Mergers and Acquisitions

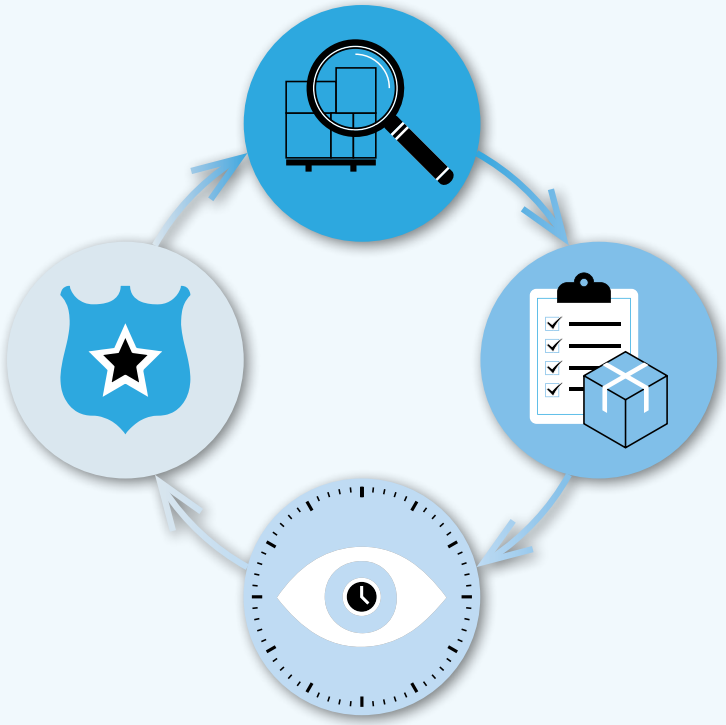
As digital channels (the web, mobile and social) have overtaken the traditional "human interaction" channels in many organizations, a secure and resilient digital presence is now a key requirement across all industries.

When evaluating a target company from a mergers and acquisitions (M&A) standpoint, the failure to properly assess the cybersecurity risks inherent in the target company's digital channels can present significant risks to the acquiring company, including:

- A potential misrepresentation of its overall valuation due to lack of clarity regarding the Internet-facing assets
- A lack of planning to address ongoing security risks as the two organizations integrate

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

This whitepaper explores some of the cybersecurity issues that organizations should consider as part of any merger or acquisition. It also explains 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, help create the perfect storm for cyber criminals and state-sponsored threat actors.

In 2014, merger and acquisition activity accelerated significantly. The number of deals in the U.S. rose ten percent to 9,802, the aggregate value of which surged 51 percent to more than $1.5 trillion—an increase of more than $500 billion in one year. Through March of 2015, the total stood at $746 billion, up nine percent from $685 billion in the same period of 2014[1].

Meanwhile, digital channels have become the predominant method of customer engagement for many of these organizations, causing an explosion of publicly facing websites, mobile apps, and social media accounts. In fact, e-commerce accounted for about 5.9% of the total retail market worldwide in 2014, or $1.316 trillion[2] making it no small wonder that the third front of this perfect storm, cyber threats, also saw an increase in activity: 2014 was also a record year for cyber attacks in both their frequency and diversity—eclipsed only by 2015[3].

As the Director of GCHQ stated earlier this year, "In GCHQ we continue to see real threats [...] on a daily basis, and I'm afraid the scale and rate of these attacks shows little sign of abating[4]."

TOO LITTLE, BUT NOT TOO LATE

An M&A process usually involves due diligence exercises focused on all aspects of a company's business. Historically, the ones focused on IT identified assets and security issues that were material in the valuation process, such as business processing and reporting systems and the hardware and networks that support them. But as businesses follow consumers outside the perimeter and onto the open web, they must account for and review their assets residing outside the firewall as well. By maintaining

1 *Deloitte, M&A Trends Report 2015 Our annual comprehensive look at the M&A market*

2 *eMarketer, Retail Sales Worldwide Will Top $22 Trillion This Year*

3 *HACKMAGEDDON, 2015 Cyber Attacks Statistics*

4 *CESG, Common Cyber Attacks: Reducing The Impact*

a complete understanding of their digital attack surface, organizations can identify all potential inroads for external threats.

Cyber risks associated with the target company's digital footprint—its known and unknown assets outside the firewall—represent a looming threat to both the acquirer's operations and brand reputation. And much to the dismay of many within the acquiring organization, these risks are often ignored during the due diligence process. In a recent survey of M&A specialists conducted by Freshfields Bruckhaus Deringer[5], 78% of respondents said that there was not adequate cyber-risk analysis being done in M&As, even though 90% of respondents believed that cybersecurity breaches would result in the reduction of deal value.

WHY IS THIS THE CASE?

There are several common reasons why organizations are not getting a complete view of potential cyber risks during the due diligence process. The first is the sheer scale of the digital presence of the company they're acquiring. It's not uncommon for a large organization to have thousands—or even 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 websites, it's almost always only a partial view of what exists. And the more decentralized an organization's IT activities are, the bigger the gap we see.

SHADOW IT

A portion of this gap will consist of forgotten assets or internal assets inadvertently exposed to the public online, but most can be attributed to "Shadow IT," or assets created via initiatives undertaken outside the IT team, typically by business units or marketing teams. Shadow IT activities can result in the creation and external hosting of websites that are unknown to central IT and security teams.

For example, mobile app development frequently takes place at a line of business (LOB) level, and the level of policing of company-owned apps across the many mobile app stores across the world varies considerably from company to company. The management of the organization's social media presence is also often decentralized at a regional or LOB level, which can result in an abundance of 'company owned' Shadow IT accounts and executive profiles across social media sites, which are susceptible to compromise and exploitation.

TIME

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 an accurate picture out of information that's often incomplete and out-of-date.

We also see that some acquiring organizations have been slow to move their security programs outside the firewall, instead focusing on the more traditional security disciplines. In these cases, the organization doesn't have an accurate assessment of the breadth of its own cybersecurity capabilities, let alone that of the target company.

WHAT ARE THE 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 data protection laws in Europe have introduced the provision for fines of two to five percent of global revenues for loss of customer data, which can also materially impact the value of an organization. Not only that, an undetected "back door" planted in a target company's network could result in intellectual property theft by a threat actor.

In the case of acquisitions involving part of an organization—a LOB, for instance—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 thorough understanding of what exists, critical digital assets could be missed, which would result in ownership and security issues later on.

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

- The security program in place will not adequately account for remediation issues, which will cause future resourcing and funding challenges
- There will be insufficient funds allocated to remediate unexpected security breaches, potentially impacting the company's quarterly/annual results

5 Freshfields Bruckhaus Deringer, Cybersecurity in M&A

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 overall corporate security program. Vis-à-vis 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 such as 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 thus represent an immediate exposure? For example, are you able to identify Indicators of Compromise (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 which app stores are they in? Is this in line with corporate policy?
- Are there rogue 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 resources to the areas needing immediate attention. They also help security teams quantify the scope of work needed to bring acquired digital assets under management.

HOW CAN RISKIQ HELP?

Of the $80B (and growing) spent annually on enterprise security, budgets are shifting towards addressing the increasing threats targeting digital channels. RiskIQ is the only company that is purpose-built to tackle this problem by preventing brand damage, reducing external threats, and eliminating rogue assets across all digital channels.

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 channels, 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, IoC's and compliance 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 program.

ABOUT RISKIQ

RiskIQ provides organizations the visibility and intelligence they need to secure their Enterprise Digital Footprint and map their Adversaries' infrastructure. RiskIQ products, powered by a proprietary virtual-user technology, threat analysis engine, and global proxy network, enable an organization to defend against threats targeting its websites, mobile applications, brands, customers, and employees. 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.