o n

Supporting Evolving Discovery Use Cases Through Information Assurance

This position paper will discuss the challenges that organizations face today regarding the proliferation, protection and use of data, and how an effective Information Assurance program can quickly sift through organizational data to identify, preserve and collect information from various data sources to support key discovery objectives efficiently and defensibly and give your organization an information advantage over your competition.

Executive summary

Governance Challenges Within Organizations Today

With business communications evolving to include collaboration apps, governing data has never been more challenging, given the volume of data within organizations, the increasing variety of sources of organizational data and how much of that data provides little if any benefit to those organizations.

Growth of Data

The term “Big Data” has become popular to illustrate the volumes of structured and unstructured data (predominantly unstructured) that overwhelm organizations on an increasing basis. And the growth of data within organizations has been stratospheric, doubling every 1 to 2 years. Back in 2010, the amount of data in the world was about 2 zettabytes: today it's about 97 zettabytes! That's over 48 times more data in 12 years! And it's expected to almost double again by 2025 – to 181 zettabytes (which is 181 trillion gigabytes)!

Cloud Sources

Global cloud adoption is expanding and will continue to expand rapidly as organizations move to the cloud for their enterprise solutions. Accu[illegible]

Discovery Challenges Within Organizations Today

In addition to the Governance challenges discussed above, there are several challenges that are adding to the discovery workload for organizations, even if they don't have any meaningful litigation. Those include compliance challenges associated with data privacy compliance, risk challenges associated with threats to your data and evolving and expanding discovery use cases.

Compliance Challenges

With the volume of personal data online, countries worldwide, including Europe and the US, have passed new data privacy laws that place a greater emphasis on data privacy protection. Part of the challenges is that each data privacy law is unique, with different requirements for protecting personal data, requiring organizations to keep "moving the target" to stay compliant with the evolving data privacy landscape. Here are recent enacted data privacy laws in Europe and the US, as well as their impact on the identification and protection of personal data.

Europe

The General Data Protection Regulation (GDPR) became effective in May 2018 and it strengthens data privacy compliance requirements more than its predecessor, the 1995 European Union Directive 95/46/EC. The United Kingdom now has its own GDPR after leaving the EU via Brexit. GDPR applies to the European Economic Area (EEA), which is the EU plus Iceland, Norway, and Lichtenstein.

GDPR applies to any organization offering goods or services to European "data subjects" or organizations controlling, processing, or holding personal data of European nationals, regardless of whether the organization location is in the EEA or not, and organizations must be able to show in clear and plain language that they obtained consent for the handling of personal data.

Fines under GDPR can be huge – up to **4 percent of annual revenue** or **20 million Euro,** whichever is greater. Since GDPR was enacted in May 2018, we have seen some significant fines related to GDPR violations, with the largest to date having been assessed against Amazon in July of 2021 of $887 million!

US

The US has no comprehensive national data privacy law. There are currently only four states that have passed data privacy laws:

- California: The California Consumer Privacy Act (CCPA) was passed in 2018 and went into effect in January 2020. Californians voted to replace it in 2020 with the California Privacy Rights Act (CPRA), which significantly expands the data privacy rights of consumers over what the CCPA covers and will replace it in January 2023.
- Virginia: In 2021, Virginia passed the Consumer Data Protection Act (CDPA) (aka VCDPA), which is set to go into effect in January 2023.
- Colorado: Also in 2021, Colorado passed the Colorado Privacy Act (CPA), which is set to go into effect in July 2023.

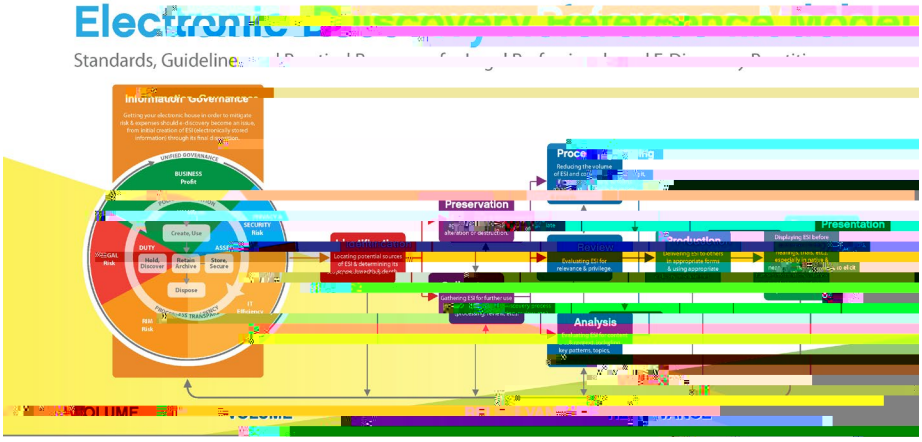
- Utah:

- Global ransomware reports were **715%** higher for the first six months of 2020, compared to the first six months of 2019 (Source: Bitdefender).
- Cyber insurance premium prices jumped as much as **40%** in 2021 — in large part due to the rise in ransomware claims (Source: CyberScoop).
- In a recent survey, **83%** of respondents said they continued accessing accounts from their previous employer after leaving the company and

With the number of use cases for discovery technology increasing, the ability to

The “Left Side” of the EDRM

Historically, the entire custodian corpus of data (including their email, file shares, etc.) has been collected and then loaded into an eDiscovery solution where the data



Instead of having to perform searches and collections of each of the endpoints locally and separately, the searches can be performed remotely, across many

opentext™

Conclusion

There's too much **data** and not enough timely **information** within organizations today. The stakes are high, and the risks are even higher and there are more discovery use cases than ever that your organization needs to support. Organizations can't afford to continue to move ever-growing volumes of data to downstream processing, hosting and review to support those use cases. This legacy approach to discovery is no longer sustainable.

An effective Information Assurance approach provides several advantages, including direct collection from various endpoints, early insight, data remediation, scalability, and defensibility and repeatability. It addresses the Big Data Governance challenges and the Compliance, Risk and Use Case discovery challenges to support a variety of evolving discovery use cases efficiently and defensibly, giving your organization an information advantage over your competition.

Video:

- Introducing OpenText EnCase Information Assurance
- Large scale collections made simple

Product Briefs/Data Sheets:

- OpenText EnCase Information Assurance product overview
- EnCase Information Assurance data connectors
- End-to-End eDiscovery solution overview

Position papers:

- Modern Data Collection: New Imperatives and Critical Requirements
- Information Assurance and Digital Forensics: A Deepening Relationship

Customer Success Stories:

- Banner Health success story
- Novelis success story
- Liberty Mutual Insurance success story