birlasoft

WHITEPAPER

It's no more about Business Continuity, it's about Business Survival



Cyber Resilience

Cyber resilience is the ability to maintain business operations during and after a cyberattack or data breach. It involves proactive strategies and measures to mitigate the impact of cyber incidents. Overall, the industry is moving towards a proactive and resilient cybersecurity posture, where organizations are not only focused on preventing cyber threats but also on building the capacity to withstand and recover from potential incidents effectively. This involves a combination of technology, processes, people, and governance to ensure the resilience of critical systems and data assets.



Cyber Resilience Challenges

Lack of Cybersecurity Awareness

Complexity of IT Environments

Resource Constraints

Evolving Threat Landscape

Third-Party Risk Management

Key Focus Areas

1. **Develop a Resilience Strategy**
   Conduct comprehensive assessments and craft a robust strategy aligning with goals, prioritizing assets, and outlining actionable steps to mitigate risks.

2. **Employee Training and Awareness**
   Invest in training programs, fostering a vigilant and responsible cybersecurity culture.

3. **Backup and Recovery Plans**
   Implement security controls, robust backup and recovery strategies ensuring continuity, regularly tested for effectiveness.

4. **Continuous Monitoring and Response**
   Utilize real-time monitoring tools, supported by swift incident response capabilities fostering collaboration with peers and experts for proactive defense mechanisms, implementing necessary updates for evolving threats with regular testing and simulations.

5. **Cyber Insurance**
   Consider cyber insurance to mitigate financial losses beyond preventive measures.

6. **Compliance and Regulations**
   Stay informed about regulations, ensuring alignment with industry standards.

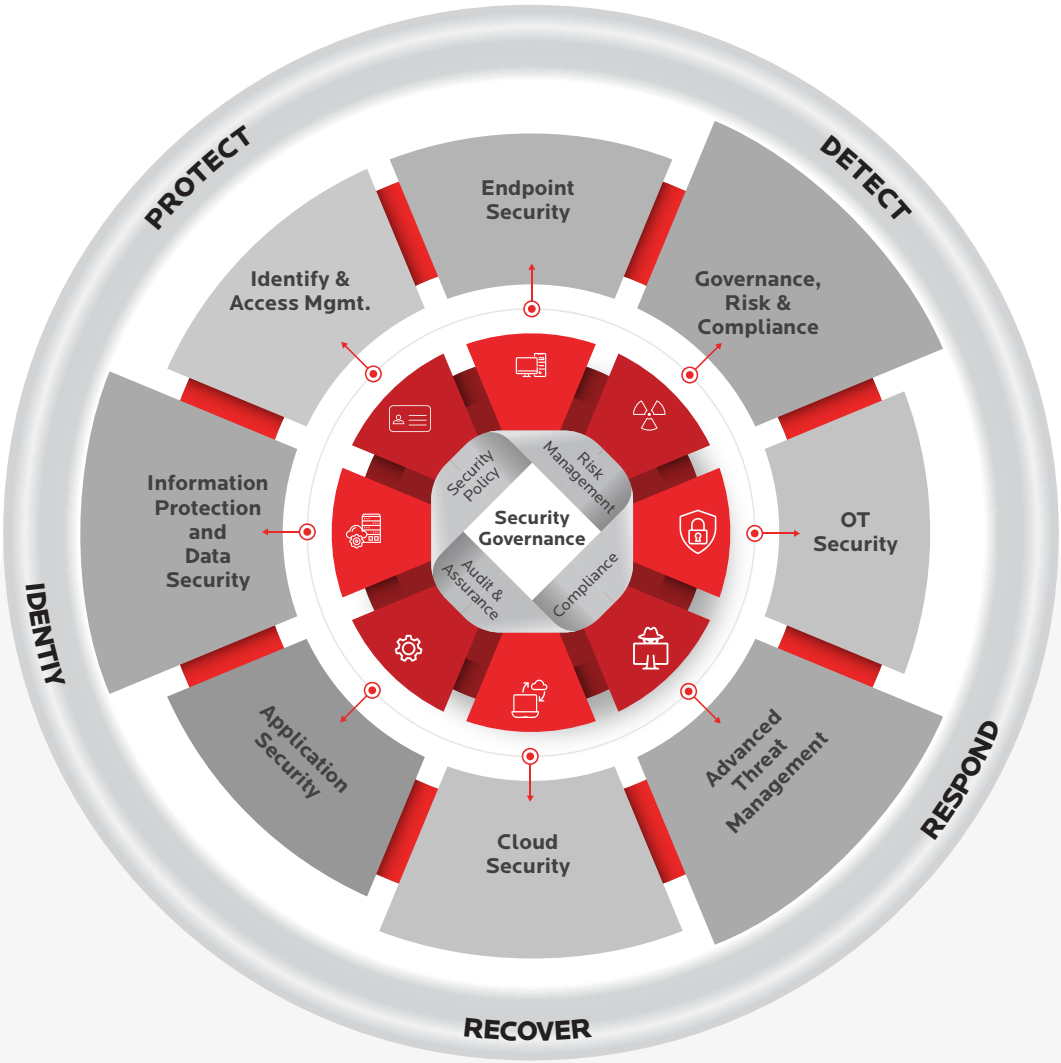
Comparison

CYBERSECURITY	CYBER RESILIENCE
It's the measures taken to ensure safety of an organization	It's the ability to recover quickly from cyber attacks
Works to reduce risk of cyber-attacks and to protect the organisation from cyber theft	Works to ensure continuity on a wider scope, compromising cybersecurity and business requirements
Can work effectively without compromising the usability of other systems	Requires organization-wide culture shift the normalizes and embeds security best practices
Includes a business plan to resume operations in the event of a successful attack	Requires the organization to become agile and adaptable in the face of cyber-attacks and incidents

Birlasoft Solution

At Birlasoft, we work with our customers to define their ransomware strategy & develop a roadmap which brings in clarity on how to improve their Cyber Resilience. We also transform their security ensemble to implement platform-based security solutions that offer an improved visibility and detection capability. To top it all up, we offer Cyber Security services to ensure that not only we manage the security operations well but also bring in a methodology of continuous improvement for our customers to stay ahead of their adversaries in this race.

Our offerings aligned to NIST & ISO 27001 are detailed below:



BSecure
Be Aware Be Secure

Improved Maturity Rating	Regulatory Compliance	Smart Automation
Advanced Security Features	Proactive Threat Management	Zero Day Protection

1 Due Diligence & assessment

6-7 weeks

- Assess current Cyber Security Incident Response Policy - 1 week
- Identify key stakeholders and validate their requirements - 2 weeks
- Understand various other streams working in parallel and dependencies - 2 weeks
- Benchmarking against NIST framework & best practices - 1 week
- Elucidate future skill set requirement and possible roles/organisation for the future state - 1 week

2 Testing

2 weeks

- Conduct a table-top stress-test to gauge present level of preparedness
- Identify possible failure modes
- Outline clear areas of improvement
- Earmark missing linkages & alignment with other Organizational policies
- Finalize specific timeline & parameters for implementation

3 Plan Prep and Implementation

20-24 weeks*

- Incident identification & severity detection criteria
- Clear response & action guidelines identification
- Finalize the key aspects of the plan Governance & ownership
- A clear ramp-Up plan & adoption approach
- Integration of plan in existing frameworks
- Continuous maintenance & validation testing for CR setup

Birlasoft experts align business objectives with the concepts of business continuity to address the critical requirements

1. **Cyber Security Architect:** Governance, Risk Assessment and Security Operations expert with focused knowledge of Ransomware Incident Management
2. **Analyst:** Experience in preparing & evaluating security guidelines, documentation and scenarios



Bold.Agile.Ambitious

Birlasoft combines the power of domain, enterprise, and digital technologies to reimagine business processes for customers and their ecosystem. Its consultative and design thinking approach makes societies more productive by helping customers run businesses. As part of the multibillion-dollar diversified CK Birla Group, Birlasoft with its 12,500+ professionals, is committed to continuing the Group's 161 year heritage of building sustainable communities.

contactus@birlasoft.com | birlasoft.com

RESOURCES

Copyright © 2024. Birlasoft and its logo(s) are trademarks of Birlasoft All rights reserved.
All other logo(s) used are trademarks of their respective owners.