CHUBB®

The Frontiers of Technology Risk

Managing Risks Associated with Technology M&As

CHUBB®

Managing Risks Associated with Technology M&As

Contributors

Chris Daniel
Technology Practice Manager
UK & Ireland, Chubb

Kay Hargreaves
Risk Engineer, Chubb

Opportunities abound in the technology sector right now, but how can businesses ensure their risk management plans grow with them?

The first half of 2021 saw record-breaking global mergers and acquisitions (M&A) activity, according to professional services company EY. Technology was one of the sectors leading this boom.

"We have seen an increase in acquisition activity within the technology industry, with many customers driving inorganic growth through M&A activity," says Chris Daniel, Technology Practice Manager, UK & Ireland, Chubb.

The trend towards acquisitions is expected to continue, according to the 23rd EY Global Capital Confidence Barometer, which found that 51% of technology executives plan to pursue M&A in the next year.

M&As can be an effective way for businesses to grow, whether they are buying up the competition, adding products and services to their portfolios or expanding into new territories. But if M&As are not managed carefully, the acquiring company can be left exposed to latent problems.

Risks related to the M&A process are not always immediately obvious. "Problems with M&As can present as a breach of contract claim, as a privacy breach claim, as a software licence infringement claim," explains Kay Hargreaves, Risk Engineer, Chubb. "Many post-loss interviews that I've done with customers in the past 12 months have found that the loss could have been avoided had the M&A process - the integration and due diligence - been undertaken more comprehensively."

However, if technology companies think carefully about strategy, decision-making, risk assessment and integration planning, then they can mitigate some of these risks.

Solid strategies make solid foundations

It might sound obvious, but having a strategy and sticking to it is a cornerstone of a successful acquisition. "The strategy needs to be aligned with corporate goals. Deals that are unplanned might not always fit those established models, which can lead to problems," says Hargreaves.

If a company that was looking to acquire direct competitors in the UK suddenly spotted a business abroad and decided to buy it, that would deviate from their strategy. "They might not have the knowledge within their organisation to make that acquisition successful. Do they have legal counsel in that country? Do they know about local privacy or employment laws?"

For listed companies, the due diligence process can only begin once the intention to acquire has been publicly announced.

of technology executives plan to pursue M&A in the next year

"If CEOs micromanage and take direct control over departments, it opens the door to impulsive decisions"

"Once that public announcement has been made, it can be very difficult to walk away from that offer down the line. But if you're sticking to strategy then the intention to buy is well thought through in the first instance," says Hargreaves.

Decision-making or decision-taking?

The culture around decision-making within an organisation can also determine the quality of an acquisition. A healthy culture involves individual departments reviewing the potential deal according to their expertise and providing that insight to the CEO, rather than the latter taking too much ownership over the process.

"It is encouraging to see a CEO who delegates responsibility to well-qualified experts so that the legal department is responsible for reviewing the contracts, project management for reviewing project management, and so on. That tends to give a much better view on the acquisition and whether it's going to work or not, leaving the CEO to make an informed decision," explains Hargreaves.

Whereas if CEOs micromanage and take direct control over departments, it opens the door to impulsive decisions. "The CEO might have an aggressive stance, they might take a 'buy it now, we'll figure it out later' approach. Or the company might have a closed culture, whereby department heads can't speak their mind and it's the CEO's way or nothing. Acquisitions taken on in that sort of culture have a lower chance of success, because impartiality has been removed from the decision-making process."

Identifying risks to the acquisition

Another safeguard technology companies can put in place during the M&A process is a risk analysis that identifies threats to the acquisition. "That risk assessment can take any form, such as documents that the company uses to assess other risks. But it needs to be done and it should begin around the same time as due diligence, because that will help them to identify what those risks are," explains Hargreaves.

To ensure the risk assessment is effective, it should be reviewed continuously and measures put in place to ensure action is taken. Hargreaves says: "There need to be specific action plans in place to address the risks and specific individuals assigned to make sure they get monitored."

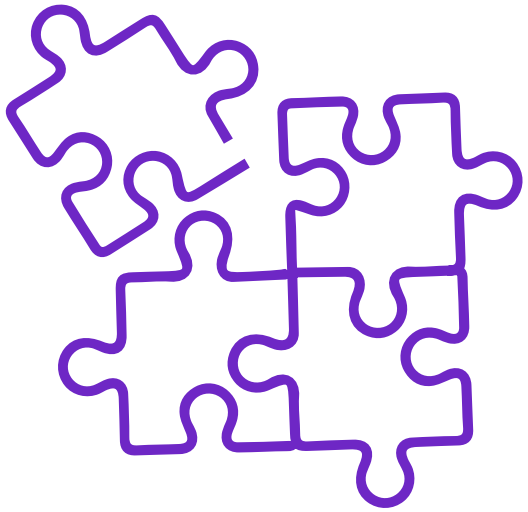
Reviewing the acquisition target's major projects and contracts should form part of the risk assessment. "The largest contracts should be reviewed by the acquiring company. You need to check what you're taking on when you buy a company," explains Hargreaves.

"It's about making sure the acquiring company understands what contracts are in place so that if there are any with unfavourable terms, they can make a note to try and get out of those or reword them at the earliest opportunity. If legal issues arise as a result of such contracts, it is the acquiring company that is ultimately responsible."

The same principle applies to project management. The acquiring company should understand the status of ongoing projects - for example, which milestones have been reached, any issues with them, any passed due dates and whether service-level agreements are being kept up to date.

M&A best practice check list

- Have you stuck to your acquisition strategy?
- Have experts from each individual department reviewed the deal according to their expertise?
- Has a risk assessment been performed, including a review of the target's major projects and contracts?
- Is an integration committee in place?
- Have baseline standards been set for the target company and are deadlines in place?
- Is a project plan in place for integration?



- Speaking to key customers to make sure they are aware of the acquisition and reassuring them is also good practice.

Integration planning

Once the acquisition is under way, setting up an integration committee helps bring the two companies together seamlessly and deal with any issues thrown up by the risk assessment.

"Having an integration committee improves accountability because specific people are assigned to manage the whole integration process. It also stops ordinary employees from being taken away from their day jobs in order to manage the acquisition, which would negatively affect the business," explains Hargreaves. "These people will hopefully be experts in integration, they'll have done it before, and being dedicated to the task means they're much more hands-on."

One of the primary tasks of an integration committee is to ensure the two companies' standards are brought into alignment. "What sometimes happens is the businesses continue to run as two separate companies," says Daniel.

"We have observed increased claims activity in acquired companies where there is often a delay in replicating risk management controls," she adds. The resulting disconnect between standards can expose the acquiring company to risks that would otherwise be mitigated within their own company procedures.

Cyber is one area where risk management controls at the company being acquired need to be rapidly brought up to the same standards as the parent company. "Acquiring companies need to look at the security and safeguards around IT systems, even at the point of due diligence, prior to integration," says Hargreaves. "They need to understand what they're buying, how the systems work, what data is on the systems, how that data is currently protected, whether it is compliant with privacy laws."

One recent example of how the process can go wrong is a digital business that suffered a brute force attack in January 2021. The company had made a series of acquisitions and was running its operations under different brands. The cyberattack came through an admin login on one of the company's platforms, resulting in attempted SMS phishing attacks on its customers and exfiltration of some data.

No group baseline security requirements had been established during the acquisition processes and technological protections were inconsistent between the companies. "Information security simply doesn't seem to have been a priority in the initial due diligence or integration of any acquired companies," says Hargreaves.

To mitigate against mismatching standards, Hargreaves recommends that acquiring companies establish baselines. "Baselines should be applied across the whole business - contract management, project management, as well as the cyber side. At an absolute minimum, the company being acquired should match your own risk management standards," she says, emphasising the importance of implementing milestones with deadlines during this process to make sure targets are actually met.

Key takeaways

- **Risks related to the M&A process** are not always immediately obvious
- **Problems can present as a breach** of contract claim, a privacy breach claim, a software licence infringement claim and so on
- **It is important to have a strong** acquisition strategy in place and resist temptation to deviate from the plan
- **CEOs should draw on the expertise** within their organisations rather than taking too much control of M&As
- **A risk assessment should be** undertaken and continually reviewed, with actions assigned to individuals to ensure that they happen
- **A dedicated integration committee** makes for a smoother M&A process

Cultural disconnect

Another common cause for concern during M&As is a failure to address differences in culture between the organisations. While one culture may not necessarily be more risky than another, a clash between them can destabilise a company.

"If the acquiring company has a less flexible attitude to, for example, casual dress codes or working from home policies, and does not manage that difference appropriately, then staff turnover could increase. Any loss of key people will mean lack of sufficiently skilled resource, which may make fulfilling contracts more difficult, potentially resulting in breach of contract claims," says Hargreaves.

With the jobs market in the technology sector increasingly competitive, this is even more of a concern at the moment. "The IT market is highly active. You can't always automatically replace critical skillsets, some of it is very specialist and if you can't find an immediate like-for-like replacement, that becomes an issue," explains Daniel.

Creating project plans helps ensure the integration phase runs smoothly. "We would encourage all of our clients to have a plan which would set clear priorities for the integration, document actions to be taken and lay out timelines for those tasks," says Hargreaves. "Similar to a risk assessment, project plans decide who is going to be accountable for completing action points. If there isn't accountability or firm deadlines then integration drags on, and four years later you're still trying to use disparate systems, processes and protocols."

As technology companies make the most of the current boom and embark on M&As, there is much to be excited about. But those organisations that chase opportunities, while also keeping an eye on the long term through good risk management, will be more likely to see their success endure.

The next report in this series will explore cyber hygiene for technology companies.

Key contacts

Chris Daniel
Technology Practice Manager UK & Ireland, Chubb
cdaniel@chubb.com

Kay Hargreaves
Risk Engineer, Chubb
khargreaves@chubb.com

Chubb. Insured.℠

SE8139-WA01/22