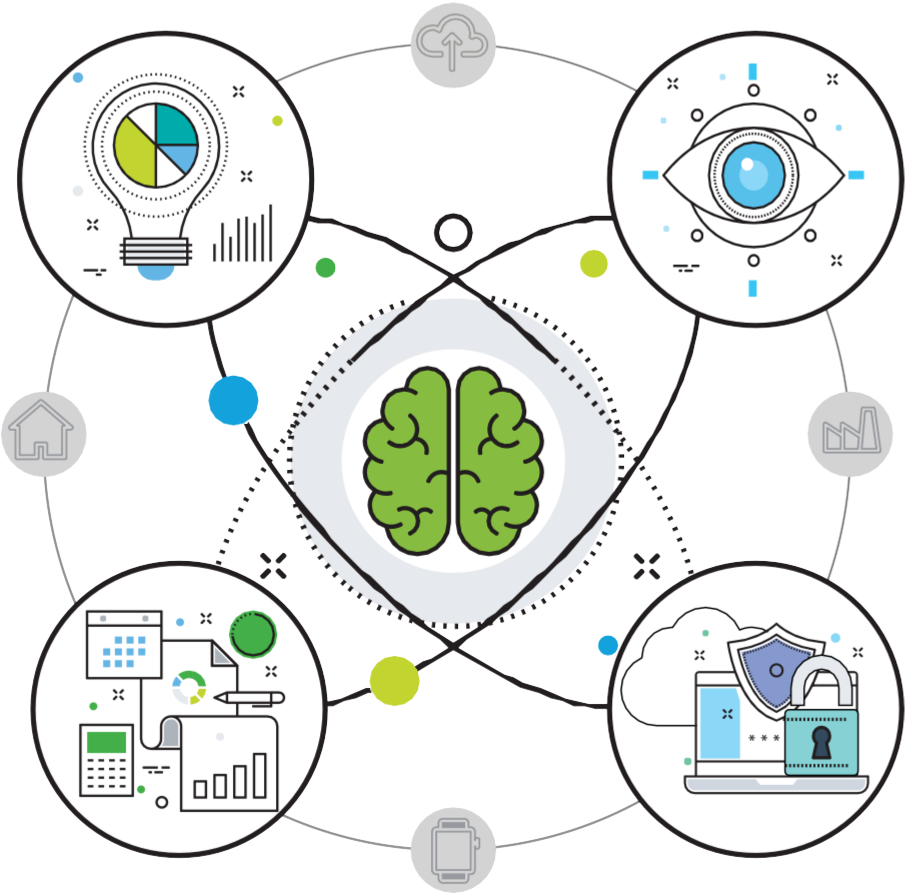
Value-based data risk management

What data is worth fighting for?



Are you losing the war on data risk management?

Do you have control over your data or is your data controlling you? With bits and bytes being generated at exponentially increasing rates, your organization may be overwhelmed when it comes to protecting your data. Learn how a new approach—**value-based data risk management**—can help you win the battles that matter.

A data deluge: Organizations under siege

Organizations today are facing two fundamental issues when it comes to data risk management.

First, an exponential amount of data is being created and monetized around the globe. Cloud computing, Internet of Things devices, the mobile workforce, and the traditional enterprise are generating data at a rate that's becoming too difficult to track, maintain, or secure.

Second, in addition to generating value for the business, exponential data growth presents new liabilities. Understanding the value of that data, putting controls around it, and monetizing it are leading to greater costs for the business.

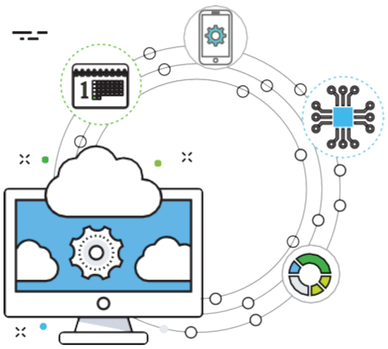
Addressing these issues calls for balance, as well as an approach that's both broad and deep.

Exponential data growth

44 billion GB of data was created every day in **2016**.

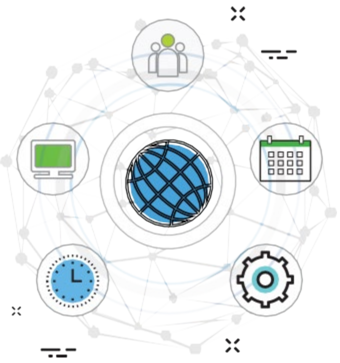
463 billion GB will be generated daily by **2026**.

Source: "Growth of Data," Micro Focus, posted on SlideShare November 6, 2017.



Machine-generated data is **growing 50x times faster** than traditional business data.

Source: "The Exponential Growth of Data," inside BIGDATA, February 16, 2017.



The size of the digital universe **will double** every two years.

Source: "The Exponential Growth of Data," inside BIGDATA, February 16, 2017.

A balanced offensive

Why balance? Because exponential data growth provides an upside and a downside, which represent both opportunities and risks. Combing through this data allows organizations to develop more targeted products and services, enhance feature sets, offer rich customer service, and more. However, the proliferation of data and the increasing complexity of how it's used exposes organizations to a tremendous amount of risk.

As a result, many organizations are elevating conversations about data to the boardroom. As leaders develop data strategies for a digital world, data must be analyzed equally as a liability and an asset.

Increasing complexity of data

Hybrid cloud adoption grew from **19% to 57%** in 2016 and 2017.[1]

By 2020, the established number of computers and mobile phones will reach 50 billion, but sensors and controllers for related IoT devices is estimated to reach **1 trillion.**[2]

One-third of companies **commercialize** or share their data for revenue.[3]

Top-performing companies are **3x** as likely to **share their data.**[4]

A broader approach to data risk management

Data isn't solely the domain of cyber professionals. It's created throughout all portions of an organization and, therefore, a broader approach to data risk management is needed. Data risk management is the responsibility of groups across the business, including marketing, human resources, operations, information technology, legal, and compliance. In fact, many companies are designating a C-suite leader to be responsible for managing data risk. This is an acknowledgement that all data is enterprise data, and that it's not owned or siloed by any one area of the business.

Because all data isn't of equal value to the business, a deeper approach is required. Organizations must determine how much protection to place around different categories of data. Building controls around all of an organization's data creates a tremendous financial burden, dooming the strategy to fail.

Most organizations have traditionally taken a "crown jewels" approach to data risk management. But a crown jewels rationale—a de facto standard that includes customer data, trade secrets, intellectual property, and so on—doesn't capture how that data affects the business and drives operational and financial performance. Organizations are evolving as they begin to understand the true value of their data.

A crown jewels mind-set is also rooted in a focus on compliance, when what's needed is an emphasis on value. For example, an organization may be diligent about how it stores and protects customers' social security numbers in order to comply with regulatory requirements. But if this data doesn't provide value to the organization, why store it at all?

[1] Louis Columbus, "2017 State Of Cloud Adoption And Security," Forbes, April 23, 2017.
[2] Barika Pace and Ruggero Contu, "Solving the IoT Security Talent Gap: Where You Look Matters," Gartner, March 8, 2018.
[3] Jennifer Belissent, Ph.D., et al. "Data Commercialization: A CIO's Guide To Taking Data To Market," Forrester, June 7, 2017. [Purchase required]
[4] Ibid.

Arming the troops: A talent reset

In addition to data risk challenges, organizations are faced with a widening skills gap. Finding the right talent and then arming those professionals with the right tools to safeguard valued data elements is no easy task.

Some key challenges include:

- High costs to recruit, hire, and retain professionals
- Difficulty finding professionals who possess both technology awareness and business acumen
- Lack of staff to implement data risk governance and controls

In the data risk management war, organizations must address exponential data growth as well as internal and external threats to that data. But the challenge is, however, that many organizations are deploying already depleted troops. There are too many tools and not enough people to configure, implement, and operate those tools properly. What's more, this situation will only intensify over time.

As organizations increasingly deploy machines in their business models, they will need professionals with advanced skills to govern those machines.

By 2021, there could be 3.5 million unfilled cybersecurity positions around the world.[1]

Organizations also sometimes find themselves sending in ill-equipped troops, forcing cybersecurity professionals to deal with business issues they may not be familiar or comfortable with. This can be likened to asking someone who has been trained to navigate an aircraft carrier to suddenly operate a rocket launcher. For example, when cybersecurity professionals are asked to discuss the data that's involved in a marketing campaign, they may be at a loss.

Not all cybersecurity resources have had the opportunity to expand their skill sets across the traditional foundations of business, nor do they fully understand how data migrates throughout the organization. Therefore, the next frontier of data risk management calls for a hybrid talent model—one-part business analyst, one-part cyber risk professional—that can bridge both worlds, from cloud computing and IoT to understanding how data risk decisions impact revenue recognition and EBITDA.

In short, a paradigm shift is required. Because the challenges and opportunities around data risk management have become broader, the skill sets needed to address it have become broader as well.

This talent gap is driving many enterprises to managed services. A managed services model can lead to scalable and accelerated business outcomes. It can also allow organizations to focus on what they do best: creating and maintaining value for their core business operations.

[1] Steve Morgan, "Cybersecurity Jobs Report 2018-2021," Cybersecurity Ventures, May 31, 2017.

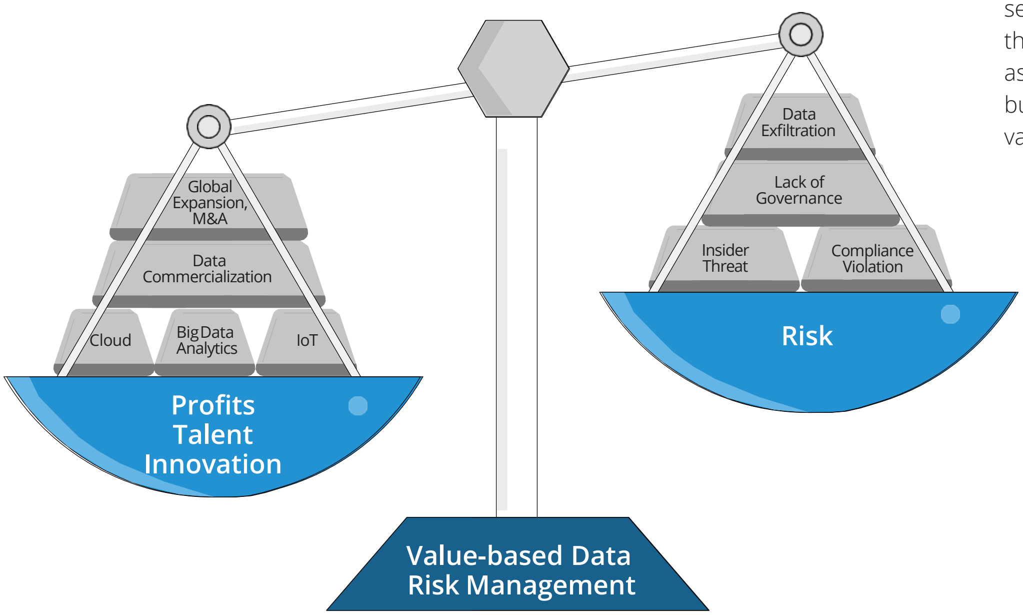
Plan of attack: Value-based data risk management

In an increasingly data-centric world, organizations must balance risk with innovation, profits, and talent. Since they can't protect all their data, organizations must focus their efforts on the data that's most valuable to their business.

To that end, organizations should:

- Understand that a crown jewels approach on its own is insufficient
- Determine the real value of their data to the enterprise
- Map that data to the corresponding value in the business
- Make informed decisions about third parties, managed services, tools and technologies, operational plans, and more

Organizations must also prioritize data risk management and put it on an equal footing with traditional information and network security, and they must dedicate as much of their budgets to true data risk management as they do to a traditional cybersecurity budget. The emphasis must be on business value and not on a technology arms race.



A winning campaign for your organization

What are the benefits of value-based data risk management? The alignment of data to the business, the use of data elements to optimize products and services and drive additional revenue, mitigated risk exposure, and opportunities to increase profits via operational efficiencies, and more. Organizations are able understand the value of data, its impact to the business, and whether it is an asset, a liability, or a hybrid.

Also, much like an International Organization for Standardization (ISO) system, value-based data risk management can become a program that's part of your organization's heartbeat. Just as an ISO program instructs organizations on how to live and breathe quality, value-based data risk management gives organizations the ability to adopt a more robust data risk management culture.

The need for a "living" program is critical because data risk management is an ongoing challenge. Implementing a value-based program will enable organizations to make decisions—from the acquisition and divestiture of data to third-party data management and emerging technologies. With the required expertise, those decisions can lead to scalable and accelerated business outcomes.

Take command of your data life cycle

It's critical for organizations to keep value-based data risk management front and center when considering the data life cycle, because this approach can help companies manage data risk more effectively.

Do you *really* know the actual versus perceived behavior of your data along the data life cycle? Here are questions your organization should answer to effectively create, collect, store, process, analyze, use, share, transfer, destroy, or archive its business-critical data in a value-based manner.

Critical data life cycle questions

	Data Management	Data reporting and analytics	Data privacy	Data protection
Create or collect	How is data curated? How are you reducing errors?	How is data tagged at entry? Can you detect malicious ingestion?	Do you need consent to collect the data? Do you need to anonymize it?	How do you classify your data and determine how it should be protected?
Store and process	Who owns your critical data, where is it stored, and how do you govern personal data?	What is the alignment between your data stores, data warehouses, and reporting platforms?	Do you have a current inventory of your personal data?	Is data secured through encryption and access controls?
Analyze and use	How do you balance the need for data access with data use?	How do you achieve responsible data interpretation?	Is data being used in accordance with legal commitments and international regulations?	How do you govern controls?
Share or transfer	What regulatory requirements apply to data sharing and transfer in/outside your company?	How is confidential data consumption and transfer monitored?	Is data transferred to third parties done so in accordance with privacy regulations?	If data in transit were accessed by a threat actor, could it be useable?
Retain and destroy	How effetive is your retention policy?	Is your data monetization strategy aligned with your data retention framework?	Can you handle individuals' requests to delete their data?	Are you keeping data too long? How are backups and archives secured?

The march to value-based data risk management

As your organization adapts to the increasingly sophisticated data risk management battlefield—from collecting and protecting your data to archiving and destroying it—organizations will be better positioned to leverage the benefits of their data while managing the associated risks. Organizations will also be better prepared to seize the competitive advantage that value-based data risk management can provide.

Does your battle plan include a value-based data risk management approach?

How Deloitte can help

Deloitte Risk and Financial Advisory can help you build a mature risk program around your organization's most valuable data. With 21,000 risk management and security professionals in the global Deloitte Touche Tohmatsu Limited network of member firms—and more than 3,000 cyber risk practitioners in the US member firm alone—we can assist you in truly discerning the value of your data and managing your data risk throughout the data life cycle.

Let's Talk

To learn more about value-based data risk management, contact:

Emily Mossburg
Principal
Risk and Financial Advisory
emossburg@deloitte.com

Vic Katyal
Principal
Risk and Financial Advisory
vkatyal@deloitte.com

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, Deloitte means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

36 USC 220506