nixu cybersecurity.

Not seeing the full spectrum

Five most common cybersecurity mistakes

Threats and risks related to cybersecurity are increasing. These incidents and data breaches can lead into losing customers trust, loss of business and regulatory sanctions. Make your organization more secure by checking out our list of most common cybersecurity mistakes.

Thinking cybersecurity is only your IT department's responsibility

IT teams are often lacking resources and sufficient support. Taking care of your organization cybersecurity is not a one-man-job, nor is it solely a technical issue. Cybersecurity must be spread in all levels of your organization.

Forgetting to train your employees

Not everyone is interested or familiar with cybersecurity related risks and threats. Employees need assistance and support to become and stay compliant with cybersecurity policies. Offer your people training and exercises to make the learning process as comprehensive as possible.

Overlooking actual cybersecurity risks

Organizations should perform cybersecurity assessments on a regular basis. If you do not regularly assess your cybersecurity risks, overlook them or do not mitigate the findings, the risks of vulnerability to cyber-attacks increases significantly. Organizations should constantly be fully aware of both their operating environment and their cybersecurity status and have the ability to implement plans rapidly into action.

Not defining specific security requirements

Cybersecurity related risks and threats pose significant challenges and should not be underestimated - especially for budget reasons. Working with an outsourced IT service company, is vital for the organization to give a clear, comprehensive brief to the service provider about their roles and responsibilities. Always stay alert and involved and always double-check.

Defining security policies, but not implementing them

Writing down your organization's cybersecurity crisis plan and policies is the right thing do. Unfortunately, policies and plans are useless unless put into use. Enforcing your security policies in both processes and ways of working ensures that your organization operates more safely and effectively at all levels.

We can help your organization by

- Assessing your organization's status and creating a clear action plan
- Balancing business needs and cybersecurity risk management
- Identifying vulnerabilities and defining remedial activities
- Facilitating cybersecurity development and increasing the organizations cybersecurity posture

nixuoy nixu-oy NixuTigerTeam

nixu.com/cybersecurity-roadmap