SAPPHIRE™

Merger & Acquisitions Cyber Security Due Diligence

During a merger and acquisition (M&A), cyber security due diligence is a critical aspect to identify any weaknesses in the target company's cybersecurity and supply chain that could pose a risk to the acquiring company and ensure that the target company's cybersecurity standards align with the acquirer's requirements and expectations.

Key areas to be considered include:

Risk Identification and Management

Identifying potential cybersecurity risks and vulnerabilities in the target company helps understand and prioritise the implementation of appropriate controls to mitigate the risks to prevent future security breaches and data losses.

Compliance and Legal Obligations

Companies are often subject to various cybersecurity regulations and laws. Due diligence ensures that the target company is compliant with these regulations, avoiding legal and financial penalties.

Financial Impact Assessment

Cybersecurity issues can have significant financial implications. Due diligence helps in assessing potential costs related to fixing cybersecurity weaknesses. Potential fines for non-compliance and the impact of past breaches.

Evaluating the target company's preparedness for cybersecurity incidents

Mergers and Acquisitions often involve the transfer of sensitive data and intellectual property. Due diligence ensures that this information is adequately protected and that the target company has not suffered any breaches that could compromise its assets.

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Supply Chain Review

Reviewing relationships with third-party vendors and assessing their access to the company's systems and data and the Third-Party's own cybersecurity measures.

Cybersecurity Culture review

Assessing the level of cybersecurity awareness and training among the target company's employees identifies the maturity and measures the risk factor of human error and insider threat.

Incident Response Plan Analysis

Evaluating the target company's preparedness for cybersecurity incidents, including response plans, recovery strategies and communication protocols.

Reputation and Brand Protection

As cybersecurity breaches can harm both the target and acquiring company's reputation. Due diligence helps in the understanding and mitigating of risks to protect the brand value and customer trust.

Integration Risks

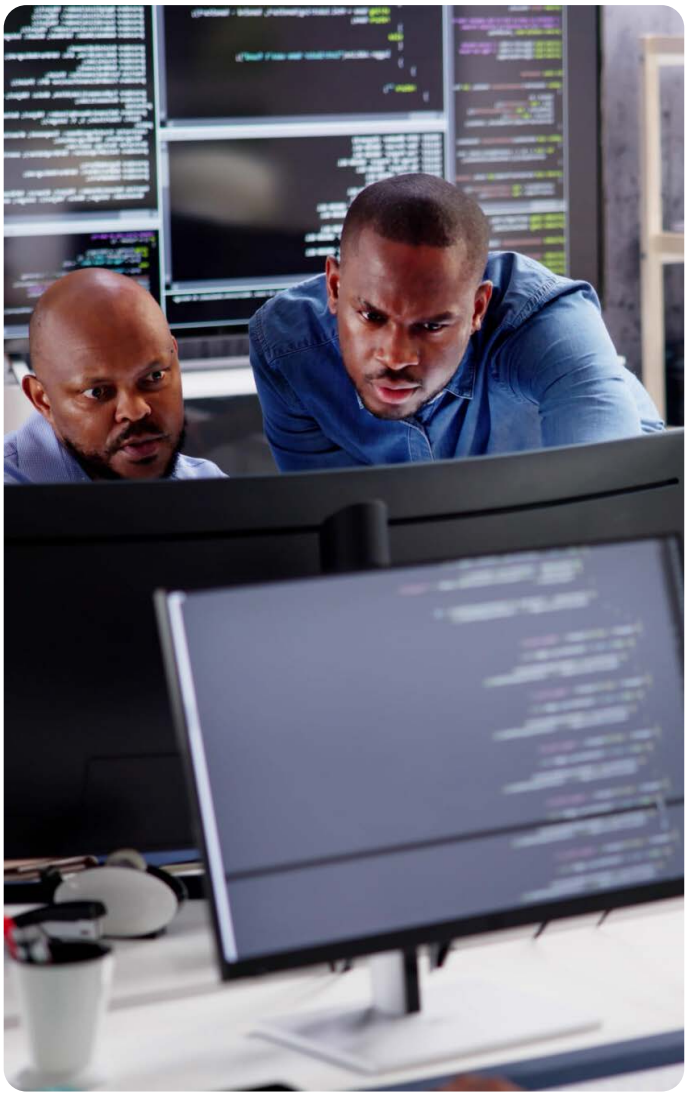
During a Merger and Acquisition, integrating different IT systems and networks can create new vulnerabilities. Cybersecurity due diligence assesses these risks and aids in planning a secure integration process.

Strategic Decision Making

Understanding the cybersecurity posture of the target company can influence the valuation and decision-making process in a Merger and Acquisition transaction.

Insurance and Liability Considerations

Evaluating the cybersecurity posture of the target company helps evaluate the adequacy of cyber insurance coverage and understand any liabilities related to cybersecurity issues.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

The criticality of addressing cybersecurity within the due diligence process of Mergers and Acquisitions has increased significantly in recent years due to the rise in digital transformation and cyber attacks because of the pandemic.

Sapphire can assist companies during Mergers and Acquisitions with the following services:

Service /Offering	Introductory
Risk Identification and Management	Independent Risk Assessment and Threat Intelligence review, with a priority list of Risks and remediation plan recommendations. IT/OT infrastructure security posture assessments Tailored Breach Attack simulations (based on threat intelligence assessment). Detailed security audits of critical systems and processes.
Compliance and Legal Compliance Review	Gap Analysis against appropriate cybersecurity standards and regulation requirements
Security Incident Readiness Reviews	Business Continuity Plan review and recommendation Business Continuity Exercises to test the validity of plans against high-risk security incident scenarios. Incident Response Readiness review.
Third-Party Risk Management	Review of key suppliers supporting the target company's critical systems. Third-Party Risk Management review through Sapphire's TPRM Managed Service to verify third-party suppliers/vendors' security maturity. This can include Compliance checks, threat intelligence reviews and on-premises audits depending on the criticality of the third-party supplier service to the target company.
Reputation and Brand Protection reviews	Open-Source Threat Assessment for previous security breaches, IP loss and Key Stakeholder posture.
Integration Risk Assessment	Cybersecurity review of the impact on the Acquiring company's security posture based on the integration with the Target company's security posture.
Strategic Decision Making and Governance	Sapphire can provide a Fractional CISO as a Service to both the Acquiring and Target companies to ensure smooth integration during the Merger and Acquisition. Project Management of the above service.

Where cybersecurity due diligence is conducted early enough in a Merger and Acquisition it can lead to reduced costs post-acquisition, mitigate damage to reputation, increase customer trust, minimise integration challenges and overevaluation of the target company, ultimately reducing business risks.

Sapphire's Service Offering

Service /Offering	Introductory	Foundations	Intermediate	Advanced
Risk Identification & Management	✓	✓	✓	✓
Compliance & Legal Review	✓	✓	✓	✓
Reputation & Brand Protection Reviews	✓	✓	✓	✓
Security Awareness & Training	✓	✓	✓	✓
Standards Review	✓	✓	✓	✓
Security Improvement Planning	✓	✓	✓	✓
Integration Risk Assessment		✓	✓	✓
Security Incident Management Review		✓	✓	✓
Third-Party Risk Management		✓	✓	✓
Governance Review		✓	✓	✓
IT/OT Asset Discovery		✓	✓	✓
Technical Review		✓	✓	✓
Network Review		✓	✓	✓
Penetration Testing		✓	✓	✓
Threat Intelligence		✓	✓	✓
Vulnerability Management Review		✓	✓	✓
Business Continuity Planning			✓	✓
Business Impact Assessment			✓	✓
Privacy Impact Assessment			✓	✓
Patch Management			✓	✓
CISO Services				✓
MXDR & Endpoint Management				✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001