M&A carries big investments

Mergers, acquisitions and alliances across all sectors have shown rapid increase over the past five years with 2015 a record-breaking year with global M&A volumes reaching $5.05 trillion. Around half of the 2015 activity targeted US-based companies, followed by Europe with a third, and Asia-Pac with around a quarter of the total value. In the UK, total M&A deals reached $621 billion and experts predict a possible surge of M&A activity in on the back of a weakening Pound caused by Brexit.

And big risks

M&A also carry a certain level of risk, demanding a highly extensive due-diligence process. Previously, acquiring companies mostly focussed on evaluating the target's fundamentals - such as financials, consumer sentiment, and strategy. However, with significant security attacks on well-known brands now hitting the headlines on a regular basis, boards of directors are finally starting to understand the importance of cybersecurity - especially in M&A.

M&A can make customers of both companies apprehensive. If that's followed up by a massive breach of sensitive customer data, the companies' customers are likely to flee in droves.

Cybersecurity as part of Due-Diligence

When involved in M&A, it's only natural for attention to turn to what the new company will look like, what business improvements will come with the new assets and client base. It can be a complex task to piece together a comprehensive vision of how the new organisation will be structured; where the staff will be located and which staff will stay on and which will not.

But to buy a company is also to buy its data. And buying data means you are buying past, present, and future data security problems. The economic impact of a transaction can shift dramatically if, after the deal is consummated, past or ongoing data breaches come to light. Greater attention is now being paid to a potential target's cybersecurity efforts during their M&A due diligence process.

SPOTLIGHT ON CYBERSECURITY

Which aspects of the target's infrastructure are being evaluated? How is the audit conducted, and who is included as part of the discovery and analysis process?

Start with a Security Audit

Security due diligence needs to start early in the deal and ensure that the target's data and environment are clean. That starts with a full audit of the target's security. Look not only at their tools and systems, but also at their policies and procedures - is it well documented, with logs and reports?

The acquiring company will also need to go through all the documentation to find any previous cybersecurity incidents. How did the target respond to the incident and how did it remediate the issue to avoid a repeat? If that documentation does not exist, this is a red flag that the organization may have much bigger issues that would require a comprehensive review by a qualified third party.

Threats to M&A

If there is even the slightest rumour that a company will be part of an M&A it will face increased attacks from people wanting details of the potential deal or looking to derail it. And from the time the merger or acquisition becomes public knowledge, through to the time when the two companies are finally combined, the networks of both companies need to be monitored daily for attacks and suspicious activity.

Two-thirds of attacks come from within organizations, usually from careless or disgruntled employees. Since an M&A process often includes restructuring and layoffs, employees can feel nervous and threatened. Fearful or disgruntled employees with access to sensitive data and systems can be a dangerous combination. It's imperative that customer data is protected throughout the process and that the value of the merger or acquisition (as well as other details) is not being leaked.

Your policy or mine?

Each company will have its own security policy. But what of the new organisation? Will the policies of the acquiring company be adopted? Should the two policies be combined or an entirely new one created?

BEING SECURE IS WORTH MORE

Good security increases the value of a target company which is why they often engage 3rd party cybersecurity experts to improve their security prior to an M&A.

Security Services for M&A

Trusted by significant organisations to provide expert security advice and managed services, Infosec Partners provides security services for all stages of an M&A.

- ✓ **Security Strategy Development**
  Ensures that the post-merger organisation's security strategy is aligned with its business goals.
- ✓ **Security Risk Assessment**
  Usually performed as part of due diligence, this facilitates integration of the two organizations, assessing potential impact of security risks on competitiveness, financial loss, and legal liability.
- ✓ **Pen-Testing & Vulnerability Assessment**
  Assess the resilience of your security controls and identify all the ways that an attacker might gain unauthorised access.
- ✓ **Architecture & Application Security Reviews**
  Crucial for evaluating the security of the organisation's network and its applications.
- ✓ **Compliance Management & Governance**
  Develop a sustainable compliance management program for the new organisation which ensures ongoing regulatory compliance while keeping the process streamlined and cost effective.

InfosecPartners
CYBERSECURITY

T. +44 1256 893 662 E. secure@InfosecPartners.com