ITW
IT Weapons
A Konica Minolta Division

Essential Cybersecurity Measures for Your Organization

Is Your Organization Protected?

The cybersecurity landscape keeps changing, and organizations of all sizes must keep up with the latest vulnerabilities and methods of protection.

Understand the current state of cybersecurity threats and debunk common misconceptions about cyberattacks. We'll help you identify the specific risks your financial institution could face and highlight the potentially significant costs of data breaches, including the loss of sensitive data, reputational damage, and regulatory penalties.

Enforce modern cybersecurity measures to protect your organization and mitigate costly attacks.

The Threat Landscape

According to recent reports, approximately 65% of organizations haven't fully recovered from a data breach event within the past 12 months. This figure highlights the growing vulnerability across sectors, which has faced increasing threats, including ransomware, phishing, and advanced hacking attempts targeting sensitive financial data.

$4.84 M

Average cost of a data breach in Canada, nearly 10% more than the global average.

Common Misconceptions:

- "I'm not a target."
- "Small and medium businesses are not at risk."
- "No one wants my data."
- "I can put it off until next year."
- "I don't have a budget for security."
- "Nobody will guess my password."

Challenges Financial Institutions Face

Impact of Cyberattacks:

276
Days it took to identify and contain a data breach across various environments.

86%
Share of businesses that experienced a disruption due to a data breach.

97%
Share of organizations that had an AI-related security incident to their models or applications and had lacked proper AI access controls.

30%
Only one-third of data breaches are discovered by an organization's own security team.

26%
Data breaches caused by human error.

Top Risks

- Outdated software and lack of patch management
- Inadequate endpoint detection and response
- Weak password management and authentication measures
- Insufficient backup and recovery solutions
- Poor third-party risk management
- Human error and lack of cybersecurity awareness

Associated Costs

Commonly Known

- Data breaches and data loss
- Regulatory fines and legal costs
- Reputation damage
- Operational downtime

Less Commonly Known

- Increased insurance premiums
- Costs associated with recovering stolen assets
- Intellectual property theft
- Customer compensation for damages
- Fraud and financial loss

Modern Cybersecurity Measures

1 Managed Access and Secure Authentication

- Implement least access and privileged access strategies.
- Enforce multifactor authentication on critical applications.
- Limit VPN access to those who require it.

2 Endpoint Protection and Response

- Utilize endpoint detection and response solutions for real-time threat detection and response.
- Ensure continuous monitoring and updating of endpoint security.

3 Modern Backup Solutions

- Establish comprehensive data backup and recovery plans.
- Regularly test backup systems to ensure reliability.

4 Risk Assessment and Asset Inventory

- Conduct regular security risk assessments.
- Maintain an up-to-date inventory of all devices and software.

5 Third-Party Risk Management

- Evaluate the security practices of all third-party vendors.
- Regularly review and update third-party risk management policies.

Stay Ahead of Threats with Services from IT Weapons

Strengthen your organization's defenses with advanced technological safeguards. Choose a customized support plan that includes managed IT services, remote monitoring, vulnerability scanning, threat management, security training, vISO services and more—specifically designed to address the unique needs of organization across industries.

Get in touch with our team today to learn how we can ensure your business runs optimally.

Contact Us

ITW
IT Weapons
A Konica Minolta Division