Toolkit D

Cybersecurity Considerations During M&A Phases

Companies involved in transactions are often prime targets for hackers and cybercriminals, because the value of confidential deal-related information is high, and the short timelines, high-pressure environment, and significant workloads associated with transactions can cause key players to act carelessly and potentially make mistakes. Cybersecurity vulnerabilities exploited during a transaction can pose risks to the deal's value and return on investment:

Short-term risks

- Paralysed operations as a result of ransomware or malware.
- Transaction period might be used by threat actors to gain entry and conduct reconnaissance, an event which often is not detected until well after the deal closes.
- Theft of inside information, including valuations, bids, etc.
- Warranty claims, a change of deal terms, or a reduction in the deal's value.
- Forensic investigations related to a data breach.

Long-term risks

- Exposure to risk from regulatory and other lawsuits.
- Regulatory investigation and penalties.
- Loss of customers, and associated impacts on sales and profit.
- Reputational damage.
- Loss of market share to competitors without a known data breach.

Directors should ask management to conduct a cyber-risk assessment for each phase of the transaction's lifecycle to confirm that systems and processes are secure, and to quantify the risks that may impact the company after the deal closes, including revenues, profits, market value, market share, and brand reputation.

Strategy and Target Identification Phase

The risk of attack starts even before an official offer or merger announcement is made. Law firms, financial advisors, consultants and other associated firms are attractive to hackers because they hold trade secrets and other sensitive information about corporate clients, including details about early-stage deal exploration that could be stolen to inform insider trading or to gain a competitive advantage in deal negotiations. A company therefore needs to have an understanding of the controls and security in place at all of the third parties assisting it during the M&A process and a thorough understanding of how sensitive data is to be shared between parties.

Attackers look for hints that a company is considering a merger, acquisition, or divestiture. They may be tipped off by industry gossip, a slowdown in a company's release cycle, staff reductions, or data leakage through social media channels. There are four primary ways that information is at risk:

- A hacker enters the network through gaps in its defences, starting with a company's Internet-facing computers.
- A hacker launches a social engineering attack against a company employee.

- Company insiders (employees, contractors, vendors) release sensitive data and information, either intentionally or as a result of negligence. The risk of insider threats heightens significantly in an M&A.
- Information is exposed through vulnerabilities in third-party vendors or service providers.

During this phase, management should gain an understanding of cyber risks associated with the target company and model the impact of those risks to compliance posture, financial forecasts, and potential valuations. Management can perform the following analysis even before direct engagement with the target company begins:

- Conducting "dark web"[88] (difficult-to-access websites favoured by hackers) searches about the target, their systems, data, and intellectual property. This helps identify whether the company is already on hackers' radar, if systems or credentials are already compromised, and if there is sensitive data for sale or being solicited. Management will need to consider the lawfulness of such searches with reference to the information being accessed.
- Profiling the target company from the cybersecurity point of view, while implementing relevant technology.
- Researching malware infections in the target company and gaps in their defences visible from the outside. This information is publicly available and can be used to compare one company to another, allowing management to save time and energy by not pursuing companies whose risk profile is unacceptably high.
- Modelling the financial impact of identified cyber risks. These risks may not only impact a company's return on invested capital, but also result in loss of competitive advantages, costly remediation, fines, and possibly years of litigation, depending on what was stolen. An initial estimate of the impact may be material enough to encourage strategy teams to alter a deal trajectory. The estimate can be refined as the transaction process continues and as risks are mitigated.

Due Diligence and Deal Execution Phases

During these phases, the company should perform confirmatory cybersecurity due diligence. Significant problems would call for negotiation of a reduction in purchase price to cover costs of necessary remediation. Depending on the risks identified, the Board may want to defer approving the transaction until remediation is complete or decide to back out of a transaction if the risks that are identified warrant such action. Identification of cybersecurity risks during the diligence phase can be accomplished by performing cybersecurity diligence that is tailored to discover these risks:

- Identify insufficient investments in cybersecurity infrastructure, as well as deficiencies in staff resources, policies, etc.
- Identify lax cultural attitudes toward cyber risk.
- Determine cybersecurity-related terms and conditions (or, the lack thereof) in customer and supplier contracts that have a potential financial impact or result in litigation for noncompliance.

[88] The Dark Web is a general term describing hidden Internet sites that users cannot access without using special software such as TOR ("The Onion Router"). While the content of these sites may be accessed, the publishers of these sites are concealed. Users access the Dark Web with the expectation of being able to share information and/or files with little risk of detection.

- Discover noncompliance with data protection laws or other applicable cyber-related regulations and requirements.
- Identify recent data breaches or other cybersecurity incidents, and response thereto.

Effective due diligence on cybersecurity issues demonstrates to investors, regulators, and other stakeholders that management is actively seeking to protect the value and strategic drivers of the transaction, and that they are aiming to lower the risk of a cyber-attack before integration. These risks and upsides can then be factored into the initial price paid and into performance improvement investments that will raise the transaction value, enabling a robust transaction proposal to be presented to shareholders for approval.

Integration Phase

Post-deal integration poses a range of challenges related to people, processes, systems, and culture. Cyber risks add another dimension of complexity and risk to this phase of the transaction. Hackers take advantage of the inconsistencies that exist between the platforms and technology operations of the company and the newly-merged or acquired entity at this phase.

Integration teams need to have the expertise to explore and delve into the smallest of details to identify and mitigate cyber risks such as the following:

- Security gaps identified during preceding phases.
- Prioritization of remediation activities based on potential impact of identified gaps.
- Prioritization of integration activities.
- Employee training on newly integrated systems.

Post-Transaction Value Creation Phase

After a transaction is completed, continued monitoring of cyber risks by management will create numerous opportunities for portfolio improvement and growth.

Management should continue to evaluate the cyber maturity of the merged or acquired entity by benchmarking it against industry standards and competition, just as they do with the core business. Low maturity could impact growth projections and brand reputation due to cyber incidents and possible fines. A breach or compliance issue could cause regulators to investigate, leading to a financial loss or stalling of post-transaction exit plans. Cyber issues can also lead to legal action by customers and suppliers causing value loss and lower returns.

A View from the Sell Side

Many of the same risks impacting the acquiring company that are described herein will of course equally apply to the seller side. In the post transaction valuation creation phase, the seller is particularly exposed to breach disclosures that may impact the deal price / timing and even the ongoing operations of the selling entity if the transaction falls through. Accordingly, a thorough understanding of existing risk vectors prior to deal execution will better inform the nature of warranties made by the selling corporation and reduce exposure.

Information flow to directors of selling companies may be more limited in its nature and frequency as time passes after deal announcement and directors should establish the thresholds and nature for any breach communications in the post announcement period.