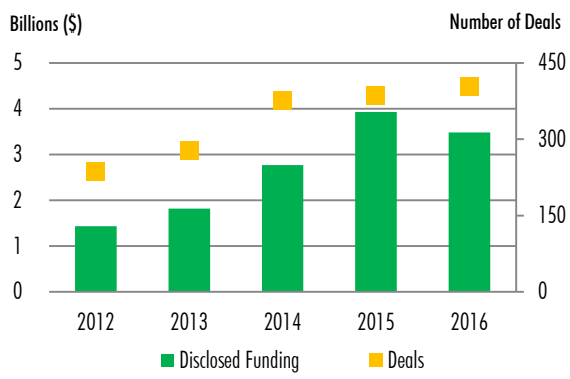
Cybersecurity under the New Administration and CRE implications

Federal and private investment in cybersecurity remains on the rise

Congress passed a stopgap bill on Friday to fund the government through May 5th, allowing lawmakers more time to reach an agreement on an omnibus bill to keep the government open through the end of the fiscal year (September 30th). In line with his focus on national security, President Trump has stated plans to make cybersecurity a priority and is working on an executive order addressing federal IT modernization and cybersecurity initiatives. Additionally, the President's FY 2018 budget proposes $1.5 billion for the Department of Homeland Security to safeguard federal networks and critical infrastructure. While both the executive order and budget proposal have yet to materialize, the increased focus on cybersecurity points to potential increase in activity for the cybersecurity industry.

Cybersecurity Historical Financing



Source: CB Insights, The 2016 Cybersecurity Recap, Q1 2017.

Private investment in cybersecurity has also seen substantial growth in recent years. Following a record year in 2015 with more than $3.9 billion of private capital investment in the sector, investment volume ended 2016 with over 400 deals totaling $3.5 billion. The D.C. metro region—along with San Francisco, New York, Boston and Los Angeles—is among the top U.S. recipients of cybersecurity venture capital.

"War for talent"

The cybersecurity industry has posted job growth in virtually every major U.S. market. The high volume of job openings, coupled with a lack of qualified candidates, has led to a "war for talent" among cybersecurity firms.

With more than 100,000 current cybersecurity-related employees, the Baltimore/Washington corridor has the most robust cybersecurity workforce in the U.S. The total of 58,000 job openings also outpaces all other U.S. markets, underscoring the sector's continued expansion in the region.

Cybersecurity Workforce by Market

Market	Current Employees	Current Openings
Washington, D.C.	83,586	47,186
New York	52,199	27,093
San Francisco / San Jose	28,851	20,375
Los Angeles	25,805	13,675
Chicago	24,120	13,177
Dallas	24,830	12,202
Atlanta	21,413	10,709
Baltimore	22,091	10,484
Boston	15,524	8,666
Denver	9,775	6,878

Source: cyberseek.org, Q2 2017.

Implications for the regional real estate markets

Cybersecurity companies need to develop both short-term and long-term strategies to manage their corporate real estate needs. Proper space planning can help facilitate growth efforts without interrupting business continuity, as well as maximize capital investment and contract revenue.

For cybersecurity firms contracting with the federal government or partnering with a contractor, secure facilities such as Sensitive Compartmented Information Facility (SCIF) and Network/Security Operation Center (NOC/SOC) may be required. Upfront costs of these specialty spaces can be substantial if not properly negotiated.

Effective real estate planning—with considerations for location, transit accessibility and amenities—can contribute to employee recruitment and retention, which is crucial in today's competitive labor market environment.

Recent Cybersecurity Leases

Tenant	Address	Submarket	Market	SF	Sign Date
ManTech	14280 Park Meadow Dr	Route 28 South	Northern Virginia	59,958	Q2 2016
Raytheon BBN	1300 N 17th St	Rosslyn	Northern Virginia	42,490	Q1 2017
Fidelis Cybersecurity	4500 East-West Hwy	Bethesda/Chevy Chase	Suburban Maryland	33,000	Q2 2016
Copper River Information Technology	4501 Singer Ct	Route 28 South	Northern Virginia	23,666	Q4 2016
LookingGlass Cyber Solutions	10740 Parkridge Blvd	Reston	Northern Virginia	20,749	Q3 2016

Source: CBRE Research, Q2 2017.