William Blair | Blog
REPRINTED FROM INVESTING INSIGHTS AT WILLIAM BLAIR

Barbarians at the Digital Gate: Can They Be Stopped?

December 3, 2021

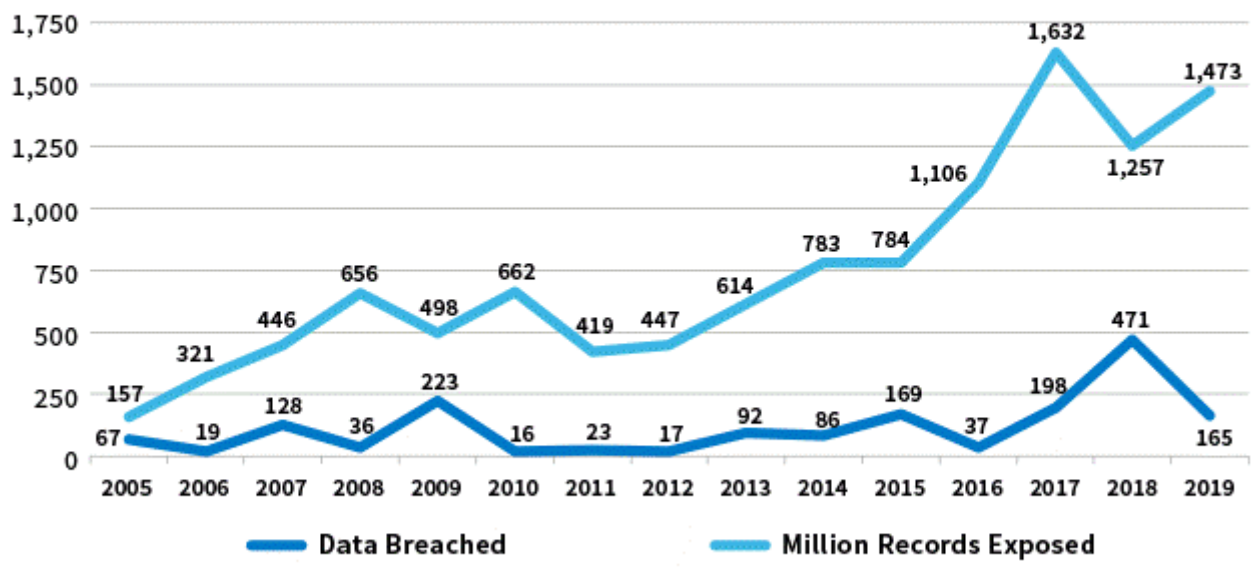
Cybercrime is one of the most daunting and fastest-evolving threats facing companies today. It also presents an opportunity for investors to capitalize on the growth of the next generation of leading cybersecurity providers. As companies shift their tactics and try to level the playing field against increasingly sophisticated attackers, we examine the state of cybersecurity today and what it means for investors.

Increasing Digitization, Increasing Cybercrime

The digitization of business has continued unabated over the past decade, accelerated by the COVID-19 pandemic. In addition to the dramatic shift to remote work, advancements in robotics, telehealth, and automated assistance increasingly define commerce and daily living.

Unfortunately, increasing digitization has resulted in a vast increase in cybercrime. According to the Identity Theft Resource Center, global cyber breaches increased by 900% from 2005 to 2019. While more than 80% of these attacks are motivated by financial gain, espionage and simple network “joyriding” remain potent drivers as well.

The scale and costs of cyberattacks have also increased dramatically. Recent examples include breaches at SolarWinds and T-Mobile, each of which resulted in extremely serious damage, either directly or indirectly. More ominously, cybercrimes are now hitting essential U.S. infrastructure, such as the 2021 attack on the Colonial Pipeline, which stretches from Houston to the Port of New York and New Jersey.



Source: Identity Theft Resource Center, 2020.

We discussed the state of cybersecurity recently as part of CONNECTIVITY 2021, a virtual conference William Blair hosted that focused on cybersecurity, privacy, and politics, and how they are affecting the investing landscape. To learn about the latest cybersecurity threats facing companies and to help investors separate myth from reality, we welcomed three experts from across the cybersecurity landscape: David Gibson, chief marketing officer of Varonis Systems; Joel Fulton, CEO and co-founder of Lucidum; and John Pironti, president of IP Architects.

Threats Evolve Amid Digital Transformation

Over the past several years, the availability of and access to sophisticated hacking tools on the dark web has increased exponentially, thus facilitating the overall increase in cyberattacks. As Pironti noted, some of these tools are being used in conjunction with advanced tools that are allegedly part of unintended leaks by various U.S. government entities.

The release of these tools has significantly lowered the barriers of entry for hacking, so that now, virtually anyone with a moderate degree of tech savvy can become a hacker. Even more striking, the growth of new hacking tools has created its own industry. “There is now the proliferation of ‘ransomware as a service’ where you can lease these prepackaged tools in exchange for a royalty payment on the ransom that you capture,” Fulton said.

Cyberattacks are also becoming more targeted. The availability of staggering amounts of personal, enterprise, and government data has allowed hackers to utilize much more precise attacks, from phishing emails to manipulating the billions of devices connected to the internet of things (IoT).

“There are many vectors to penetrate an organization’s defenses,” Gibson said. “All it takes is one vector that’s open to get to important data and really do a lot of damage.” Unfortunately, it’s not an exaggeration to say that even one’s smart TV or refrigerator may not be safe.

While digital transformation has made collaboration easier, it has also eliminated a clear perimeter for security. In short, every endpoint has become an access point—and the amount of information that these access points connect to is profound. For example, the average U.S. employee now has access to 17 million files on their first day of employment, according to Gibson. From that perspective, an average company’s “blast radius” (i.e., the amount of damage that a breach in one employee’s files can do) is predictably extensive.

Unfortunately, the cybersecurity battlefield seems to be tilted dramatically in the attackers’ favor. “Adversaries are two to three generations ahead of defenders,” Pironti said. He added that companies have accepted high degrees of risk for long periods of time by allowing software and code deficiencies to persist, thus giving attackers a daunting advantage.

Evolving Responses from CISOs and the Importance of Good Digital Hygiene

Against this backdrop, the manner in which chief information security officers (CISOs) protect their companies continues to evolve. In years past, many companies adopted a “castle and moat” model of cybersecurity, in which they tried to limit or eliminate external access to their networks.

Now, however, most companies assume that cyberattacks will come from internal access points. As a result, many companies have adopted a zero trust model of security that assumes that every employee, file, and network access point may be at risk. From a resource standpoint, this means that many companies have substantially increased their cybersecurity spending, and will continue to do so.

Many cyberattacks are enabled through human negligence, but Gibson noted that cybersecurity companies can often fortify the infrastructure they monitor. More precisely, artificial intelligence and machine learning can help automate many systems and eliminate or mitigate the damage from human mistakes. “We can actually reduce risk programmatically,” Gibson said.

While it may be tempting to assume that technological breakthroughs will create simple-to-implement techniques to thwart cybercrime, according to our expert panel, that’s the wrong way to think about cybersecurity.

Fulton said that the systematic steps companies can take to accelerate their path toward good digital hygiene are as close as it gets to having a “magic pill” in addressing the cybersecurity threat. “When you get the basics right, you eliminate the bulk of the barbarians,” Fulton said. “If you can eliminate a lot of the playing field of enemies [through good hygiene], now [companies] have an advantage.”

These basics include addressing a set of core questions about a company’s data and potential exposures:

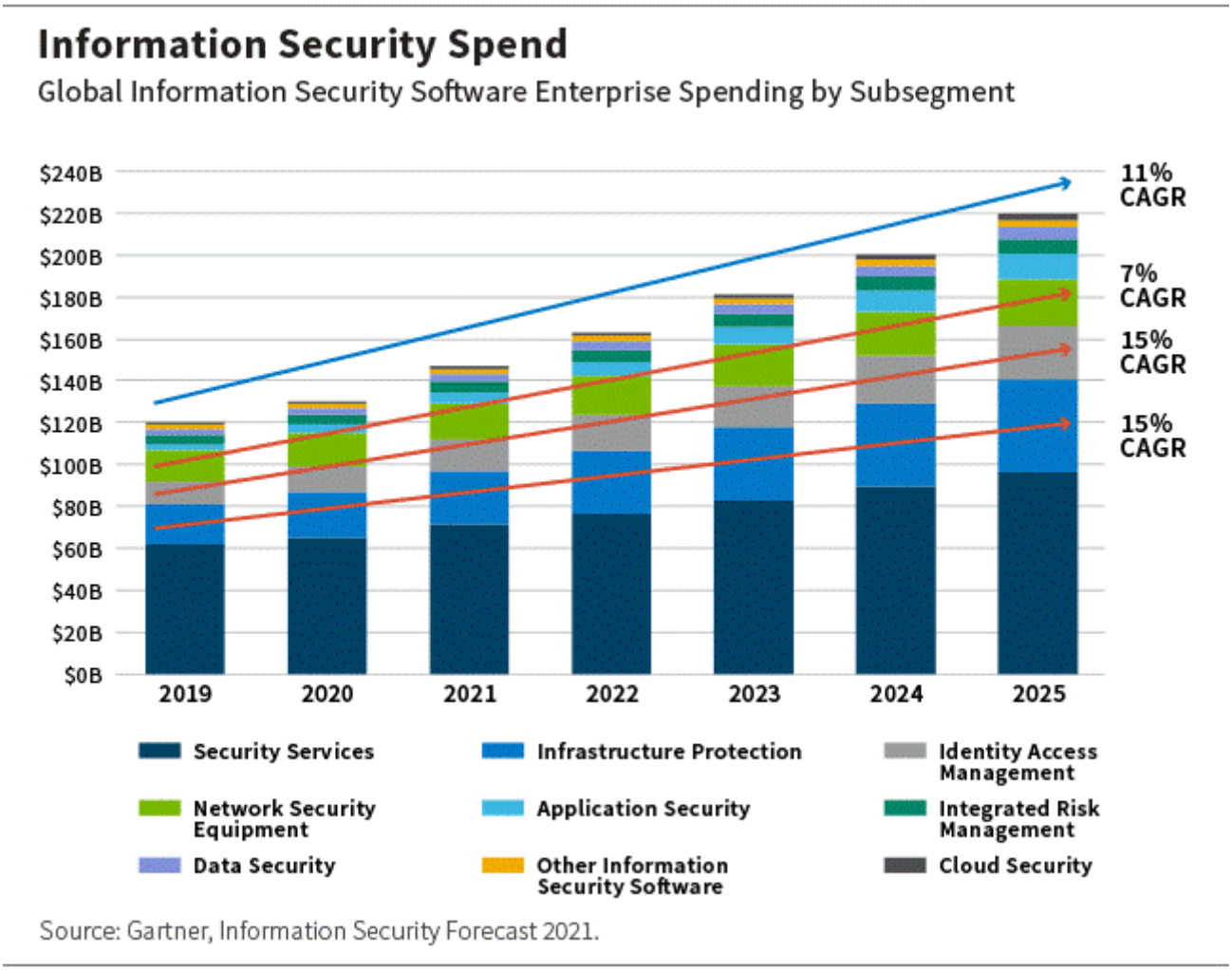
- Where is the company’s most sensitive data?
- Is sensitive data accessible to the right people?
- How quickly can the company detect a breach?
- How can the company effectively investigate, recover, and respond to a breach?

- How can the company reduce risk without disrupting its systems?

Finding Investment Opportunities in a Rapidly Evolving Sector

While the on-the-ground reality of increasing cybercrime is sobering, we believe that these threats present opportunities for investors to identify the next-generation of winners in this critically important field. These opportunities continue to expand amid the COVID-19 pandemic, the shift to the cloud, and the shift to zero trust security postures.

We anticipate that the cybersecurity software sector will grow at approximately 12% year-over-year in the intermediate term, reaching $220 billion by 2025, making it one of the fastest-growing segments of the software market, behind only customer relationship management and database management. Within cybersecurity software, identity endpoint access management and network security equipment are growing the fastest.



When evaluating high-growth cybersecurity companies, there are several factors we monitor closely to determine whether their growth is sustainable and is the stock mispriced in our clients' favor. These include the company's position in cloud computing, barriers to entry, its total addressable market, and return on investment, among other items.

Despite the overall attractiveness of cybersecurity, there are several key areas of concern that we're debating as we test our investment themes:

- Are the expectations for a changed market, which underly the premium valuations for perceived next-generation, realistic?
- Have competitive moats changed as security moves to the cloud?
- Do cloud models, data, or network effects reduce or increase the technology leapfrog risk that has historically marked the cyber security industry?
- Does the need for an integrated view of security posture move the market toward integrated suite-based buying?

By evaluating these questions, we seek to effectively identify current and future investment opportunities effectively within in a sector—and a battlefield—that's rapidly evolving.

To access more insights about how cybersecurity, privacy, and politics are affecting the investing landscape, we invite you to explore other posts about the sessions at our 2021 CONNECTIVITY conference: Privacy and Policy Implications of Connected Commerce and The New Cold War: China

.

Corey Tobin, partner, is a research analyst and co-director of research on William Blair's U.S. Growth and Core Equity team. Nabil Elsheshai, CFA, is a research analyst for William Blair Investment Management.

Disclosure:

This content is for informational and educational purposes only and not intended as investment advice or a recommendation to buy or sell any security. Investment advice and recommendations can be provided only after careful consideration of an investor's objectives, guidelines, and restrictions.

Information and opinions expressed are those of the authors and may not reflect the opinions of other investment teams within William Blair Investment Management, LLC, or affiliates. Factual information has been taken from sources we believe to be reliable, but its accuracy, completeness or interpretation cannot be guaranteed. Information is current as of the date appearing in this material only and subject to change without notice. Statements concerning financial market trends are based on current market conditions, which will fluctuate. This material may include estimates, outlooks, projections, and other forward-looking statements. Due to a variety of factors, actual events may differ significantly from those presented.

Investing involves risks, including the possible loss of principal. Equity securities may decline in value due to both real and perceived general market, economic, and industry conditions. The securities of smaller companies may be more volatile and less liquid than securities of larger companies. Investing in foreign denominated and/or domiciled securities may involve heightened risk due to currency fluctuations, and economic and political risks. These risks may be enhanced in emerging markets. Different investment styles may shift in and out of favor depending on market conditions. Individual securities may not perform as expected or a strategy used by the Adviser may fail to produce its intended result.

Investing in the bond market is subject to certain risks including market, interest rate, issuer, credit, and inflation risk. Rising interest rates generally cause bond prices to fall. High-yield, lower-rated, securities involve greater risk than higher-rated securities. Sovereign debt securities are subject to the risk that an entity may delay or refuse to pay interest or principal on its sovereign debt because of cash flow problems, insufficient foreign reserves, or political or other considerations. Derivatives may involve certain risks such as counterparty, liquidity, interest rate, market, credit, management, and the risk that a position could not be closed when most advantageous. Currency transactions are affected by fluctuations in exchange rates; currency exchange rates may fluctuate significantly over short periods of time. Diversification does not ensure against loss.

There can be no assurance that investment objectives will be met. Any investment or strategy mentioned herein may not be appropriate for every investor. References to specific companies are for illustrative purposes only and should not be construed as investment advice or a recommendation to buy or sell any security. Past performance is not indicative of future returns.