start looking at their data sets through advanced analytics to identify trends and risks. Big organisations are already starting to augment their existing SIEM technology with behaviour analytics capabilities to this end."

7. Organisations crack down on IoT security policies

Rodgers also notes that the increase in DDoS attacks powered by IoT devices in 2016 will "force many organisations to finally make themselves accountable for discovering and monitoring the security of all proprietary IoT assets." He adds, "Without the proper visibility, organisations in 2017 will inevitably fail to protect themselves or their stakeholders."

8. IoT gets dumber, not smarter

"A lot of attention has been given to 'smart devices' as proof of IoT's growing influence," notes Matt Dircks, chief executive officer at Bomgar. "The reality is a connected device doesn't make it a smart device. The 'things' that are being connected are in many instances fire-and-forget in their simplicity, or are built-in features and tools we may not even know are there. This leads to a mindset of ignoring these 'dumb' devices without paying attention to the fact that these devices, while inherently 'dumb', are connected to the biggest party-line ever made: the Internet."

9. Passwords finally grow up

"The recent DDoS attack that wreaked havoc on a huge portion of the Internet this past October is to blame, in part, on unchanged default passwords on IoT devices that hackers exploited," says Matt Dircks, chief executive officer at Bomgar. Use of simplistic, common or old passwords, continues to make hackers' jobs easy. The best passwords are those that users and vendors can't control — i.e., more companies will begin to use solutions that securely store passwords and regularly validate and rotate them to ensure safety and user security.

10. CISOs will shift toward granularly identifying information

Protecting data by containing it behind hyper secure firewalls, deploying DLP (data loss prevention/protection) technologies at the parameter, locking down USB ports and so on are helpful but "don't prevent the issue" of data theft. "In 2017 and beyond, you will see a more deliberate movement by CISOs toward first identifying what exactly it is they are securing and assigning security levels to that content. This isn't about locking down more data to make it unusable — rather, it's about making the data usable with pervasive, invisible governance around it," explains Ankur Laroia, solutions strategy and security leader at Alfresco.

11. Organisations will step up defences against ransomware

Ransomware has proved to be one of the most effective ways to infiltrate an organisation. "In 2017, organisations will take ransomware more seriously and implement ways to rapidly identify compromised content and automate its recovery," predicts Don Foster, senior director of solutions marketing and technical alliances at Commvault. "Organisations need to figure out how to classify, separate, and wall off their data to reduce the risk of data being inappropriately accessed and permanently lost."

12. Comfort in the cloud

“The concerns about security and loss of control in the cloud will be a thing of the past in 2017,” predicts Christian Gonzalez, chief executive officer and co-founder of Wovenware. What will drive a new level of cloud worshippers in 2017 is the growth of PaaS solutions, which provide a platform for customers to run and manage their applications in the cloud without the complexity of building the associated infrastructure or algorithms.

Source: Health Data Management
Image Credit: Pixabay

Published on : Mon, 20 Feb 2017