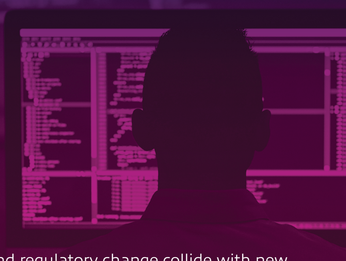
Insight

The Reality Of Data Security And The New Normal



As the standard challenges of data growth and regulatory change collide with new concerns posed by the global shift to remote work and growing wave of economic uncertainty, businesses need to adapt their approach to data security.

This infographic uncovers considerations from data security and business experts to help you evolve your approach in three key areas.

01 Securing remote work environments

The attack surface has expanded dramatically.
The heightened risk of distributed security environments demands that businesses update their approach to security.

- Implement Multifactor Authentication (MFA)
- Enable secure remote access
- Assess app security and compatibility

Businesses of all sizes are expected to increase security spending this year.

Cross-team training is critical for effective security.
Your entire organization is responsible for data security. Training all employees on security protocols can help protect Personally Identifiable Information (PII) and prevent leakage.

Read the guide: "The security impact of rapidly enabling remote workers"

02 Surveying your data landscape

Understanding your data landscape and environment is key.
Survey your data landscape by asking these questions:

Classify: What is the data we're trying to protect?

Control: How do we protect it?

Data classification needs to be an ongoing process.
Like painting the Golden Gate Bridge, data classification is a continual process due to constant data growth and changing regulations.

Watch the video: "Data Classification and Data Loss Prevention"

03 Seeing the bigger picture

The larger your organization, the more important least privilege becomes.
Many organizations give access to everyone — even when it's not safe. Given the weaknesses of a distributed security environment, it's critical for businesses to limit access with identity-based controls.

22%
of all folders in a company are open to every employee

53%
of companies have found more than 1,000 sensitive files open to every employee

Identity and Access Management (IAM) is about more than compliance.
Businesses can — and should — leverage the efficiency and control gained from IAM programs to propel productivity and transformation.

- Efficiency
- Control
- Compliance
- Productivity
- Risk mitigation
- Business continuity

Read the whitepaper: "Mastering Identity and Access Management"

Evolve your approach to security

Growing security challenges call for a fresh approach. Improve your security posture and protect your workforce with assistance from industry-leading security professionals.

Contact us to discuss your security concerns with an expert.

Insight

Sources:
Avant, Venky, Caso, Jeffrey, and Schwarz, Andreas. (2020, July 21). COVID-19 crisis shifts cybersecurity priorities and budgets. McKinsey & Company.
Varonis. (2019). 2019 Varonis Global Data Risk Report.