

Cybersecurity Proliferates Across the Venture Landscape

brought to you by



start path + Cyber & Intelligence

in association with



Executive summary

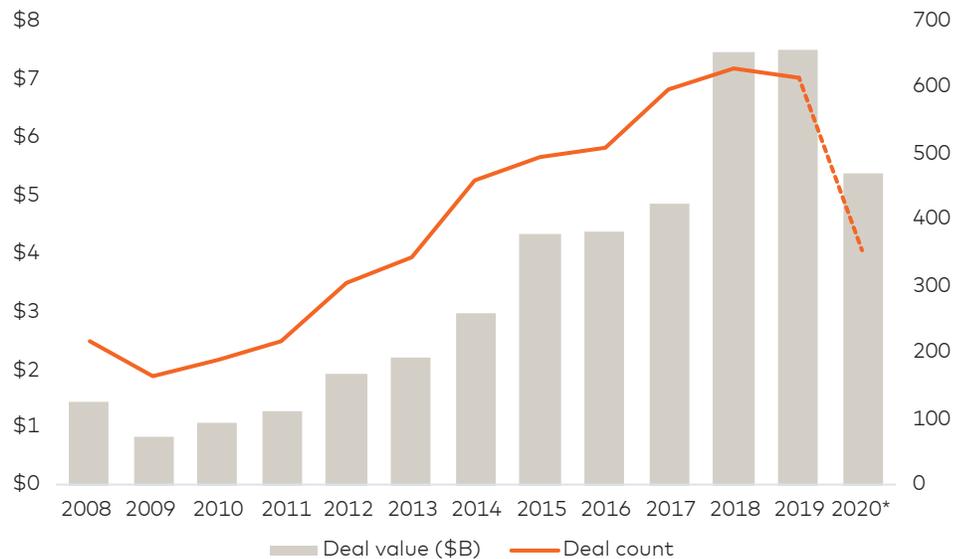
Hybridization of the digital and physical in business and everyday life continues to evolve. Cybersecurity challenges have multiplied as the march toward digitization proceeds. Particularly given the impact of the COVID-19 pandemic, shifts to remote or flexible workflows and a surge in e-commerce have underlined the need for digital security. The growing number and variety of threats can overwhelm incumbents locked into existing architectures, creating an opening for innovative players to invent new techniques and tools to help keep business systems and information flows secure.

This market review focuses on cybersecurity as it relates to financial services, payments, and the future of commerce. We address the intersection of corporate and startup innovation, venture investment, and broader industry shifts to provide a concise overview of key venture trends in cybersecurity. We also deep dive into three key segments: fintech & cybersecurity, digital commerce & identity, and cybersecurity & IoT.

KEY FINDINGS

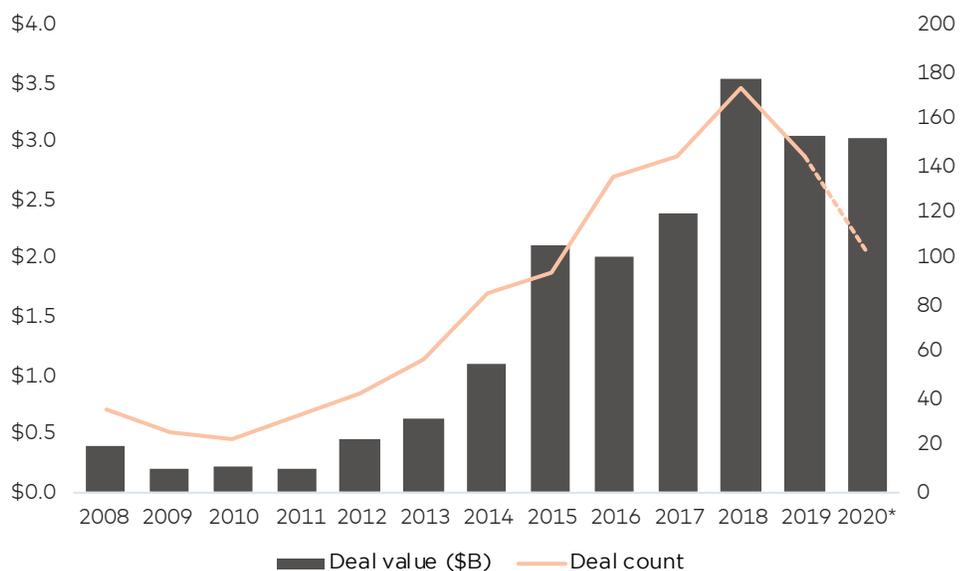
- 2020 is on pace for record VC investment, potentially to exceed \$8 billion, even as global venture funding slides slightly.
- Corporates have played an integral role in terms of both liquidity and investment, but given the market's fragmentation, the bulk of innovation still is derived from smaller, newer players.
- Upward-trending deal metrics suggest maturation and emergent category leaders in cybersecurity across IoT and identity management.

FIGURE 1.1: VC activity in cybersecurity



Source: PitchBook | Geography: Global
*As of August 18, 2020

FIGURE 1.2: VC activity in cybersecurity with corporate participation



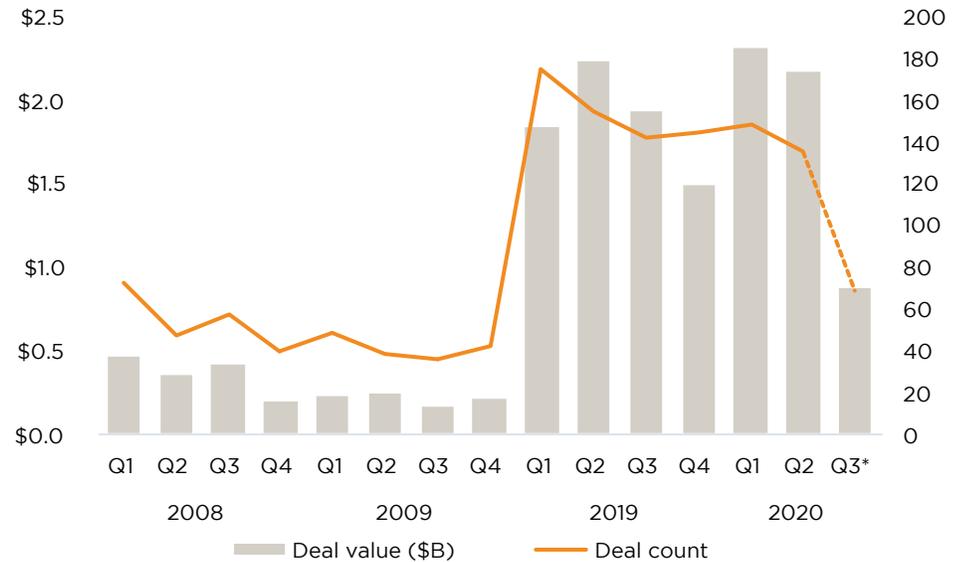
Source: PitchBook | Geography: Global
*As of August 18, 2020

Market overview

2020 is on track to be a record-breaking year for the cybersecurity vertical. The first quarter of the year already set a single-quarter record with \$2.3 billion, reaching \$5.4 billion by mid-August. While current deal pace indicates a slower third quarter at \$1.6 billion, 2020 remains on track to be the best year on record, reaching \$8.3 billion in total.

The COVID-19 pandemic did little to slow the acceleration of investment in cybersecurity, even while global venture funding is slowing; as of midyear, 2020 is on pace to record approximately \$250 billion in aggregate deal value relative to \$272.1 billion in 2019. The need for robust security systems and digital infrastructure became evident as the pandemic forced businesses to further digitize. With that shift came an uptick in attacks across multiple points in the chain of communications and commerce, from classic email phishing to multi-vector large-scale attacks. As a result, VC firms are

FIGURE 2.1: VC activity in cybersecurity by quarter

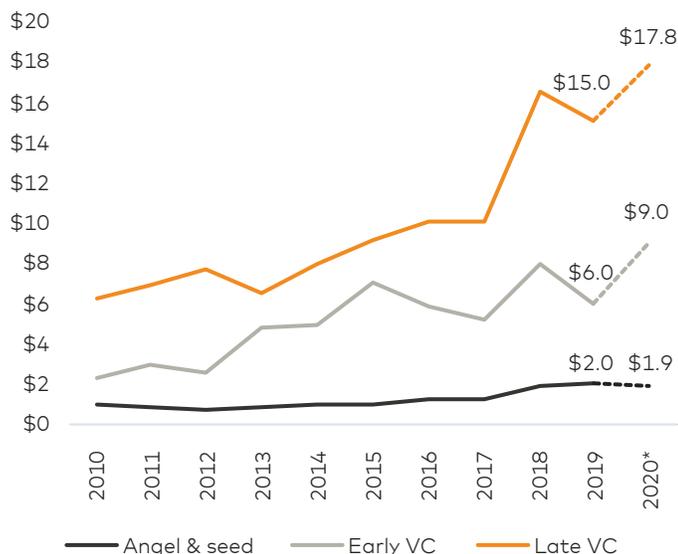


Source: PitchBook | Geography: Global
*As of August 18, 2020

plowing even more capital into well-positioned mature startups as well as diversifying into newer ventures focused on leveraging increasingly powerful DevOps and artificial intelligence mechanisms to create

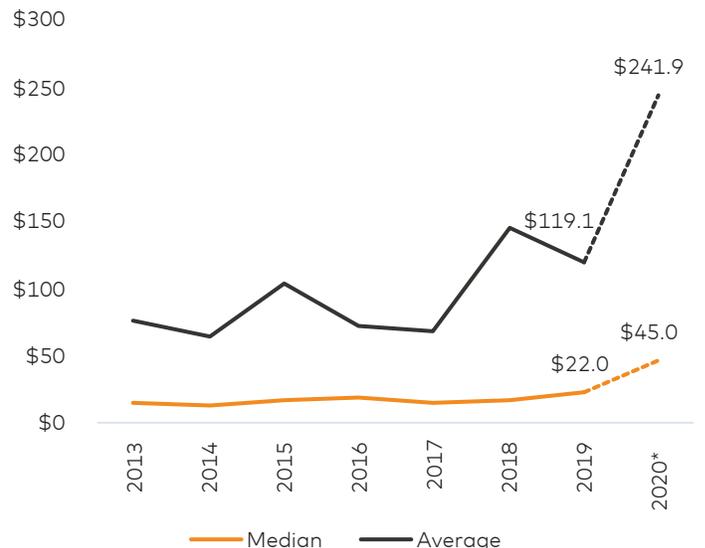
segment-specific tools for IoT and fintech, among others. Median late-stage valuations have soared to a new high; overall, albeit choppy, deal size metrics have grown more robust.

FIGURE 2.2: Median VC financing size (\$M) by stage in cybersecurity



Source: PitchBook | Geography: Global
*As of August 18, 2020

FIGURE 2.3: Average & median pre-money valuations (\$M) in cybersecurity



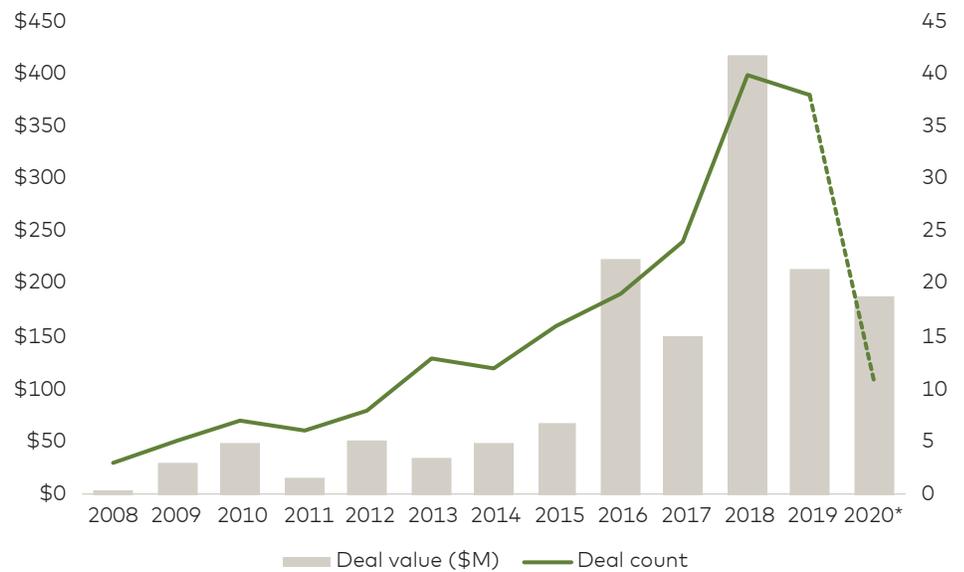
Source: PitchBook | Geography: Global
*As of August 18, 2020

Fintech & cybersecurity

The proliferation of fintech throughout the 2010s has led to the emergence of mature, venture-backed fintechs as category leaders. In turn, this has led to significant investment by incumbent financial services giants into digitization of tools and workflows. With stakes increasingly high in the mostly remote working environments prompted by COVID-19, there are a growing number of large companies across the fintech spectrum investing heavily in cybersecurity. As frictionless payments increasingly become the norm, ensuring their security—from routing remittances to executing capital markets transactions—continues to grow in importance and complexity. Not just data but controls systems and infrastructure are being attacked, often in subtle ways that lay the groundwork for future breaches rather than immediate threats. In parallel, educating financial services professionals—about the full and evolving array of sophisticated phishing, messaging, and false flaws in their tools—is an ongoing challenge. Cyber threats aside, empowering users in best practices as well as general education is likely to be a growing field.

Consequently, venture firms are also backing more new businesses that focus on security solutions for fintechs. Given the fledgling nature of the market, venture investment has not been nearly as robust as observed in other cybersecurity

FIGURE 3.1: VC activity in fintech & cybersecurity



Source: PitchBook | Geography: Global
*As of August 18, 2020

FIGURE 3.2: VC activity in fintech & cybersecurity by quarter



Source: PitchBook | Geography: Global
*As of August 18, 2020

segments, although promising signs exist. At \$189.3 million invested through mid-August in 2020 across just 11 financings, the year is off pace from the prior highs observed in 2018 and 2019 in terms of volume and VC invested (see figure 3.2). However, Q2 2020 did see the largest quarterly investment yet at \$116.2 million, which suggests some businesses are maturing and gaining ground. Corporates are also increasingly active, participating in 12 financings in 2019 (see figure 3.3); a more recent example round is the April 2020 \$12.5 million funding of Sayari, which developed a platform that helps financial institutions and multinationals mitigate risk and manage compliance related to KYC and money-laundering regulations. Alongside the flow of venture funds, more established incumbents and category leaders are redoubling resources allocated to this critical segment.

The growth in the fintech ecosystem overall as well as the massive COVID-19-driven shift to digitize commerce flows has expanded the overall market, so future inflows of capital are to be expected. Pure-play solutions will have to compete with the expansion of broader product suites into their focus areas, but segment leadership is still possible across key areas such as cryptographically secured asset management or specialized risk analytics for select fintech segments such as insurers.

FIGURE 3.3: VC activity in fintech & cybersecurity with corporate participation

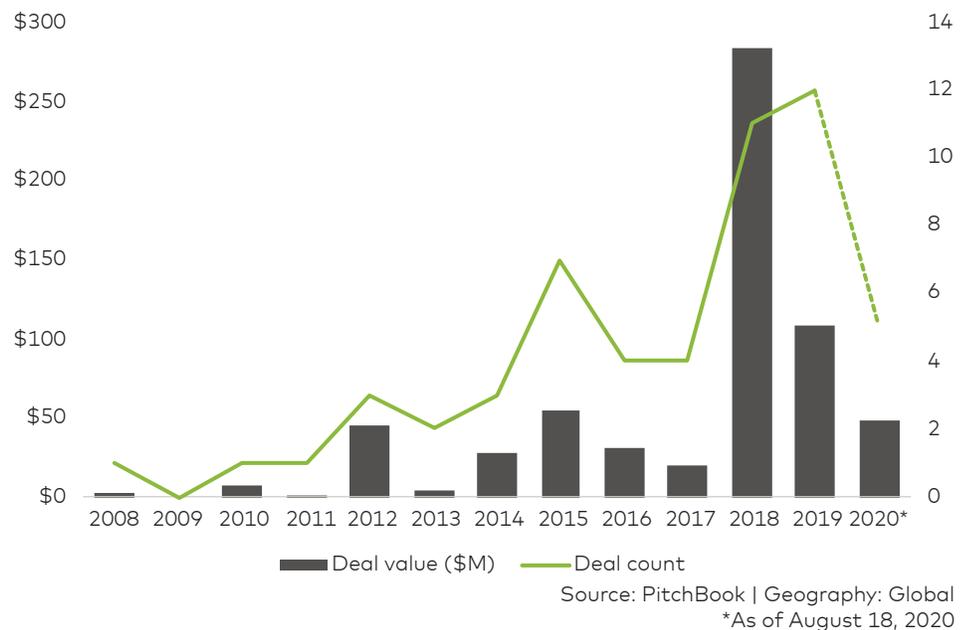
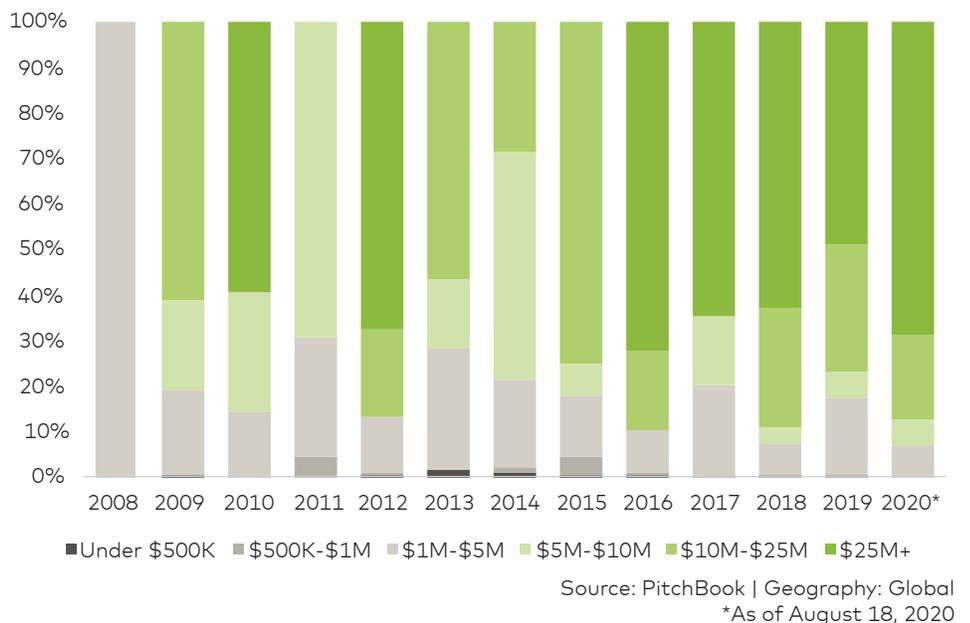


FIGURE 3.4: VC activity (\$) in fintech & cybersecurity by size

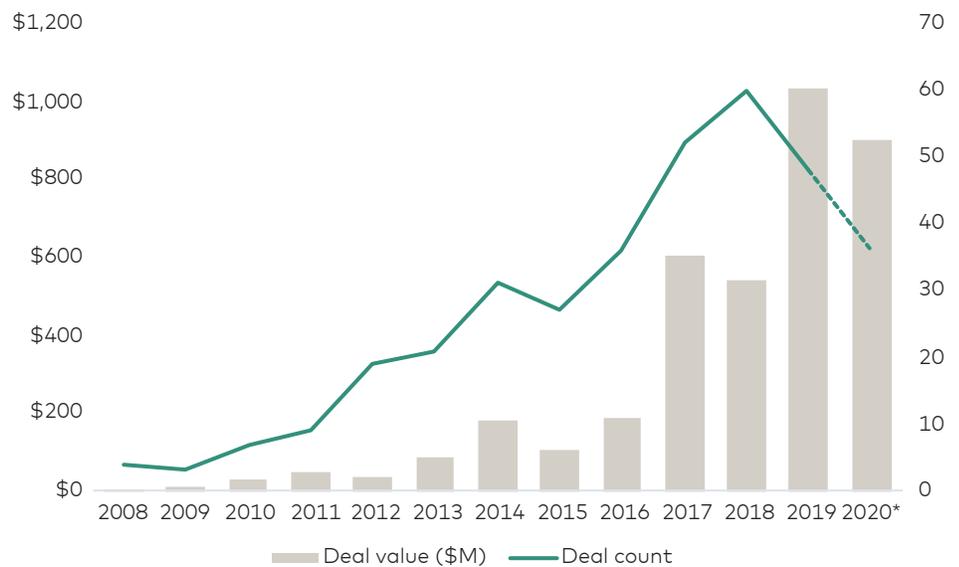


Digital commerce & identity

Fintech's internal processes and handling of data streams may preoccupy many within the cybersecurity realm, but the uptick in massive consumer identity breaches is utmost in the typical consumer's mind. As commerce and media increasingly move online, digital identities are becoming more unified across the major tech platforms as they consolidate their market share and relative power. However, multifarious consumer profiles—often linked by relatively similar security protocols given the popularity of two-factor authentication, single password prompts, and usernames alone—still exist, scattered across the array of business websites visited.

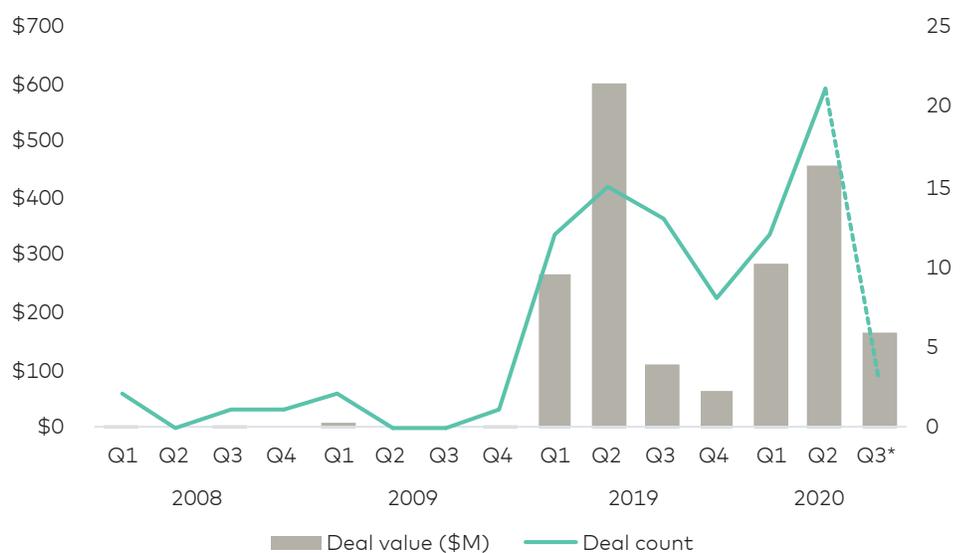
These streams of digital commerce, laden with individuals' personal information, are flowing more heavily as 2020 progresses, presenting targets ripe for simple-to-complex hacking methods. Theft of credit card information, government identity, and other personal data is too lucrative for bad actors to resist. Simply put, legitimate business innovation/investment still lags behind criminal schemes. As businesses and consumers share the blame for lax security protocols, considerable amounts of capital and investor interest are being directed to developing solutions to secure both entities. Techniques include monitoring queries for personal information based on a website's authentication protocol and location, plus tools for businesses or consumers to transform their passwords in a variety of ways, such as employing more secure numeric certificates. Centralized platforms for monitoring multiple accounts at the organizational level are also garnering funding, as are customer-verification tools.

FIGURE 4.1: VC activity in digital commerce & identity



Source: PitchBook | Geography: Global
*As of August 18, 2020

FIGURE 4.2: VC activity in digital commerce & identity by quarter



Source: PitchBook | Geography: Global
*As of August 18, 2020

Although it is relatively early days, and there is stiff competition from incumbent technology giants, venture funding has surged for startups targeting the digital commerce & identity space, peaking at 60 financings in 2018, with an aggregate of nearly \$2.5 billion invested from 2018 to mid-August 2020 (see figure 4.1). 2020 is well on pace to exceed any other single-year tally, however. Quarter-over-quarter comparisons yield a significant uptick for Q2 2020 over Q2 2019 in terms of volume, although VC investment shrank somewhat. Given the size of this market, it is important to recognize that outlier financings can skew results, as was the case with Auth0's \$120 million funding in July of 2020. However, barring any significant moves by incumbents, or pivots by tech giants, it is hard to foresee anything but continued investment flows into this space. A key theme for the wide-ranging arena of cybersecurity is that as threats and methods of attack evolve, so too will solutions, which will require a proliferation of innovators from both individual enterprises and nimble teams across larger organizations. Consequently, there has been significant investment in development and VC by corporate players; they joined in a record aggregate of VC invested across 16 financings, topping 2019's tally of \$447.4 million by well over \$200 million (see figure 4.3). It is difficult to imagine such interest will slacken any time soon, so we expect significant capital flows into this space going forward.

FIGURE 4.3: VC activity in digital commerce & identity with corporate participation

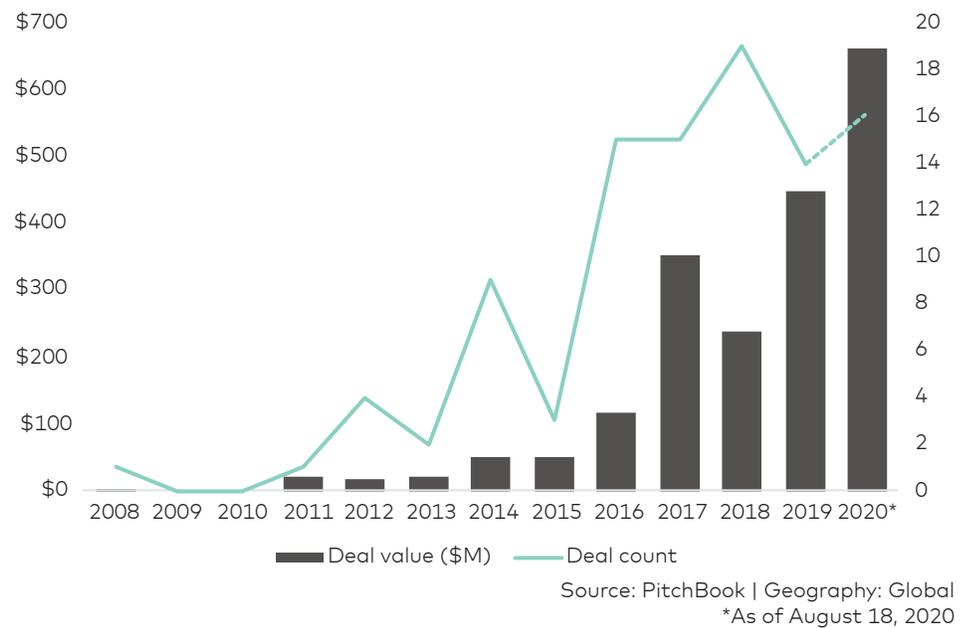
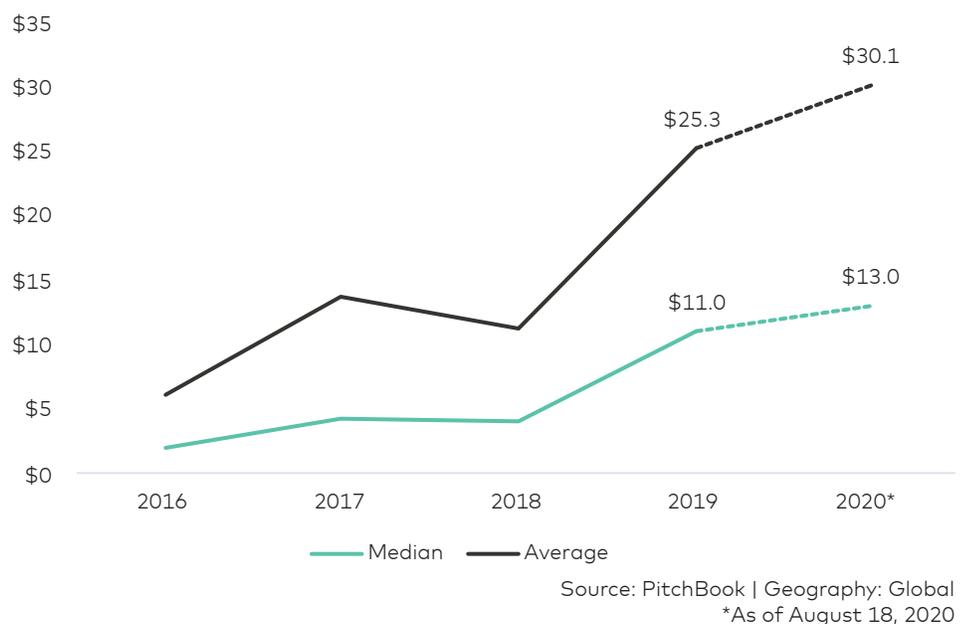


FIGURE 4.4: Average & median VC financing size (\$M) in digital commerce & identity



Cybersecurity & IoT

The Internet of Things (IoT) has enjoyed ups and downs in its hype cycle, but as is usual in the development cycle of a budding technological field, progress has remained steady. Taking advantage of advances in general connectivity, near-field communication (NFC), and the onset of 5G wireless, entrepreneurs and larger tech companies alike have been developing devices and tools for multiple use cases. The working conditions resulting from COVID-19 have made an urgent case for connected smart homes, factories, offices, and warehouses to better monitor and respond to shifting conditions. Each of those primary location categories has different needs, but given the rise of flex-location workflows, consumer considerations are taking precedence more and more in 2020. Residences and offices are primarily geared toward ideal working conditions for people with respect to comfort, efficiency, and hygiene. Using residences as an example, especially with flex-location workflows likely to become more popular, home networks will increasingly interact with critical business systems and thus must also be secured. Interoperability across all devices also lays bare some potential security vulnerabilities, particularly when it comes to smart wearables and broader home wireless networks. Accordingly, access attempts or logins across any types of devices into business accounts and tools will all have to be monitored, especially per the types of requests being made.

FIGURE 5.1: VC activity in IoT & cybersecurity

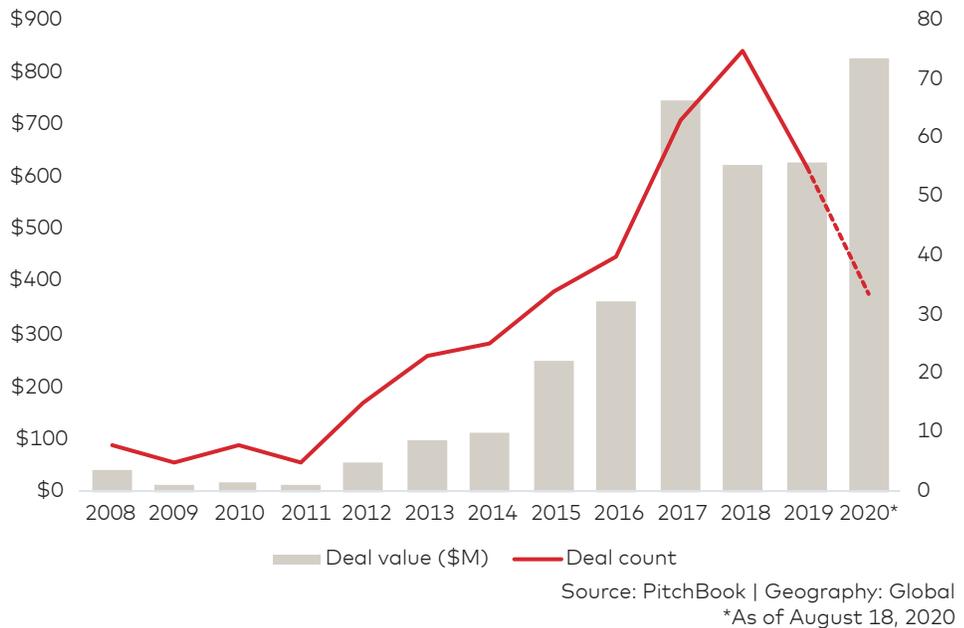
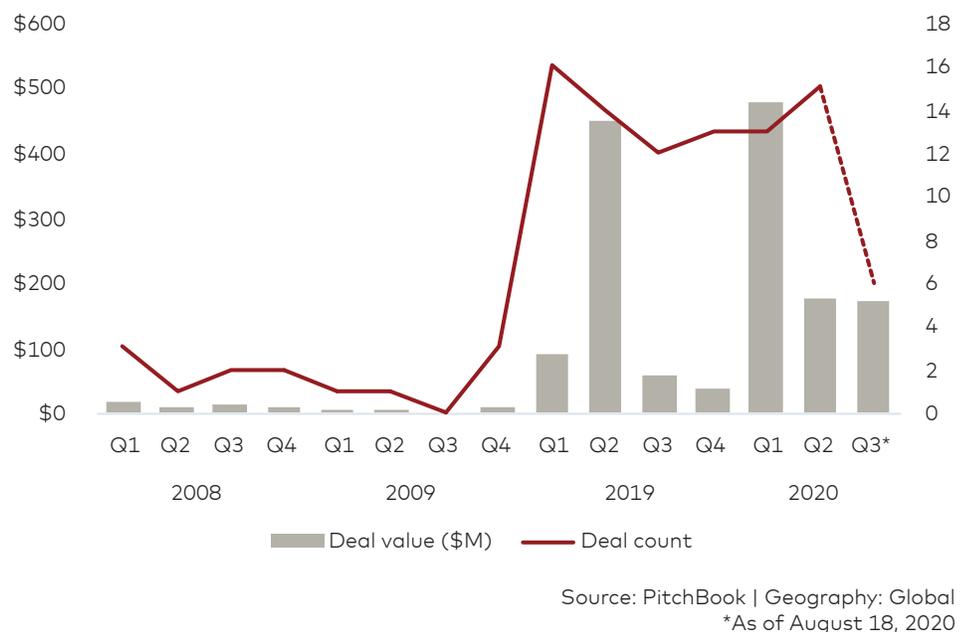


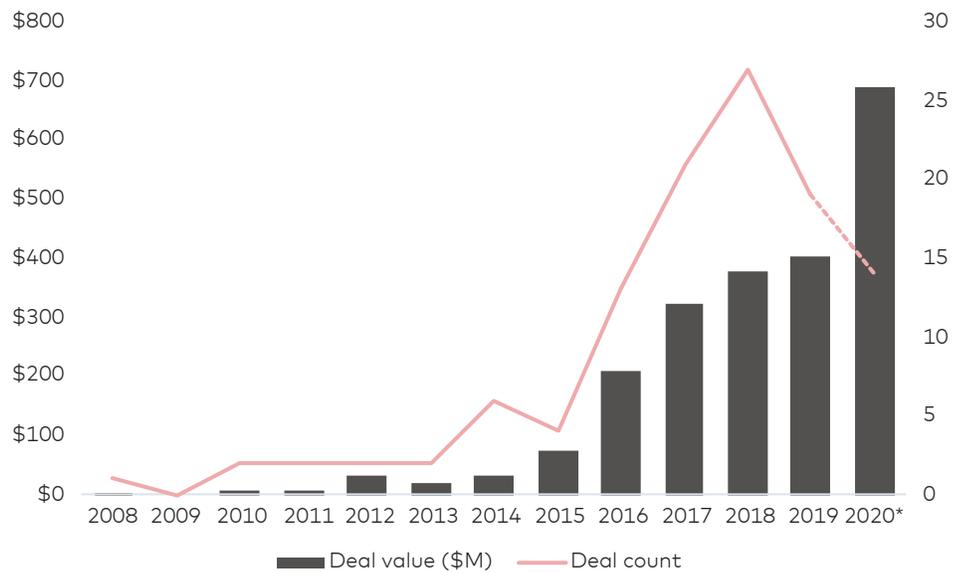
FIGURE 5.2: VC activity in IoT & cybersecurity by quarter



With such a compelling market opportunity, VC investment has flooded into enterprises targeting the confluence of cybersecurity and IoT over the past several years. 2020 has already seen a record high of nearly \$830 million in venture invested, eclipsing the previous high of \$748.6 million set in 2017 (see figure 5.1). Although volume has slowed considerably, suggesting that market and/or category leaders may be emerging and raising larger and larger sums, Q2 2020 still saw 15 completed rounds, just a single financing higher than the tally seen in Q2 2019 (see figure 5.2). However, 2020 has observed more consistent funding flows, with Q1 bolstered by outlier rounds to notch \$478.0 million invested yet Q2 recording \$176.0 million and Q3 \$172.9 million by mid-August. That pace potentially puts Q3 on target to surpass \$300 million, one of the more robust single quarters on record.

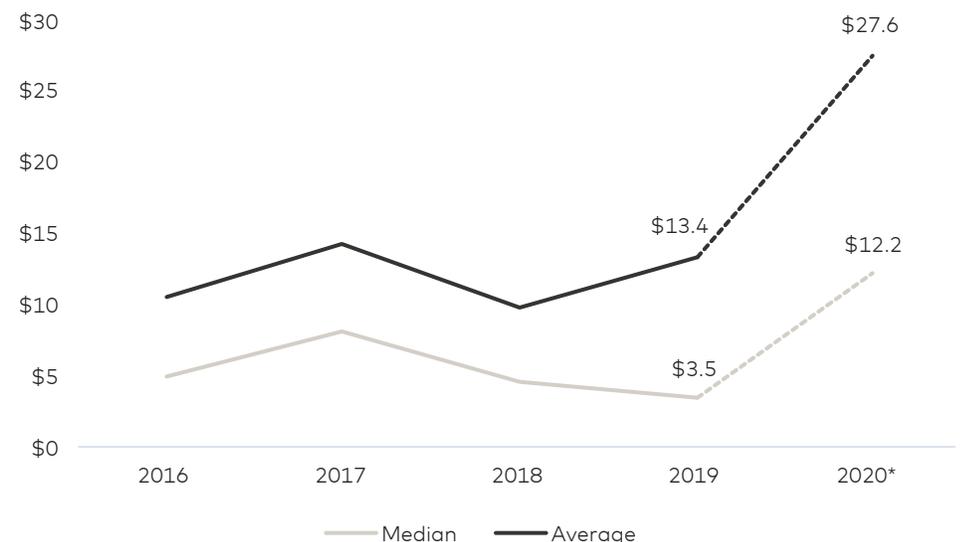
Given the variety of use cases within this space, it is not surprising that corporate players have contributed to a record amount of deal value thus far this year, and, moreover, have been involved in dozens of rounds over the past several years (see figure 5.3). As is common when more established traditional and corporate venture firms participate, average financing sizes have skewed upward with a handful of companies garnering significantly sized rounds. The median has also soared to a new high in 2020 year to date (see figure 5.4), likely due to the unique deal-making conditions this year in which only the most robust businesses are readily securing funding.

FIGURE 5.3: VC activity in IoT & cybersecurity with corporate participation

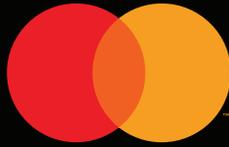


Source: PitchBook | Geography: Global
*As of August 18, 2020

FIGURE 5.4: Average & median VC financing size (\$M) in IoT & cybersecurity



Source: PitchBook | Geography: Global
*As of August 18, 2020



start path
wave **17**



to find out more about our new wave of startups visit
startpath.mastercard.com

