INVESTMENT STRATEGY UPDATE

September 30, 2013

CYBER SECURITY

"To err is human, but to really foul things up requires a computer."
Farmer's Almanac, 1978.

Definition of Cyber: of, relating to, or involving computers or computer networks. In today's world, where practically everyone is digitally connected to everyone else via computer or at least cell phone, the need for cyber security has assumed tremendous importance. In recent years the number, size, and sophistication of cyber attacks have increased dramatically. Because the means and avenues of attack have vastly expanded, and attacking thousands is as easy as attacking one, the stakes have been raised for individuals, companies, and governments throughout the world. The challenge is to maximize the value of the Internet while preventing its abuse by those who would exploit it for criminal or malicious purposes, and to do so in a manner that continues to protect privacy and maintain individual freedom.

All of this provides a significant tailwind to the companies that participate in the cyber security industry. Cyber security has for years been among the highest priorities for corporate chief information officers, and spending in this area is increasing considerably in both the private and public sectors. Significantly, public spending has been increasing even at a time of serious budget pressure, a clear signal of its importance.

The Growth of the Internet

The idea of developing technology that could bring the world's accumulated knowledge to virtually anyone was raised as far back as 1970 by the science fiction writer Arthur C. Clarke. Little more than twenty years later, the Internet as we know it today (i.e., the global system of interconnected computer networks) had come into being and with it the system of interlinked documents known as the World Wide Web.

The growth of the Internet has been nothing short of phenomenal. A 2011 article in *Science* estimated that in 2007, fully 97% of the information flowing through all forms of two-way communication was over the Internet. The economic impact is tremendous. International Data Corp. estimates that global e-commerce transactions will approximate $16 trillion in 2013. Add in the $4.4 trillion global market for digital products and services and the estimated total digital economy now comes to $20.4 trillion, or roughly 13.8% of global sales.

The Inherent Threat

The architecture of the Internet makes it possible to identify where, when, and how users are accessing the Web as well as the content of their interactions with other individuals and websites. For example, every time a web page is requested from a web server, the server can identify the digital address from which the request arrived. Furthermore, web browsers record the web pages that have been requested and viewed. The same applies to any personal information that a user might supply, such as name, address, or preferences. This allows web-based organizations to develop and build profiles of individual users, and enables their marketing arms to pitch appropriate products with a presumably higher degree of success, which is a relatively innocuous and possibly even desirable outcome. The same architecture also permits law enforcement, counter terrorism, and espionage agencies to identify and track criminals, terrorists, and spies – another desirable outcome.

However, should personal information for innocent citizens fall into the wrong hands, the results can be devastating. So in this sense, the Internet is a double-edged sword. Its design has yielded untold benefits by providing a vehicle for more open communication, the democratization of knowledge, and the expansion of global commerce, but our willingness to contribute to that openness can put at risk our personal data, property, and reputations. Today's highly popular social networks (e.g., Facebook, LinkedIn) encourage users to provide extremely personal information, including pictures, because such information makes use of these social networks more realistic and engaging. But in so doing, these networks represent a giant leap towards public exposure and potential targeting.

Enter the Age of Cyber Crime and Cyber Warfare

The darker side of the Internet results from the inevitable tendency of certain elements of society to exploit the vulnerabilities of any system for their own ends. And unlike the average user looking to research a product on Google or buy it from Amazon, a hacker or cyber terrorist can use his programming skills and knowledge of the inner workings of the Internet to hide his tracks. The instances of criminal exploitation of the Internet have grown exponentially in recent years and include attempts to disrupt day-to-day business; wanton destruction of personal files and media; theft of money, identities, and ideas; and politically-motivated efforts to destabilize governments or destroy critical infrastructure. For example, in what is possibly the most advanced cyber attack ever executed, the Iranian nuclear enrichment facility at Natanz was sabotaged in 2010 by the Stuxnet worm, resulting in the destruction of over 1,000 centrifuges, thereby delaying Iran's efforts to build a nuclear bomb.

Just within the U.S., the Identity Theft Resource Center reports that at least 470 companies, government agencies, and other institutions were forced to acknowledge material breaches to their computer networks during 2012, and that figure is headed towards 600 in 2013, based on information through July. According to the U.S. Computer Emergency Readiness Team, the number of cyber attacks reported by federal agencies has skyrocketed 782% since 2006 to nearly 49,000 in 2012. And this is only the number reported, which many

believe is a fraction of those that actually occur. According to the Pentagon, Defense Department computers are "probed" thousands of times each day.

Combating Cyber Attacks

This *Investment Strategy Update* is not intended to scare our clients into hoarding gold and heading for the hills. The myriad threats posed by cyber criminals are not unknown. Cyber security is a priority not only of corporations, but also of our government intelligence agencies and our Departments of Defense and Homeland Security. In fact, the potential for cyber attacks displaced terrorism and transnational organized crime as the foremost threat to national security in the most recent "Worldwide Threat Assessment of the U.S. Intelligence Community." Some estimates have the federal government as a whole spending upwards of $25-30 billion annually on cyber security goods and services. Meanwhile, the Pentagon announced earlier this year that it was undertaking a major expansion of U.S. Cyber Command (which is under the purview of a four-star general), raising the number of personnel from 900 to approximately 5,000 by 2015. When that expansion is complete, one-third of these cyber warriors will be focused on protecting critical national infrastructure, one-third will defend the DoD's networks, and the rest will be combat mission forces who will, among other things, initiate cyber attacks.

Clearly, the DoD is serious, focused, and pursuing a proactive strategy of defense. It should come as no surprise that the Stuxnet attack on Iran is widely credited to the U.S. National Security Agency, which is under the same four-star general's command. The Defense Department has set up training facilities and is using computer skills contests to identify computer prodigies in high school and even middle school. So, while it is impossible to know how many cyber attacks are thwarted for every one that succeeds, we believe that the authorities responsible for protecting our critical infrastructure are doing the right things.

While we are confident such authorities will be able to keep the planes flying and the social security checks coming, we should all understand that no government authority can secure everything, and that our personal digital lives are our own responsibility. At the individual level, there are a number of simple steps we can take to protect our information. After all, many cyber attacks rely on simple human carelessness or ignorance for success. The first step is to maintain the integrity of one's passwords. In the future, we expect biometric authentication (e.g., fingerprint or retina scans) to become more popular, as it eliminates the need for passwords. Beyond password security, the FBI and others advise activating the firewall on one's wireless router, and enabling security and operating system software to update automatically. Also, turning the computer off when not in use severs its connection to the Internet, thereby cutting off a hacker's means of access. Using a search engine rather than typing out a web address directly will avoid connections to fraudulent websites resulting from typographical errors. Finally, all email attachments should be treated as suspicious and not opened until they are known to be legitimate.

Investment Implications

As always, the relevant question is whether and how an investor can profit from the efforts being put forth in the field of cyber security. The most obvious choices are those hardware and software companies whose businesses are essentially "pure plays" in computer and network security. There are a number that are well-enough established to be publicly traded with valuations over $1 billion. We continue to monitor industry developments in order to identify and invest in those with the right combination of technical skills, secure intellectual property, strong customer bases, and reasonable valuations. As there are currently no exchange-traded funds that focus on this area, we would consider the purchase of several smaller-than-normal positions in order to achieve diversified exposure to this theme.

Another option would be to invest in companies that have successful security-related divisions. This includes not only the major networking equipment companies, but also the prime defense contractors, publicly held consulting companies, and insurance companies that have chosen to enter the cyber insurance business. Unfortunately, for many of these companies, this slice of their revenue and earnings is unlikely to become sufficiently large as to make them thematically meaningful.

Market Outlook

Over the long term, corporate earnings growth drives stock prices, and the environment for earnings remains positive. The U.S. economy continues to grow (albeit below trend), China's economy is showing signs of stabilization, and Europe seems to have emerged from its recession. Are there things to be worried about? Certainly, as there always are. But BTR's client portfolios are invested with a two- to three-year target time horizon, and it is the environment in the future that will most affect our success. Thus we are not overly focused on the interim fluctuations.

History has demonstrated that equities move from undervaluation at stock market bottoms to overvaluation at market tops. Seldom have the interim trends stopped at fair value. So given the current environment of reasonable valuations and favorable earnings-growth prospects, we remain comfortable with being invested, and are concentrating our efforts on sector and stock selection.

Regarding fixed income, a continuing pause in the recent trend of rising interest rates appears likely. Nonetheless, our expectation is that interest-rate normalization will lead to still higher rates down the road. As such, we continue to focus on quality and relatively short maturity schedules.

ADDITIONAL INFORMATION IS AVAILABLE UPON REQUEST. The information contained herein is based on sources which we believe reliable but is not guaranteed by us and is not to be construed as an offer or the solicitation of an offer to sell or buy the securities herein mentioned. Opinions expressed herein are subject to change without notice. This firm and/or its individuals and/or members of their families may have a position in the securities mentioned and may make purchases and/or sales of these securities from time to time in the open market or otherwise.