Stepping-up Cybersecurity Risk Management in the M&A Process

Problem – Efficient Due Diligence of IT Infrastructure and Digital Assets

- M&A is a key instrument to achieve strategic goals - margin increase (synergies), time to market, market share consolidation or innovation. In 2018, Dealogic reported 7,791 US transactions involving M&A advisors, with a $1.7T. investment volume[1].
- M&A is not exempted of risks. In average over 2/3 of M&A transactions failed to deliver the expected shareholders' value[2].
- With the digitalization of business and the introduction of regulation (i.e. GDRP), Digital Assets could represent a significant portion of the asset / liability allocation of a company – this includes Software, Customer Data, Intellectual Property and Brand.
- Research reveals that "increasing awareness of cyber risk has not resulted in meaningful changes of the M&A process" [3]. Deal makers should step up their due diligence and business integration procedures for IT infrastructure and cyber-risk to the level of legal and financial routines.
- Cyber-risk might have a material impact on the price and closing of a transaction. In the Verizon's Yahoo take-over in 2017, the post-signing discovery of a massive cyber- incident on Yahoo clients' data led to a price reduction of USD 350m[4].
- Successful cyber-security due diligence requires a cost-efficient routine at each phase of the process – from assessing potential targets, to mapping risks and remedies in a thorough cyber-risk due diligence, or formulating a "down to earth" integration plan.

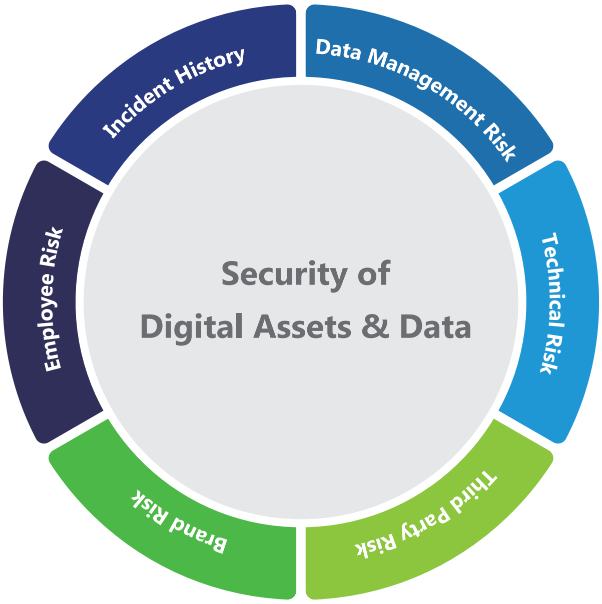
Solution

The Scope of a Cyber-Risk Due Diligence

The message to deal-makers is to evaluate cyber-risk the same way they would any other risk that could affect the value of a target.

The objective is two folds: (i) to prevent taking over liabilities or, if any, to quantify them, (ii) to identify gaps and devise a plan for post-merger integration.

The journey starts with the **Asset Mapping** of the organization to create a holistic understanding of all the digital assets exposed, to classify them in geographies, in access to valuable assets. It includes domain, subdomain, roots, IPs, Shadow IT, Applications, Vendors, etc.



[1] Dealogic - M&A Highlights Full Year 2018

[2] Numerous sources including Harvard Business Review, KPMG, A.T. Kearney

[3] Freshfields Buckhaus Deringer LLP, Cyber Security in M&A, July 2014

[4] Techcrunch, February 21 2017

We recommend to building a thorough cybersecurity assessment routine covering 6 risk-factors:

Data-Management Risk – it requires to build an understanding of what data the company holds, where it sources the data and how it is used in the value chain. Inquiries should focus on how the company protects and exploits data.

IT Infrastructure Risk – if valuable data is used, it is to assess how it is encrypted, what firewalls and tools are deployed to keep data safe.

Third Party Risk – any business security is as strong as its Vendors. A company needs to manage actively its network of third party and fourth party suppliers to verify that they are robust enough to protect the value of data and its brand. Companies contracts would need to be audited to certify suppliers' responsibility in protecting company's data assets.

Brand Risk – it requires to verify that a company's brand and reputation is not compromised in malicious or other improper activities. It would require a thorough review of mirror sites, spam activities, social networks and dark web chat rooms, among others.

Employee Risk – human activity is the biggest risk to data and IP security. It is critical to verify what processes a business has in place to protect its digital assets. The leackage of credentials, verification of IPs in third party applications (i.e. Github, Dropbox, etc.) will help to understand threats and the maturity of processes in place.

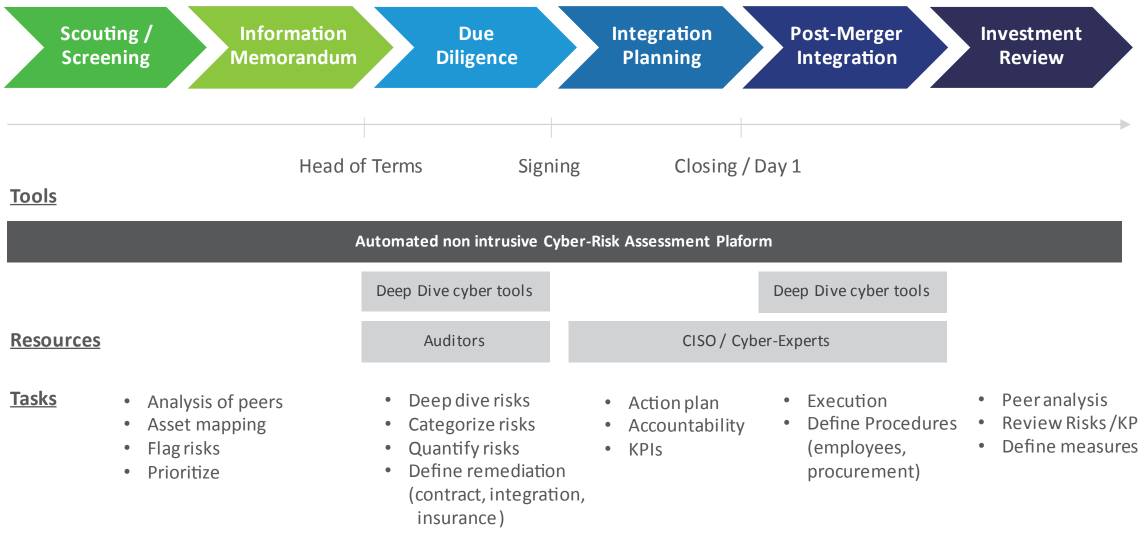
History of Incidents – whether the company suffered a data breach or cyber incident, and if so, why it happened and how it was resolved, are critical information to collect and assess.

The Organization of a Cost-Efficient Cyber-Risk Management in M&A

Cyber-Risk management is complex. It encompasses a myriad of activities and information. The difficulty increases when these activities are applied to a third-party organization. The job needs to be performed while managing carefully the cursor of confidentiality and the use of non-intrusive procedures.

The use of a Third-Party Cyber-Risk Assessment Platform will be instrumental at each step of the M&A process. We recommend a staged approach with the combination of automated tools, external resources and dedicated tools to drill down areas of risks.

Management of cybersecurity in the M&A Process



Scouting / Screening

Information Memorandum

Due Diligence

Integration Planning

Post-Merger Integration

Investment Review

Head of Terms

Signing

Closing / Day 1

Tools

Automated non intrusive Cyber-Risk Assessment Plaform

Deep Dive cyber tools

Deep Dive cyber tools

Resources

Auditors

CISO / Cyber-Experts

Tasks

- Analysis of peers
- Asset mapping
- Flag risks
- Prioritize

- Deep dive risks
- Categorize risks
- Quantify risks
- Define remediation (contract, integration, insurance)

- Action plan
- Accountability
- KPIs

- Execution
- Define Procedures (employees, procurement)

- Peer analysis
- Review Risks /KPIs
- Define measures

About C2SEC iRisk Cyber-Risk Assessment Platform

iRisk enables continuous monitoring, assessment and bench-marking of cyber risks for target companies' IT assets, its vendors, and its employee's behavior. Specifically, the platform provides a fast turnaround, Peer group and bench-mark analysis and high confidentiality, meeting the expectation of our clients' M&A teams.

Find out more about C2SEC iRisk on **https://www.c2sec.com** and contact us for a free trial at **info@c2sec.com**