DFIN

CYBERSECURITY LANDSCAPE

How consolidation is driving the M&A cycle

Data provided by PitchBook

DFINsolutions.com

Contents

Executive summary

A strong M&A cycle within cybersecurity is set to result in a new high for volume in 2018. At its current pace, cybersecurity M&A in the US will just barely eclipse the prior high of 145 closed transactions and hit 148, while deal value is already at a near-record value of $33.2 billion.

Consolidation has characterized cybersecurity for the majority of the cycle. Driven by not only maturation of emerging market leaders in key segments, but also the need to stay abreast of innovation, consolidation has been the primary factor in cybersecurity M&A for years now. Deal size metrics have steadily increased as a result.

Broader market factors, from regulations to the acceleration of technical development, look set to incentivize a steady pace of dealmaking going forward. Regulations are slowly being implemented to match the evolution of cyberthreats, most dramatically in Europe's General Data Protection Regulation. Threats in general are growing more sophisticated, calling for extensive preparation, investment and rethinking of protective measures.

Costs and spending are rising at a remarkable rate. The cost of a data breach is fast approaching $4 million, with an average cost per user of $148 for records lost or stolen. Overall, the market for cybersecurity solutions is poised to reach $172 billion in value by 2022.

> "You can outsource the technology but not the responsibility."
>
> **TOM WARD**
> **MANAGING DIRECTOR, DFIN**

Industry developments

6.4% increase in the cost of a data breach

The cost of an average data breach to companies worldwide in 2018 was $3.9 million—for US companies, the cost was $7.9 million. That former tally represents a 6.4% increase in cost year over year.

500M

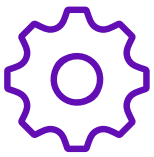
In September 2018, some 500 million guests of Marriott International's Starwood Hotels & Resorts Worldwide saw their account details compromised, with details such as passport numbers left vulnerable.

$124B

Spending on information security products and services is forecast to grow by 8.7% to $124 billion in 2019, per Gartner.

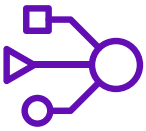
Cloud-centric

Many of the top transactions completed thus far in 2018 have all been of cloud-centric security offerings. Companies such as Barracuda Networks, which was acquired by Thoma Bravo for $1.6 billion, or Duo Security, for which Duo Security paid $2.35 billion, all focus on cloud-related issues such as managing network performance, securing accounts, etc.



IoT

A critical, growing area for risk with regard to cybersecurity is IoT. Solutions that span the entirety of the hardware to software continuum must be developed in order to secure the myriad points of access that could yield control over entire systems.



Continuity

Beyond simple business continuity, cybersecurity providers are increasingly focusing upon where their product or service fits into a given value chain, as well as security along workflows, product cycles and more.

Q&A

Dannie Combs

Chief Information Security Officer, DFIN

Dannie Combs is the Chief Information Security Officer at DFIN. Dannie has overall responsibility for cybersecurity and brings 24 years of cybersecurity and information assurance.

Prior to DFIN, Dannie was the senior leader responsible for overall network security for the fifth-largest US-based wireless operator, supporting ~20M mobile subscribers. From 2001 to 2009, Dannie consulted with a number of organizations to build and mature technology security programs and organizations as interim CISO, security architect and more.

Dannie is a 10-year veteran of the United States Air Force where he served as a cyberthreat specialist supporting a variety of military and national security organizations. He is a three-time combat veteran with deployments in Bosnia, Afghanistan and Iraq.

What are the primary concerns of your clients with regard to the cybersecurity aspects of Donnelley's products and tools?

Combs: Typically a primary focus is articulating what our security framework includes, which begins with our network of service centers and our distributed platform for Venue. Second, we must emphasize that our products are developed primarily here in the United States. Several of our competitors cannot make that claim. Then clients usually want to discuss security infrastructure, what types of technologies we employ that provide our front line of defense for blocking and tackling the broadest set of risks with a set of repeatable procedures to respond in those moments that matter. Lastly, authentication protocols are always discussed. We have to keep our requirements for strong passwords flexible for our customers to integrate, for example, through their federated single sign-on within their own corporate environment so that these experiences are pleasant.

What are the primary technical challenges faced in your product suite with which you have to contend, and how do they align with client concerns mentioned above?

Combs: There are several areas of interest on which we have to focus given what our clients prioritize, namely network, database, application and endpoint security. For many years, foundational network security was where most companies invested their dollars. They put a big wall around their perimeters, safeguarding their assets, and kept the bad guys out with strong network firewalls and intrusion prevention systems along with creating a lot of logs to analyze. We continue to see those technologies as appropriate and necessary. But we also see that distributed denial of service attacks, for example, is a very realistic threat with which all SaaS providers and all service providers must contend as well. Consequently, DFIN has invested into the capability to prevent DNS attacks. Those issues typically can be grouped under the category of network security.

Moving up the stack, though, whether it be employees, contractors, consultants or clients, it's important that passwords and privileged access are vaulted, encrypted in storage, and changed regularly, and that there's technology in place to understand the behaviors of users. Regarding activity and access management, I would add that multifactor authentication is no longer something that's used to demonstrate that some organizations are more committed. It's a foundational expectation today. Meanwhile, database security comprises three areas that are top of mind for us and our clients. First, encryption at rest is no longer an option but a minimal expectation for clients. If you're not encrypting your data that day, the odds are that it's just expected to be compromised quickly. Second, compliance with the regulatory changes that occurred in the past 18 months is essential. In addition, I would expect of any product company with which I do business—and my clients expect this of us—a penetration test that doesn't just validate you've got firewalls, encryption and other foundational items, but also investigates fraud use cases, ensuring you can't use the application in a manner for which it wasn't intended.

Finally, I expect my vendors to demonstrate that their employee base has appropriate malware, disk encryption and real-time monitoring across their laptops and servers. Years ago, we were all protected by that strong wall of firewalls around a perimeter, but today we're all floating between airports, hotels, corporate offices and our home ISPs. We're always working, as it were, so that perimeter is gone. That puts a lot of pressure on security teams to protect the employees with real-time monitoring.

Is there one area that's more successful over others? What other mitigating tactics really curb the problems presented by the human factor?

Combs: It's really about striking that appropriate balance between security and functional user experience. Even

with network security, database security, application security and endpoint security in place, at the end of the day, there is not a single organization out there that can be 100% secure. As long as you're connected to the internet, there's always a risk. So it's important to have resources monitoring systems 24/7. When there is an alarm or any activity of interest, you need to know how to respond with repeatable procedures to provide a very quick and yet accurate assessment of what's occurring, what exposure may be or what the risk level is. Where we look to really stand out—and where differentiation can be achieved—is firstly in the realm of orchestration and automation of security. In plain English, we have machine learning and AI-enabled capabilities to systematically eliminate not only a certain event caused by human error but also the human time delay in shutting down a bad connection, for example.

Second, we've been working for more than 10 years now on cyber-threat intelligence. We've seen a resurgence of nation-state attacks, not just in general, but targeting financial institutions within the United States. When we see IP traffic originating from those geographic locations, knowing there is no justifiable business reason to allow it into our environment, we block it instantaneously. We maintain a database of bad domains, suspect IP addresses and the like that we attribute to bad actors that could be nation states or others that we've identified ourselves or in partnership with some of our clients such Cloud Strike or other US intelligence agencies such as the NSA and other DHS organizations.

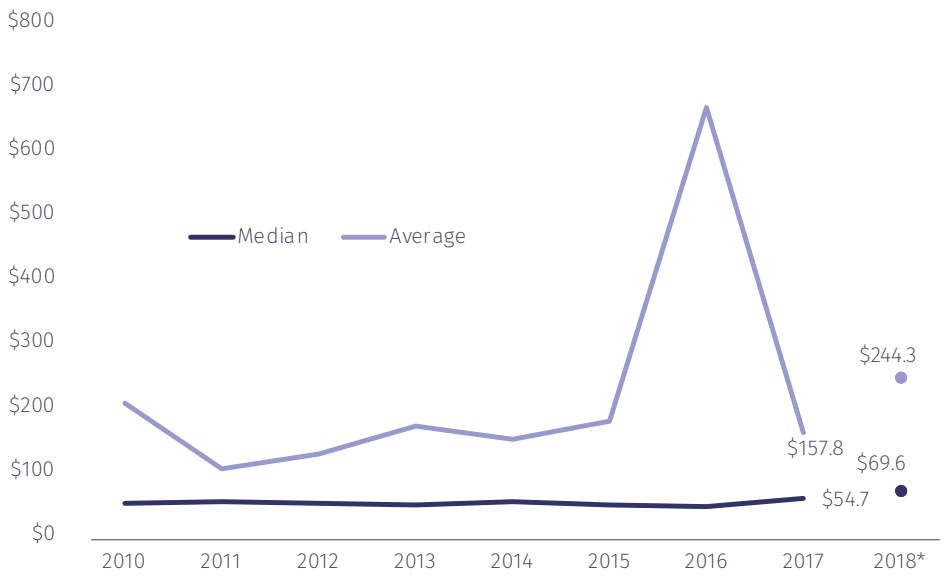
What are the primary concerns that should be focused on more by clients, in your view? What macro trends are you watching going forward?

Combs: We see more and more organizations continue to fall victim to improperly configured cloud assets. There's more and more folks sprinting to the cloud, but there's a tremendous, almost crisis-level lack of security skill on how to protect those cloud assets. That has resulted in many breaches over the last year. We expect that to increase, along with the theft of cloud-computing resources. We also see a strong likelihood of significant penalties being applied to "tier-two" organizations—tier-one being the Facebooks, Amazons and Googles of the world—as a direct result of falling short of data protection regulations such as GDPR. We're going to see a lot of eight-figure penalties occurring, in our opinion. Lastly, we see a sharp increase in AI-driven automated attacks against organizations. Think of these as botnets that continuously seek out vulnerabilities across the internet and self-adjust their attack technique as soon as they discover that vulnerability. Years ago, the terms were zero-day vulnerabilities and zero-day exploitation of attacks, in reference to the time between an attack and when a patch can be released, but now it's down to minutes or even a few hours.

Re macro trends, the IoT and, generally, consumer electronic devices can be exploited in large volumes. It has been a bit of a record-breaking year for specific campaigns motivated by financial gains targeting particular companies, including British Airways, which was especially interesting because of the very advanced techniques of card scraping deployed. We've also witnessed cloud expansion bringing a plethora of new vulnerabilities, causing many different businesses to struggle with being organized and prepared to secure those assets. As a result, we see a tremendous increase in overall encryption of data on the internet leaving organizations, which can make it very difficult to get the insights needed to protect companies. A shortage of cybersecurity talent also isn't helping matters much. Lastly, over the past year, we've seen that major technology providers continue to have to issue a record number of patches to address vulnerabilities that come out about every three to four weeks. Consequently, organizations like Donnelly need to bake in procedures to ingest those updates while not compromising the ability of their own technologies to provide security during the reboots and follow-on testing these patches require.

Cybersecurity landscape

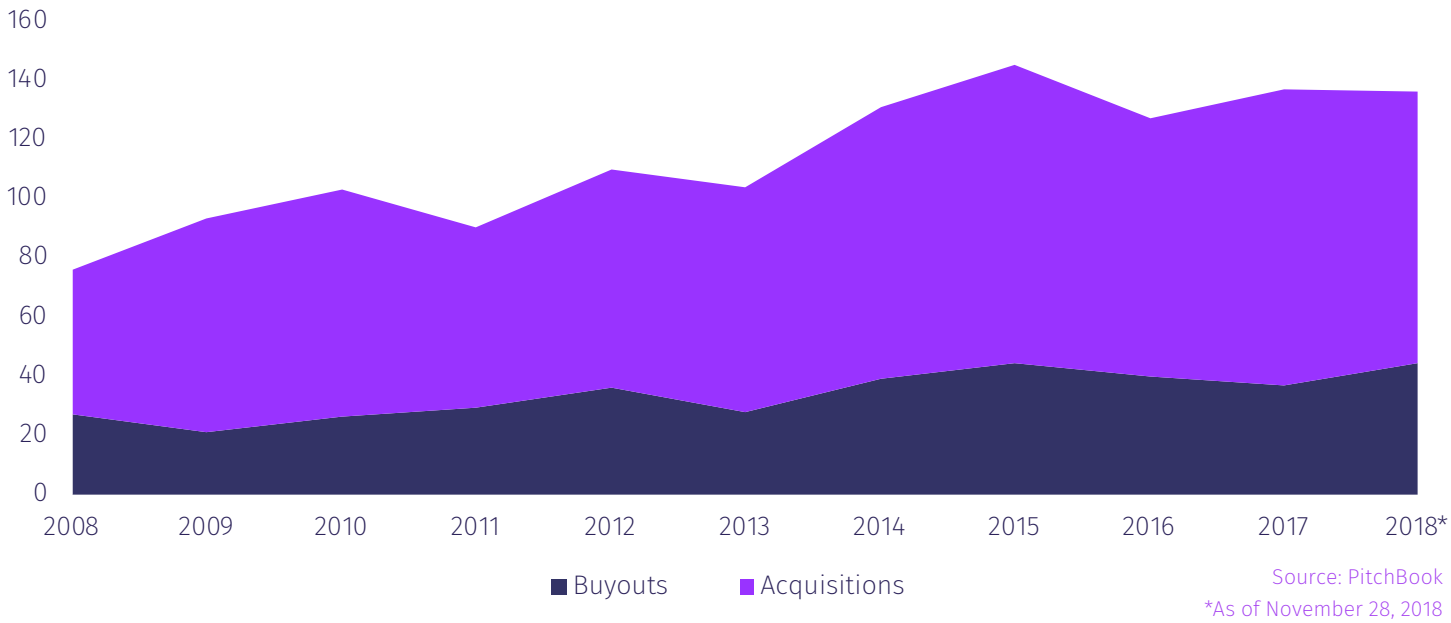
US M&A median and average deal size ($M) in cybersecurity



Source: PitchBook
*As of November 28, 2018

Consolidation in cybersecurity has slowly pushed M&A sizes steadily higher; even PE funds have increased their activity within the space as part of a broader push into tech.

US M&A (#) by sponsor type

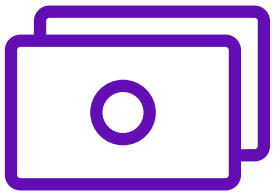


Source: PitchBook
*As of November 28, 2018

US M&A of VC-backed companies by strategic acquirers, 2010-2018*

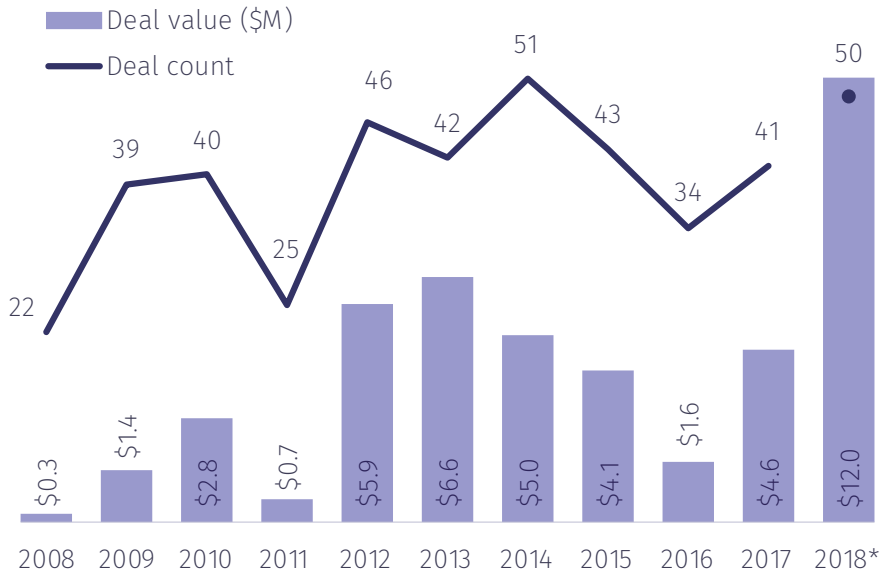
Investor Name	# of Investments	Investor HQ
Thoma Bravo	9	Illinois
TA Associates Management	4	Massachusetts
Providence Equity Partners	3	Rhode Island
Vista Equity Partners	3	Texas
K1 Investment Management	3	California
Bain Capital	2	Massachusetts
Francisco Partners	2	California
Audax Group	2	Massachusetts
Welsh, Carson, Anderson & Stowe	2	New York
Marlin Equity Partners	2	California

Source: PitchBook
*As of November 28, 2018



Thoma Bravo exemplifies how even PE firms are now contributing to consolidation amid middle-market firms with cybersecurity offerings.

US M&A of VC-backed companies in cybersecurity



Source: PitchBook
*As of November 28, 2018

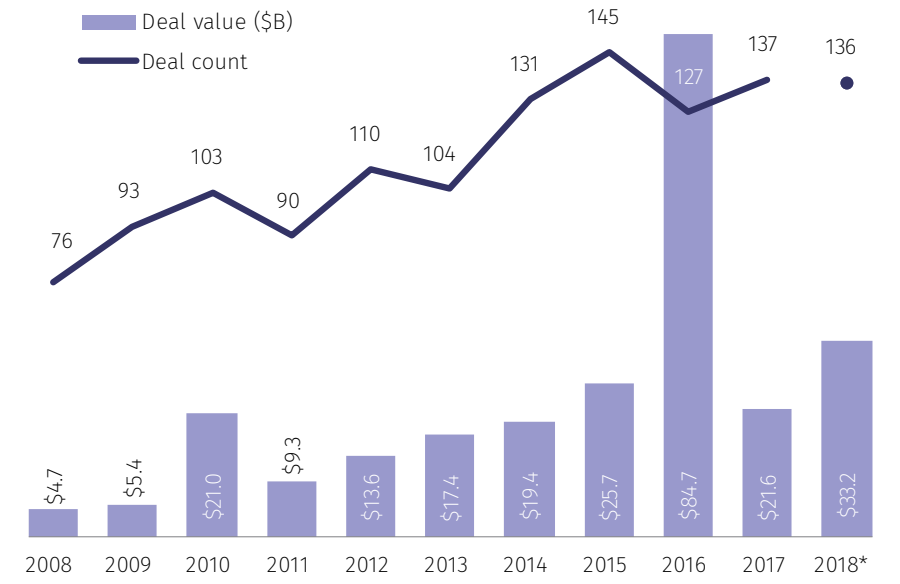
2018 to date has marked a clear high in deal value for venture exits in cybersecurity—a testament to the need for innovation

Dealmaking landscape

For the fifth straight year, cybersecurity M&A in the US held strong, as 136 transactions for an aggregate of $33.2 billion in value closed in 2018 through the end of November. In fact, those tallies put 2018 on pace to be potentially the most active year on record in terms of count and second-highest in terms of overall value. The persistence of the M&A cycle within cybersecurity is striking; the steady rise in total deal value while counts have stayed relatively constant suggests that consolidation is one of the primary driving factors behind the ongoing strength, although transaction multiples in general have also been higher than typical in the past five years as well. The second-highest average transaction size of the decade, $244 million, also suggests as much, as does the record median of $70 million.

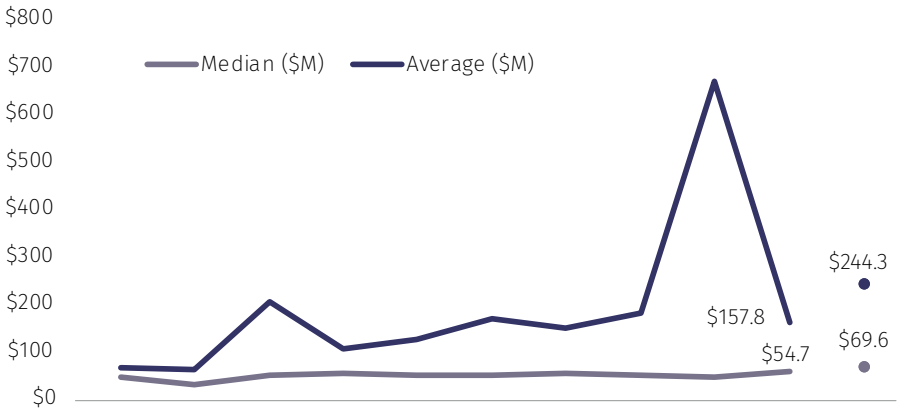
As this consolidation proceeds across the landscape, it is driven more by two key factors: established incumbents looking to harness more innovative products and services, as well as strategic acquirers looking to achieve a commanding presence within a given segment. One key area of focus that unifies elements within both of those is the trend of transitions to the cloud of multiple aspects of services and resources. "We've seen a huge uptick in the theft of cloud computing resources, for one," says Combs. "The incentives for that theft can vary considerably—currently the most significant driver is the demand for cryptocurrency mining, for example." What that degree of specificity also suggests relates to the imperative for innovation and consequent impetus for acquisitions.

US cybersecurity M&A activity



Source: PitchBook
*As of November 28, 2018

Median and average US cybersecurity M&A deal sizes



Source: PitchBook
*As of November 28, 2018

$244M

the second-highest tally of the decade

The trend of median and mean deal sizes moving in tandem suggests steady concentration and competitive bidding.

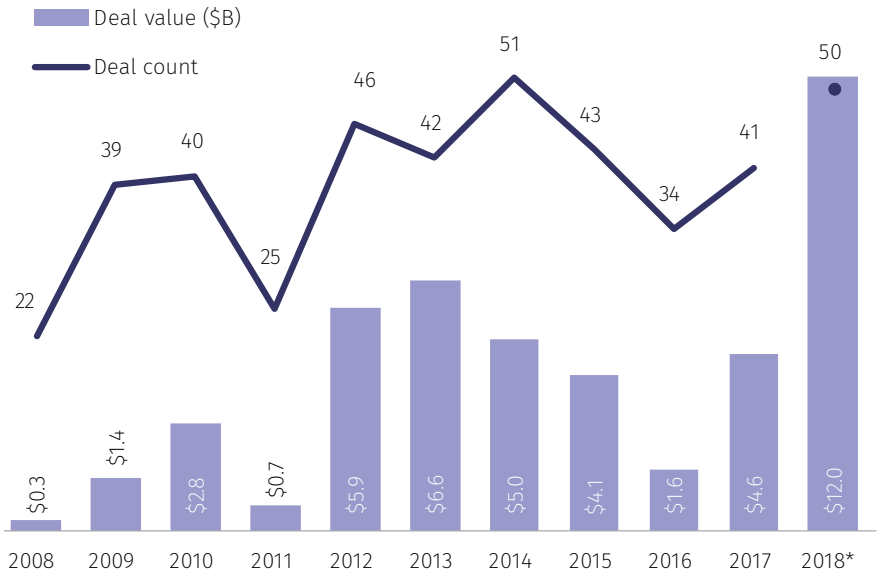
With this myriad of threats swirling amid the cloud-based space, especially concerning matters of continuity, the plethora of major acquisitions this year that skewed M&A averages higher being concentrated within cloud-centric offerings is hardly surprising. AT&T bought AlienVault, a crowdsourced threat intelligence platform, for $1.6 billion in August 2018, in just one of several notable deals. Given enterprises' all-encompassing switch to the cloud, the trend of software-focused PE firms also keeping up a healthy pace of activity, targeting the middle- and upper-segments of the middle market in the US, also underpinned robust M&A. From a portfolio perspective, PE firms are cognizant that as central hosts of multiple portfolio companies' information, security is paramount. "For corporates and PE managers, cybersecurity is at the board level across every enterprise now," says Tom Ward.

Granted, not many PE firms are primarily tech-focused in the first place, and thus the absolute tallies may not impress. However, as more take up tech investing, building out value creation theses that suit software and consequently parts of the cybersecurity universe, PE fund managers may become a more integral part of the M&A cycle going forward within cybersecurity. Thoma Bravo is already an exemplar of such a trend, having accounted for no fewer than nine acquisitions of VC-backed cybersecurity companies in the past decade. PE firms are cognizant that as central hosts of multiple portfolio companies' information, they have to be especially cognizant of security.

61

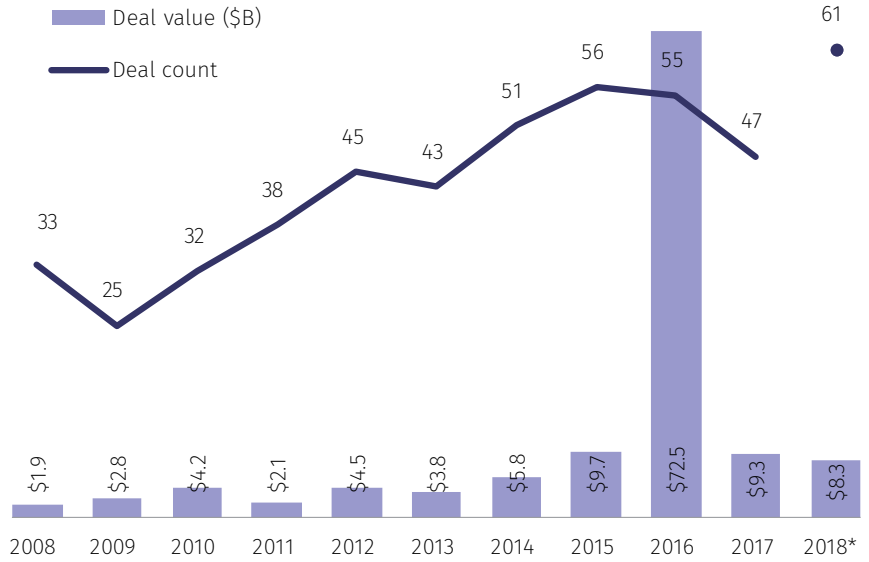
PE deals in cybersecurity in 2018 to date—a decade high

US VC-backed cybersecurity M&A activity



Source: PitchBook
*As of November 28, 2018

US PE cybersecurity activity



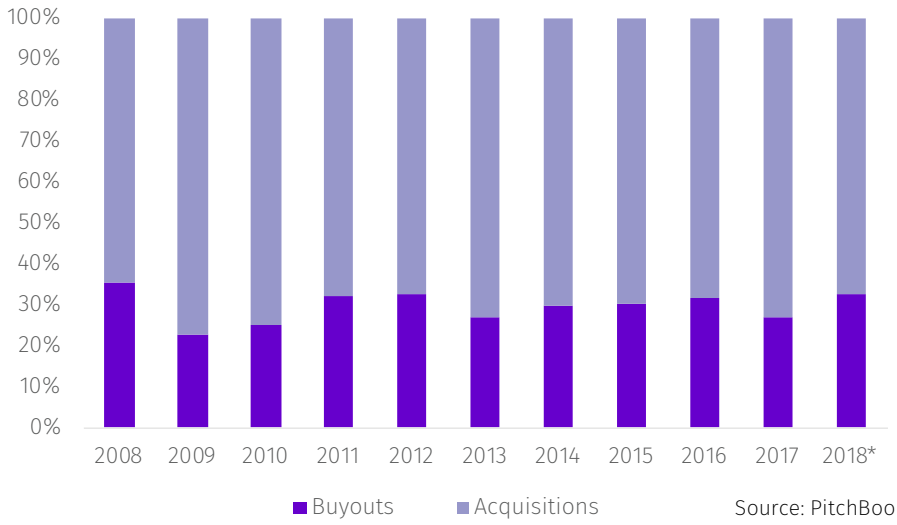
Source: PitchBook
*As of November 28, 2018

Dealmaking landscape cont.

"For corporates and PE managers, cybersecurity is at the board level across every enterprise now," says Ward.

Beyond the need for innovative products and services to bolster extant offerings, or strategic maneuvers to establish a commanding position in one segment, various regulatory frameworks that are slowly being built around cybersecurity are also compelling change and investment. "When you distill the latest array of regulations down—GDPR, for example—our clients are liable should they have a breach," says Tom Ward. Consequently, companies have yet another incentive to invest in M&A, which could serve to keep the cycle robust in the future.

US M&A (#) by sponsor type in cybersecurity



Source: PitchBook
*As of November 28, 2018

PE buyers of US VC-backed companies (2010-2018)*

Investor Name	# of Investments	Investor HQ
Thoma Bravo	9	Illinois
TA Associates Management	4	Massachusetts
Providence Equity Partners	3	Rhode Island
Vista Equity Partners	3	Texas
K1 Investment Management	3	California
Bain Capital	2	Massachusetts
Francisco Partners	2	California
Audax Group	2	Massachusetts
Welsh, Carson, Anderson & Stowe	2	New York
Marlin Equity Partners	2	California

Source: PitchBook
*As of November 28, 2018

US M&A of VC-backed companies by strategic acquirers (2010-2018)*

Investor Name	# of Investments	Investor HQ
Cisco Systems	12	California
Proofpoint	9	California
Symantec	7	California
Palo Alto Networks	7	California
Intel	6	California
CA Technologies	5	New York
International Business Machines	5	New York
Microsoft	5	Washington
Dell EMC	5	Massachusetts
VMware	5	California

Source: PitchBook
*As of November 28, 2018

About us

Donnelley Financial Solutions (DFIN)

DFIN is a leading global risk and compliance solutions company. We provide domain expertise, enterprise software and data analytics for every stage of our clients' business and investment lifecycles. Markets fluctuate, regulations evolve, technology advances, and through it all, DFIN delivers confidence with the right solutions in moments that matter.

Slam the door shut.

Why take chances with your data? Venue® from Donnelley Financial Solutions (DFIN) is the virtual data room platform that protects your most sensitive deals and transactions with industry-leading security from the ground up. Venue lets you easily manage viewer permissions, uses 256-bit encryption for system security, and is 101-compliant at the infrastructure level. For top security, here's your Venue.

DFINsolutions.com

DFIN