Statement of Venky Ganesan
Managing Partner, Menlo Ventures
Chair, National Venture Capital Association
before the U.S. Senate Committee on Commerce, Science and Transportation:
"The Promises and Perils of Emerging Technologies for Cybersecurity"

March 22, 2017

Chairman Thune, Ranking Member Nelson, thank you for the opportunity to testify before the Senate Committee on Commerce, Science, and Transportation today. My name is Venky Ganesan and I serve as one of the Managing Partners of Menlo Ventures. Menlo Ventures is one of the oldest (41 years) venture capital firms in Silicon Valley. We manage approximately $4.5 billion in assets and have invested in over 400 portfolio companies whose aggregate value if held post going public would be over $200 billion. We have been fortunate to be early investors in many iconic companies, including F5 Networks ("FFIV"), Gilead Sciences ("GILD"), Hotmail (acquired by Microsoft), Siri (acquired by Apple), and Uber. We also have a long and successful history investing in cybersecurity. Menlo Ventures was the lead investor in Q1 Labs, which was acquired by IBM and has now become a major part of IBM Security. Additionally, Menlo was also the lead investor in IronPort, which was acquired by Cisco for $830 million and is a critical part of Cisco Security. I was one of the lead investors and was on the board of Palo Alto Networks ("PANW") which today has a market capitalization of over $10 billion. I am here today in my capacity as Chair of the National Venture Capital Association (NVCA), which advocates for pro-entrepreneurship policies that create jobs and grow the U.S. economy.

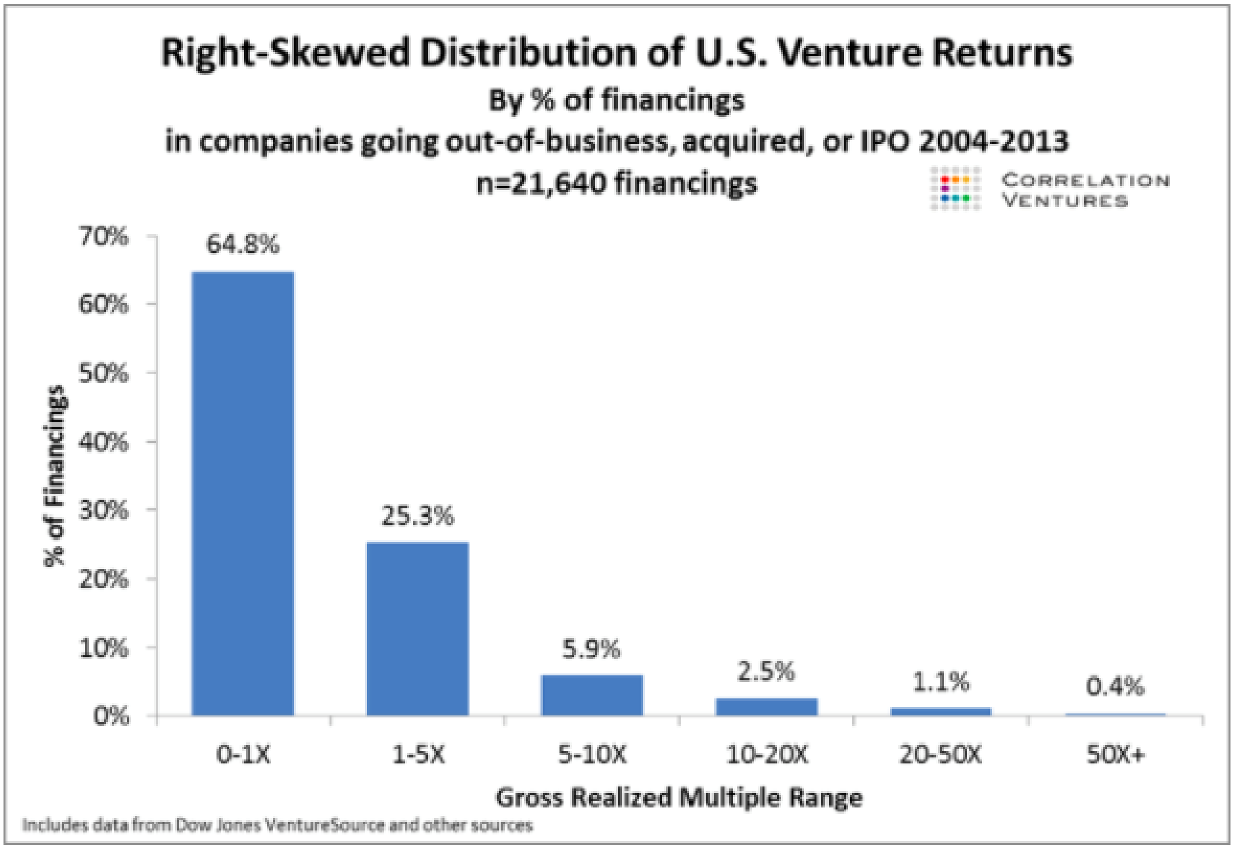
Venture Capital and Entrepreneurship

Venture capital and entrepreneurship go hand in hand. Some people mistake venture capital as a passive investing function in which venture capitalists pick companies, write checks, and then wait for the returns to roll in. While that would be nice, the reality is much different. A better analogy to understand the relationship between venture capitalists and entrepreneurs is to think about startups like a baseball team. The entrepreneurs are the players on the field. The venture capitalists are the coach and the managers. Ultimately, the players need to deliver on the field and that is what entrepreneurs do. However, as the coach/manager, venture capitalists help recruit players, negotiate contracts, run training sessions, make real-time tactical decisions during the game, and decide on the playing roster.

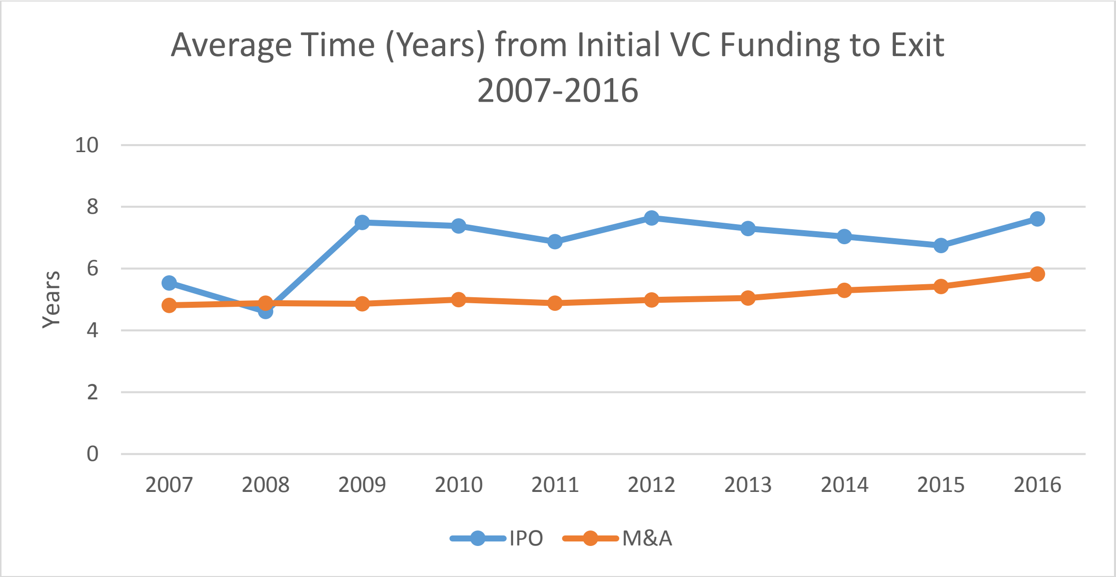
To give you additional context, in the last three weeks I have personally done the following:

- Evaluated over 5 new investments;
- Negotiated compensation agreements with a CEO;
- Identified and sourced potential executives for one of our companies;
- Interviewed and convinced a young marketing executive to join one of our companies;
- Done reference calls with prospective customers and encouraged them to buy from one of our early stage companies; and
- Held strategy sessions with salespeople from our portfolio companies.

Venture capital is hard and unfortunately not always successful. According to research by Professor Shikhar Ghosh of Harvard Business School, 75 percent of venture backed startups do not return investors capital. Correlation Ventures, which evaluated over 21,000 financings spanning the years 2004-2013, showed that 64.8 percent of financings resulted in less than 1x return of capital.



Even when venture capitalists are successful, it takes a long time. The average time to exit for venture-backed startups according to the NVCA 2017 Yearbook is more than 5 years for an acquisition and more than 7 years for an initial public offering (IPO). In life science, those time periods are often even longer.



Source: NVCA 2017 Yearbook, Data Provided by PitchBook

However, when venture capital works, it really works. Some of the most prominent technology companies in the world, e.g. Facebook, Twitter, Snapchat, Google, Amazon, Microsoft, etc., were all venture backed. At one point in 2016, the five largest companies by market capitalization in America were technology companies (Apple, Microsoft, Alphabet, Amazon, and Facebook) all of whom were venture-backed. Three of these companies were built with venture capital within the last 22 years. According to a 2015 study by Ilya Strebulaev of Stanford University and Will Gornall of the University of British Columbia, 42 percent of all U.S. company IPOs since 1974 were venture-backed.[1] Collectively, those venture-backed companies have invested $115 billion in research and development (R&D), and created $4.3 trillion dollars in market capitalization, accounting for 85 percent of all R&D spending and 63 percent of the total market capitalization of public companies formed since 1974. Specific to the impact on the American workforce, a 2010 study from the Kauffman Foundation found that young startups, many of them venture-backed, were responsible for almost all the 25 million net jobs created since 1977.[2]

These incredible contributions to the U.S. economy are due, in significant part, to the right blend of public policy priorities. For example, our tax code rewards long-term, patient investment of capital that enables venture capitalists to work alongside entrepreneurs for many years before they see any return on investment. I encourage all Members of Congress to make new company formation a priority in tax reform. In addition, the federal government has prioritized investment into basic research, which often forms the building blocks for new companies and even whole

[1] "The Economic Impact of Venture Capital: Evidence from Public Companies," Stanford University Graduate School of Business Research Paper No. 15-55, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2681841.

[2] "The Importance of Startups in Job Creation and Job Destruction," Kauffman Foundation Research Series: Firm Foundation and Economic Growth," (July 2010), *available at* http://www.kauffman.org/~/media/kauffman_org/research%20reports%20and%20covers/2010/07/firm_formation_importance_of_startups.pdf.

industries that fuel economic growth with rapid advancements that improve our well-being and extend our lives.

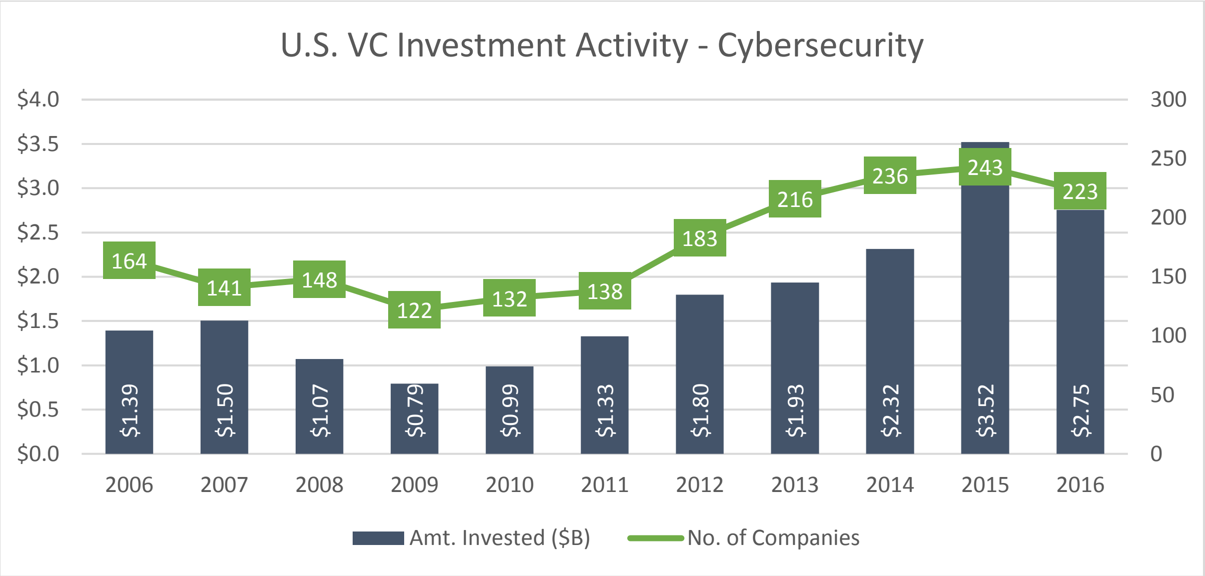
Venture Capital's Impact on Cybersecurity

Cybersecurity innovation and venture capital have been inextricably intertwined right from the beginning. Some of the biggest innovations in cybersecurity have been introduced by venture capital backed startups. For example:

- The stateful inspection firewall which is a critical component of almost all perimeter security products was invented by Checkpoint;
- SSL encryption was invented by Netscape; and
- Next generation firewall based on a "single pass" architecture was pioneered by Palo Alto Networks.

In addition, almost all of the major independent cybersecurity companies in the public market were funded by venture capitalists, including Symantec, Palo Alto Networks, FireEye, Proofpoint, Imperva, Fortinet, Qualys, and Cyberark, to name a few.

Venture capitalists are also incredibly active in the private markets. Since 2010, they have invested over $14.6 billion in more than 740 cybersecurity companies including $3.52 billion in 2015 and $2.75 billion in 2016.[3]



Source: PitchBook-NVCA data

America's leadership in cybersecurity is directly attributable to the strong expertise and significant patient investment capital provided by U.S. venture capitalists.

[3] Pitchbook-NVCA data (Note: Some companies raised a round of venture funding in more than one year, in which case they are counted separately in each year.)

Cybersecurity Threat Landscape

Cyber threats at a consumer level really started to emerge in the 1990's with the commercialization of the Internet. Until the advent of the Internet, viruses could only pass to other computers through floppy disks or other storage media. Once consumers and businesses started connecting their computers to the Internet, viruses with names like Melissa and ILOVEYOU could propagate massively across the Internet and infect millions of users. The first generation of protection against these viruses were anti-virus companies such as Symantec and McAfee that used signature based techniques to create anti-virus software. In order to protect themselves from hackers, corporations started implementing perimeter security solutions. Prominent among these solutions were firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS). While there was a cat-and-mouse element to this fight, for the most part people felt that the cybersecurity problem was in check until the advent of two major developments.

- The first major development was a discovery by researchers in 2010 of a malicious computer worm known as Stuxnet that targeted industrial computer systems. What made Stuxnet different from other viruses was that it targeted programmable logic controllers (PLC) which were not connected to the Internet and were previously thought to be unhackable. Stuxnet showed that many elements of our critical infrastructure, such as dams, electric grids, water treatment facilities, hospital systems, factory assembly lines, and power plants, which use supervisory control and data acquisition (SCADA) and PLC systems, are now under threat, even when they are not connected to the Internet.

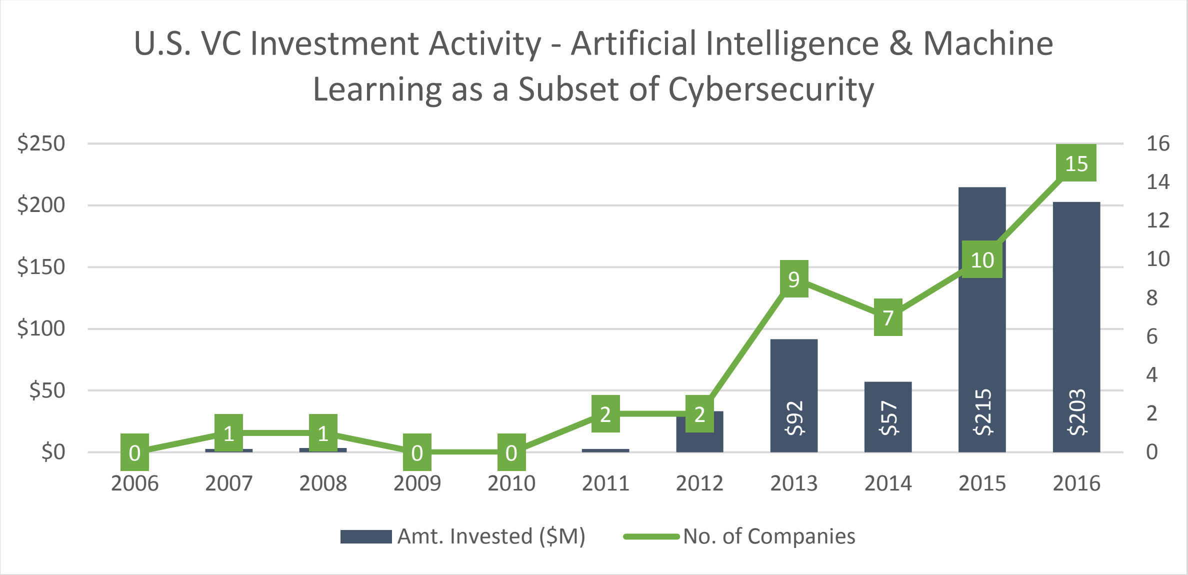
- The second major development was the advent of highly sophisticated malware called Advanced Persistent Threats (APT) in 2013. These malwares function quite differently from the viruses of the past. The hackers goal is espionage and data theft. Once they infect a target, they use sophisticated root kit techniques to disguise themselves. They then connect to command and control servers on the Internet and both exfiltrate data and take new instructions. These sophisticated malwares can remain undetected for months or even years while slowly traversing across the entire network of the victim and grabbing valuable data. All the big breaches you have heard about recently – Anthem, Office of Personnel Management (OPM), Target, Sony – were victims of this technique. Legacy security vendors never architected their solutions to handle threats like this, and unless governments, enterprises, and consumers upgrade their security infrastructure to a modern architecture they are all exposed to this threat.

In addition to these new threats, there are some major developments in other technical areas such as artificial intelligence, Blockchain, Internet of Things and quantum computing which have the potential to impact cybersecurity. Below is a brief overview of each of these emerging areas of technology and how they might impact cybersecurity.

Artificial Intelligence/Machine Learning

Artificial intelligence (AI) in a computer science context is defined as the study of intelligent agents. It is the idea that computers mimic cognitive functions such as "learning" and "problem solving" that is normally associated only with humans. Prominent milestones in AI include IBM's Deep Blue becoming the first computer chess-playing system to beat a reigning world champion, IBM's Watson defeating two Jeopardy champions, and Google's AlphaGo beating a professional Go champion. In popular culture, AI is usually captured as the evil machines taking over the world a la "Hal" in the movie "2001: A Space Odyssey" or "The Matrix."

Artificial intelligence and machine learning have been areas of considerable excitement among venture capital investors. As a subset of U.S. cybersecurity venture investment, 15 artificial intelligence and machine learning companies raised $203 million in 2016. In 2015 and 2016, 21 companies raised a combined $417 million in venture funding. To put this into context, only 13 companies raised a total of $191 million from 2006 to 2014.



Source: PitchBook-NVCA data (Note: Some companies raised a round of venture funding in more than one year, in which case they are counted separately in each year).

It is undeniable that we have made significant progress in AI. The factors that have enabled this progress include the availability of inexpensive computing through the cloud through such innovation as Amazon Web Service (AWS), sophisticated machine learning techniques and algorithms, and availability of huge data sets to be used as training data. Some of the progress we have made towards a self-driving car is directly attributable to machine learning techniques like "Deep Reinforcement Learning." To date, artificial intelligence and machine learning seems to show strong results when we apply it to a narrow problem or constrain the solution space, i.e. Chess, Go. However, we are not close to a general-purpose AI solution any time soon. While estimates vary considerably, no credible expert estimates that we will have general purpose AI sooner than 2045.

Rather than thinking in the context of Man vs. Machine, a better exercise would be to think in the context of Man *plus* Machine. But, as we come to rely on this technology to bolster our capabilities, could hackers and nation state actors use artificial intelligence to hack into our cyber infrastructure? Here again the answer is mixed. We are far from an AI machine that can hack any infrastructure in a general-purpose way. However, people could use machine learning techniques to make progress. Still, most experts believe that the existing techniques of capitalizing on human error (e.g., clicking on malware links, opening attachments) are so effective that there currently is little incentive to invest in expensive AI research for cyber hacking. On the positive side, there are a variety of startups trying to use AI/machine learning to help automate security operations. One of the biggest challenges in cybersecurity today is the avalanche of security alerts every enterprise gets. There are not enough security professionals in the world to chase down and resolve every security alert. There has been some promising advances in using artificial intelligence to automate some of these mundane activities thus freeing the experienced security professionals to focus their energies on the high value alerts.

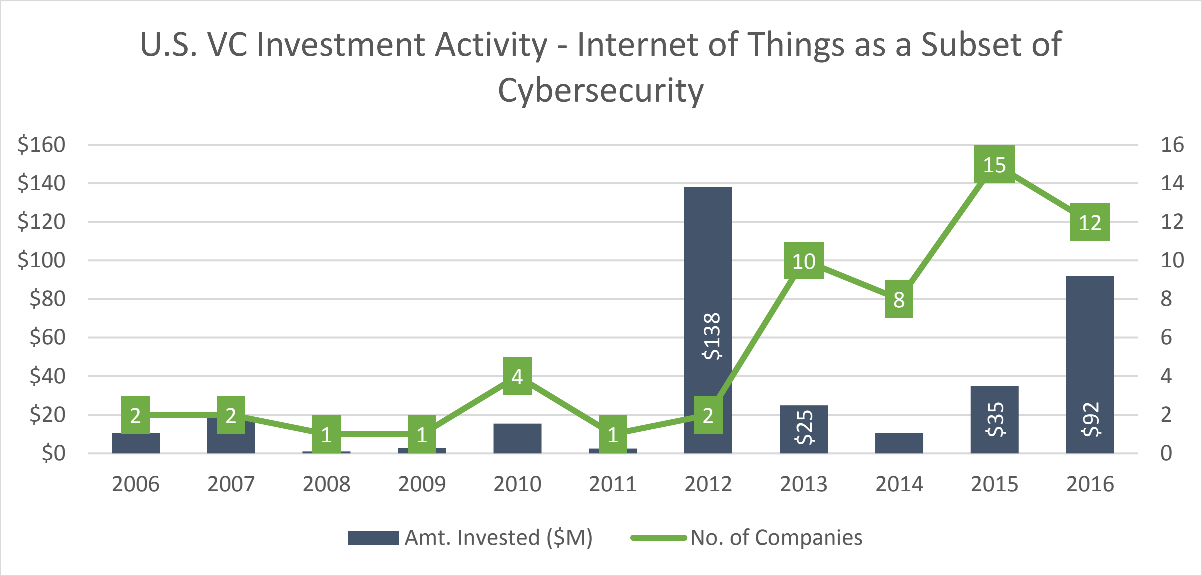
Internet of Things (IOT)

The Internet of Things refers to the inter-networking of physical devices, vehicles, connected devices, and buildings whereby physical objects can collect and exchange data with each other. The canonical example of IOT are smart TVs, which are connected to the Internet and allow you to watch over-the-top content not available through your cable or satellite feed. Another example would be a connected car, such as a Tesla, which can be upgraded or modified with an over-the-air software update.

IOT interfaces with cybersecurity in two major ways. First, as more and more appliances get "connected" and join the Internet they are now vulnerable to hacking. Recent reports have shown that state actors and sophisticated hackers can take over connected devices such as TVs, refrigerators, vehicles, and yes, even microwaves. Once taken over, these devices can then be used to spy and gather confidential information. A good example of this would be voice assistants like Amazon Echo and Google Home. These devices are connected to the Internet and are always listening for voice commands. A hacker could take over one of these devices and listen and record all voice conversations happening around the device.

Second, and even more worrying, is that these devices once taken over can be used as a weapon in a broader attack. There was a major denial of service attack (DDOS) in October 2016 targeting a domain name service (DNS) provider called Dyn. This attack brought down Dyn, which in turn affected major parts of the Internet, including major websites such as Amazon, Airbnb, Comcast, and The New York Times. It was discovered that the attack was orchestrated through a botnet consisting of millions of IOT enabled devices, such as webcams and cameras. An additional concern would be the ability of hackers to take over the controls of a connected car and use it as a weapon for terrorism purposes. The structure of the consumer electronics industry perpetuates and exacerbates these security threats. Consumers are not well informed about the inherent security risks in these products to demand strong security solutions and there are not well-established security certifications for consumer devices. As a result, vendors often have not made the necessary investments in product security, and have not implemented even basic capabilities such as password management or the ability to perform over-the-air security upgrades.

In 2016, 12 cybersecurity IOT companies raised $92 million in venture funding, the second highest annual total for both metrics in the past decade.



Source: PitchBook-NVCA data (note: some companies raised a round of venture funding in more than one year, in which case they are counted separately in each year).

Blockchain

Blockchain refers to a digital ledger in which transactions made in Bitcoin or any other cryptocurrency are recorded chronologically and publicly. Blockchains are critical for the functioning of cryptocurrency since they act as the ledger of record to show who owns what and how ownership changes from one person to the other. Regardless of your views on cryptocurrencies, experts are excited about Blockchain because it is a distributed database with built in validation. Blockchain is effectively an independent, transparent, and permanent database existing in multiple locations and shared by a community. No person controls it, nor can anyone manipulate it so it can serve as the single source of truth for transactions. Blockchain can be used to document anything, including record titles of digital goods.

Blockchains are exciting from a cybersecurity perspective since they are currently perceived as much safer than traditional databases and less impervious to manipulation and fraud. The drawback of Blockchain, however, is that as they scale and get big, they need massive computational power, which in turn needs significant electrical power. Recently, a financial institution estimated that if 400 different virtual currencies were created, they would need 200 times the amount of electrical power Ireland consumes. Governments who have access to unlimited computational and power resources should however consider Blockchain as a promising way to store their critical data. High-profile hacks of databases like with OPM demonstrate the vulnerability of information held by the government. Blockchain could play an important role in data authentication and transparency in the healthcare and financial sectors. There are numerous use cases through which Blockchain could be used for identity and key management, domain name system (DNS) authentication, and patient record management.

Quantum Computing

Traditional computers encode their data in binary form, i.e. data is stored either as a 0 or a 1. There are only two states and traditional machines read these binary files, which are just sequences of 0s and 1s and make sense of them. Quantum computers, on the other hand, store their data in something called "qubits". A quantum computer with n qubits can store a complex combination of up to 2^n states. The technical details are quite complex and complicated to explain, but a simplistic way of thinking about it is that a quantum computer will allow you to solve certain computer problems that are intractable on conventional computers.

The way quantum computing intersects with cybersecurity is that all of our current encryption standards are based on traditional computing standards. If a large-scale quantum computer can be built, then our current public key cryptography standards (e.g. RSA, ECDSA, DSA) could all be broken, allowing anyone to decrypt the data. The best estimates for what it takes to build such a quantum computer, according to National Institutes of Standards and Technology (NIST), are 15 years, $1 billion in spend, and electrical power tantamount to a small nuclear power plant. This is beyond any private actor, but possible for a state actor like China or Russia who do have the resources to invest in quantum computing. This is a possibility that should greatly concern policymakers because if we are beaten in this race the country could be at a severe strategic disadvantage. Fortunately, we do have a number of academics developing post-quantum cryptography. There is reasonable confidence that we can find acceptable cryptographic techniques capable of withstanding quantum computing attacks in the future. My view is that quantum computing is still very nascent and not close to commercialization. There are far more immediate acute problems in cybersecurity that demand action before we need to focus on quantum computing.

Recommendations

As an experienced investor in cybersecurity and a concerned citizen of this great country, I have a few recommendations for the Committee to consider on this topic:

1. Modernize government procurement systems so that the government has access to the best technologies: The world's best cybersecurity solutions are developed in America but unfortunately our government's procurement laws are outdated and make it hard for young startups to sell to the government. As noted before, sophisticated malware threats like APT can only be countered by modern security software. I do want to acknowledge the efforts of entities such as In-Q-Tel[4] and DIUx[5] that have made progress in helping startups interface

[4] In-Q-Tel is "is the non-profit strategic investor that accelerates the development and delivery of cutting-edge technologies to U.S. government agencies that keep our nation safe." *See* https://www.iqt.org/. In-Q-Tel is a member of NVCA.

[5] With locations in Silicon Valley and Boston, "Defense Innovation Unit Experimental (DIUx) serves as a bridge between those in the U.S. military executing on some of our nation's toughest security challenges and companies operating at the cutting edge of technology. . .[DIUx] continuously iterate[s] on how best to identify, contract, and prototype novel innovations through sources traditionally not available to the Department of Defense, with the ultimate goal of accelerating technology into the hands of the men and women in uniform." *See* https://www.diux.mil/.

with government. However, these initiatives are focused on the defense side of the government and do not help any of the federal agencies focused on civilian issues. Our procurement practices are based on old frameworks that view software solutions in a static, object-oriented way. The fact is, modern software is cloud based and updated continuously and our procurement practices need to evolve to accommodate that. As a starting point, the Committee should collaborate with agencies within its jurisdiction to improve their procurement practices to better enable purchase of startup-generated technology. Beyond that, I recommend a more comprehensive examination of federal procurement practices by the Trump Administration to ensure the best technology is used to defend our government against 21st century threats.

2. Setting standards around cyber-hygiene: One way the government can help drive market solutions is by setting standards around cyber hygiene and expectations. I do want to commend this Committee's leadership and support, especially Chairman Thune's efforts in regard to the Cybersecurity Framework proposed by NIST. I recommend that NIST develop a systematic way to update the Cybersecurity Framework periodically and also establish test guidelines that all security products can be objectively compared against. In cybersecurity, we are only as strong as our weakest link so it is imperative that we create incentives for industry participants to practice cyberhygiene. I would caution, however, that whatever solutions that may be crafted in this area be limited in scope and remind lawmakers to be careful not to unduly interfere in business practices which can lead to unintended consequences.

3. Enable legal frameworks for companies to share and exchange data: There is limited information flow today between companies and government. The CIA and NSA possess very sophisticated techniques and detailed information about threats and malwares, but there is no systematic and safe way for that expertise to be shared with the civilian sector. There is also minimal data sharing between companies, as people are worried about legal liabilities from disclosing data around breaches and malware. We need a better legal framework that allows more data sharing so that companies can team up against external threats, learn from each other, and benefit from each other's solutions.

4. Create a generation of cyberwarriors: Countries like Israel have sophisticated programs like Talpiot that identify talented high schoolers in computer science and orient them to cybersecurity careers. We need to create a generation of cyberwarriors and should consider different strategies, including perhaps setting up a cyber-academy like the U.S. Naval Academy where we can recruit, train, and develop the best young cyber talent in our country. Attempts to weaponize technology will not recede in our lifetime; it is time for us to build our institutions to recognize this fact.

5. Use cyberinsurance to pool and minimize existential risk: Regardless of how much precaution companies take, there is always a risk of security and data breaches. The cost of these breaches can be astronomical and beyond any single company's ability to handle. Similar to earthquakes and hurricanes, we need to develop a deep cyberinsurance industry so that companies have a way to pool and minimize existential risk.

Conclusion

The challenges we face in cybersecurity are daunting, but I am an optimist. The pilgrims on the Mayflower faced insurmountable odds but found a way to build a home and a country that is the leader of the free world. My own personal investing experience gives me confidence that there are market-based approaches that can be used to battle the cybersecurity conundrum.

In 2011, two MIT graduate students applied for a small grant from the National Science Foundation (NSF) with an idea to create a cybersecurity ratings organization. In 2013, Menlo Ventures, along with other venture firms, funded them. Six years later, their company — BitSight Technologies — employs 225 people, counts more than 700 customers across 25 different sectors, and has raised $95 million in venture funding. The company was recently named a Forbes "Next Billion Dollar Startup."

As a cybersecurity ratings company, BitSight measures the security performance of organizations on a scale of 250-900. A higher rating indicates better security performance. It is a simple concept – very similar to the credit ratings model companies such as Moody's and Standard & Poor's have championed for credit and debt.

BitSight is an example of a venture-backed cybersecurity company providing market-based solutions through its ratings system. It is a system that can be used by market participants that can quantitatively improve the global state of cybersecurity. BitSight is also an outstanding example of how government and the private sector can work together to solve our cybersecurity challenges. What started as an NSF grant turned into a successful company that was backed by private, risk capital. Our firm's long-term investment is rewarded because policymakers understand the value of that investment to our national economy. Due to this collaboration, American jobs were created and cybersecurity challenges are being addressed. If we all continue to work together, we can achieve a tremendous amount.

Finally, my greatest recommendation is to use all policy tools available, including tax and regulatory policy, immigration, patent, and federal investment in basic research, to encourage new company formation. It is through the innovation created by entrepreneurs partnering with venture capitalists that we will have the greatest chance to defeat this challenge.