WELLS FARGO

Digital Safeguards

Prioritizing cybersecurity at the corporate level

Data provided by PitchBook

WELLS FARGO

The opportunities and risks of a more connected world

"The future is here." While different people have said it in different contexts and in different years, it's a timeless quote that captures the sentiment of how quickly things can change without our noticing. The most recognizable context for the quote revolves around technology and the growing need to keep pace.

In conjunction with PitchBook, a private markets data provider, Wells Fargo is releasing a series on the opportunities and risks of today's technology sector. This report covers cybersecurity, which plays a quiet but critical role in keeping the broader digitized economy intact.

This series, guided by our industry experts, is geared toward a corporate audience. PitchBook Data has provided numbers that help contextualize these trends as they play out in the venture capital, private equity and M&A markets. Deals and investments happen every day, but as any dealmaker knows, every transaction has a thesis behind it. When many similar transactions begin to happen across entire industries, it often means something bigger is going on.

For more insights on cybersecurity and tech, please visit us at welcome.wf.com/tech-banking.

WELLS FARGO

Introduction

A digitized world brings many benefits, both for individuals and the for the broader economy. Things are less expensive, more personalized, and easier to use. Over time, those benefits become addictive, which, in turn, spurs companies to find ways to digitize more aspects of our everyday lives. As we automate and simplify our daily tasks and experiences, more data is required, almost all of which must be stored online.

As larger portions of the economy migrate online, the task of keeping information secure becomes increasingly challenging. Security breaches are an unavoidable reality in today's connected world. Smart devices that are secure today might not be tomorrow, and companies that cannot keep customer data secure might not survive for long.

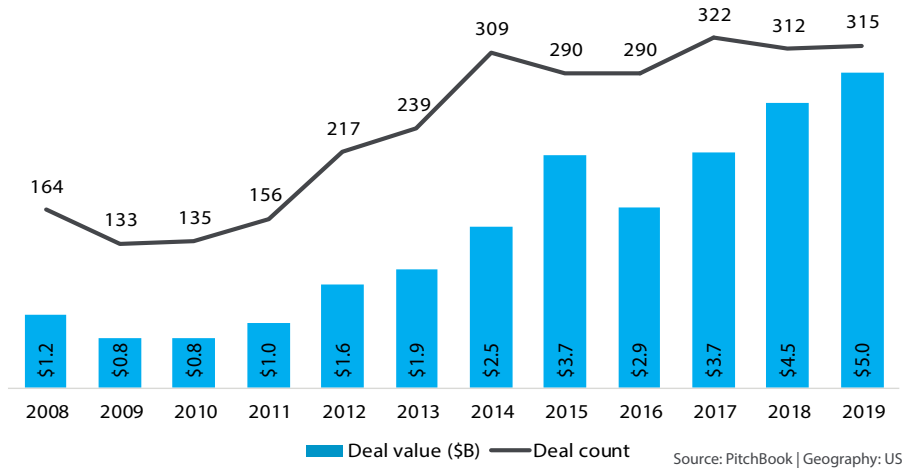
Cyber attacks occur for multiple reasons. All data hacks, whether they target social media companies, airlines or jewelry stores, seek to capture personal information for later, targeted use. Much of that information is sold on the black market, and some information is more valuable than others. Many attackers take a long-term approach, collecting personal information over time in order to tailor future attacks to particular individuals. According to Clearwater, a cybersecurity consulting firm, individual medical records are ten times as valuable as credit card numbers on the black market. As more devices are connected and more information is stored online, the number of potential targets available to hackers exponentially increases.

The vulnerability of innovation

The venture capital (VC) ecosystem incubates several new markets that promise to change the way we live and work. The push to design and manufacture technology-infused products is largely centered within Silicon Valley, which has increasingly backed the cybersecurity market alongside its push for more sophisticated gadgets. The last five years have been remarkably consistent in volume, suggesting a large ecosystem of startups addressing an even larger ecosystem of potential customers.

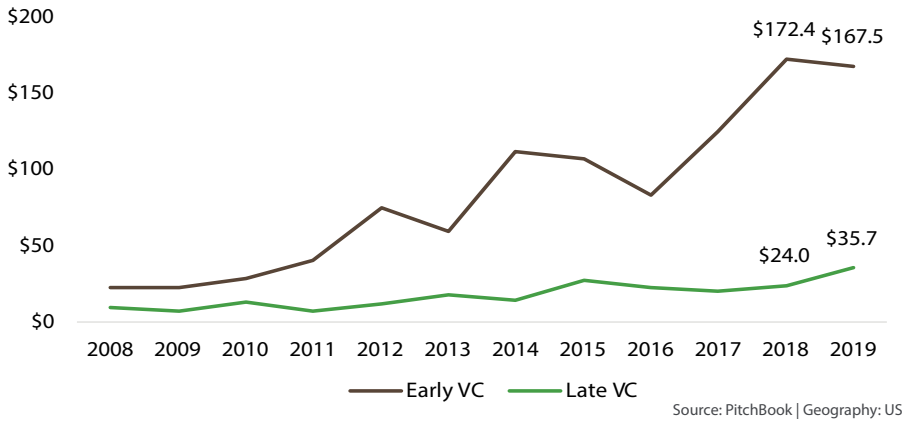
The Internet of Things (IoT), for example, comprises a promising set of technologies that will significantly affect several pockets of the economy. The dynamics of the IoT ecosystem dictate that the first to market generally sets price points and market dominance. That dynamic plays well

Venture capital activity in cybersecurity by year



Source: PitchBook | Geography: US

Venture capital valuations ($M) in cybersecurity startups by year



Source: PitchBook | Geography: US

WELLS FARGO

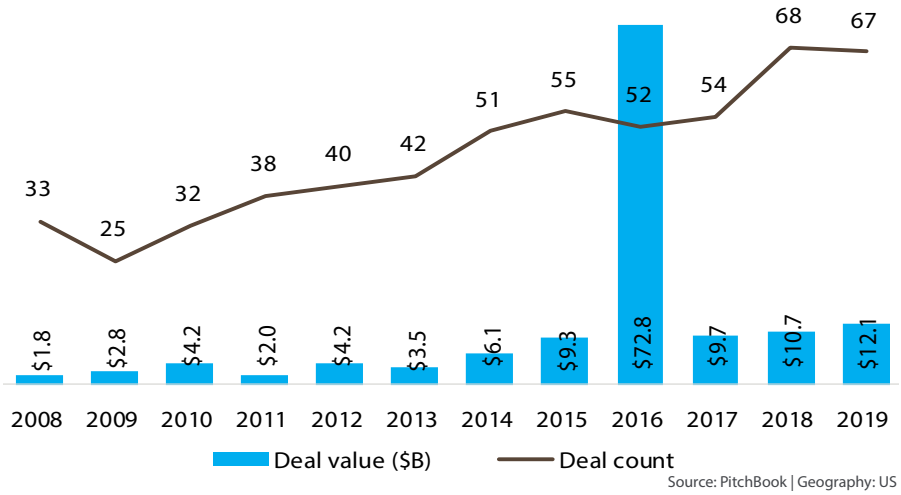
with the VC model, which works best with fast timelines. From a security standpoint, however, that dynamic is decidedly unhelpful. Optimal security takes time to configure and drives substantial cost increases due to time constraints placed on re-engineering and recoding those products.

Vulnerabilities aren't isolated to individual products, however. New markets also emerge at rapid speeds and tend to invite more scrutiny from hackers, thanks in part to a greater reliance on data. Personal information is core to new markets like wearables and DNA testing. Security providers have yet to fully understand the potential impact of a successful attack on a large DNA company, for instance.

Companies that enjoy early success and gain massive audiences in short periods of time tend to have difficulty adopting to scale. Older companies face different (but no less significant) challenges. While younger companies can benefit from engineering and building their products using the latest technology available, older technology companies often struggle to keep re-engineering their legacy products.

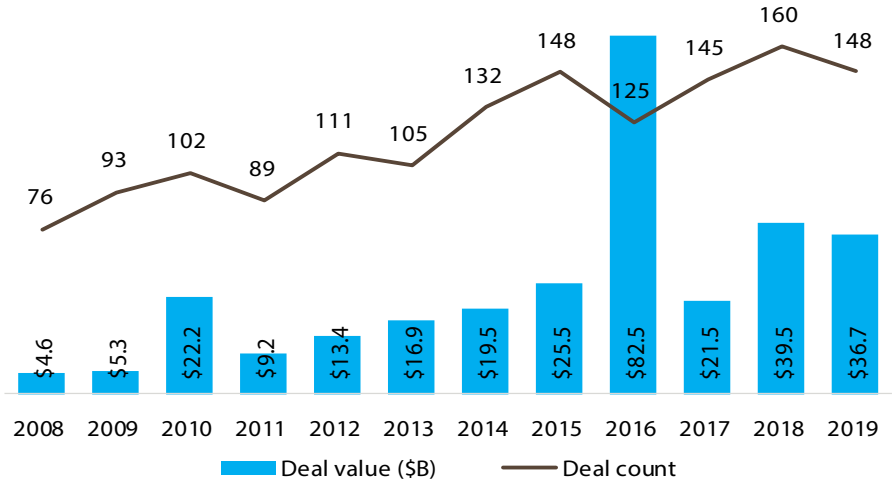
For both young and old companies, however, software complexity increases while a simplified user experience becomes more critical for market viability. Products have to be simple for users yet remain compatible with a range of media platforms and devices, which increases their vulnerability to cyber-attacks. It remains to be seen what level of security can be ensured at various levels of the economy, as each segment and corner of the broader market presents their own unique business challenges.

Private equity activity in cybersecurity by year



Source: PitchBook | Geography: US

M&A activity in cybersecurity by year



Source: PitchBook | Geography: US

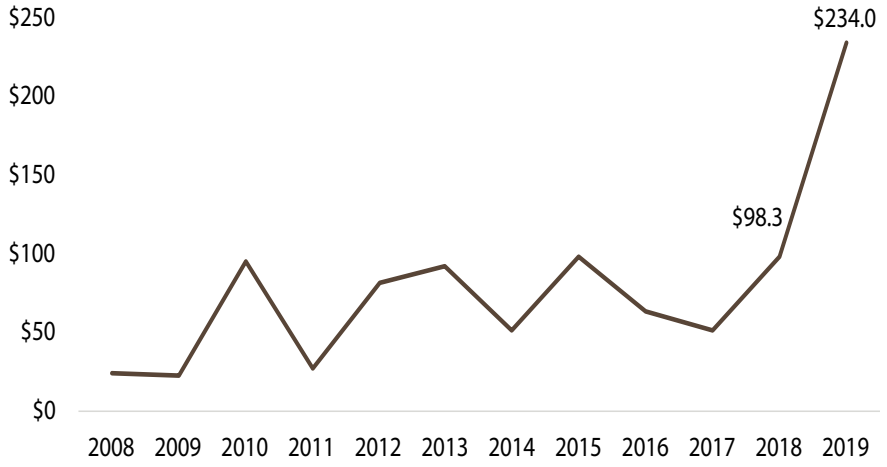
Security at the corporate level

Outside of 2016, which saw the largest cybersecurity-related transaction in history (the $67 billion Dell/EMC merger), mergers & acquisitions (M&A) activity has been consistently high since the financial crisis. In 2019, about $37 billion was spent on cybersecurity M&A through 148 transactions, just off the record 160 transactions in 2018. PE volume has likewise remained strong, with another $12 billion invested in 2019 through 67 deals. The prior year saw $10.7 billion invested through 68 transactions. A significant volume of smaller, private technology companies reflects the cyclical dynamic between these specialty shops and their large multinational counterparts.

When cybersecurity became a popular commercial offering, a wave of boutique private companies emerged. As they matured, the cybersecurity industry witnessed a range of acquisitions by larger technology companies that realized they lacked the agility of newer startups. Adaptation was achieved through M&A.

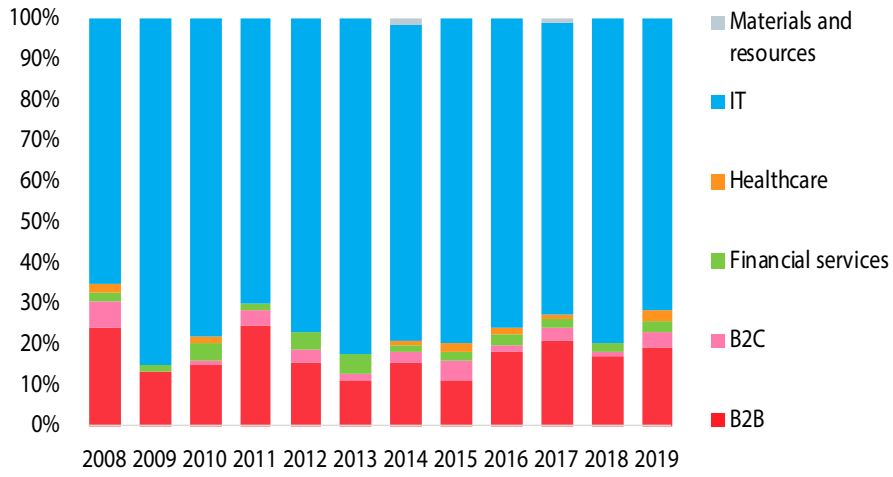
Yet, as the cybersecurity industry itself evolves, the need for highly specialized and niche experts becomes paramount. Security companies no longer pursue "do-it-all" products. As recent history has shown, single solutions don't generate the same benefits as they once did. Companies instead pursue capabilities that can be customized to fit varying operating models and a wider range of applications. For example, the automotive and medical sectors are two industries that rely on niche security expertise. Here, smaller private companies lead the effort on developing the technology required to continue pursuing product innovation.

Median M&A cybersecurity deal size ($M) by year



Source: PitchBook | Geography: US

M&A (#) in cybersecurity by industry



Source: PitchBook | Geography: US

Trends in the larger ecosystem

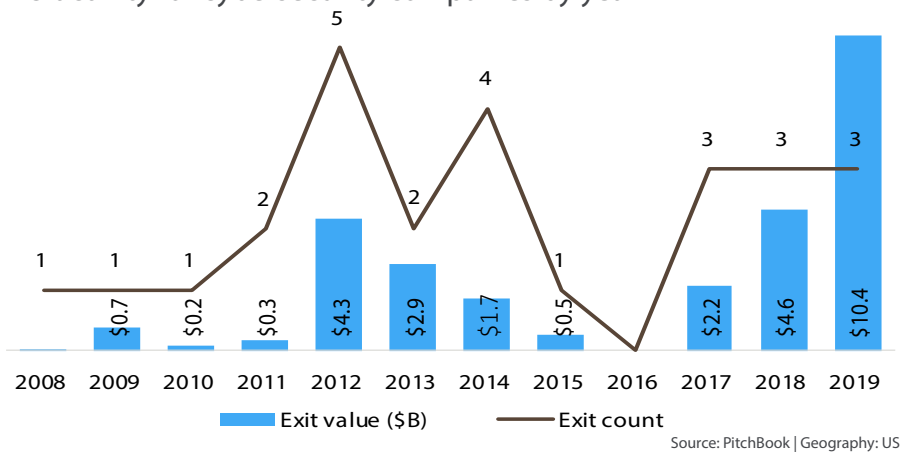
Technology itself will continue to change, virtually assuring a robust market in the near- to medium-term for both conventional and emerging security solutions. The threats themselves will remain specific to the companies being targeted, and the companies that are attacked will need to maintain adequate security measures to minimize potential fallout. Moreover, technology dynamics will continue to change within industries themselves, which will uphold today's trend toward specialized capabilities instead of single solutions.

One way a business can measure the broader market's direction and priorities is by observing M&A trends. The cybersecurity market has seen significant consolidation in recent years as providers seek to amass several solutions to meet the needs of a broad variety of clients. More than other industries, the cybersecurity market will likely replenish itself at a faster rate, as new providers form and offset the consolidation trends seen at the highest end of the market.
As governments around the world become increasingly involved, they strengthen data privacy regulation and design stricter penalties for companies that fail to protect their data appropriately. Companies and individual users are approaching a crossroads with respect to data ownership. As digital information becomes more valuable to hackers, users may try to reclaim their data to the extent they can. As those attempts gain traction, however, it will become more apparent to society at large that data, while easy to capture, is difficult to remove once it is attached to an ecosystem.

Technological development has never been as fast as it is today, and security risks will keep evolving as technology itself evolves and new applications emerge.

Given these developments, companies should treat cybersecurity like any other business risk, weighing its cost against potential impacts.

IPO activity for cybersecurity companies by year



Source: PitchBook | Geography: US

Summary

Smart devices that are secure today might not be tomorrow, and companies that cannot keep customer data secure might not survive for long.

All data hacks, whether they target social media companies, airlines or jewelry stores, seek to capture personal information for later, targeted use. For example, according to cybersecurity consulting firm Clearwater, individual medical records are ten times as valuable as credit card numbers on the black market.

The dynamics of the startup ecosystem dictate that the first to market generally sets price points and market dominance. From a security standpoint, however, the first-to-market dynamic presents significant issues. Security providers have yet to fully understand the potential impact of a successful attack on a relatively large DNA company, for instance.

Moreover, technology dynamics will continue to change within industries themselves, which will uphold today's trend toward specialized capabilities instead of single solutions.

While more data stored online has resulted in many benefits—improved business decisions, enhanced user experiences and further inroads in overall innovation—companies and individual users are approaching a crossroads with respect to data ownership.

Technological development has never been as fast as it is today, and security risks will keep evolving as technology itself matures and new applications emerge. Given these developments, companies should treat cybersecurity like any other business risk, weighing its cost against potential impacts.

Yonesy Nunez, Group Information Security Leader, Wells Fargo Enterprise Information Security

Yonesy F. Nunez is the Group Information Leader for Wholesale, Wealth & Investment Management (WIM) and International for Wells Fargo Information Security (IS). He is responsible for ensuring effective business and global IS alignment while promoting and inculcating appropriate information security risk management practices across the Wholesale, WIM and International operational culture with the aim to effectively protect the firm's data and its various information assets. He has held similar roles with Citigroup, PwC, The New School and The Pall Corporation. He holds a doctorate from Pace University in Professional Studies in Computing.

TECHNOLOGY BANKING

- GLOBAL TREASURY MANAGEMENT
- PAYMENTS
- FOREIGN EXCHANGE
- CREDIT AND TRADE
- INVESTMENT BANKING*
- WELLS FARGO STARTUP ACCELERATOR

A better perspective can help you build a better future for your company.

Our experience in areas such as financing, treasury management, M&A, and more runs deep through the tech community. So whether you're expanding or launching in a new market, Wells Fargo has the financial and intellectual capital to help you build toward your next step. We'll help you build the future.

wellsfargo.com/techbanking

*** INVESTMENT PRODUCTS:**

Not Insured by FDIC or any Federal Government Agency	May Lose Value	Not a Deposit or Guaranteed by a Bank of Any Bank Affiliate

*Wells Fargo Securities is the trade name for the capital markets and investment banking services of Wells Fargo & Company and its subsidiaries, including but not limited to Wells Fargo Securities, LLC, a member of NYSE, FINRA, NFA and SIPC, Wells Fargo Prime Services, LLC, a member of FINRA, NFA and SIPC, and Wells Fargo Bank, N.A. Wells Fargo Securities, LLC and Wells Fargo Prime Services, LLC are distinct entities from affiliated banks and thrifts.