Grant Thornton

An instinct for growth™

# Cyber Security

## The Peculiarities of Mergers, Acquisitions and De-Mergers

**April 2019**

Organisational change is inevitable. In fact, it's essential: as the late Sir John Harvey-Jones, former chairman of ICI once put it: "If you are doing things the same way as two years ago, you are almost certainly doing them wrong".

Change is organic, or at least driven and controlled from within the organisation. Those making the changes understand the business and the people within it, and with sensible management and oversight it's possible to manage all aspects - not just in an information security sense but right across the organisation: finance, HR, IT, and so on.

This can all go out of the window when you acquire a company, or a company acquires you, or you spin off part of the organisation to become an entity in its own right. The HR people have a raft of employees to deal with, the IT teams face the fun of either integrating systems or splitting them off, and the cyber security specialists similarly have their own set of challenges … and an environment they probably know little or nothing about.

## The first mistake of mergers

It's frighteningly common to find that key departments aren't engaged at the inception of a major change - particularly an acquisition. And this makes no sense - it's perfectly conceivable, after all, that the involvement of the security team in a due-diligence exercise may well turn up unexpected surprises that affect the valuation of the acquiree company - or could even derail the exercise altogether. The IT team tend to have a similar problem, incidentally: the call often comes into them as a *fait accompli* once the deal has been done.

## The opportunity to do it better

Another temptation is for the acquiring company to take a default position when integrating systems and security regimes following an acquisition - namely to apply (one might even say inflict) its own security regime onto the acquiree. This can be a mistake in two ways: first of all, changing the security regime may affect any formal security accreditations the acquiree company already holds; and secondly, who says the acquirer is doing everything right anyway? Any major change is an opportunity to take a step back and think: should we be implementing something new and evolving both organisations into a new framework? Sometimes the answer is "no", of course - total change can equal major upheaval. But sometimes there's benefit to be had from giving the whole process that little bit more consideration.

## Pass the atlas

A common impact of a merger (and, for that matter, a common motive for doing it in the first place) is international expansion.

Some concepts have a reasonable level of similarity from country to country - IT systems, for example - but in many areas, particularly where there's a legal or regulatory focus, there are entirely new concepts to consider. HR law varies from country to country, for instance, and the information security concepts can likewise be significantly different. So, a US-based company expanding by acquisition into Europe has the delights of GDPR to contend with in the field of data protection; conversely, the European entity might find itself constrained by the notoriously draconian US data export laws.

## What about de-mergers?

As we gave GDPR a name-check in the previous section, this brings a timely opportunity to dip into the concepts of de-mergers. As we know, the General Data Protection Regulation is a European law that restricts how personal data - that is, information about living people - is stored and processed. When a company splits, however, it's absolutely crucial to understand thoroughly what personal data exists and where it's going. On a technical level it can be far from trivial to split out (say) the HR data of the employees who are being spun off, and from a data protection point of view it's common for both entities to retain some of the same personal data - in historic HR records, for example, or as part of a legacy pension scheme. As with any significant change, a proper Data Protection Impact Assessment (DPIA) is crucial.

## Sometimes you're doing both

Just to add complexity, perhaps you can try combining a merger with a spin-off. On one occasion in my pre-security career as an IT manager, an overseas organisation took over

just a part of the UK-based company I worked for: so, we had to combine the exercises of splitting off a subset of the company and then integrating it into the new owner's world. The main challenge here can be the overlap period when shifting data from A to B: the most effective way of doing this from a technical point of view is to connect the two companies' systems together temporarily, but from a security angle this of course opens both organisations to potential security attacks.

## Even closing down can be tricky

One should also consider that breaking off part of a company may be happening because you're closing it down. Of course, you don't have security issues such as transferring data securely to another company, but there are still potential risks and liabilities - data protection will be at the top of the risk list as usual, but there's also a wider responsibility to ensure that you're not breaching contractual terms that demand the erasure or destruction of commercial, non-personal data.

## The top five cyber tasks for major change

So, when it comes to dealing with the security aspects of mergers and de-mergers, what would we consider to be the top five things to consider first?

**Unsurprisingly, given the numerous mentions it's had, data protection comes in first.** It's such a huge deal since the introduction of GDPR and the rise in general awareness of the importance of protecting the rights of data subjects by using their data responsibly and lawfully. It's particularly relevant when you're splitting parts of your organisation off, either to become stand-alone entities or to be sucked up by another company.

**Next, certifications.** If you're making changes to how an organisation operates, you need to be absolutely sure that you're not inadvertently trampling over its security controls and ending up in breach of its accreditations - ISO 27001, PCI DSS, or even more basic concepts such as Cyber Essentials.

**Thirdly, don't be what I call an "arrogant acquirer".** If you're acquiring another company, consider that in some ways they might be doing things better than you in a security sense. Take the chance to make the merged organisation greater than the sum of the parts.

**Fourth, ensure that the security team are engaged as early as possible in the process** - and preferably right at the inception of the exercise. By trusting your teams - particularly the data protection and security people, along with the IT team - you'll end up with the best possible outcome.

**Finally, learn from what you do.** The first acquisition or split you go through is unlikely to be the last, and neither are you going to get everything right. Review what you do all the way through the project, and conduct thorough lessons-learned activities (as you should with every major change) at the end.

And as well as evaluating what you did wrong, look also at what went well: next time you may be able to do it even better.

**For more information please contact:**

**David Cartwright**
Senior Consultant, Information Security
**T** +44 (0) 1534 885813
**E** david.cartwright@gt-ci.com

Grant Thornton

An instinct for growth™

**grantthorntonci.com**