BAIRD PERSPECTIVES

Cyber Risk, Repriced

How Evolving Realities are Lifting Valuations and Driving M&A

In This Report

January 2020

Key market drivers contributing to the increased demand for cybersecurity solutions.

Mounting implications for businesses and governments due to the rise of the cybercrime market.

Network perimeters have become more complex and thus increasingly porous.

In many scenarios, traditional cybersecurity approaches are struggling to facilitate modern business.

As companies reprice cyber risk and face the prospect of potential fines, spending on cybersecurity continues to grow.

Introduction

The digital transformation of business continues apace, and the demand for cybersecurity solutions is only strengthening. As business goes digital, data is becoming more valuable and enterprise infrastructures are becoming more complex. Cyber risk is increasing as these trends accelerate. Thus, businesses are beginning to place a higher premium on managing cyber risk, which is contributing to a broader repricing of cyber risk and driving M&A activity in the cyber space.

Key Market Drivers

Data Volume and Value

As companies continue to shift to digital modes of work, communication and business dealings, data is becoming more and more valuable. This trend will only continue to accelerate with the wider adoption of Big Data, artificial intelligence (AI) and the internet of things (IoT).

Data aggregation – the merging and analysis of low-value data sets to create higher-value, more actionable insights – is also growing with the proliferation of fast, inexpensive, powerful analytics technologies and processes. This is giving way to an easily accessible supply of valuable data that companies must protect (and bad actors seek to access).

Complexity of Enterprise Infrastructure

The shift from on-premises models to hybrid and cloud solutions is creating new complexity for businesses. This change is resulting in a need for new tools to monitor and manage data, access, applications and security. Companies are facing new demands of their infrastructure, including:

- Shift from threat detection (versus prevention), including the application of machine learning and artificial intelligence
- Mounting regulation and data protection/fraud requirements, including the EU's General Data Protection Regulation (GDPR)
- Cloud systems, which allow for near-infinite scalability

All of these factors are contributing to the increased demand for cybersecurity solutions.

2.5 quintillion bytes of data is created every day

Source: Forbes[1]

[1] forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-every-one-should-read/#66dfba5260ba

Rise of the Secondary Market

Enterprises are becoming increasingly concerned about refining and leveraging their data – but bad actors are also eager to tap into the power of these data sets. The availability of readily accessible and refined data is driving more organised crime and activity by state actors. This is further fuelled by the wide availability of tools that enable data exfiltration and penetration.

As such, the barriers of entry into the cybercrime market are now much lower, as a new ecosystem has emerged to supply this secondary market. The combination of valuable data and opportunities for monetisation on the secondary market provides incentives for “steal to order” techniques.

The rise of this secondary market has mounting implications for businesses and governments across the globe:

- The cybercrime frontier is expanding and even reaching the political sphere, as evidenced by increased interactions between state actors and cybercrimes.
- Cybercrime will cost the world an estimated $6 trillion+ annually by 2021, up from $3 trillion in 2015. Additionally, gains from these transfers will be more profitable than the combined global trade of all major illegal drugs.[2]
- It is estimated global cybersecurity spending will exceed $1 trillion cumulatively for the five-year period from 2017-2021, which suggests 12-15% year-over-year growth in the cybersecurity market through 2021.[2]

More than $6 trillion
Cost of cybercrime annually by 2021
Source: Herjavec Group[2]

[2] herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Porous Perimeters

Network perimeters have become more complex and thus increasingly porous. The shift to a real-time, "always-on" economy has blurred network boundaries. Enterprises now must monitor more connected systems, sensors, devices and integrated supply chains on their networks. Traditional "endpoint + perimeter" security solutions are simply no longer sufficient to protect the data residing on many endpoints.

The internet of things (IoT) is driving exponential growth in endpoints and, in turn, a massive expansion of the enterprise perimeter. This expansion will continue in the coming years. As IPv4 protocol approaches capacity, the transition to IPv6 will accelerate. According to a Cisco report, an estimated 9.4 billion mobile devices will be IPv6 capable by 2022, as well as 8.9 billion fixed devices.[3]

Additionally, the ubiquity of mobile devices combined with the rise of the gig economy[4,5] is contributing to perimeter complexity. Managing an enterprise perimeter is time- and resource-intensive to begin with. It is even more complex when who works for you and what they can access is constantly in flux.

It is crucial that businesses know where their "crown jewel" intellectual property and proprietary data is held and who (within and outside of the organisation) can access it. The Edward Snowden leaks arguably represent the most high-profile, publicly disclosed impact of "insider risk." However, even customer lists or partial data sets can be targeted by and exploited through temporary workers.

[3] cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html

[4] According to Deloitte Global Human Capital Trends survey, 33% of IT functions extensively use alternative labor/workforce, 25% of Operations functions, 15% of Marketing functions, 15% of Innovation/R&D functions (source: Deloitte Insights, see appendix 1 for details)

[5] Global online marketplaces that fuel the gig economy could be worth around £43 billion by 2020 (source: PwC, published by The Gazette Official Public Record)

As Traditional Approaches Fall Short, Companies Are Repricing Risk

In many scenarios, traditional cybersecurity approaches are struggling to facilitate modern business. Within many companies' technology stacks, the provision of network detection, antivirus and firewalls is compromised or subject to inflexible access controls, which struggle to be both effective and conducive to regular business.

Key limitations include:

- The decreasing effectiveness of antivirus software, which is generally looking "behind the curve"
- The still-nascent nature of AI – while it shows promise as a tool to identify outliers, it still requires human intervention and isn't yet wholly reliable
- Network and security operations center (SOC) tools are struggling to keep up – they are often leveraged in "firefighting" exercises
- Tight labour market for highly skilled technical cyber workforce

At the same time, cyber risk is being repriced. A number of factors are driving this change, including a massive increase in regulation and consequent penalties and fines, as well as a significant uptick in the number of announced data breaches and their direct and indirect costs.

Notable Data Breaches

Company	Breach + Costs
Capital One	July 2019. Hacker exploited a configuration vulnerability and stole personal details of approximately 106 million clients. *Cost: As much as $150 million; share price down ~10% since July*[6,7]
Marriott	September 2018. Exposed data of up to 500 million Starwood guests. *Cost: $123 million GDPR fine*[8]
British Airways	2018. Data breach resulting from malicious attack on airline's website. *Cost: £183 million GDPR fine*[9]
Equifax	May-July 2017. Data breach exposed personal information of 143 million U.S. consumers. *Cost: Settlement of up to $700 million*[10]
Uber	2016. Cyberattack exposed data of 57 million customers and drivers *Cost: Settlement of $148 million*[11]

Historically it has been difficult to insure against these types of events, though this market is evolving.

[6] nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
[7] bbc.com/news/world-us-canada-49159859
[8] forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/#556d22dd4525
[9] bbc.com/news/business-48905907
[10] bbc.com/news/technology-49070596
[11] bbc.com/news/technology-45666280

M&A Themes

Growing Budgets and the Need for Internal Alignment

As companies reprice cyber risk and face the prospect of potential fines, spending on cybersecurity continues to grow. Cybersecurity budgets increased 141% from 2010 to 2018 globally, across industries. Meanwhile, spending for cloud security has grown 148% since 2017 and spending on other information security software was up 25% from 2017 to 2019. Globally, the top spending area within cybersecurity is security services as many companies and consumers remain anxious after the data breach scandals of recent years.[12]

C-suites are being forced to change their approach to mitigating their organisations' cyber risk. Perimeters have expanded and, in many cases, the C-suite has yet to adapt. One of the greatest challenges to ensuring an appropriate cybersecurity budget is aligning all internal decision-makers. Technical understanding of cybersecurity challenges often differs between IT professionals and C-suite executives. The latter group may occasionally doubt the efficacy of preventative measures championed by cybersecurity professionals.

A lack of internal alignment and collaboration between executives and IT experts contributes directly to data breaches. Sixty percent of C-level executives believe their organisations' current solutions provide sufficient protection against hackers, but only 29% of IT professionals believe the same. What's more, 70% of cybersecurity breaches are caused by people and process failures within an organisation.[12]

Thus, providers who offer solutions to help companies navigate the ever-evolving risk landscape are receiving premium valuations. Regulatory forces are also accelerating the need for enterprises to "get smart fast" and adapt to the current technology environment. Thirty percent of organisations worldwide will spend on Global Data Protection Regulation (GDPR)-related consulting and services in 2019.[12]

Transaction Market

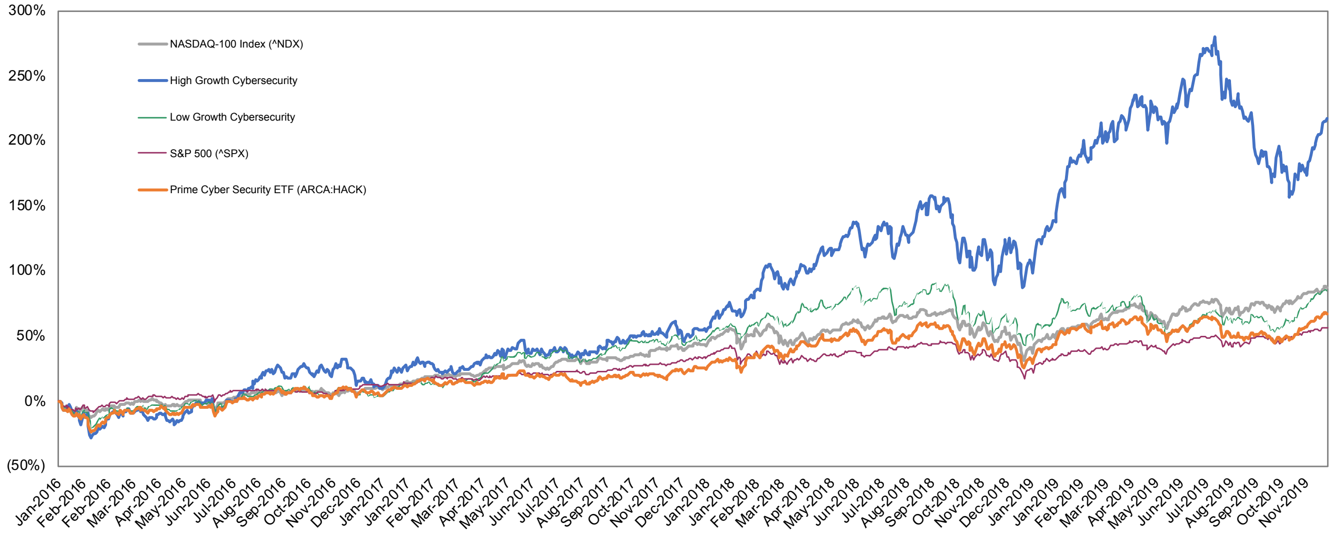
With the backdrop of an increasingly data-driven, connected economy, the M&A transaction market is vibrant and investors and strategic players alike are hungry to keep up with the relentless pace of change in the market.

A lack of technical understanding, increased volume and complexity of data, and fragmented internal collaboration is pushing non-tech players to acquire the appropriate software assets to leverage the latest technology (versus doing it in-house). Forty percent of M&A transactions of tech companies are realized by companies in other industries.[12]

Cyber is playing a prominent role in the overall enterprise software M&A market, which saw $71 billion in transaction activity in the first half of 2019. Some of the most desirable assets, as reflected in their pricing, occurred across the wider cyber market.

[12] RSA Conference https://www.rsaconference.com/industry-topics/blog/the-future-of-companies-and-cybersecurity-spending

Relative Stock Performance (4 years)

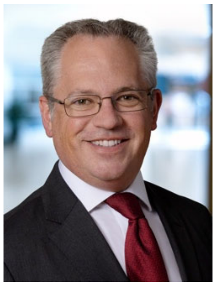


Source: Capital IQ.

Notable Recent Cybersecurity M&A Deals by Size

08/02/2018	Cisco acquired Duo for $2,350m
08/27/2018	Allstate acquired Infoarmor for $525m
09/13/2018	Bomgar acquired BeyondTrust for $625m
10/10/2018	Thoma Bravo acquired Imperva for $2,100m
11/05/2018	Thoma Bravo acquired Veracode for $950m
11/16/2018	BlackBerry acquired Cylance for $1,400m
02/07/2019	Carbonite acquired Webroot for $618.5m
02/19/2019	Palo Alto Networks acquired Demisto for $560m
05/30/2019	Insight Partners acquired Recorded Future for $780m
08/08/2019	Broadcom acquired Symantec’s Enterprise Security Business for $10,700m
10/14/2019	Thoma Bravo to acquire Sophos for $3,900m
01/06/2020	Insight Partners to acquire Armis for $1,100m

Baird's Cyber Investment Banking Team



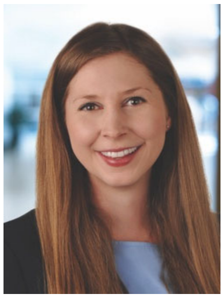
Simon Pearson
Managing Director
+44-207-488-1212
spearson@rwbaird.com

Jean Stack
Managing Director
jstack@rwbaird.com
+1-703-394-1831

John Song
Managing Director
+1-703-394-1800
jsong@rwbaird.com

Craig Rogowski
Managing Director
+1-650-947-6810
crogowski@rwbaird.com

Evan Mueller
Director
+1-503-273-4956
emueller@rwbaird.com



Chelsea Smith
Vice President
+44-207-488-1212
cmsmith@rwbaird.com