From Deal to Defense:

Crafting a Post-Acquisition Cybersecurity Strategy

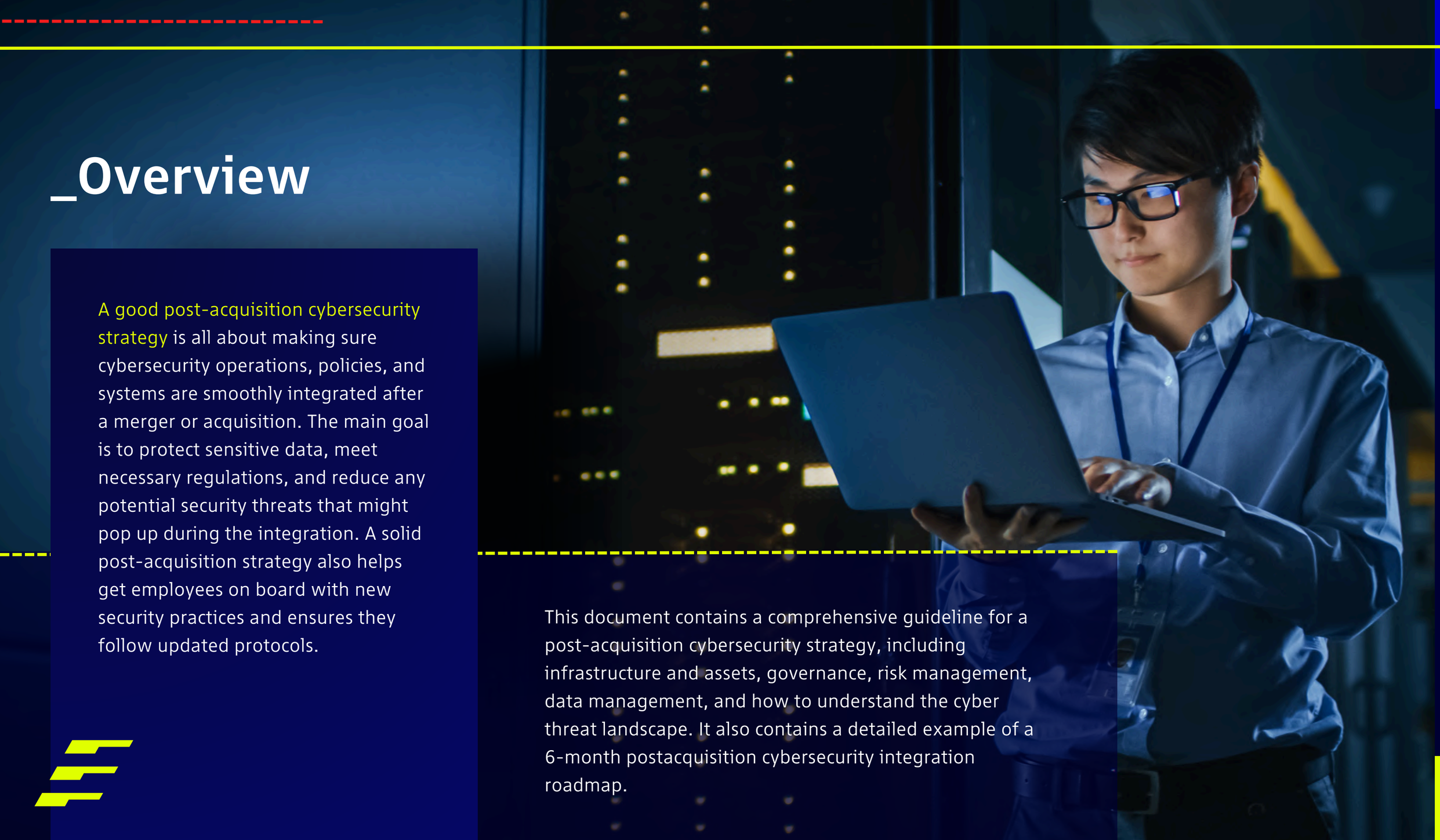
By: Matt Donato

ECHELON RISK + CYBER

_Contents

_Overview

A good post-acquisition cybersecurity strategy is all about making sure cybersecurity operations, policies, and systems are smoothly integrated after a merger or acquisition. The main goal is to protect sensitive data, meet necessary regulations, and reduce any potential security threats that might pop up during the integration. A solid post-acquisition strategy also helps get employees on board with new security practices and ensures they follow updated protocols.



This document contains a comprehensive guideline for a post-acquisition cybersecurity strategy, including infrastructure and assets, governance, risk management, data management, and how to understand the cyber threat landscape. It also contains a detailed example of a 6-month postacquisition cybersecurity integration roadmap.

_Overview

The Importance of Business Objectives and Org Culture for Your Cyber Strategy

As you review the guidelines and timeline below, it’s important to remember that aligning the integration plan with both the business objectives and organizational culture is critical for a smooth transition post-acquisition.

Every company has its own set of values, workflows, and communication styles that should be taken into account. Failing to consider these factors during integration can lead to inefficiency, resistance to change, and cybersecurity gaps. An integration plan that aligns with business goals ensures that cybersecurity measures are not seen as obstacles, but as enablers of growth and productivity.

By embedding security practices within the culture, employees are more likely to adopt and adhere to new policies, creating a cohesive and secure environment.

Moreover, aligning the strategy with the company's goals helps identify the most critical assets and systems that need protection, prioritizing resources and efforts where they will have the greatest impact.

A thoughtful integration plan reduces friction, enhances collaboration, and fosters trust between teams, allowing the business to seamlessly integrate operations without sacrificing security.
Ultimately, a well-aligned post-acquisition cybersecurity plan supports both the technical and cultural needs of the organization, ensuring that cybersecurity is not just a policy, but a core component of the company’s ongoing success.

ECHELON
RISK +
CYBER

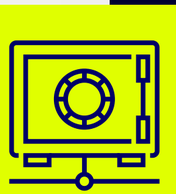
_POST-ACQUISITION CYBERSECURITY INTEGRATION PLAN

POST-ACQUISITION CYBERSECURITY INTEGRATION PLAN

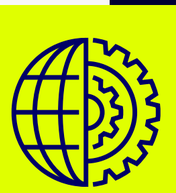
Infrastructure and Assets: Assess and Integrate IT and Security Infrastructure
A successful post-acquisition integration requires evaluating and consolidating the IT infrastructure and security tools, while also addressing any legacy systems to ensure alignment with the parent company's environment

Governance: Align Policies, Procedures, and Governance Structures
A robust governance framework is critical to ensuring consistent security practices, compliance, and efficient operations during post-acquisition integration.

Risk Management: Ensure Risk Assessment and Mitigation Processes
A comprehensive risk management approach is essential for identifying, assessing, and mitigating potential risks across the organization, particularly during the integration phase.



Data Management: Safeguard and Integrate Data Practices
Effective data management is critical to maintaining security and compliance during the postacquisition integration process. This involves understanding, organizing, and safeguarding sensitive data, as well as ensuring proper handling of data throughout its lifecycle.



Cyber Threat Landscape
Identify and prepare for threats relevant to the acquired organization. This includes evaluating both industry-specific and global threats to ensure that the company is equipped to handle targeted attacks, vulnerabilities, and emerging threats that could disrupt operations.

Infrastructure and Assets:
Assess and Integrate IT and Security Infrastructure

Tool Usage

Assess Tool Capabilities: Evaluate the tools used by the acquired company to determine their effectiveness and complexity

Identify Redundancies and Gaps: Identify redundant or suboptimal tools that don't meet security standards and decide whether to maintain the current tech stack or migrate to the parent company's infrastructure

Legacy Systems

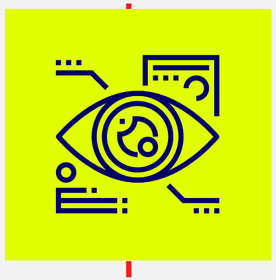
Document and Plan for Legacy Systems: Catalog the purpose and function of legacy systems and create plans for their migration or retirement based on business needs and security considerations

Asset Inventory

Comprehensive Asset List: Create a full inventory of assets, including servers, endpoints, and hardware, ensuring all are accounted for in the integration process

Assess Vulnerabilities and Ensure Patching: Evaluate hardware vulnerabilities and verify that patching is up to date to reduce security risks

Integrate with Parent Environment: Ensure proper integration of assets with the parent company’s infrastructure and security tools, ensuring seamless operational and security alignment



Governance: Align Policies, Procedures, and Governance Structures

Policies and Procedures

Review Existing Policies: Examine existing security policies such as IAM, IRP, BCDR, and TPRM to ensure alignment with the acquiring company's standards

Identify Ownership and Gaps: Assess the ownership of each policy, ensuring accountability, and identify any gaps, updates or additional policies that are required

Organizational Structure

Document Roles and Redundancies: Clearly document the roles and responsibilities of IT and security teams across both organizations, identifying any redundancies or areas of overlap

Evaluate Performance and Optimize: Review team performance metrics to ensure effectiveness and develop an optimization plan to improve efficiency, collaboration, and resource allocation

Cyber Insurance

Review Existing Policies: Examine existing security policies such as IAM, IRP, BCDR, and TPRM to ensure alignment with the acquiring company's standards

Align with Parent Company Requirement: Ensure the acquired company's coverage aligns with the parent company's cyber insurance requirements, addressing any gaps.

Legal/ Regulatory Compliance

Identify Relevant Laws and Regulations: Identify applicable laws and regulations affecting the acquired company's operations, including industry-specific requirements.

Assess Impact on Parent Company Compliance: Evaluate how these regulations impact the parent company's existing legal and regulatory obligations and ensure compliance across both entities.

Risk Management: Ensure Risk Assessment and Mitigation Processes

Penetration Testing

Review Past Testing: Assess prior penetration test results and verify that all findings have been addressed, and vulnerabilities were remediated.

Continuous Penetration Testing: Establish a regular schedule for penetration testing to continuously identify new vulnerabilities and ensure systems remain secure.

Existing Risk Assessments

Review Prior Risk Assessments: Analyze previous risk assessments from both the acquiring and acquired organizations, noting any outstanding risks or unresolved issues.

Classify Risks: Categorize risks as mitigated, in progress, or outstanding to prioritize further action and ensure consistent follow-through.

Vulnerability Management

Evaluate Processes: Review current vulnerability scanning, documentation, and remediation workflows to ensure they are thorough and up to date.

Standardize Prioritization: Implement standardized criticality scoring for vulnerabilities and develop a clear process for patch prioritization based on business impact.

Risk Management:
Ensure Risk Assessment and Mitigation Processes

Vendor Risk Management

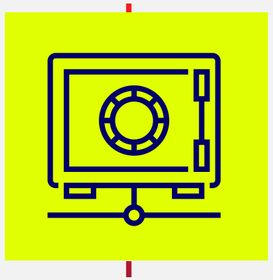
Assess Vendor Overlap: Evaluate existing vendor relationships and streamline contracts to avoid redundancy.

Align Vendor Risk Ratings: Align vendors to the acquiring company's established risk rating criteria, ensuring consistency.

Refine Processes: Implement or improve vendor risk questionnaires and renewal processes to maintain a secure supply chain.

Risk Register

Evaluate and Standardize: Review the risk register to ensure consistent and comprehensive documentation of all identified risks and mitigation efforts, providing clear visibility across the organization.



Data Management: Safeguard and Integrate Data Practices

Data Mapping and Classification

Map and Label All Data Types: Identify and categorize all data within the organization, distinguishing between sensitive data types such as PCI-DSS, PII, and PHI.

Identify Regulatory Implications: Understand the regulatory requirements tied to each data type.

Data Retention

Define Retention Periods: Establish clear guidelines for data retention based on legal, regulatory, and business requirements, and define how long each data type needs to be kept before it can be disposed of or archived, ensuring compliance with data protection laws.

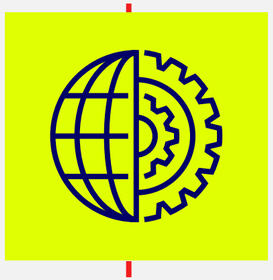
Implement Data Disposal Procedures: Develop and enforce protocols for securely disposing of data once the retention period expires.

Storage and Backup

Review Backup Schedules and Recovery Processes: Regularly review and update backup schedules to ensure critical data is backed up frequently enough to minimize data loss and implement an effective recovery process to restore data quickly in case of an incident.

Assess Backup Locations, Redundancy, and Immutability: Evaluate the locations of backup storage (e.g., on-prem or in the cloud) to ensure redundancy, and ensure backups are immutable,
preventing unauthorized modifications or ransomware attacks.

Test Backup Restoration: Regularly test the restoration process from backups to ensure that data can be quickly and accurately restored in the event of a data breach, disaster, or system failure, helping maintain operational continuity.



Cyber Threat Landscape

Threat Identification

Evaluate Industry-Specific Threats: Identify common threats relevant to the acquired company's industry (e.g., fraud, ransomware) by analyzing past incidents and attack vectors like phishing, malware, and insider threats.

Analyze Regional and Global Threats: Assess regional risks, including those from political climates and local adversaries, while also preparing for global threats like state-sponsored attacks and supply chain risks.

Identify Emerging Threats: Stay proactive by monitoring new threats such as evolving malware, phishing tactics, and the rise of AI-driven attacks.

Internal Threats and Insider Risks: Address insider threats by reviewing employee access, system permissions, and promoting proper security training.

Preparing for Threats

Establish Mitigation Measures: Develop strategies to mitigate identified threats, including stronger endpoint protection, advanced detection tools, and enhanced encryption.

Build a Resilient Incident Response Plan: Integrate the acquired company's systems into a unified incident response plan, ensuring rapid coordination during an attack, with regular exercises to test readiness.

Continuous Monitoring and Intelligence Sharing: Implement real-time monitoring through SIEM tools and share threat intelligence with trusted partners to stay ahead of emerging risks.

ECHELON
RISK +
CYBER

_POST-ACQUISITION CYBERSECURITY TIMELINE

6-MONTH PLAN

_Integration Timeline

Assessment Phase

Gain a comprehensive understanding of the acquired company's cybersecurity posture.

Month 1-2

Kickoff and Planning:

- Assemble the integration team with key stakeholders (IT, security, compliance)
- Define roles, responsibilities, and establish communication channels
- Outline short-term and long-term cybersecurity goals

Cybersecurity Assessment:

- Conduct an in-depth review of the acquired company's security posture, including:

1. Network architecture analysis
2. IT and OT asset inventory
3. Vulnerability scans and penetration testing

- Review security policies, compliance frameworks, and regulatory requirements (e.g., GDPR, ISO 27001)

Risk Prioritization:

- Identify critical cybersecurity risks (e.g., unpatched systems, weak access controls)
- Classify risks by severity and business impact
- Develop a prioritized action plan based on risk levels

Data and IAM Audit:

- Map sensitive data flows and identify critical assets
- Audit user accounts, roles, and permissions
- Assess third-party access and vendor relationships to mitigate external risks

Integration Phase

Begin unifying and strengthening cybersecurity processes across both organizations

Month 3-4

Policy and Process Alignment:

- Update or create new cybersecurity policies that align both organizations
- Implement compliance frameworks such as ISO 27001, NIST CSF, GDPR

Security Tool Integration:

- Consolidate security tools (e.g., SIEM, endpoint protection, IAM systems)
- Centralize monitoring and logging for improved threat visibility

Access Control Implementation:

- Enforce uniform identity and access management (IAM) policies across both companies
- Deploy multi-factor authentication (MFA) for access to critical systems
- Address identified risks from the IAM audit (e.g., weak passwords, excessive access rights)

Incident Response Integration:

- Merge incident response plans and establish clear escalation paths
- Conduct joint tabletop exercises to test response effectiveness across both teams

Mitigate Critical Risks:

- Address high-priority vulnerabilities (e.g., patching systems, retiring legacy tools)
- Implement quick fixes (e.g., firewall rule updates, strengthening endpoint protections)

_Integration Timeline

Optimization Phase

Refine processes and establish a long-term cybersecurity foundation.

Month 5-6

Unified Threat Monitoring:

- Deploy or optimize a centralized Security Operations Center (SOC)
- Begin proactive threat hunting across all integrated systems

Ongoing Risk Management:

- Develop a continuous vulnerability management program to regularly assess security gaps
- Schedule periodic risk assessments and penetration testing to stay ahead of potential threats

Employee Training and Awareness:

- Roll out cybersecurity awareness training for the acquired company's employees
- Run phishing simulation campaigns to reinforce secure behavior and reduce human error

Data Security Enhancements:

- Finalize encryption policies for data in transit and at rest
- Implement data loss prevention (DLP) tools to monitor sensitive data movement across systems

Cyber Insurance and Legal Compliance:

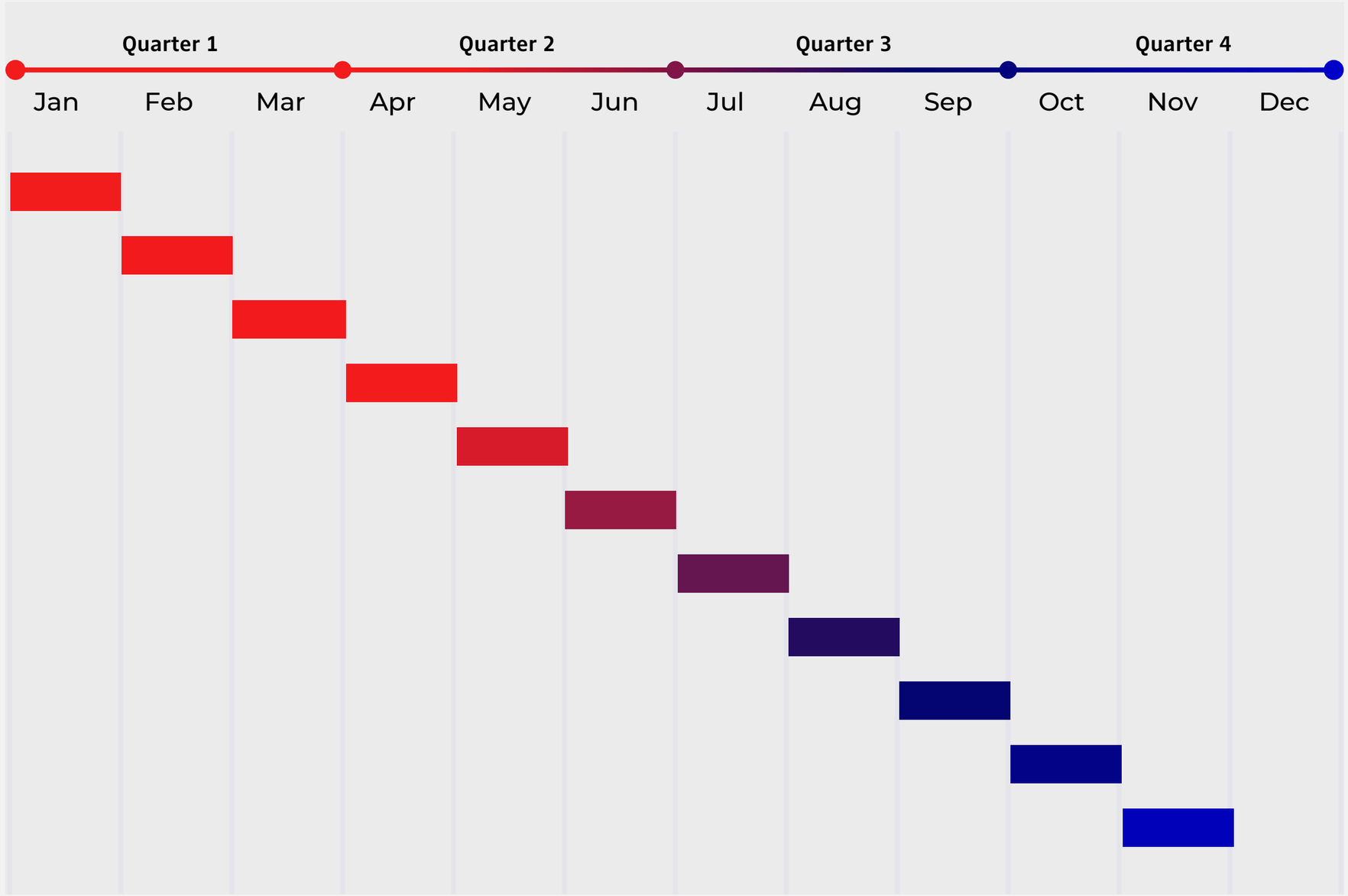
- Review and adjust cyber insurance policies to cover the integrated entity's risks
- Ensure compliance with relevant industry regulations and contractual obligations

Performance Metrics and Handover:

- Define KPIs to track cybersecurity improvements (e.g., incident response times, vulnerability remediation rates, incident frequency)
- Transition to a steady-state operational model, ensuring clear ownership of ongoing cybersecurity activities

_POST-ACQUISITION CYBERSECURITY

6-MONTH TIMELINE



_Post-Integration Outcomes

Unified cybersecurity policies and procedures

Centralized monitoring and incident response capabilities

Mitigated high-priority risks and vulnerabilities

Trained and aligned workforce

Framework for continuous cybersecurity improvement

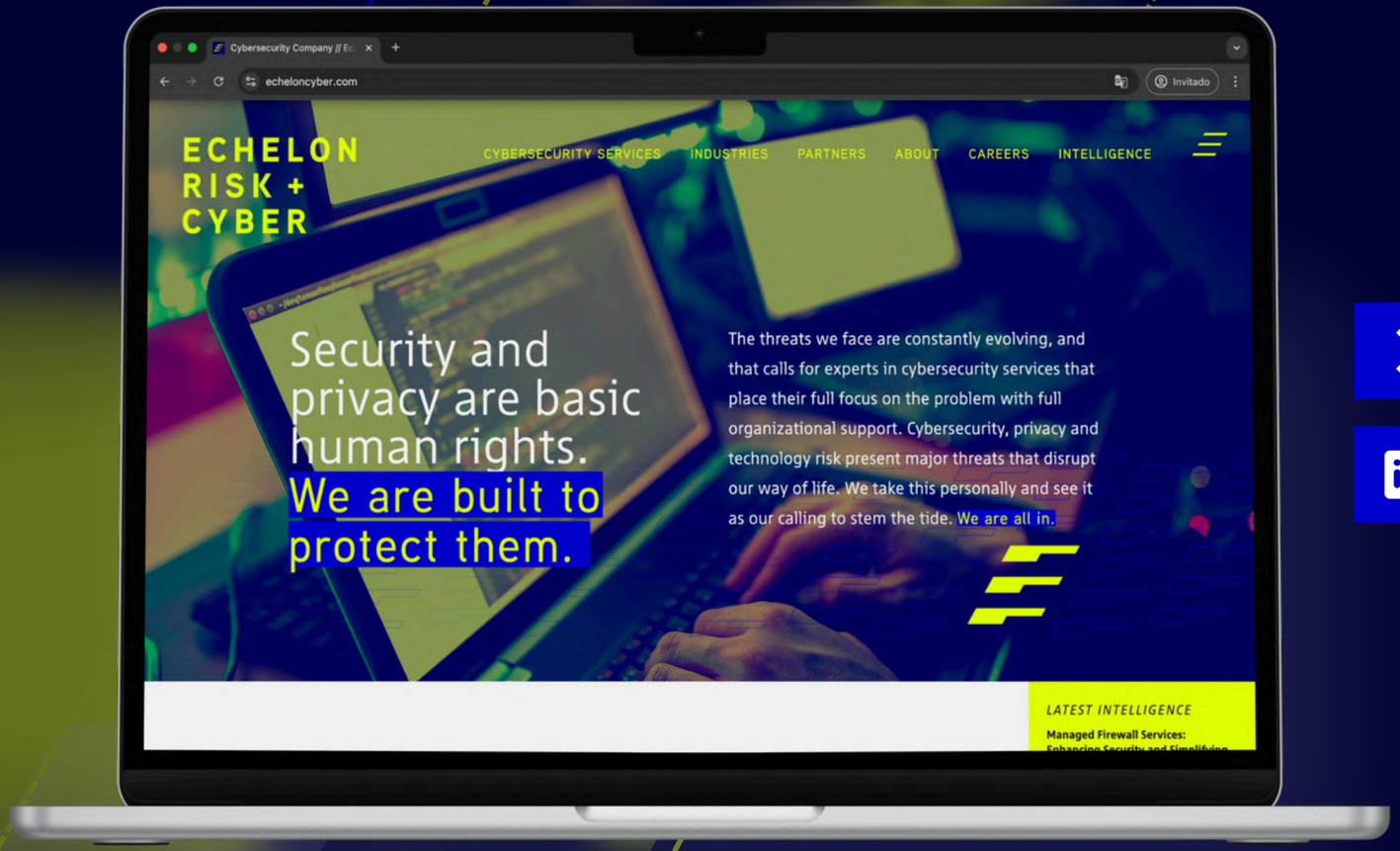
_Conclusion

Getting the cybersecurity integration right after an acquisition is key.

Getting the cybersecurity integration right after an acquisition is key to keeping both companies secure and making sure everything runs smoothly. By assessing potential threats, streamlining IT systems, aligning policies, and staying on top of risks, you can protect valuable data and strengthen security across the board. Making sure the integration plan matches your business goals and company culture also helps employees get on board and work together efficiently.

With cyber threats constantly changing, a proactive and thorough approach is crucial for navigating the post-acquisition phase. In the end, a solid cybersecurity strategy doesn't just protect your assets—it builds trust and helps the new organization thrive for the long-term.

ECHELON
RISK +
CYBER



_Learn more

echeloncyber.com/intelligence

linkedin.com/company/echelon-risk-cyber