The risks of cybersecurity are not only coming from the outside, but as stated by Arsenault (2023), companies need to be aware of their exposure to risks that come from inside their organizations. In addition, more than 300 million people are working remotely, consequently producing, sharing, accessing the data wherever they go. 'Data breaches arising from insider threats and simple mishaps can cost businesses an average of $7.5 million annually' (Arsenault, 2023). In order to minimize the costs of data leakage and to follow best practices, each organization should hold to the standards provided by the ISO/IEC organization. The following standards are a good way to prevent unwanted activities within the organization itself:

**ACCESS CONTROL:**

Ensuring that the people go through the proper access control is the simple and effective starting point to avoid unauthorized access. Ideally the people would only have access to the data that they need for their everyday work. On the other hand, unauthorized access to data that should not be accessed imposes a direct threat to the system.

**AUDIT:**

Monitoring all the activities is a great approach to prevent the breaches in advance. Ideally, each activity should be monitored, however this rises another question regarding privacy. However, at least most risky actions should be monitored, to track the changes, in order to prevent the actions that may happen.

**INFORMATION SECURITY CONTINUITY:**

Continuous data protection is mandatory, as the organization can't know when the activity is about to happen. Ongoing and adequate data protection allows organizations to avoid weak chains in their systems, hence utilizing continuous data consistency.

**INFORMATION SECURITY INCIDENT MANAGEMENT:**

Focuses on the procedures required in the case of a breach. These include detecting, reporting, assessing, responding etc.

**COMPETENCE:**

In order to prevent important data from being exploited, organizations should hire professionals, responsible for implementing proper precautions and nevertheless spread awareness among other employees regarding data breaches.

**References:**

Arsenault, B. (2023). Your Biggest Cybersecurity Risks Could Be Inside Your Organization. Harvard Business Review. Available from: https://hbr.org/2023/03/your-biggest-cybersecurity-risks-could-be-inside-your-organization [Accessed 13 May 2023]

ISO. (2018) ISO/IEC 27000:2018 (en) Information technology - Security techniques - Information security management systems - Overview and Vocabulary. Online Browsing Platform (OBP). Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:sec:3 [Accessed 13 May 2023]

Tags: [iso standards,](https://www.my-course.co.uk/mod/oublog/view.php?id=810592&amp;taglimit=500&tag=iso+standards) [precautions,](https://www.my-course.co.uk/mod/oublog/view.php?id=810592&amp;taglimit=500&tag=precautions) [cybersecurity,](https://www.my-course.co.uk/mod/oublog/view.php?id=810592&amp;taglimit=500&tag=cybersecurity) [data breach](https://www.my-course.co.uk/mod/oublog/view.php?id=810592&amp;taglimit=500&tag=data+breach)