Mergers and Acquisitions
Addressing the Cybersecurity Risks

Introduction

A secure and resilient digital presence is a key requirement for high performing organisations across a range of industries. Digital channels (web, mobile and social) have overtaken the traditional "human interaction" channels in many organisations to become a critical dependency. When evaluating a target company from an M&A standpoint, the failure to adequately evaluate the cybersecurity risks inherent in their digital channels can present significant risks to the acquiring company, including:

- a potential misrepresentation of the overall valuation due to unknown risks in public facing digital assets
- incomplete planning to address cybersecurity risks as the two organizations integrate

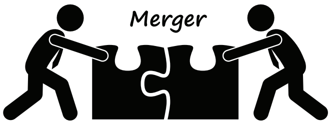
Unfortunately, cybersecurity risk assessments all too often get overlooked or marginalized in the pre (due diligence) and post acquisition process.

This white paper looks at some of the cybersecurity issues that should be considered as part of any merger or acquisition. We'll also explain how RiskIQ technology can play an important role in uncovering issues early in the due-diligence process and in reducing risk once the M&A transaction is complete.

The Impact of Cyber on M&A

What do M&A, digital channels and cyber threats have in common? They are all enjoying rapid growth and together create the perfect storm for cyber criminals and nation state actors.

2014 was a record year for mergers and acquisitions in Europe, both in number and overall value, which was up by 39% over 2013[1]. This trend is continuing through 2015 with spending in Q3 2015 up by 136% over Q3 2014[2]. In recent years digital channels have become the predominant method of customer engagement for many organisations, bringing with it an explosion of publicly facing web sites, mobile applications and social media accounts. In 2015 online commerce across Europe increased by 18% to £157bn[3] and the run up to Christmas saw the first £1bn digital day in the UK[4]. 2014 was also a record year for cyber attacks both in terms of number and diversity. As the Director of GCHQ stated earlier this year, "In GCHQ we continue to see real threats to the UK on a daily basis, and I'm afraid the scale and rate of these attacks shows little sign of abating[5]."



39%
Increase in European M&A Activity

18%
Growth in European Online Commerce

10%
Increased Cost to Businesses Hit by Cyber Attacks[8]

For organisations considering a merger or acquisition, the cyber risks associated with the target company's digital footprint represent a potential threat to both operations and brand reputation and as a result should be factored in during the due diligence process. However, all too often this is not the case.

A merger and acquisition process usually involves a due diligence exercise focused on all aspects of a companies business including IT. Historically, IT due diligence engagements were focused on identifying assets and security issues that were material in the valuation process such as business processing and reporting systems and the hardware and networks that supported them. As businesses and consumers have both moved outside the perimeter and onto the open internet, it's now vital that assets residing outside the firewall are accounted for and reviewed in order to get a full understanding of the company's digital attack surface.

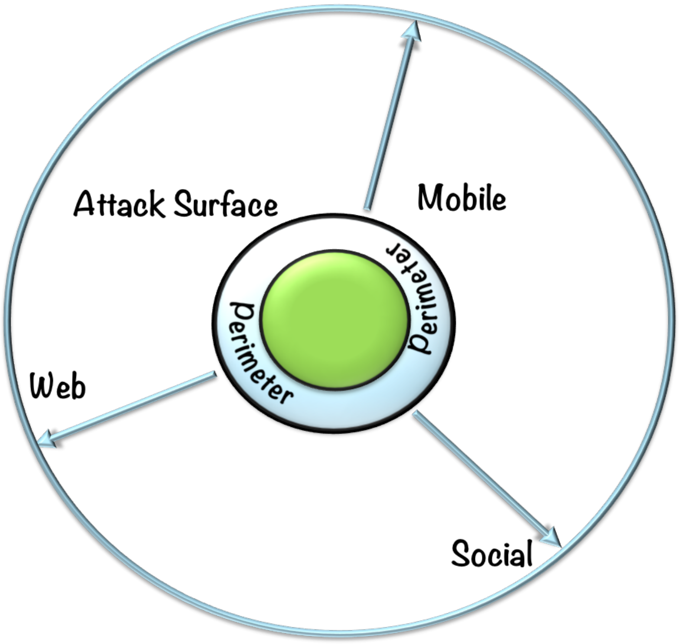
In a recent survey of M&A specialists conducted by Freshfields Brockhaus Derringer, 78% of respondents said that there was not adequate cyber risk analysis being done in M&A's even though 90% of respondents believed that cybersecurity breaches would result in the reduction of deal value. This is especially the case in Europe where 39 percent of European respondents said that cybersecurity had become a key part of due diligence in the last year compared to 53% of respondents from North America.[6]

Why is this the case?

There are a number of common reasons why organisations are not getting the full picture of cyber risks as part of due diligence. The first is the sheer scale of the digital presence of the company being acquired. It is not uncommon for a large organisation to have thousands or tens of thousands of active websites and other publicly exposed assets. While IT and Security teams in the to-be-acquired company will have an asset register of web sites, we have found that it is almost always a partial view of what really exists. The more decentralized an organization's IT activities are the bigger the delta we see.

A small percentage of this delta will consist of forgotten assets or internal assets inadvertently exposed on the public web, but most can be attributed to "Shadow IT"; activities driven outside of the central IT team, typically by business units or marketing. Shadow IT activities can result in the creation and external hosting of web sites that are unknown to the central IT and security teams. Mobile application development frequently takes place at a line of business level and the policing of company owned apps across the many different mobile app stores varies considerably from company to company. The management of the organisation's social media presence is also often decentralised at a regional or line of business (LOB) level resulting in a large number of company "owned" accounts and executive profiles across social media sites, all of which are susceptible to compromise and exploitation through social engineering tactics.

All in all, we typically find 30% more publicly exposed digital assets than are recorded by the to be acquired organisation.



The Growing Digital Attack Surface

Time is another contributing factor. In most cases there is an urgency to complete the acquisition before the value materially changes. Cybersecurity audits can take a long time as auditors try to build up an accurate picture based on incomplete and out of data information.

We also see that some acquiring organisations have been slow to move their own security programs "outside the firewall", instead focusing on the more traditional security disciplines. In this case the cybersecurity posture of their own organisation is not accurately known, let alone the cybersecurity posture of the target company.

While these can be valid reasons they must be weighed up against the possible consequences. A successful cyber attack could have a material impact on the value of a company in the short to mid-term. In addition to reputational damage, new EU data protection laws have introduced the provision for fines of 2 to 5 percent of global revenues for loss of customer data[7], which again can materially impact the value of an organisation with less than adequate security defences. From a nation state perspective, an undetected "back door" planted in the target company's network could result in intellectual property theft once the two networks are connected.

In the case of acquisitions involving part of an organisation, for instance a line of business, it is essential to identify and document the assets being transferred, which also include digital properties such as brand assets, domains and social accounts. Without a through understanding of what currently exists, critical digital assets may be missed resulting in ownership and security issues later on.

> ***"A successful cyber attack could have a material impact on the value of a company in the short to mid term."***

Without a clear understanding of the risks and their potential monetary and reputational impact:

- There will be insufficient funds allocated to remediate unexpected security breaches potentially impacting quarterly/annual results of the company
- The planned security programme will not adequately account for remediation issues causing resourcing and funding challenges later on

A good understanding of cyber risks is not only needed for the due diligence process, it is also a key requirement in successfully managing the risks once the transaction is complete.

Post M&A

As responsibility for the security of acquired digital assets transfers to the acquiring company, the work begins to bring those assets under management as part of the corporate security programme. With regards to public facing digital assets, the following questions are usually posed at an executive assessment stage:

- what assets exist and where are they located?
- are they compliant with corporate standards (platforms, third party components, approved hosting providers, brand and legal compliance, etc)?
- are there health & hygiene issues that could present easy opportunities for a hacker; deprecated frameworks, outdated web servers, broken links, expired certificates, etc.?
- are there insecure forms collecting personally identifiable information (PII)?
- have any assets been compromised and therefore represent an immediate exposure? (Are you able to identify IoC's in the acquired digital footprint? Did you buy a Trojan horse and are about to plug it into your network?)
- what official mobile applications exist and what app stores are they in - is this in line with corporate policy?
- are there back level or re-engineered corporate mobile apps in any of the official or third party app stores.
- what corporate social media accounts exist and on what social media platforms - is this in line with corporate policy?

Answers to these questions can help direct resource to the areas needing immediate attention. They also help security teams quantify the scope of work needed to bring acquired digital assets under management from a security perspective.

How can RiskIQ help?

RiskIQ Digital Footprint can provide M&A teams with a complete view of the to-be-acquired company's public facing digital footprint across web, mobile and social, highlighting areas of potential risk and providing the detailed information needed for risk scoring. It serves as a single pane of glass providing a continuously updated view of what exists and its current state. It automatically highlights a wide range of hygiene issues, Incidents of Compromise (IoC's) and compliances issues, giving M&A teams the baseline they need to conduct a cyber risk assessment and security teams the visibility they need to drive their post M&A programme.

[1] Mergermarker, Deal Drivers EMEA:2014

[2] Factset, Flashwire Europe Quarterly 3rd Quarter 2015

[3] http://www.retailresearch.org/onlineretailing.php

[4] http://www.i4u.com/2015/10/95701/black-friday-2015-online-sales-uk-top-1-billion

[5] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

[6] Freshfields Bruckhaus Deringer, Cybersecurity in M&A

[7] http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm

8 http://www.octree.co.uk/Documents/2014-Global-report-on-the-Cost-of-Cybercrime.pdf

About RiskIQ

RiskIQ provides organizations the visibility and intelligence they need to secure their known and unknown Digital Footprint. Using a global proxy network of synthetic clients, RiskIQ continuously discovers and creates an inventory of documented and undocumented web assets, and scans them for copycat mobile apps, drive-by malware and malvertisements. Leading financial institutions and both consumer and B2B brands use RiskIQ to protect their web assets and users from security threats and fraud. RiskIQ is headquartered in San Francisco and is backed by growth equity firms Summit Partners and Battery Ventures. To learn more about RiskIQ, visit www.riskiq.com.