Mitigating Risks During M&As with Identity and Access Management

Times during mergers and acquisitions are trying ones. Among other things, they present steep security challenges. Data is being consolidated and can be compromised in the process. Employees in fear of being laid off are potential insider threats as they hoard data and try to access files they shouldn't, in order to gain footing with future employers. During mergers and acquisitions businesses must protect themselves more than when the business is simply running daily operations. Here's why and how.

Data breaches can hit at any time in a business' lifecycle. But, if they occur mid-way through an M&A process, they can be particularly damaging. For British payday loan company, Wonga, the breach of the personal data of 270,000 customers happened in the middle of a major restructuring. For media conglomerate Talk Talk, it cost them £60m, 100,000 customers, and a record £400,000 fine from the Information Commissioner, all in addition to a damaged reputation. And, for Yahoo, who were in the middle of an M&A deal with Verizon a second data breach occurred, the deal was put at risk and $350 million was lost from the final purchase price.

Mergers and acquisitions happen primarily for reasons of combining customer bases and intellectual property or data. For many businesses, such property is their lifeline. If a business is breached during the M&A process, the very reason for merging is put in jeopardy. It is also a time in which data breaches are more likely to occur.

So, due to the fact that it is critical business property that is lost, the added fact that this property is the reason for the merger or acquisition in the first place, and because M&A periods are highly susceptible to data breaches, this period in any business' lifecycle is critical from a security standpoint.

Insider threats can be particularly nasty. M&As make employees nervous. This makes them unpredictable. They might start looking for new jobs and aggregating company data to take to new employers. Privileged users are, in particular, a major threat. Such users are not just executives, but IT admins with panoramic access to a business' IT systems which they must maintain in the course of their jobs. Such users have access to highly sensitive data that they might even try to leverage to keep their jobs, or steal maliciously to get back at their employers.

And ordinary insider risks still exist during a merger. Compromised passwords that were written down on paper or in computer documents, malicious links in emails that are clicked, and sidestepped security policies are all an even bigger threat during M&As.

A business needs a dependable IAM solution during M&A to mitigate these risks.
Single Sign-on (SSO) prevents compromised passwords due to password fatigue.
Password Management ensures that password policies are enforced and that stringent measures are taken when passwords are reset. Identity Governance and Administration employs Access Recertification campaigns. These are periodic reviews of all access within an

organization. An access that is flagged as inappropriate can immediately be dealt with. Many mandates such as GDPR and SOX must be complied with as well; non-compliance can put a halt on an M&A, damage company reputation, and cost millions in compromised data and reputation loss.

IAM additionally offers modules such as context-based authentication and adaptive authentication can further mitigate insider threats. Context based authentication ensures that authentication attempts are valid only when predefined criteria of time, location, and other factors are met. Adaptive authentication tracks user behaviour and bars access when behaviour sways too much from normal. For instance, if an account is being logged into from one geographic area and then from another, impossibly distant one, in a short time frame, the system can detect this and lock the account. It can also detect suspicious behaviour as employees who suddenly start staying late at the office typically represent a possible insider threat. Such employees are often disgruntled and causing a breach might be in their minds.

IAM offers other benefits during and after mergers and acquisitions. Merging entities will likely have differing policies and processes for managing user identities. In addition, an M&A might involve a reduction in workforce or reassignment of roles. IAM is critical for integrating all this.

Mergers and acquisitions are a trying time for the businesses involved. Critical data is changing hands, and roles are being changed or being made redundant. This is a time in which the very reason for the merger; ie. critical assets must be protected. Security risks include disgruntled or soon-to-be redundant employees and privileged accounts. IAM solves a host of these issues with its ability to streamline role changes and detect insider threats. It is of particular value during an M&A, although it is always a nearly essential solution to have on deck.