NetScout: Addressing the Most Overlooked Threat to Our Privacy and Financial Well-Being

On August 22, 2013 the Nasdaq shut down for several hours.

As the world's largest electronic stock exchange, nearly two billion shares trade on the Nasdaq each month, including industry-leading companies like Microsoft, Google, Kraft-Heinz, Apple, Starbucks, Costco and Facebook.

The shutdown took place between 10:00 a.m. and 3:30 p.m. That means investors could not buy or sell some of their favorite stocks for almost the entire trading day.

Top officials at the Nasdaq offered little information about what happened. We still don't really know. Some say it was a technical glitch. Others suggest it was a minor software problem.

However, some experts believe the Nasdaq was hacked by a foreign regime. In fact, one theory says that several countries have built "cyber brigades that are capable of shutting down any major exchange for days." Russia is sitting on a "cyber brigade" of more than 6,000 hackers. China also has a cyber brigade of thousands targeting U.S. businesses.

These brigades are capable of hacking anything from personal bank accounts, to power facilities, to our military contractors.

In fact, a year-long probe by the Senate Armed Services Committee determined that the military's U.S. Transportation Command (Transcom) was hacked 20 times over a 12-month period. More important, Transcom was only aware of two of these 20 intrusions.

Cybersecurity threats are growing by the day. That's because more and more people are turning to the Internet for their everyday needs.

NETSCOUT SYSTEMS (NASDAQ: NTCT)

Positives:

- In the last three quarters, NetScout generated $108M in free cash flows, more than any single full year in the company's past.
- On pace to boost its operating margins by 50%+ in five years.
- NetScout has more than 330 Internet service providers as customers, and together they provide almost all of the world's Internet service.
- By 2020, organizations are expected to spend more than $100 billion a year on cybersecurity.
- Several of the world's largest hedge funds have been buying up shares of NTCT in the last few quarters.

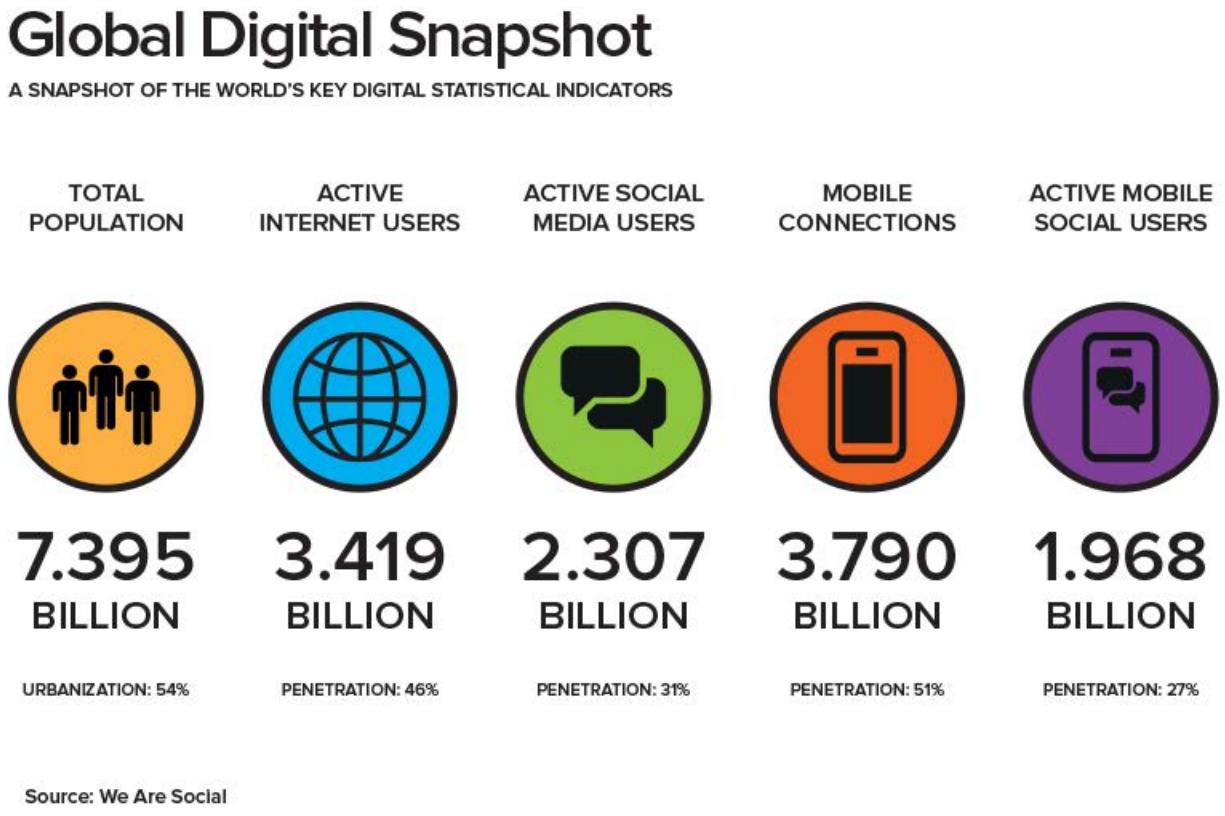
Risk Factors:

- The Internet and cable service providers that make up more than half of NetScout's customers might decide to limit their spending on business assurance ser-vices, due to budget constraints.
- DDoS attacks might fall out of favor and hackers might discover other types of attacks that NetScout isn't prepared to address.
- NetScout's competitors could come out with products that are better.

Investment Synopsis:

- **Buy-up-to price:** $40
- **Fair value:** $70
- **Position size:** 2% of portfolio
- **Exit strategy:** Sell half of the stake once the stock doubles, and let the rest ride long term.

For example, there are now more than 3.4 billion active Internet users, and over 3.7 billion people are mobile phone users. That's more than half of the world's population storing personal and business data over some sort of digital platform.



In the U.S. alone, almost everyone over the age of 12 uses the Internet. Most of us have social media accounts (Facebook or Twitter), use the Internet for banking purposes, and have swiped our credit cards at a gas station or as we buy groceries.

Soon, our appliances and thermostats will be operated through our mobile phones (smart homes), cars will be able to drive themselves (autonomous cars), and industrial machines will have sensors attached to track and improve efficiency (the "Industrial Internet").

In short, almost everything we do will somehow be connected to the Internet.

This will leave us more vulnerable to cyberattacks, where hackers could gain access to our personal information and even our homes, or simply block us from accessing important parts of our online lives.

In fact, cybercrime is one of the most overlooked threats to our privacy and financial well-being and is one of the biggest challenges facing corporate America and our government today.

Cyberattacks: "An Act of War"

In December 2009, President Obama hired Howard Schmidt to be the first U.S. cybersecurity coordinator (better known as the cyber czar).

Schmidt's job was to ensure the safety of stored data throughout the Internet and help the U.S. gain ground in the ongoing "cyber war." Up until then, things had not been going well. A few months prior to his hiring, the U.S. electricity grid was hacked and security officials at the time believed that hackers from Russia and China were trying to steal our infrastructure plans.

Even before that, in 2007, hackers broke into the Department of Defense, Department of Energy, and Department of Commerce, stealing loads of classified information. As of today, officials still do not know who was responsible for these thefts.

A year after Schmidt's appointment, defense contractors Northrop Grumman, Lockheed Martin, and L-3 Communications disclosed that their computer networks had all been hacked.

That's when things got serious, and the Pentagon declared cyberattacks an "act of war." In other words, the U.S. would employ military force if a foreign nation hacked into our government computer systems.

Over the past three years, some of the largest corporations in the world have been hacked.

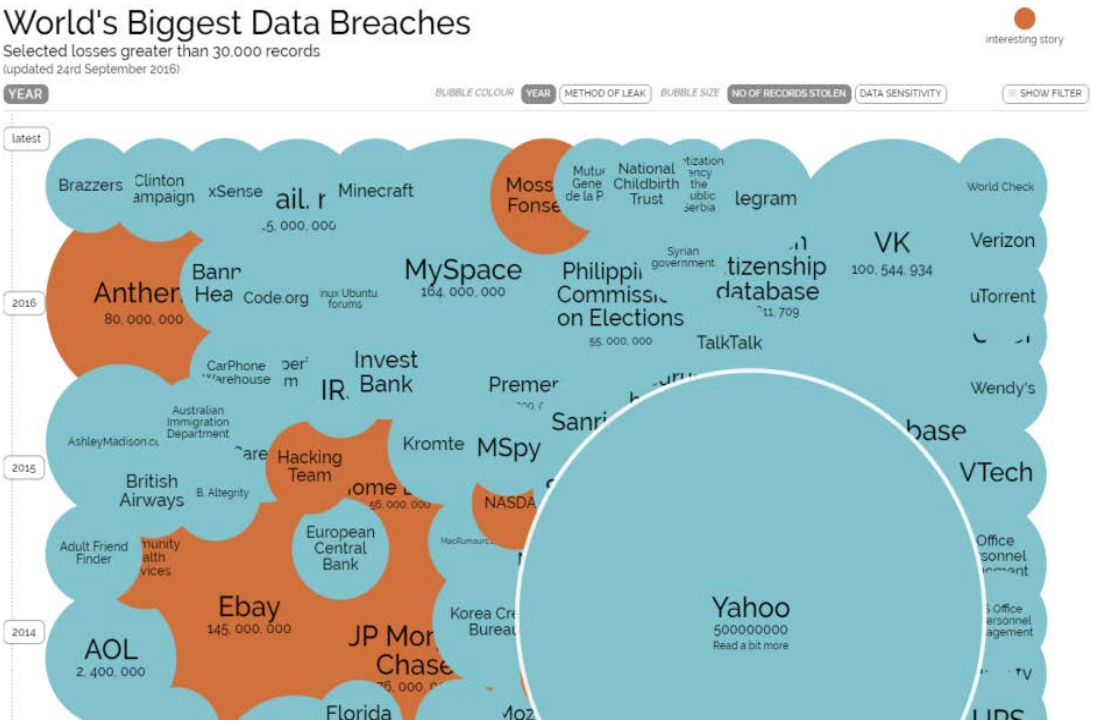
- Sony's PlayStation Network was broken into and more than 100 million user identities were compromised.
- Citigroup was hacked, and data for about 200,000 bankcard holders in North America were compromised.
- Home Depot was hacked, and data on 56 million customers were compromised.
- Target was hacked, and data on over 70 million of its customers were compromised.
- JP Morgan was hacked, and data on 76 million of their customers were compromised.

The list goes on and on.

Ebay, Adobe, AOL, Zappos, Apple, AT&T, Ohio, Texas and California Berkley Universities, hospitals, banks in South Korea and Australia, Experian, British Airways, Sony Pictures, Uber, Ashley Madison and hundreds of other companies have also been hacked.

But it's Yahoo! that gets the gold medal when it comes to being hacked. Over the course of the last few years, the Internet company has been hacked repeatedly, including a recent breach in which personal information for ONE BILLION of its users was compromised.

That marks the biggest breach in the history of the Internet.



Source: GLEAMsocial

As bad as these breaches are on the surface, the implications of this rising trend are even more daunting.

Google keeps track of all the sites its users visit. Credit card companies store all of our personal information. Many of us pay our bills electronically. We post the places we visit on social networking sites like Facebook. These sites also list all of our friends and family members.

Imagine what would happen if all of that information got out.

And utility companies and transit systems are run on computers. Almost every Fortune 500 company has huge amounts of data stored within their networks.

Imagine hacking into the databases of AT&T, Comcast, or Intel. People would pay millions of dollars to get their hands on this kind of intellectual property.

In fact, I wouldn't be surprised if these companies have already been hacked.

The Tiny Company That's Becoming the Industry Leader

One of the most common types of cyberattacks is called a DDoS attack. That's short for Distributed Denial of Service. (And it's often pronounced "dee-doss.")

Basically, what happens in a DDos attack is someone spreads a virus over the Internet that gives a hacker control of the infected computers. Then, the attacker uses all of those computers to bombard a victim's website with traffic, with the goal being to overload the site's servers and force it to shut down.

The army of infected computers that is used in a DDoS attack is called a "botnet." Since viruses are so easy to spread—tip: the next time you get an email from someone offering you a $1 million prize if you "click here," don't do it—it doesn't take a lot of time or money to build botnets that are tens of thousands, or even millions, of devices strong.

Your computer or phone could be part of a botnet right now without you even knowing it.

DDoS attacks aren't new, but they are getting more advanced. In fact, selling access to botnets is an actual black market business now.

According to a paper by TrendMicro Research, you can buy a DDoS attack on the Russian black market for as little as $10. If you want to attack a website for a week, that can be done for just $150.

That's all it would take to knock a small, unprepared company offline. For a week.

Remember the Nasdaq shutdown I mentioned earlier?

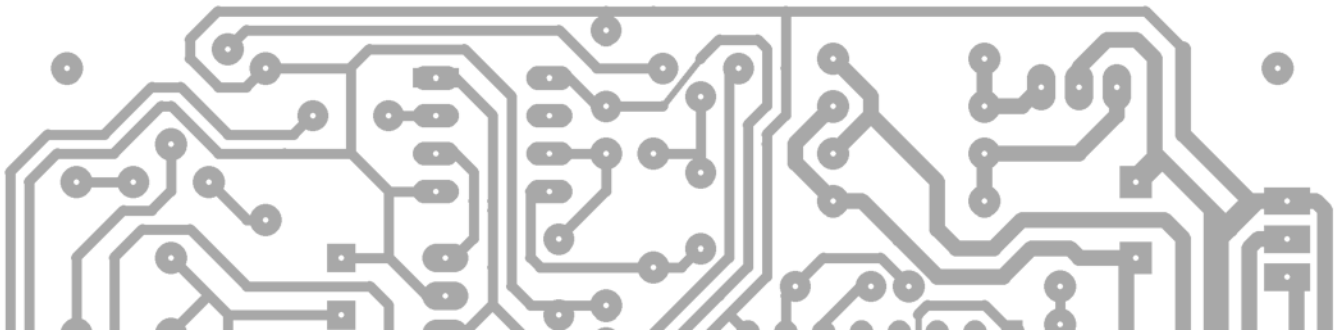
Cyber criminals around the world carry out more than 2,000 DDoS attacks every day.

So how do companies and governments identify these threats and stop them quickly? Most of them rely on a company called **NetScout Systems (Nasdaq: NTCT).**

NetScout is a leader in what's called "business assurance." It helps companies and organizations monitor and protect their networks. And NetScout is fast becoming an industry leader in this market.

In 2015, NetScout acquired a company called Arbor Networks, which has since become NetScout's cybersecurity division.

Arbor began its life as a project sponsored by the Defense Advanced Research Projects Agency (aka DARPA), the very same organization that funded the creation of both the GPS system and the Internet itself.



NetScout's Arbor is the world's top provider of DDoS protection. It has more than 1,200 customers that use its security solutions in 107 countries, including:

- 3 of the 5 largest social media networks
- 4 out of the top 6 U.S. banks
- 5 out of the 6 largest U.S. cable broadband providers
- 8 out of the 10 largest cloud service providers
- More than 90% of the world's tier 1 service providers, including companies like Verizon, AT&T, Sprint, CenturyLink, Telefonica in Spain and Deutsche Telekom in Germany.

Through Arbor, NetScout has more than 330 Internet service providers as customers. Together, these customers provide **almost all of the world's Internet service.**

This has allowed the company to create an all-seeing global Internet traffic monitor that it feeds into its "Digital Attack Map," which shows global DDoS attacks in real time. It looks like this:

Source: Arbor Networks

When you can monitor almost all of the world's Internet traffic and collect data on it in real time, a lot of doors open.

Aside from cybersecurity, NetScout also offers business intelligence services and it helps companies reduce costs and improve the quality of their services.

Last fall, for example, Netscout launched a real-time information platform called InfiniStreamNG. The platform allows users to keep tabs on business performance and cybersecurity and to analyze the incoming data.

Two large tier 1 carriers, one in Europe and one in North America, started using InfiniStreamNG last quarter. The carrier in America signed a five-year $75 million contract.

In other words, because of its unique, worldwide network, NetScout is able to develop all kinds of valuable products and services. And its new, higher margin products are helping customers cut costs as they move into the cloud, while helping NetScout make more money.

Plus, the market for these products and services is huge, and growing.

According to the International Data Corporation (IDC), the world spent about $74 billion on cybersecurity last year. By 2020, it expects organizations to spend more than $100 billion a year.

NetScout (NTCT)			
Market Cap:	$3.4B	Insider Ownership:	35.8%
Revenue (TTM):	$1.1B	52-Week Hi-Low:	$38.40-$26.25
Earnings (TTM):	$0.08	**Balance Sheet**	
P/E (forward):	17x	Cash:	$359M
Free Cash Flow:	$176M	Long-Term Debt:	$300M

NetScout generated about $1.1 billion in revenue last year.

More important, NetScout is focusing on the sectors within cybersecurity that will be a big part of this $100 billion market by 2020. These sectors include:

- Advanced analytics (business intelligence), **expected to grow at 9% per year**
- Application performance management, **expected to grow at 12% per year**
- Cybersecurity and intelligence, **expected to grow at 13% per year**

Over the past three years NetScout has spent $2.5 billion on acquisitions to improve analytics. It built its sales and research & development teams up from 300 to 1,000 people each. And it now has more than 4,000 global customers.

But there is still much more to this story.

NetScout Is Just Getting Started

NetScout's new and growing line of software products have super high margins. They are also more desirable to customers. That's why I expect the company to report strong earnings and higher cash flow in the years ahead.

In fact, these trends are just starting to show up in the company's results.

Last year, NetScout's operating margins came in at 21%. That's up from about 19% a year earlier. And the company expects to boost its operating margins up to 31% within five years. *That's a 50% increase.*

In the last three quarters, NetScout generated $108 million in free cash flows. That's already more than any single full year in the company's past.

NetScout uses this cash to reinvest in the business, make acquisitions, and buy back stock. The company's board has authorized a 20-million-share repurchase plan, of which 6.8 million shares remain. Considering there are 92 million shares outstanding now, that's another 7% of its stock.

Fewer shares mean higher earnings per share (EPS). NetScout grew its EPS by about 12% last year and expects 13%-15% EPS growth in 2017.

That's far better than the average company in the S&P 500, which grew its earnings by 5% last quarter.

Yet, NetScout's stock trades as if earnings are growing at the same pace as the S&P 500. They both trade at 17x forward earnings. Based on the company's huge growth potential, that's incredibly cheap.

Risk Factors

As with any investment, there are risks.

The biggest one with NetScout is the possibility that its service provider customers limit their spending on business assurance services. Internet and cable service providers make up a little more than half of NetScout's overall business, and because these companies compete on the prices of their services, budgets are tight.

If these service providers limit their spending, NetScout's sales could fall… and so could the stock.

That's a risk we're willing to take, though. Any company that doesn't spend enough on the type of services that NetScout offers could end up taking far larger losses down the line.

And they know it.

If a DDoS attack takes down their site, or if their service quality falls because they're not able to monitor it closely enough, customers will cancel. They'll sign up with a more reliable provider. One that is willing to spend to keep its service quality high.

Plus, as service providers around the world roll out their 4G services, they have to spend on business assurance services at the same time. NetScout's international presence offsets a lot of the domestic risk.

Another risk is that NetScout's competitors could come out with products that are better.

That doesn't seem likely, though. The company's global service provider network is a big competitive edge, and already customers are starting to buy NetScout's latest products.

Cyberattacks are getting worse and more frequent, and NetScout offers the best solution to one of the biggest problems. DDoS attacks are the most common type today, but there is always a chance that hackers will create new types of attacks that NetScout isn't prepared to defend against.

But, were that to happen, we would have bigger problems than just NetScout's stock price, and the company is well-positioned to pivot and address any new threats. Most of the top Internet service providers, social media networks, and U.S. banks have all chosen to use NetScout's services.

Smart Money Is Buying

Jeffrey Ubben founded ValueAct Capital in 2000. The fund now manages nearly $13 billion, making it one of the world's largest activist hedge funds. Ubben likes to make concentrated bets in undervalued businesses, then work with management to improve shareholder returns.

Last quarter, **Ubben bought 1.6 million shares of NetScout**, or about 1.8% of the company. It was his only new purchase last quarter, and it's now one of just 14 stocks in ValueAct's portfolio.

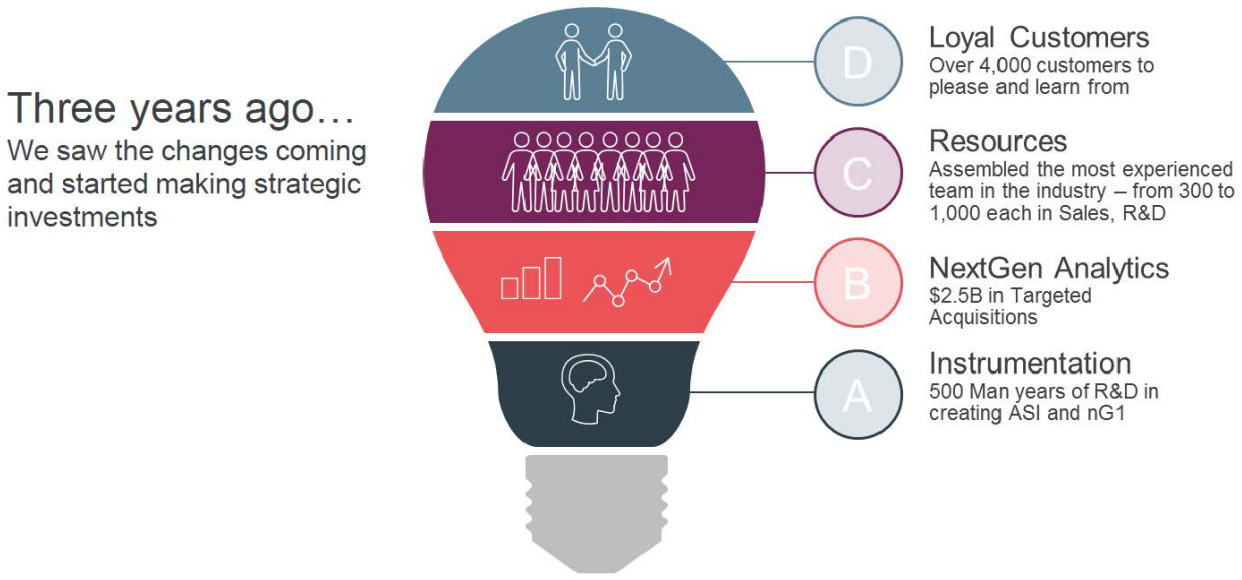
Turtle Creek Asset Management is a Canadian hedge fund that has a stellar 18-year history. It generated compound average annual returns of 25% since inception, turning every $20,000 investment into $1.1 million. The fund **bought 951,000 shares of NetScout** last quarter, or about 1% of the entire company.

Private equity giant **KKR owns 2.7 million shares of NetScout**, a $100 million stake.

And BlackRock, Neuberger, Vanguard, and Franklin Resources all added to their NetScout stakes last quarter. These firms hold NetScout stakes worth between $130 million and $390 million, representing 3.9% to more than 11% of the company's outstanding shares.

These top investors know that cyberattacks are getting worse and more frequent, and they know that NetScout could become the dominant player in this $100 billion-plus growth industry.

Plus, most of the top Internet service providers, social media networks, and U.S. banks all use NetScout's services, along with thousands of other companies around the world.



NetScout's business will grow and become much more profitable in the coming years. If you want to take part in those profits, you need to buy shares now, before NetScout starts blowing away its quarterly numbers and Wall Street starts piling into the stock.

Based on my estimates, NetScout is worth at least twice the current price based on valuation and its huge growth potential.

Longer term, we could see shares move much higher as the company becomes one of the dominant players in the cybersecurity megatrend.

Right now, shares are trading at around $37, far below their fair value of at least $70 per share.

I recommend building a position in NetScout Systems that's 2% of your portfolio, with a buy-up-to price of $40 per share.

On the exit, I recommend selling half of the position once the stock doubles and then letting the rest ride long-term. Based on my estimates, this stock has at least 100% upside potential over the next 12 months.

ALTUCHER'S TOP 1% ADVISORY

SEE YOU NEXT MONTH!

We welcome comments or suggestions at feedback@thealtucherreport.com. This address is for feedback only. For customer service inquires please email customerservice@thealtucherreport.com or call (800) 206-8358. Please note: The law prohibits us from giving personalized financial advice.

Choose Yourself Media forbids its writers from having a financial interest in any security they recommend. All employees of Choose Yourself Media, other than writers, must wait 24 hours after a recommendation is published before acting on that recommendation.

Choose Yourself Media does not recommend or endorse any brokers, dealers, or advisors. This work is based on SEC filings, current events, interviews, corporate press releases, and our own personal networks. It may contain errors, and you shouldn't make any financial decisions based solely on what you read here.