# INVESTING IN CYBERSECURITY

JANUARY 2022

The need for cybersecurity has exponentially increased over the years, with the pandemic-driven transition to a work-from-home environment accelerating the trend. With this increased focus on cybersecurity comes opportunity for investment in companies in this industry with solid fundamentals.

A major theme of the pandemic lockdown was an acceleration of American work and commerce from brick-and-mortar shops and offices to an online format. From buying goods, to education, to the white-collar workplace, activities shifted onto connected internet devices out of necessity, making the U.S. economy more dependent than ever on secure, reliable, and efficient connections to computer networks at the workplace as well as in our homes.

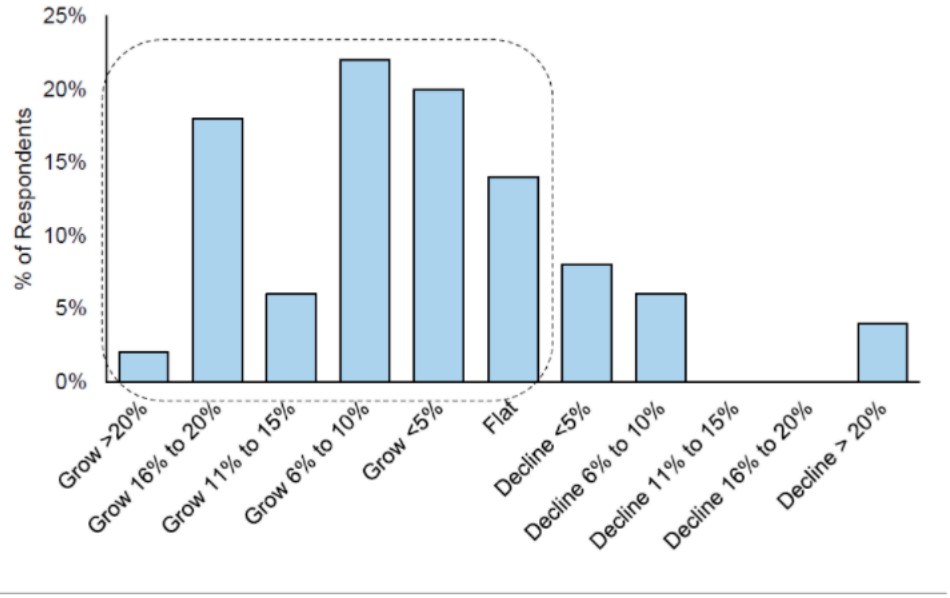
The relatively quick transition to a work-from-home environment was a challenge for corporate IT managers and an opportunity for cyber criminals. The World Economic Forum estimated that cyberattacks jumped 238% globally between February and April 2020. Perhaps this was a unique window of vulnerability, but there is evidence that cyber threats revealed an undercurrent of risk which is still around. We've read the news headlines about ransomware (Colonial Pipeline shutdown), network breaches (Solar Winds hack), and hijacked accounts (Twitter's Bitcoin fraud). Cybersecurity has become an issue of existential importance to many organizations today, forcing management to devote greater resources to fortify and monitor systems and networks. Every employee working from outside the office has the potential to become a weak link in their defenses, maintaining the urgency to defend the network. It serves as a call for both heightened personal diligence, and at the same time, creates a potential opportunity for investors.

## DEMAND FOR CYBERSECURITY ON THE RISE

Technology spend by corporations is on the rise, particularly on moves toward cloud infrastructure. According to a survey from Goldman Sachs, 80% of respondents expect their digital transformation spend to stay flat or increase in 2021 as compared to an already expensive 2020.

Spending on cyber defense is a growing portion of that budget. Microsoft President Brad Smith recently told The Wall Street Journal that in January the company surpassed $10 Billion in revenue in its security business, and security continues to be a significant focus for Microsoft and U.S. companies in general. According to Smith, across organizations nationwide, there are approximately 462,000 job openings that require cybersecurity skills.

COMPANIES PLANNED SPENDING INCREASE ON DIGITAL TRANSFORMATION




Source: Goldman Sachs Global Investment Research

## INVESTING IN CYBERSECURITY

We expect a mix of in-person and remote work will likely persist as workers' preference for a flexible working environment remains strong. This provides a strong mid-term tailwind for the entire cybersecurity industry, although companies within that category create different products and services:

1. Cloud security companies that monitor networks for anomalies
2. Hardware companies building firewalls and secure network gear
3. Software designed to detect malicious code and halt its damage
4. IT service contracts that provide daily management and expertise

Some companies are dedicated to one of these tasks, but most present a combination of products and services. For example, Accenture is a global consulting firm serving large corporations and government agencies with outsourcing and strategy, 80% of which is technology consulting. Accenture has the scale and scope to bring to bear complete technology security service at the organizational level, what it calls cyber resilience, in the face of sophisticated global network threats.

Cisco Systems Inc., on the other hand, continues to manufacture secure network hardware, from modems to routers, but more recently offers secure file sharing services and secure web conference hosting services as part of its small but growing software and services business.

Perhaps the best example is Fortinet, Inc., which is dedicated to a full suite of network security for companies small, medium and large. This company builds network firewall hardware embedded with sophisticated internal software alongside additional cybersecurity software solutions. That integrated product offering serves to manage internet-connected devices, walls off the company network, and seeks out malware in incoming emails and company operating systems. It all adds up to comprehensive protection that's both hardware- and software-oriented.

What's important for investors is selecting the right investment with solid profit margin, sustainably growing sales, and a competitive position that makes it easy for customers to "hire" this company or pay up for the product while making it difficult for a competitor to enter. Seeking out companies that exhibit these characteristics is a potential recipe for investment success, and we believe that there are good companies in the cybersecurity landscape today fitting this investment profile.

Ashfield expects organizations to continue allocating larger budgets to security investments designed to be more conducive to a digitized, hybrid work environment. We believe the changes forced by the pandemic are here to stay, and employers large and small will appreciate the importance of investing in cybersecurity technologies. Digital transformation continues to drive growth, and we want to be invested in this long-term secular tailwind.