





## M&A DUE DILIGENCE

Evaluation of the cybersecurity risk of the business being acquired is an important component of proper due diligence. While a few years ago “78% of global respondents believe cybersecurity is not analyzed in great depth or specifically quantified as part of the M&A due diligence process, “\*\* acquirers have come to appreciate the critical importance of evaluating target’s cyber risk. The security posture of target can materially affect target value, elevate the operational and compliance risks to the combined entities on a post-deal basis and require significant remediation expenditures.

Acquisition due diligence demands speed and thoroughness. IO Security excels at both due to the advanced automation it applies in its assessment work and its use of best-of-breed software from incumbent and start-up US and Israeli companies.

There are many different types of cyber risk that an acquirer may be buying as part of an acquisition. These may include the risk of:

- Theft of intellectual property and trade secrets.
- Loss or disclosure of confidential and sensitive business information and strategies.
- Loss or disclosure of personal data relating to customers, employees and others, and damages to reputation and consumer confidence.
- Failure of systems critical to the operation of the business.
- Litigation and regulatory compliance risk.
- Remediation cost.
- Loss of shareholder value.\*\*

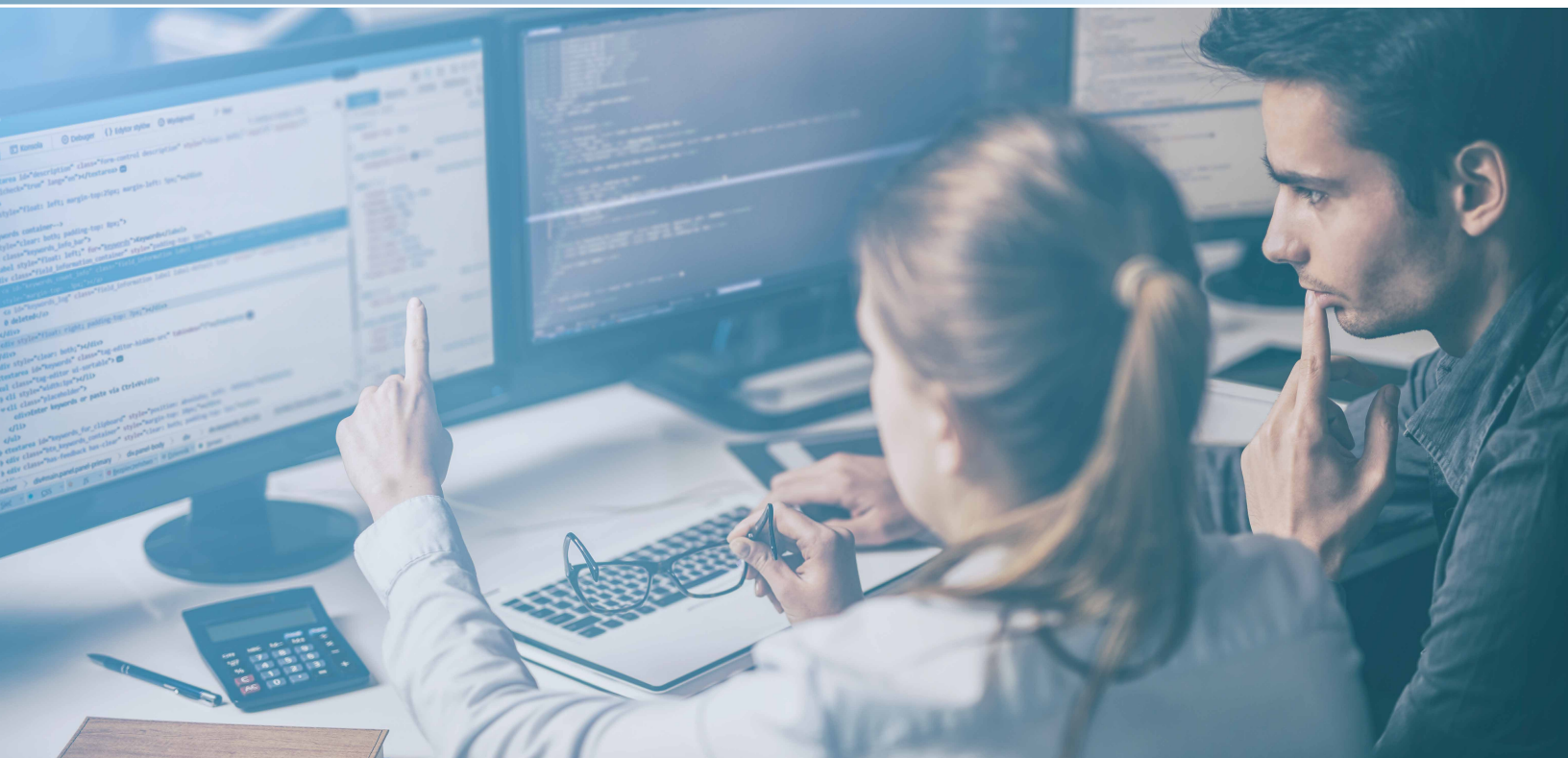
The assessment should evaluate the enterprise's security posture, including satellite offices, and foreign-owned entities. Specifically, the company should examine:

- Firewall protection.
- Endpoints, remote access.
- Log servers.
- Network security.
- Email systems.
- Website protection.

The M&A due diligence procedures should include:

- Vulnerability assessment.
- Audit and document requests, questionnaires and interviews.
- Asset inventory audit.
- Network mapping.
- Assessment of third parties such as vendors and contractors who are granted access to the network.

IO Security's expert analysts provide comprehensive assessment of target's security risks and recommend solutions which will strengthen the organization's security posture.



\*Freshfields

\*\*M&A Cybersecurity Due Diligence, Thomas J. Smedinghoff