Cybersecurity & Innovation: The Key to a Secure Future

October 2021

Nasdaq Index Research

As the world becomes more digitally connected, cybersecurity's role in business, technology, and society has become mission critical. Simply put, the modern world is built on cybersecurity. Without it, capital cannot flow freely, information cannot be stored safely, and businesses, governments and critical infrastructure cannot operate securely. One major challenge in securing a world that relies on data and connectivity is that the rapid pace of technological change has created more vulnerabilities and opportunities for cyber threat actors, e.g.: nation states, groups, or cybercriminals, to exploit. As a result of these rapid technological advancements across several different technologies, businesses, organizations, and cybersecurity companies have been forced to embrace new, innovative technologies to make the world more secure. Since the world has become more digital, cybersecurity has also become a key element in the way businesses make decisions and innovate. For example, in a KPMG article, they stated that businesses and organizations have shifted from a paradigm of asking, "How do I mitigate and manage risk?" to "How do I leverage cyber security to give my business a competitive advantage?"[1] Said another way, cybersecurity is a key component of unlocking innovation.

In this report, we'll explore innovation through various angles and highlight why innovation and cybersecurity are synonymous with one another. Finally, we'll highlight key technologies that are helping to transform the cybersecurity investment theme.

What is innovation?

Innovation is hard to define, as its meaning and definition can vary from sector to sector, or from business leader to business leader. With that in mind, let's look at what innovation means by exploring it from different perspectives. To start, US President Barack Obama once said, "Innovation is the creation of something that improves the way we live our lives."[2] From this perspective, within the broader society, innovation is key to **improving our lives**. But how does innovation occur? According to the Harvard Business School Review, "Innovation is the embodiment, combination, or synthesis of knowledge in original, relevant, and valued new products, processes, or services."[3] Innovation occurs through the **synthesis of knowledge**. Another take on innovation can be found in *The Little Black Book of Innovation,* which defines innovation as "a process that combines discovering an opportunity, blueprinting an idea to seize that opportunity, and implementing that idea to achieve results? Remember — no impact, no innovation."[4] Innovation creates **impact**. Yet there's more. According to the Conference Board, "innovation is broadly defined as an activity or set of activities that results in the creation and use of a new or significantly improved product or service; production or operating process; way of attracting customers by enhancing their experience; and organization practice, work design, human capital competency, or use of resources that creates value."[5] Innovation, particularly from the business and technological angle, is also about **creating value** and **creating something new.** Just like how innovation untaps an endless array of possibilities, so too are the number of ways to define or interpret the meaning of innovation. But when you unpack these perspectives on innovation, there are some common themes that emerge, centering around synthesis,

change, improvement, opportunity, and impact. In all, these interpretations can be applied to how innovation and cybersecurity relate to one another.

Innovation & Cybersecurity

What does innovation have to do with the cybersecurity theme? Everything. When exploring innovation and cybersecurity, it's important to approach through two lenses. First, from the standpoint of the innovation that takes place within the technologies and strategies being developed and utilized to secure the world's networks, computers, data, financial systems, etc. Cybersecurity is now mission critical to the way businesses and organizations operate around the world. Just how critical is cybersecurity? According to a Price Waterhouse Coopers (PWC) survey, "nearly all (96%) [businesses] say they'll adjust their cybersecurity strategy due to COVID-19. Half are more likely now to consider cybersecurity in every business decision — that's up from 25% in our survey last year [2019]."[6] Think about that for a second. Over half of the businesses surveyed will consider cybersecurity in every business decision. Second, it's imperative to understand that cybersecurity enables businesses and organizations to function, meaning that cybersecurity plays a role in the way business is done. In fact, James Nunn-Price, Deloitte Australia & Asia Pacific Cyber Risk Services Leader for Global Risk Advisory, said it best, "We're all in this together. Digital is impacting everyone and cyber is naturally embedded in that everywhere as we go forward."[7] Said another way, the world is digital; the world relies on cybersecurity.

Why is innovation important?

Today, innovation within the cybersecurity theme is just as critical as the cybersecurity itself. This is due in part to the rampant technological change taking place across both sides of the cybersecurity aisle – the businesses and organizations deploying cybersecurity to protect their data, networks, etc. and the threat actors who are looking to steal, destroy, and wreak havoc on those systems being protected. What's happening though is that the threat actors are beginning to use more advanced methods and technologies, making it paramount for cybersecurity firms and cybersecurity technology to keep up with this change. How? Through innovation. According to the World Economic Forum in *The Global Risk Report 2021*, "Business, government, and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cyber-crimes, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability."[8] Cybersecurity must innovate to keep up with the sophistication and frequency of cybercrimes.

Innovation in Cybersecurity: Emerging Technologies

While cybersecurity enables innovation to take place across every sector in the modern digital economy, innovative technologies also enable cybersecurity companies to secure businesses, organizations, networks, and data around the world. Let's explore a few important innovations that are impacting, changing, and creating value within cybersecurity.

Artificial Intelligence: Machine Learning & Deep Learning

Artificial Intelligence (AI) provides a foundation for innovative technologies and processes to be deployed across the cybersecurity space. AI is defined by John McCarthy, the late computer and cognitive scientist, as "the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable."[9] In essence, AI is "a field, which combines computer science and robust datasets, to enable problem-solving."[10] AI is being used to help automate threat detection, analyze large volumes of data, such as breaches and network activity, and speed up threat response time.

Machine Learning (ML) comprises a field of AI which "focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy." [11] Within the field of cybersecurity, ML can be used in a wide array of uses, such as the discovery of vulnerabilities, automated breach investigations, and attack response, just to name a few.[12] Another subset of AI is Deep Learning (DL) which is "designed to mimic the functionality and connectivity of neurons in the human brain" and given its use of "deep" networks, through more layers, giving this process the ability to learn and analyze massive amounts of complex data.[13] DL technology can help detect threats, such as malware, as well as monitor network traffic and analyze user behavior.

Almost every major cybersecurity company is utilizing AI in their cybersecurity offerings. Splunk (NASDAQ: SPLK), a leading provider of software and cloud security solutions, is utilizing machine learning in its threat detection tools, helping clients to eliminate threats and breaches quickly. CrowdStrike (NASDAQ: CRWD), a pioneer of endpoint security protection and threat intelligence, is another leading cybersecurity company using machine learning and views this technology as the "first line of defense against modern threats."[14] CrowdStrike uses machine learning across its platform for threat detection and protection across all endpoints. Okta, Inc. (NASDAQ: OKTA), a leading identity and access management company, has incorporated AI and ML technologies in its authentication product. Through Risk-based Authentication, Okta, uses "machine learning to deliver automated detection and response to identity-based attacks."[15]

Quantum Computing

Quantum computing has the potential to disrupt cybersecurity. ZDNet defines quantum computing as "a subfield of quantum information science—including quantum networking, quantum sensing, and quantum simulation—which harnesses the ability to generate and use quantum bits, or qubits."[16] A report on quantum computing from Harvard's Belfer Center for Science & International Affairs stated, "Quantum computers have the potential to solve certain problems much more quickly than conventional, or other classical, computers. They leverage the principles of quantum mechanics to perform multiple operations simultaneously in a way that is fundamentally different from classical computers."[17]

How does this impact cybersecurity? For starters, quantum computing opens an infinite array of decryption capabilities and could mean an end to the current method of public-key encryption technologies. There are estimates that this is a little more than a decade away.[18] But, innovation begets innovation. Quantum computing will also be used within cybersecurity itself, helping to identify and deter quantum-based attacks.

We have already observed several cybersecurity companies invest in quantum computing innovation. Thales Group (EPA: HO) cyber-based defense company, started working on post-quantum cryptography back in 2013 and today they are developing a future generation of cybersecurity products.[19] In September 2021, it was announced that Thales and the National University of Singapore (NUS) partnered to develop and test new security technologies utilizing quantum computing capabilities.[20] Fortinet (NASDAQ: FTNT), a leading network security company, has partnered with ID Quantique to provide a quantum-safe VPN platform, providing another layer of security against the potential use of quantum computing to break through security barriers.[21] Booz Allen Hamilton (NYSE: BAH), a leading technology consulting firm, is investing heavily in quantum computing and has a dedicated team exploring and developing ways of utilizing quantum computing in their business and for their clients. According to DJ Dulny, Chief Scientist of Booz Allen's quantum computing research team, Booz Allen's "quantum computing effort has three major components: basic research, applied analysis, and technical consulting" and they are looking to "bring value from quantum computing to our clients' missions, and to help them understand its coming impact."[22]

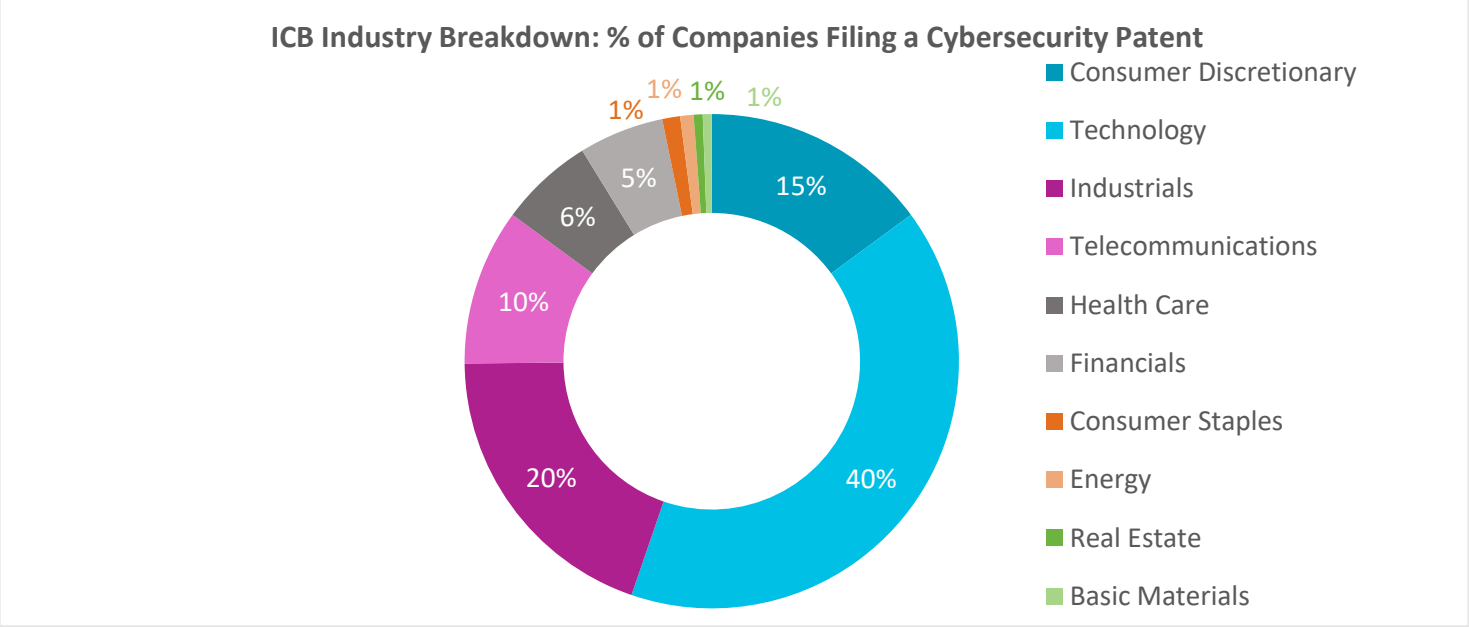
Innovation through Cybersecurity Patents

We highlighted in the introduction that cybersecurity has become integral to the way in which companies innovate and how it provides them with a competitive advantage. To examine this further, let's look at a key marker of innovation: patent filings. According to the World Intellectual Property Organization,

> *"Inventions are the bedrock of innovation. An invention is a new solution to a technical problem and can be protected through patents. Patents protect the interests of inventors whose technologies are truly groundbreaking and commercially successful, by ensuring that an inventor can control the commercial use of their invention."*[23]

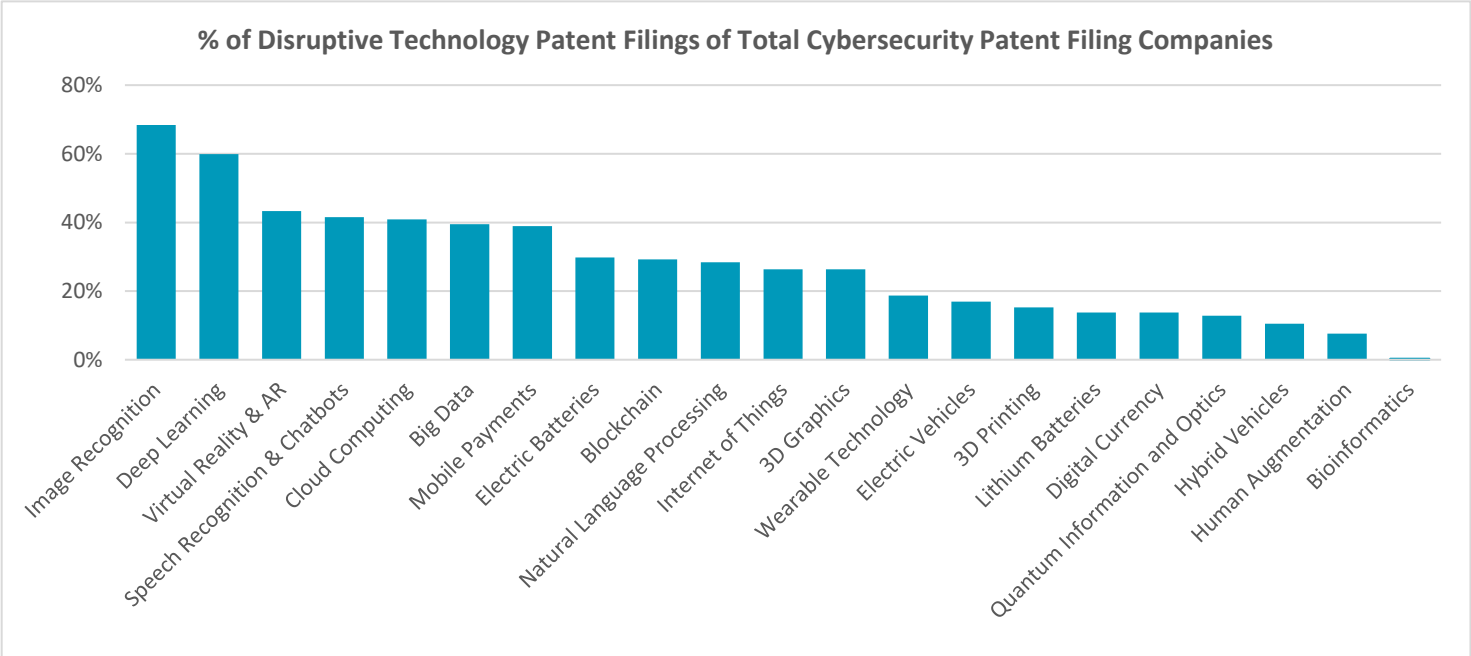
By identifying trends in cybersecurity patent filings, we're able to observe important trends in cybersecurity innovation. To start, we analyzed trailing 12-month patent filings across 35-sub themes that, together with our partner Yewno, we have identified as relevant disruptive technologies. Starting with the Nasdaq Global Index (NQGI) of approximately 9,000 companies as well as any non-NQGI US-listed companies, using Yewno data, we identified companies filing cybersecurity patents along with other disruptive and emerging technologies in areas such as, artificial intelligence, data computing and processing, healthcare innovation, etc. The premise here is that patent filings shed light on where companies are engaging in research and development, and how they are investing in their future. In other words, companies filing patents in a specific technology is an indication that the company is either linked to the theme or they are using the technology to unlock value or maintain a competitive advantage.

The data presented below is based on the companies' collective patent contribution scores (i.e., the proportion of total patents filed relating to each sub-theme among the approximately 9,000 companies tracked in the Nasdaq Global Equity universe in addition to the other non-NQGI US-listed companies). In the trailing 12-month period examined, ending May 2021, roughly 27.5% of securities in the universe that have filed any patent in the 35 disruptive tech sub-themes filed a cybersecurity patent (342 of 1,245). Not surprisingly, technology companies made up a large portion of the group, as 40% of the cybersecurity patents filed over the 12-month period were classified as technology companies, followed by industrials and consumer discretionary at 20% and 15% of the universe, respectively. Keep in mind, many of the patents filed are primarily for the use within their products and may not be sold as a standalone cybersecurity service or solution. For example, a large refrigerator company might file a patent for a cybersecurity solution for an IoT based refrigerator. Why is this relevant? It provides evidence that cybersecurity is becoming an integral part of future innovation across several industries, and that cybersecurity is now becoming embedded in almost every element of the modern digital economy.



(Data through May 2021) (Source: Nasdaq, FactSet, and Yewno)

As the cybersecurity arms race continues, many companies have been innovating in other technologies as well, highlighting the fact that those that are engaging in some aspects of cybersecurity are some of the leaders in technological innovation in other disruptive or emerging technologies. One way to observe this is by analyzing what other technology patents were filed by cybersecurity patent filers over the time. The following top five technologies stand out – image recognition, deep learning, virtual reality / augmented reality (AR), speech recognition, and cloud computing. In fact, 70% of companies that filed a cyber patent also filed an image recognition patent, followed by deep learning at 60%. It's the latter that is particularly related to the cybersecurity theme today.



(Data through May 2021) (Source: Nasdaq, FactSet, and Yewno)

Cybersecurity Investment Theme & Innovation

Innovation is a key element of the cybersecurity investment theme. As new technologies are developed, new threats emerge as well, making it crucial for cybersecurity companies to deploy new and innovative technologies, such as AI or even quantum computing. In addition, cybersecurity companies as well as companies across other themes must consider cybersecurity in every business decision – whether it's the development of a new technology, product, or even a new business model. Simply put, the modern world is built on cybersecurity

Nasdaq's Cybersecurity Indexes offer investors a simple way to track this investment theme. To learn more, please visit the Nasdaq Cybersecurity Indexes website.

[1] https://advisory.kpmg.us/issues/leverage-cybersecurity-drive-innovation.html

[2] https://www.slhd.nsw.gov.au/innovation/about.html & https://www.bloomberg.com/news/articles/2007-11-15/proposed-presidential-innovationbusinessweek-business-news-stock-market-and-financial-advice

[3] https://hbsp.harvard.edu/product/7195BC-PDF-ENG

[4] https://hbr.org/2012/05/four-innovation-misconceptions

[5] https://www.conference-board.org/future-of-innovation/

[6] https://www.pwc.com/us/en/services/consulting/cybersecurity/library/assets/pwc-2021-global-digital-trust-insights.pdf

[7] https://www2.deloitte.com/au/en/blog/innovation-blog/2020/what-cybersecurity-do-with-innovation.html

[8] https://www.weforum.org/reports/the-global-risks-report-2021

[9] https://borghese.di.unimi.it/Teaching/AdvancedIntelligentSystems/Old/IntelligentSystems_2008_2009/Old/IntelligentSystems_2005_2006/Documents/Symbolic/04_McCarthy_whatisai.pdf

[10] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

[11] https://www.ibm.com/cloud/learn/machine-learning

[12] https://cset.georgetown.edu/wp-content/uploads/Machine-Learning-and-Cybersecurity.pdf

[13] https://www.infocyte.com/blog/2019/08/13/5-amazing-applications-of-deep-learning-in-cybersecurity/

[14] https://www.crowdstrike.com/blog/defending-against-malware-with-machine-learning/

[15] https://www.okta.com/blog/2020/01/ai-is-changing-security-heres-how/

[16] https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity

[17] https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity

[18] https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity

[19] https://www.thalesgroup.com/en/worldwide/group/magazine/quantum-computing-thales-researchers-work-prevent-crypto-apocalypse

[20] https://www.computerweekly.com/news/252507484/NUS-and-Thales-to-develop-quantum-technologies

[21] https://www.insidequantumtechnology.com/news-archive/id-quantique-partners-with-fortinet-to-commercialize-a-quantum-safe-vpn-solution/

[22] https://thequantumdaily.com/2020/02/04/tqd-exclusive-booz-allen-hamiltons-qc-research-team-offers-quantum-industry-insights-outlook/

[23] https://www.wipo.int/ip-outreach/en/ipday/2017/innovation_and_intellectual_property.html