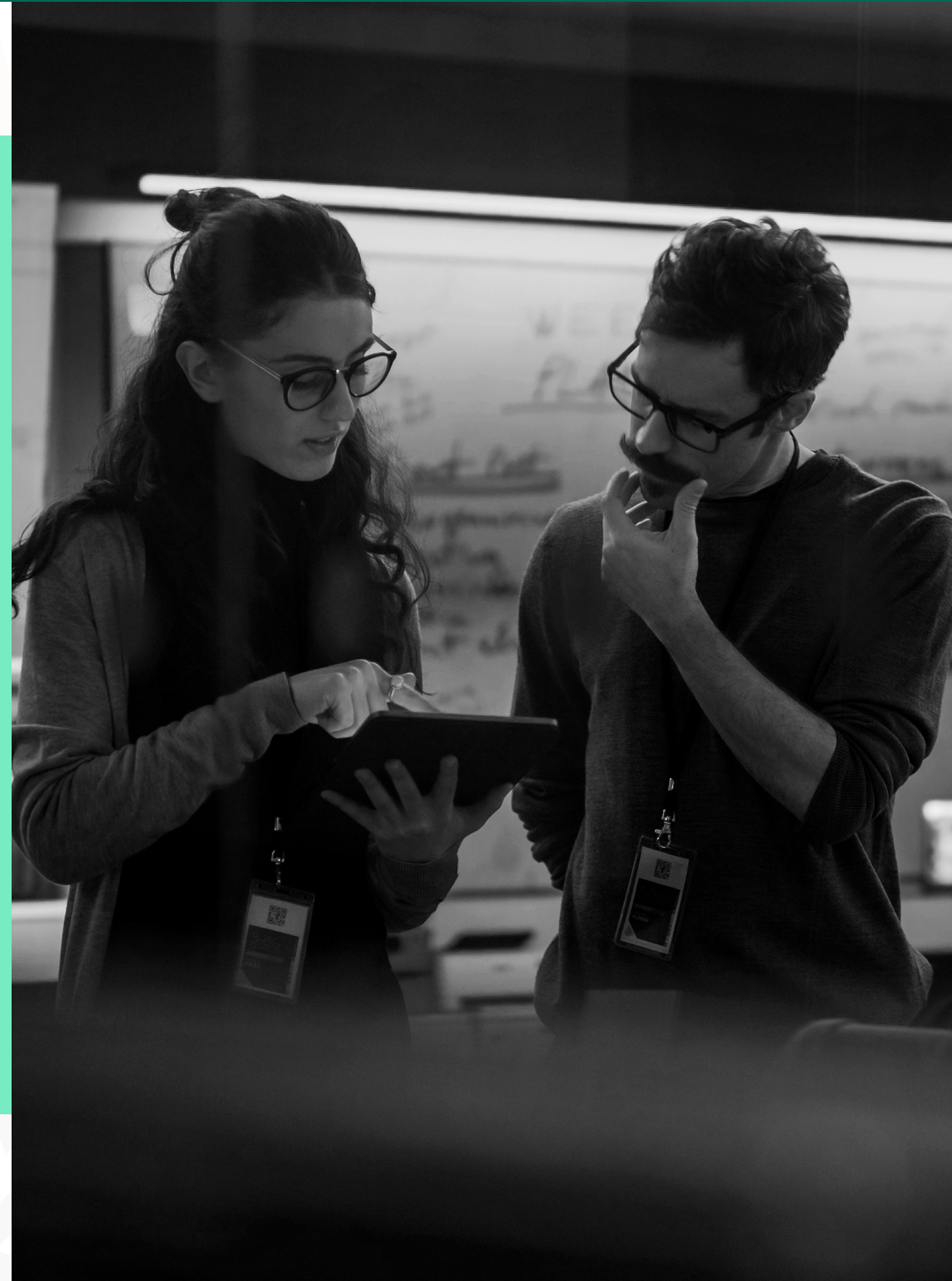


FORTRATM

10 Data Classification Mistakes to Avoid

Nearly every CISO knows the importance and value of classifying their data. Having a data classification policy in place makes it easier to locate and retrieve data; it's also a must for any effective data security plan, especially if you're looking to address any risk management or compliance needs.

While data classification is critical to an effective information security program, rolling out data classification alone does not equal data security. To gain more insight into some of the struggles companies have when it comes to properly classifying data, let's look at 10 data classification mistakes organizations should try to avoid.



1

Lack of enterprise-wide data management standards and governance

By not looking at information from across the enterprise, organizations aren't getting a comprehensive look at their business. Organizations need an [enterprise-wide data governance policy](#), one that identifies critical data elements, where they originated from, and how they're used. Then they can define rules and processes on data creation and consumption. Without that scope, businesses may be relying on inaccurate or incomplete data to run dashboards or generate insights.





Before forming your policy, ensure you've established key goals, objectives, and the strategic intent around it. Make sure everyone at the business is on the right page about how the policy can support increased revenue, reduce costs, and eliminate risk. Make sure there are standards and methodology in place for assessing impact levels, specifying data usage guidelines, and how data classification will be assigned to data types and data sets.

Not properly defining a data classification policy

2

3

Inconsistency and incompleteness in classification data

Poorly defined classification—either too broad or ambiguous—can jeopardize the future of your [data protection program](#). The way you gather and classify data, how its collected, and how its measured, is essential to how is utilized and interpreted. Failing to consistently classify data and address weaknesses in datasets can lead to incorrect classification and even missing data. Having a solution to detect and fix anomalies like consistencies in data sets is crucial.

4

Not knowing what your organization's goal behind classifying data is

What's the point? Organizations should have a clear goal in mind before embarking on their data classification journey. It shouldn't just be done to check a box. Locating and labeling your data can only help your data security and compliance needs so much. Decide what kind of influence you want your data to have on decision making before spending time and money on the project.





Having buy-in from the C-Suite is always important. Without having senior leaders onboard to publicly support data classification and stress its importance to business leaders how their partnership is key to making the effort a success, the effort will have very little chance of reaching its goals.

Lack of corporate sponsorship

5



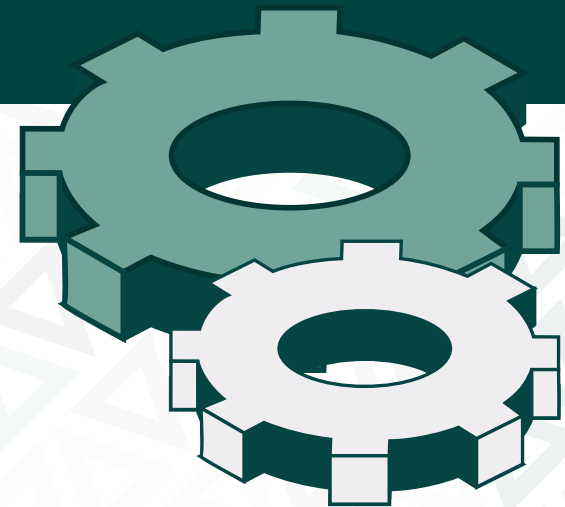
Failing to realize that data is always in flux

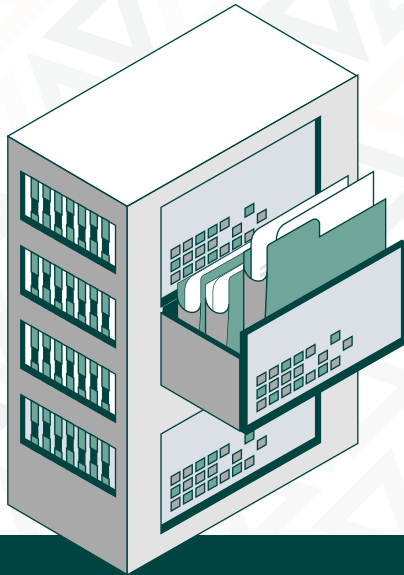
Make sure your data classification policy takes into account the fact that data is always changing. There can be changes in volumes of data or data sensitivity, something which can affect classification efforts. Keep in mind that if you're classifying data in an ad-hoc fashion, you run the risk of diminished accuracy. Knowing data changes throughout its lifetime, the classification level of a particular data type, and having controls in place to secure it, are a data classification best practices.

7

Not involving automation in the data classification process

Automation plays a central role in data governance. It helps to maintain the required balance between technology and people-focused operations to achieve a comprehensive security culture. [Using automated content and context-based classification](#) as well as manual user classification, optimized for regulatory compliance, is highly recommended when rolling out your data classification program.





One of the biggest benefits of data classification is being able to understand what type of data you store and where it's located. After, it can be used by [downstream solutions](#) to enforce baseline data protection policies. Intuition can be your worst enemy though. When practitioners are narrow-minded and stick to their own preconceived notions about data sets, they can fail to look beyond how the data is used day-in and day-out. That can lead to incorrect, imbalanced classification.

**Failing to look at the big picture,
beyond classification, to see
how data is used**

8



When users don't understand the basis and benefits behind classifying data

Corporate policies governing how data should be managed need to exist and employees need to be educated on them. While data classification programs are great at identifying sensitive company assets, they can be educational too. What's being enforced should be based on company policies, as these policies are generally created by the legal, privacy, and compliance teams. Consistent classification educates employees on what is sensitive according to company rules and highlights how they should handle that data.

10

Thinking of data classification as strictly a security effort

Embarking on a data classification project should be a partnership between all teams. Stakeholders from the security, corporate, legal, privacy, and compliance departments should all have a hand in its creation. Classification programs should be based on company policy and can be more successful if done in partnership with the owners of those policies.



Why Zero Trust Needs Data Classification To Work

Read this eBook to learn how to lay the correct groundwork to effectively guard against threats and strengthen your security posture using a Zero Trust strategy.

[READ NOW](#)





About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.