Session date

Session subject

Enterprise Risk Management: Integrating Cybersecurity

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Anthony Silinda
Future Spot Technology

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Agenda

01 Identify Key Cybersecurity Risks

02 Assess Data Protection Strategies

03 Develop Response Plans Effectively

04 Integrate Risk Frameworks Seamlessly

05 Measure Compliance and Performance

06 Foster Organizational Awareness Culture

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Introduction to Risk Management Importance

Risk Assessment

Identify potential threats to the organization's assets and operations.

Data Encryption

Implement encryption protocols to protect sensitive data both at rest and in transit.

Policy Framework

Establish comprehensive policies for risk management and response strategies.

Incident Response

Develop and test an incident response plan to ensure rapid recovery from breaches.

Employee Training

Conduct regular training sessions to enhance cybersecurity awareness among staff.

Continuous Monitoring

Regularly review and update risk management practices to address new threats.

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Agenda Overview and Key Topics

Risk Assessment

Identify and evaluate potential cybersecurity threats and vulnerabilities.

Compliance Framework

Implement frameworks that align with regulatory requirements for data protection.

Incident Response

Develop and test response plans for cybersecurity incidents and breaches.

Employee Training

Educate staff about data protection and cybersecurity best practices.

Technology Solutions

Adopt advanced tools for monitoring and mitigating cyber threats.

Third-Party Risks

Evaluate and manage risks associated with external vendors and partners.

Regular Audits

Conduct frequent assessments to ensure compliance and risk management effectiveness.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Objectives of Cybersecurity Integration

01

Enhance

Strengthen security measures across all digital platforms and data.

02

Mitigate

Reduce risks through proactive threat identification and management.

03

Align

Ensure cybersecurity strategies align with business objectives and goals.

04

Educate

Provide regular training to employees on best security practices.

05

Monitor

Continuously assess systems for vulnerabilities and emerging threats.

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Vision for Enterprise Risk Management

Vision

To establish a resilient framework for managing enterprise risks, focusing on cybersecurity and data protection.

Mission

To empower organizations to effectively mitigate risks while ensuring robust cybersecurity and comprehensive data protection strategies.

Values

Integrity, collaboration, accountability, and innovation in managing enterprise risk and protecting digital assets.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Understanding Current Threat Landscape

01

Threat Identification

Regularly assess and identify potential cybersecurity threats through comprehensive risk assessments, leveraging threat intelligence reports to stay ahead of emerging risks and vulnerabilities.

02

Incident Response

Develop and implement an incident response plan that outlines the steps to take in the event of a data breach, ensuring quick containment and communication with stakeholders.

03

Employee Training

Conduct ongoing cybersecurity awareness training for employees, focusing on identifying phishing attempts and other cyber threats to reduce human error in data protection efforts.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Identifying Key Cybersecurity Challenges

Key Points

- Constantly evolving threats demand adaptive security measures.
- Increased data exposure leads to higher breach risks.
- Stricter regulations necessitate robust data protection strategies.
- Lack of training increases vulnerability to cyber attacks.

Context Overview

01

Market Trends

Emerging technologies shape the future security landscape.

02

Regulatory Impacts

Changing laws influence enterprise risk management strategies.

03

Cultural Shifts

Growing emphasis on security-awareness throughout organizations.

04

Technological Innovations

Advancements improve defenses against cyber threats.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Gap Analysis of Existing Frameworks

- Existing frameworks lack integration with cybersecurity needs.
- Data protection measures are often poorly implemented.

Action Plan

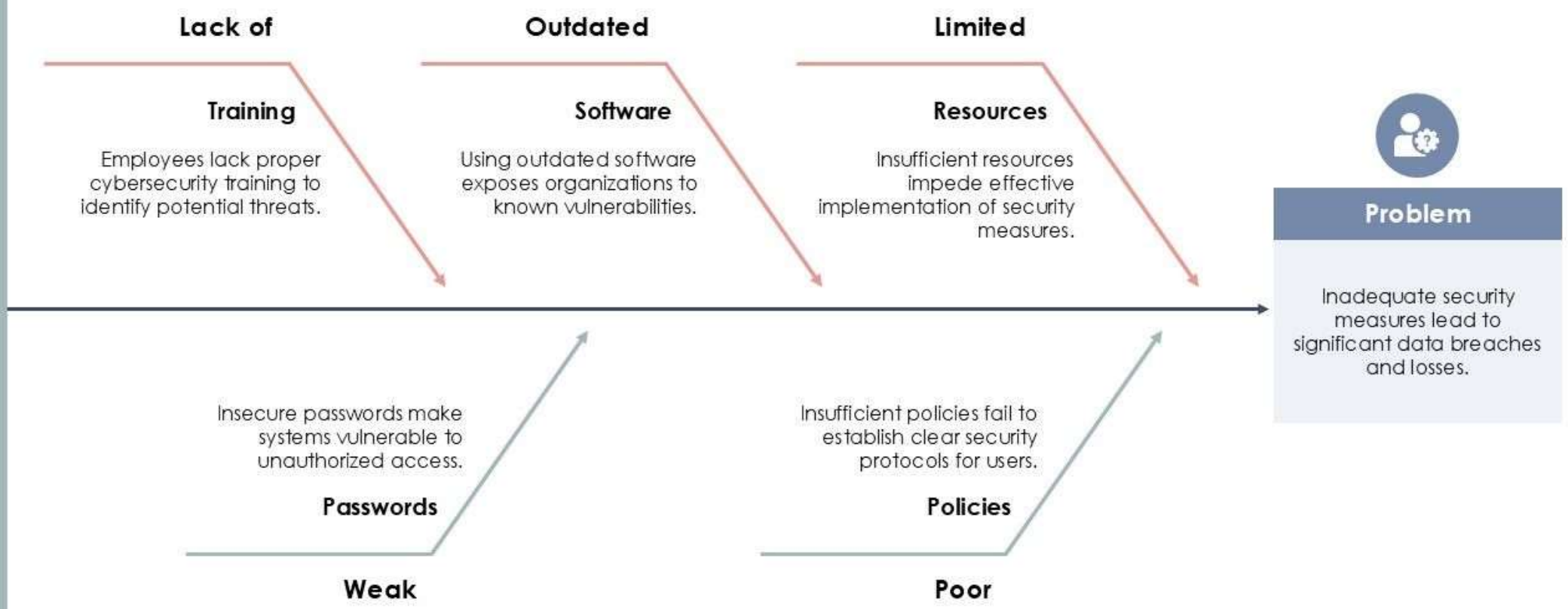
01 Conduct a thorough assessment of current frameworks.

02 Develop a roadmap for integrating better security practices.

- Frameworks should comprehensively integrate cybersecurity practices.
- Data protection policies must be fully enforced organization-wide.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Root Cause of Cybersecurity Vulnerabilities



CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Multi-Faceted Risk Assessment Techniques

Identify Risks

Systematically recognize potential risks and vulnerabilities in the organization.

Mitigation Strategies

Develop actionable plans to prevent, reduce, or eliminate identified risks.

Evaluate Impacts

Analyze the potential impacts and consequences of identified risks thoroughly.

Compliance Check

Ensure adherence to regulatory requirements and industry standards for risk management.

Prioritize Risks

Rank risks based on their likelihood and potential severity for effective management.

Continuous Monitoring

Implement ongoing monitoring practices to detect changes in risk profiles and emerging threats.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Scenarios for Cyber Risk Impacts

01 **Cost**

Cyberattacks cost companies million.

02 **Growth**

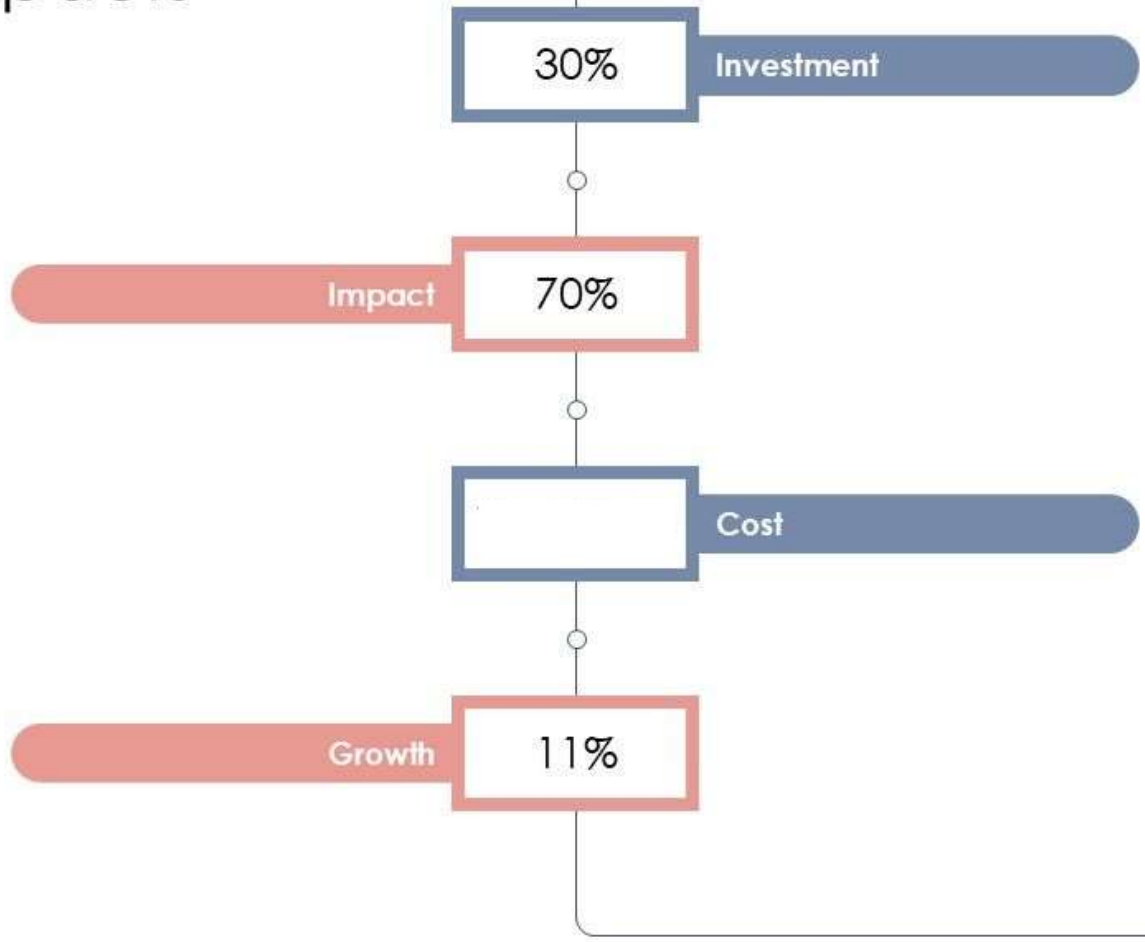
Data breach incidents grew by 11% in recent years.

03 **Investment**

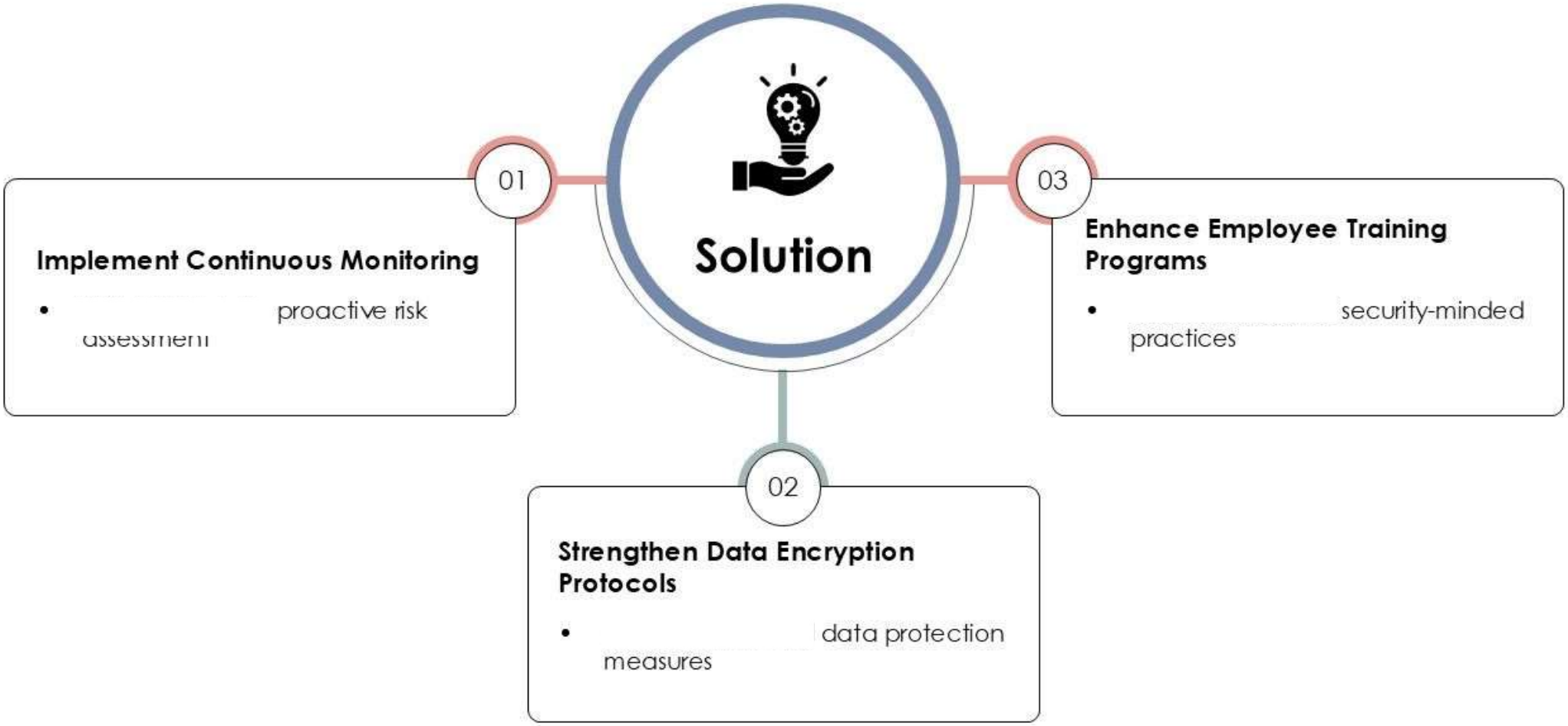
Businesses increased cybersecurity budgets by 30% annually.

04 **Impact**

70% of small businesses suffer from cyber threats.



Strategic Solutions for Risk Mitigation



CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Value of Cybersecurity Investments

Costs

01 Initial setup and implementation costs

02 Ongoing maintenance and support fees

03 Training staff on security protocols

04 Potential costs from data breaches

Benefits

01 Reduced risk of data breaches

02 Enhanced customer trust and loyalty

03 Improved compliance with regulations

04 Greater operational resilience and recovery

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Competitive Landscape in Cybersecurity

	Market Share	Growth Rate	Impact
Major Players	40%	10%	High risk of breaches
Emerging Threats	15+	25%	Increasing focus on cloud security
Investment Trends	25%	15%	Cybersecurity spending up significantly
Regulatory Changes	5+	30%	Stricter compliance required annually

Core Findings

01

Market Dominance

Top three firms cover 60% of sales.

02

Rising Threats

Phishing attacks rose 45% in 2023.

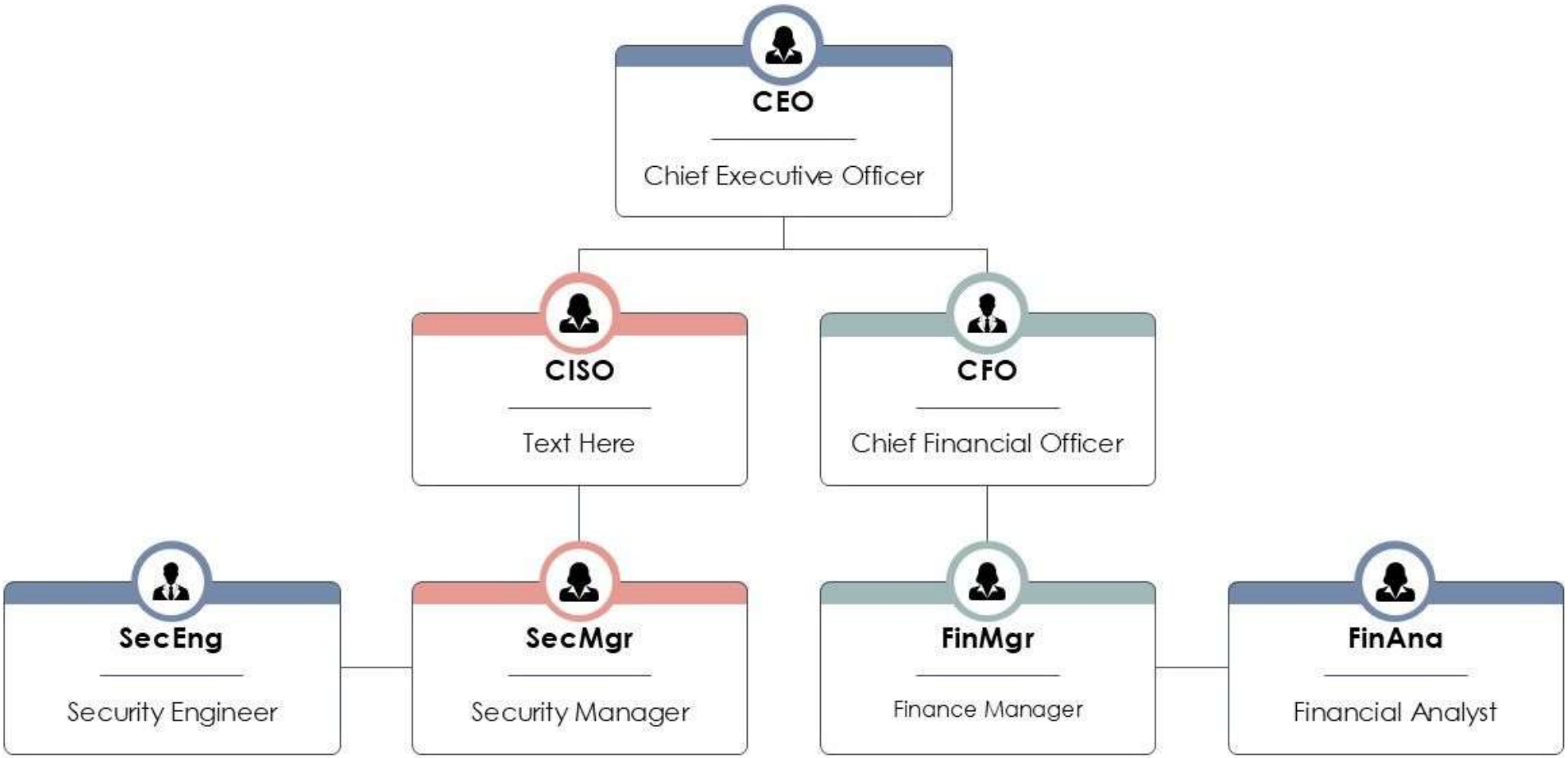
03

Regulatory Updates

New laws increase compliance costs for all.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Understanding Stakeholder Responsibilities



CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Emerging Market Trends in Cybersecurity

01 **AI Usage**

Leveraging artificial intelligence for threat detection and response.

02 **Zero Trust**

Implementing zero trust architecture to enhance security posture.

03 **Risk Management**

Integrating risk management frameworks for cybersecurity strategies.

04 **Data Privacy**

Adopting robust data privacy protocols to comply with regulations.

05 **Cloud Security**

Enhancing security measures for cloud-based applications and services.

06 **Incident Response**

Establishing incident response plans for swift breach mitigation.

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Analyzing Customer Data Protection Needs

Strengths

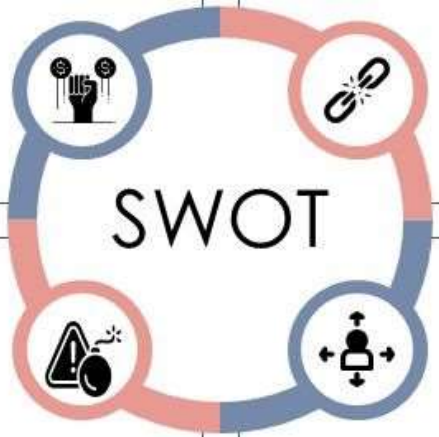
Strong commitment to data privacy increases trust among customers and stakeholders alike.

Established protocols for data management ensure systematic handling of sensitive information.

Weaknesses

Limited internal resources for comprehensive data protection assessments may exist.

Compliance with evolving regulations can strain existing cybersecurity frameworks significantly.



Threats

Constantly evolving cyber threats pose significant risks to existing data protection strategies.

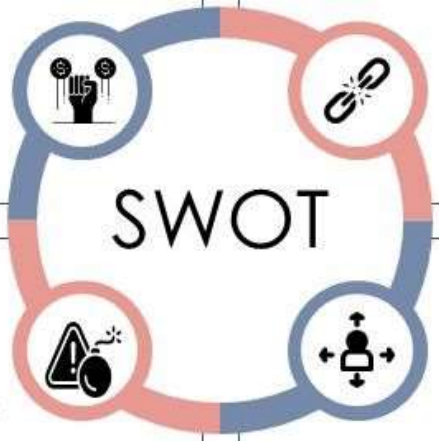
Breaches of trust from high-profile data leaks could severely harm brand reputation.

Opportunities

Emerging technologies present new ways to enhance data protection and cybersecurity measures.

Expanding market demand for secure data solutions offers growth potential for service providers.

SWOT Analysis of Current Strategies



Strengths

Comprehensive policies promote a strong culture of cybersecurity awareness among employees.

Robust data protection measures can enhance customer trust and loyalty in the organization.

Weaknesses

Limited resources can hinder effective risk management implementations and response strategies.

Outdated technology may expose vulnerabilities against advanced cyber threats and attacks.

Threats

Increasing sophistication of cyberattacks poses significant risks to organizational data integrity.

Regulatory changes may increase compliance costs and impact operational flexibility and efficiency.

Opportunities

Emerging technologies can improve detection and response to potential cybersecurity threats.

Partnerships with cybersecurity firms can enhance defense capabilities against evolving attacks.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Pros and Cons of Cybersecurity Approaches

Pros

Enhanced Security

Improved safeguarding of sensitive data against cyber threats and breaches.

Regulatory Compliance

Assists organizations in meeting legal and industry-specific compliance requirements.

Risk Mitigation

Proactively reduces potential risks and vulnerabilities in the IT infrastructure.

Cons

High Costs

Implementing strong cybersecurity measures can be financially burdensome for many organizations.

Complex Integration

Integrating cybersecurity with existing systems may lead to operational challenges.

False Sense of Security

Over-reliance on cybersecurity tools may overlook human factors in risk management.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Financial Implications of Cyber Risks

01

Loss Impact

Cyber incidents lead to significant financial losses.

02

Regulatory Costs

Compliance failures result in hefty penalties and fines.

03

Text Here

Downtime from breaches causes revenue loss and recovery costs.

04

Reputation Damage

Data breaches negatively affect customer trust and market value.

Activity Stream

Risk Assessment

Identify and evaluate potential cyber risks regularly.

Mitigation Strategies

Develop effective measures to reduce identified risks.

Monitoring

Continuously track risk management efforts and incidents.

Response Planning

Establish clear guidelines for responding to breaches.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Resource Allocation for Cybersecurity

	Date	Date	Date	Date	Date
Budget Allocation					
Cyber Risk Assessment					
Training Programs					
Incident Response Plan					

Insights

01

Budget Growth

Cybersecurity budget increased by 50% since 2021.

02

Training Importance

Employee training reduces breaches by up to 80%.

03

Incident Response

Effective plans minimize damages significantly post-incident.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Data-Driven Decision Making Techniques

01

Data Analysis

Utilize analytical tools to process large volumes of data for better risk assessment outcomes.

02

Predictive Modeling

Implement predictive models to forecast potential cybersecurity threats and prioritize responses accordingly.

03

Risk Metrics

Establish clear metrics to measure cybersecurity effectiveness and guide data protection strategies.

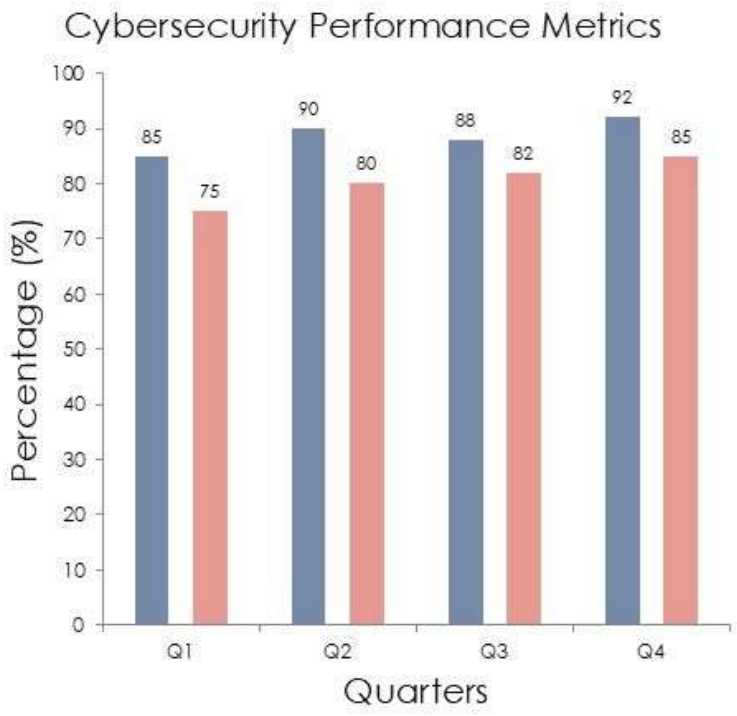
04

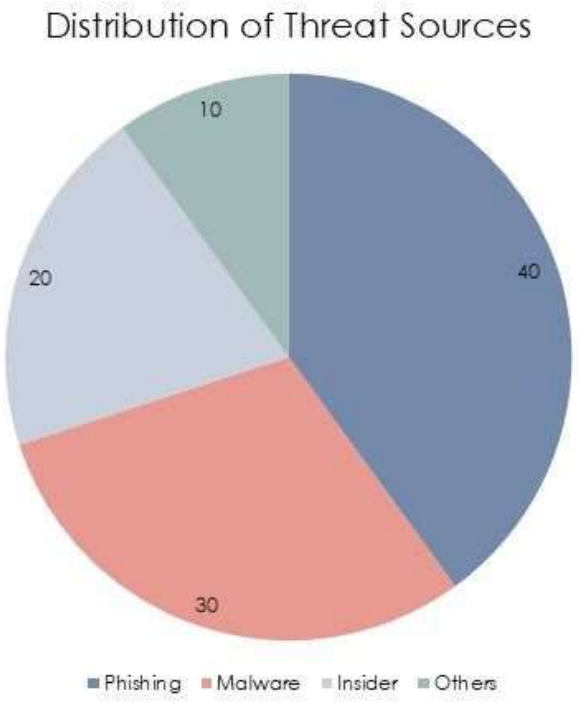
Continuous Monitoring

Adopt continuous monitoring systems to collect data in real-time for prompt decision-making.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Key Performance Indicators for Cybersecurity





Detection Rate

95%

Breach Count

5

Response Time

1 hr

User Training

100%

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Detailed Budget and Cost Planning

	2023	2024	2025	2026	Total	Variance
Projected Costs						
Risk Mitigation						
Resource Allocation						
Compliance Expenditures						

Highlights

01

Cost Growth

Projected costs rise by 25% annually.

02

Risk Focus

40% of budget goes to risk management.

03

Compliance Costs

Compliance expenditures double by 2026.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Implementation Strategies for Solutions

	Action Steps	Timeline	Impact	Status
Risk Assessment	Identify potential threats		Improved threat awareness	
Policy Development	Draft security policies		Clear protocol guidelines	
Training Program	Conduct staff training		Enhanced employee skills	
Incident Response	Develop response plan		Effective crisis management	

Text Here

01 Firewall

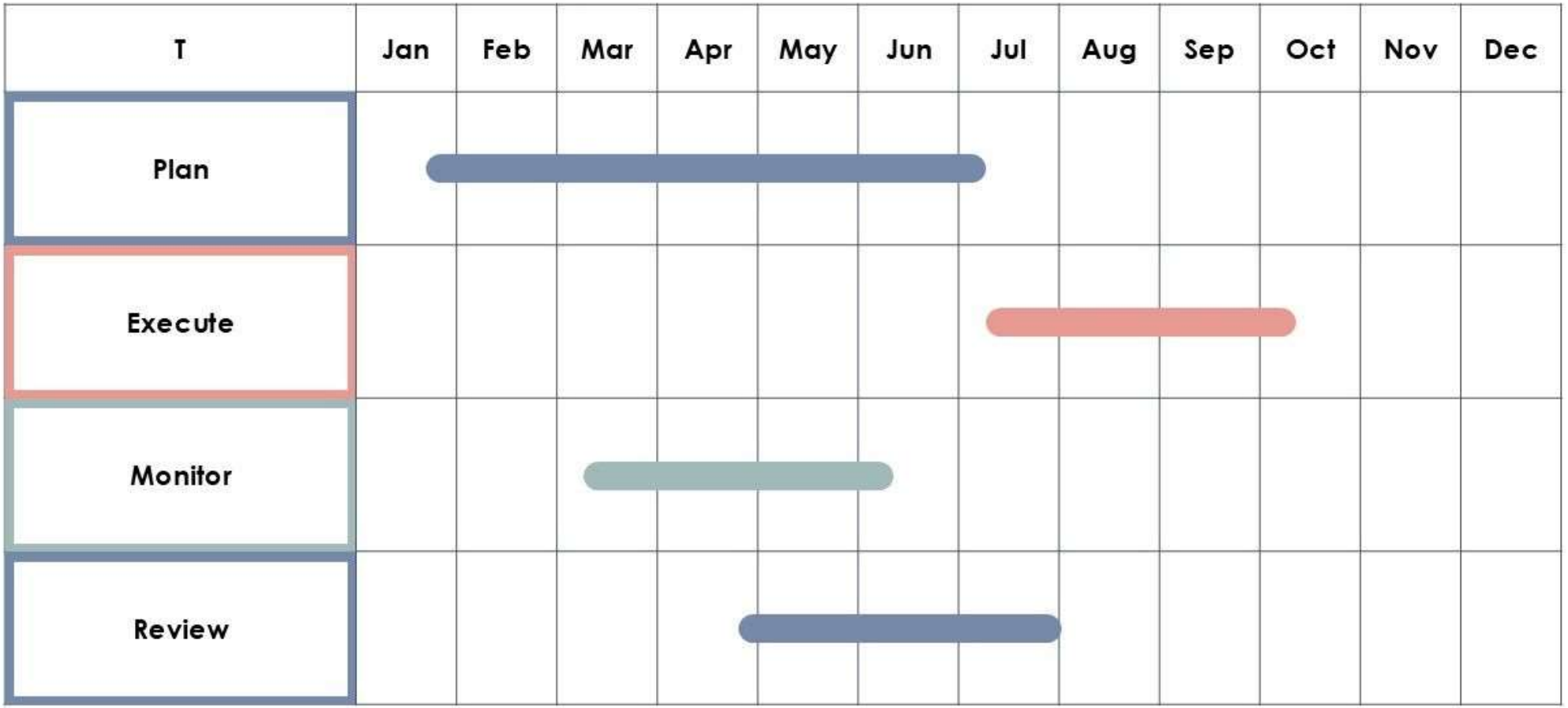
02 Encryption

03 Monitoring

04 Training

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Timelines for Risk Management Initiatives

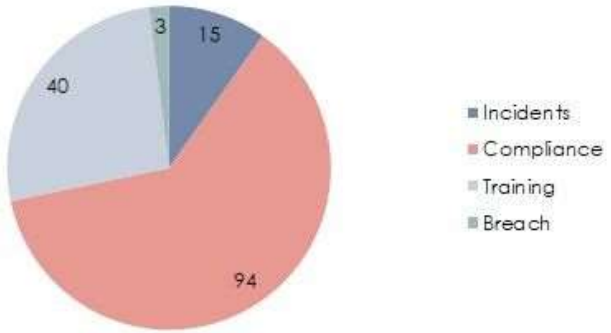


CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

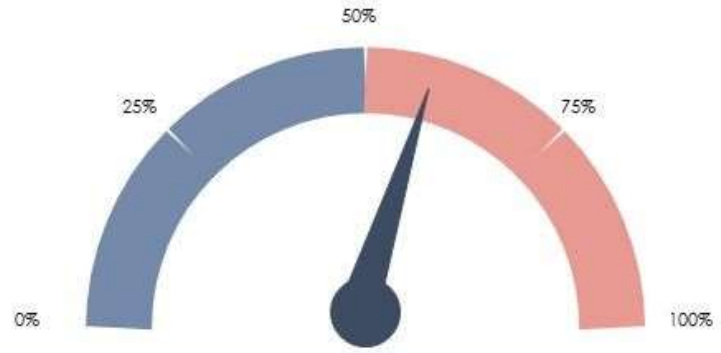
Evaluating Success Metrics for Strategy

Incident Rate	Data Breaches	Compliance Score	Training Hours
15 ▲	**3** ▼	**94** ▲	**40** ▼

Cybersecurity Metrics Overview



Overall Risk Management Score



KPI Achievement Progress

Risk Assessment Progress

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Communication Strategy for Stakeholders

02

Stakeholder Engagement

Facilitate discussions to gather feedback and assess concerns proactively.

03

Clear Language

Use straightforward terminology to ensure all stakeholders understand risks.

01

Regular Updates

Provide frequent information on cybersecurity initiatives and changes.

04

Reporting Metrics

Share quantifiable outcomes related to cybersecurity and data protection.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Preparing for Legal and Compliance Issues

01

Data Privacy

Implement robust data protection policies to ensure compliance with relevant privacy regulations and standards.

02

Incident Response

Develop a clear incident response plan to address legal repercussions following a data breach or security incident.

03

Employee Training

Regularly train employees on compliance requirements and legal obligations related to cybersecurity and data protection.

04

Third-Party Risk

Evaluate and manage risks associated with third-party vendors to ensure their compliance with security standards and regulations.

Thank You!

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body