ACJRD Presentation

GETVISIBILITY

9th December 2020

www.getvisibility.com in Getvisibility @get_visibility

2020

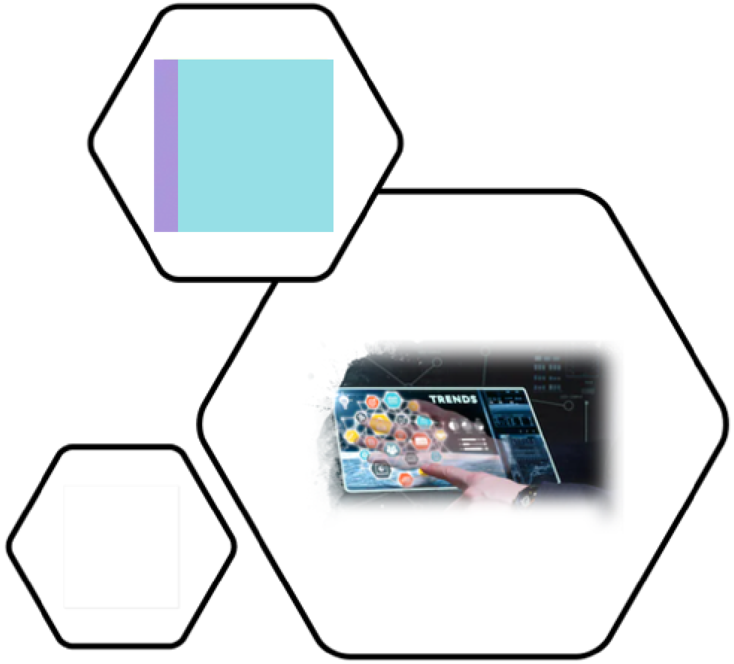
In the first six months of 2020, various Fortune 500 companies became the target of massive data breaches where hackers sold account credentials, sensitive data, confidential and financial information of these organizations' cybercriminal forums.

In 2020 so far:

- **16 billion records** have been exposed this year
- **8.4 billion records have been exposed in the Q1 of 2020 alone**
- This number is a **273% increase** year on year
- In 2019 during **4.1 billion records** were exposed

  (*Source: Security Boulevard*)

2020 State Of Play



Key Trend

- **Fines** Uber $148m, EquiFax $575m, Yahoo $85m, Capital One $80m, Morgan Stanley $60
- **Regulations** GDPR, CCPA, CMMS, CCPA
- **Public Pressure /Scrutiny** Facebook/Cambridge Analytica
- **Reputational and Share Price Damage** Marriott, Yahoo, & Facebook
- **Nature of Work**– Remote Working COVID-19, Cloud adaption and Mobile
- **New Technology** – AI, Automation, Cloud adoption

What We Have Found – Dark Data

53% of companies found **over 1,000 sensitive files accessible to every employee**

51% of companies found **over 100,000 folders open every employee**

22% of folders were **open to every employee**

17% (117,317) of all sensitive files were **accessible to every employee**

58% of companies found **over 1,000 stale user accounts**

53% of data, on average, **was stale**

The Exponential Growth Of Unstructured Data

Unstructured Data

- Data scientists estimate that 80% of the world's electronic information is unstructured
- Data that is defined as unstructured is growing at 55-65 percent each year
- Emails, documents, spreadsheets, presentations, even system activity log files – that an organization is not using, has not categorized and, in some cases, may not even know exists

Risks with Dark Data

- **Increased attack surface.** The more data you store, the more you must secure
- **Potential compliance violations.** Further to the above, your organization's dark data stores might be violating data privacy regulations
- **Unused security intelligence.** In addition to valuable business intelligence, can contain actionable security intelligence

Exponential Growth

- Data is growing at an **exponential** rate without oversight and control. This is a big problem for organisations GRC

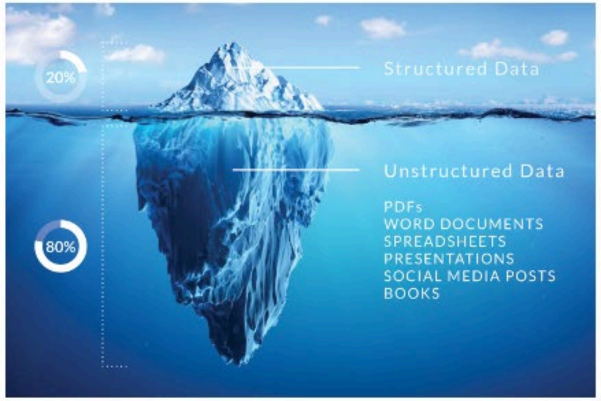
- 80% of data is now **unstructured**, in formats like Word, PDF, Excel, emails, web portals

- Data is being stored and created on **mobile** devices, **laptops**, on the **cloud** in different formats

- Hundreds of **new applications** are now being used

- Cloud Migration enables data to be created more quickly and in a **different** locations

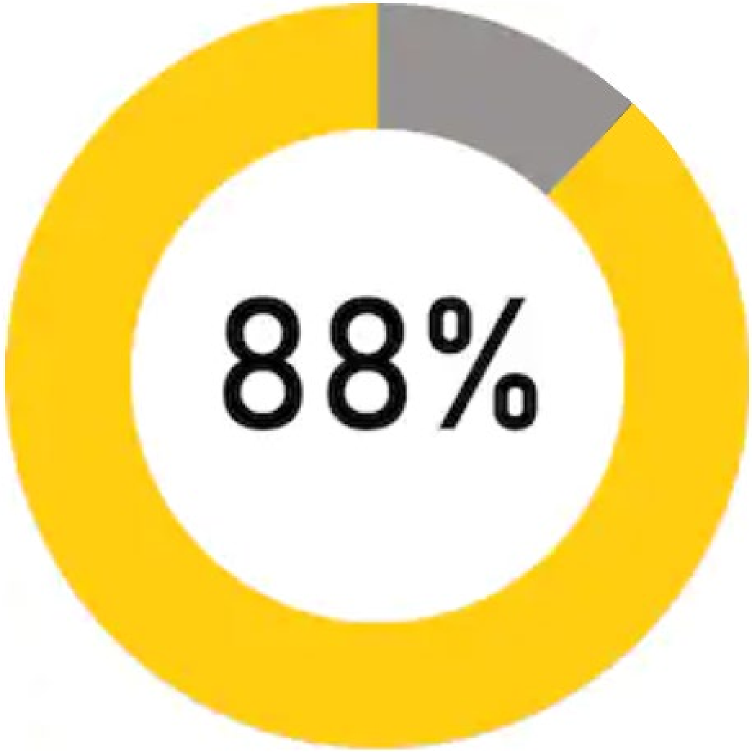
- Remote working increases the **complexity** of managing and leveraging unstructured data



The Urgency For Control Of Dark Data

According to IBM, about **88%** of all data is "dark," or unused by the organizations that collect it.

Getting dark data under control is a matter of implementing robust data governance so that enterprises fully understand what's in their existing data stores, as well as what they are continuing to save and collect.



The Urgency For Control Of Dark Data (Cont.)

Old and unused data that is not subject to compliance holds needs to be disposed of.

Data containing PII, PHI, and other sensitive information must be properly secured.

Moving forward, organisations shouldn't collect or store data that they don't need for business or compliance purposes.

With the GDPR in effect organisations can't afford not to invest in data governance and shine a light on their dark data.

Dangers Of Dark Data Debt

Noticeable example

A widely used hotel reservation platform has exposed 10 million files related to guests at various hotels around the world, thanks to a misconfigured Amazon Web Services S3 bucket. The records include sensitive data, including credit-card details.

Prestige Software’s “Cloud Hospitality” is used by hotels to integrate their reservation systems with online booking websites like Expedia and Booking.com.

Dangers Of Dark Data Debt (Cont.)

- The incident has affected 24.4 GB worth of data in total
- Many of the records contain data for multiple hotel guests that were grouped together on a single reservation
- The number of people exposed is likely well over the 10 million
- A disjointed approach to data governance led to this organisation not know what data it held, where it held it or how it was exposed

The Path Forward

For organizations that are heavily regulated, compliance issues can be costly in time, money and reputation.

Understanding dark data is made possible by natural language processing:

- sentiment analysis
- pattern recognition
- speech-to-text conversions
- machine learning and artificial intelligence algorithms

Left unsecured, dark data can morph into a mountain of consequences. To prevent that from happening, it’s imperative to define your data.

The Path Forward (Cont.)

Discovery

Find all of the data, where it resides, who has access and what is sensitive

Assess

Risk analysis, unnecessary data, gap analysis to GDPR, security

Remediate

Implement a framework (e.g. ISP27001), policies and appropriate tooling and training

Control

Strong top leadership lead governance policies, strong reporting tools and a framework that scales

Key Advice

Data security and compliance needs buy in from the **top levels** of every organization. Understanding the unique challenge that each individual organisations faces in regard to their data is critical.

Education and **adoption** of data governance at every level of an organisation is very important.

The best way to educate is to first **understand**, whether it’s the Board or the end user, making the challenge relatable and relevant is key.

Key Advice (Cont.)

This has to start with quantifying the challenge:

Classify your Data. Without proper classification, it’s impossible to store data securely because you haven’t even defined what it is and who has — or should have — access to it.

By classifying data, you can begin to create and enforce processes for handling it, including the ability to encrypt it and store it securely in a manner that meets your needs.

Don’t wait until its too late to take action. Instead, talk to the right people and rely on the right tools so you can eliminate blind spots and create a posture that adequately defends all of your data.

Questions and feedback

www.getvisibility.com Getvisibility @get_visibility