SPRING 2016

William Blair

Client Focus

Cybersecurity: The Battle for Vigilance

Technology solutions are getting better at fighting cybercrime but the risks of being tricked remain

First Line of Defense in Cyber Threats

The first quarter of 2016 had its share of surprises with markets hit early in the year by a freefall in oil prices and fears about the Chinese economy.

The good news is that the markets have bounced back with most stock indexes turning positive by mid-March.

But markets will likely remain volatile given the many wild cards being dealt investors—weak global demand, terror threats, the Fed's posture on interest rates, the health of U.S. wages and jobs—all during an unpredictable U.S. presidential campaign.

The subject of this issue of *Client Focus* features yet another headline-grabbing topic: cybersecurity. Fortunately this is a challenge we can, as individuals, have a direct hand in managing.

It's no secret that modern societies are more and more dependent on the wonders of the internet. But there is a flip side: we can also become victims of the internet. The dangers presented by hackers, identity thieves, and other online criminals surround us. So it is helpful to know that being more diligent and aware of the dangers can be half the battle against such threats.

This issue's featured article, *Cybersecurity: The Battle for Vigilance*, highlights steps we can take to be more safe and secure online.

At William Blair, we believe education and awareness about cybersecurity are key to helping investors protect themselves from possible scams.

We also know that one of the best security measures comes from having a solid relationship with your financial advisor, someone who knows you well and understands your personal financial needs. In many ways it comes down to a common-sense approach to serving clients: ongoing communication and trust.

Our relationship with you is important to us. As always, thank you for the trust you place in your advisor and William Blair.

Sincerely,

John Ettelson
President and CEO

Cybersecurity: The Battle for Vigilance

Target. Sony. WikiLeaks.

Headlines from incidents of online hacking, identity theft, and cyberwarfare just keep piling up. So do the risks and costs. Yet experts say the extent of the problem is still not fully appreciated as it is fed by a basic human feeling: "It can't happen to me."

"Technology solutions are getting better at protecting against attacks. Unfortunately the human element remains," says John Brady, vice president of cybersecurity at the Financial Industry Regulatory Authority (FINRA). "That's where the biggest risks are in well-defended organizations."

Hacking—the criminal invasion and theft of digital records—comes in all shapes and sizes. Hackers target massive computer databases, ATM banking codes, social media networks, email, and messaging.

The only thing that protects that information is a username and password, Brady says.

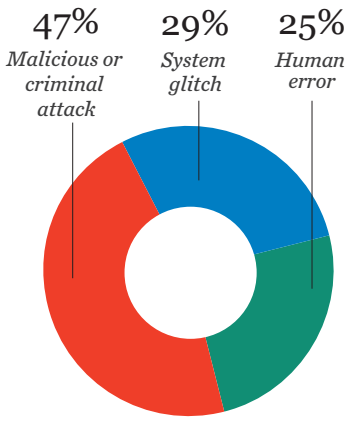
Problems often begin for consumers by sloppy web browsing, opening multiple windows while online in personal accounts, or most commonly clicking on attachments or web links in emails from senders you don't necessarily recognize.

Those attachments, sent by criminals "phishing" for the gullible, are by far the most productive way that "the bad guys," as Brady calls them, invade your computer to inject "malware"—programs that can capture your credentials, record your keystrokes, and track your online behavior and transactions, often without you even being aware of it for weeks, months, or even longer.

Hackers are also becoming more adept at copying designs of corporate websites or banking websites. "They can send a phishing email that diverts you to another website and make it look like you're logging into your real bank," Brady says.

"The fundamental issue is that the attackers hacking the system are very clever," says Larry Ponemon, a cybersecurity consultant for corporations and governments. "They make life challenging," he says.

Root causes of data breach



Source: Ponemon Institute 2015, study of 350 companies in 11 countries

Cyber experts say hacking damage, already in the billions of dollars every year, is likely to worsen before it gets better as the digital collection and storage of personal data—medical and government records, credit card transactions, social networking—continues to grow exponentially as everyday life becomes more exposed to cybersecurity risks.

In addition, the number of devices feeding this global ocean of information grows. These include not just our ubiquitous cell phones, tablets, and e-readers but also, in the expanding universe known as the Internet of Things (IOT), it is plugging us in as users to web-linked devices from home security systems, home appliances, automobiles, and even personal medical devices.

"Your refrigerator, your cars are all going to be connected to the internet," says William Blair equity research analyst Jonathan Ho. "A Chrysler 300 was hacked through its entertainment system. It has happened with medical devices like insulin pumps, heart pacemakers, anything that has Bluetooth Wi-Fi access. People designing these things never thought this would happen."

They call it "the cloud" for a reason—it is a vast expanse of storing and accessing data over the internet instead of one's hard drive—accessible

from a trillion points on the ground. As the cloud becomes more complex, the technology becomes more complex and creates more points of entry to break in.

"The reality is that no industry is immune from hacking activity—governments, retail, healthcare, financials, high tech, law firms," Ho says. "Everyone has data that is valuable in the wrong hands."

> *Cybersecurity breaches are coming in all shapes and sizes.*

The big ones catch all the headlines. In 2008, an estimated 100 million credit card numbers were stolen from Heartland Payment Systems by a hacking ring. In 2013, hackers stole more than 70 million credit card numbers from Target Corp. In 2014, Sony Pictures was hacked allegedly by North Korea after Sony's satirical film *The Interview*. In 2015, the U.S. government said two databases with 22.1 million employee records were stolen by what authorities said were China-based hackers. And late last year Juniper Networks reported its firewall protecting many government and corporate systems had been breached by foreign hackers.

By the numbers

100 million
credit card numbers were stolen from Heartland Payment Systems in 2008

70 million
credit card numbers were stolen from Target Corp. in 2013

Sony Pictures
was allegedly hacked by North Korea after Sony's satirical film The Interview *in 2014*

22.1 million
U.S. government employee records were stolen by what authorities said in 2015 were China-based hackers

$80 billion
cybersecurity market in 2015 growing at 8% annually to defend systems

$19 billion
called for in President Obama's 2017 budget proposal to strengthen cybersecurity

2-factor
authorization step being added by many companies for enhanced security

Cost of protection

Cybersecurity risks and defending company systems are top priorities for companies, governments and not-for-profit groups, with investments in the industry expected to continue to expand. Industry experts who participated in a February webinar sponsored by *Mergers & Acquisitions* magazine estimated this as an $80 billion market in 2015 growing at 8% annually, with about half the spending going into technology products and the balance invested in consulting and advisory services.

Director of National Intelligence James Clapper on February 9 presented his annual threat assessment in testimony to the U.S. Senate Armed Services and Intelligence Committees.

He described in detail the top two imminent national security threats to the United States. One was "homegrown" terrorist groups. The other was cyberattacks that "could lead to widespread vulnerabilities in civilian infrastructures and U.S. government systems."

SECURITY CHECKLIST

Tips for Protecting Your Identity

Keeping clients' accounts safe is a top priority at William Blair, but even the best procedures cannot prevent identity theft if you do not take steps to protect your personal information. Here are some basic steps you can take to help prevent identity theft, according to the Financial Industry Regulatory Authority (FINRA).

- *Use strong passwords and PINs, keep them secret.*
- *Maintain your computer security, up-to-date software.*
- *Use your own computer.*
- *Log out completely.*
- *Use apps wisely.*
- *Be cautious using wireless connections.*
- *Check for secure websites, starting with "https" and displaying a key or closed padlock icon.*
- *Be careful when downloading software.*
- *Do not respond to emails requesting personal information.*
- *Review your account statements when they arrive.*
- *Secure your confidential documents.*
- *Protect your Social Security number.*
- *Do periodic credit checks.*

President Obama's 2017 budget proposal in February called for $19 billion in spending to strengthen cybersecurity by investing in next-generation tools and workforce and fund the Cybersecurity National Action Plan, a strategy to enhance cybersecurity awareness and protections.

In particular, the U.S. government is expected to be a significant customer of security solutions.

"We've had tremendous innovation in security technology over the last five years. In the short term I think things are going to get worse but longer term we will win the war because we have people who are very smart developing some of the most interesting and sophisticated security codes I've ever seen," says Ponemon, head of the Ponemon Institute, which has conducted an annual cost of data breach study of companies globally since 2005.

"Most of the technology in the security space is very good if implemented correctly," he says. "There's a lot of demand for people with the right skills in security."

The latest generation of security intelligence technologies (SIT) are more sophisticated in monitoring the cyber ecosystem, creating forensic maps of criminal activity and pinpointing a threat before it happens.

Companies are getting smarter using more advanced encryption or converting data into an unrecognizable form to keep sensitive information out of the hands of criminals. In addition to usernames and passwords, companies are adding a two-factor authorization step, which auto-generates a new sign-in code electronically for authorized users to complete their log-ins.

What will remain the challenge with every cybersecurity system, however, will be the individual user.

"The risk that people will get duped—I don't think ever goes away," Brady says. "There is no real technology solution to that problem."

Investment Boom in Fighting Cybercrime Seen Getting Bigger

As businesses strive to meet consumers' demands for convenience created by online technology, cybersecurity risks will keep rising and with it the demand for industry innovation, products, and training, says William Blair equity analyst Jonathan Ho, who covers the cybersecurity sector.

"We continue to view cybersecurity as a sector that growth investors need to have exposure to as the value proposition continues to increase for these technologies," says Ho in a recent report. "The need for better algorithms, machine learning, and automated tools that can discern threats from false positives is creating the next wave of start-ups and technologies," he says.

Ho says the explosive growth of "smart" devices from home appliances and autos to personal health, recreation, education, and online commerce—a technology movement known as the "Internet of Things"—is creating a universe of web-linked technology businesses use to track consumer behavior.

"It is simply a matter of time before these areas are targeted by hackers, which will create even more opportunities for cybersecurity companies," Ho says.

Ho closely follows three of his favorite cybersecurity companies: Palo Alto Networks, known for firewall technology; Proofpoint, an email specialist; and Imperva, recognized for database technology.

Cybersecurity stocks have seen a steady rise over the past five years with valuations high at the end of 2015. But as the market consolidates, he expects plenty of opportunities to increase sector exposure.

"It is a long-term growth area because cyber problems are not going to be fixed anytime soon," Ho says.

To receive Ho's report, contact your William Blair advisor. Visit **williamblair.com/ResearchCoverage** *for disclosure information.*

An Insider's Look at Personal Security, Online and Off

Frank Rodman has spent his career protecting diplomats, CEOs, and billionaires. Think Princess Diana, Nelson Mandela, Michael Dell, Madeleine Albright. Not to mention the many others who work hard to keep their names out of the headlines.

Today Rodman is president of New York-based TorchStone Global, a consultancy that he started with several security veterans, including Eljay Bowron, a former director of the U.S. Secret Service. Its mission is managing the security risks of the world's wealthiest organizations and individuals.

William Blair advisor Bob Fix has worked with Rodman since TorchStone was founded in 2010.

From advising on cybersecurity to terrorism scares, this business is growing. The world seems to become more risky by the day.

Rodman says clients are concerned about their physical security. But as the collection and storage of data mount, they increasingly worry about their online security, especially identity theft and fraud.

"Protecting yourself from cybercriminals is actually not that much different than protecting yourself from traditional criminals," Rodman says. "Both require adopting good security habits both online and in the physical world. Unfortunately, most people don't change bad habits until they have a compelling reason."

The sad lesson for victims, he says, is that "a cybercrime can be just as personal and invasive and violating as a physical crime."

TorchStone encourages companies interested in evaluating their cybersecurity safety to start with assessing real-world physical security issues—doors, drawers, locks, windows, luggage, purses, wallets, papers.

Even if a client has the most sophisticated software on the planet, he says, it won't help if someone can get hands-on access to your computer, network, or old-fashioned paper documents.

Rodman tells the story of a client whose laptop bag was stolen while he was traveling. The client later recovered the laptop bag but he came to Rodman very upset that someone might have gained access to his computer.

The stolen bag, the client said on questioning, had also contained his driver's license, checkbook, a letter from the IRS about an audit that included his Social Security number, and a letter from his divorce attorney outlining how his assets might be divided.

Rodman's Beginnings in the U.S. Diplomatic Security Service

Frank Rodman began as a special agent for the U.S. Diplomatic Security Service in the late 1980s after the Beirut embassy was bombed. Congress decided to expand security for embassies worldwide.

One of his many postings was heading diplomatic security for the U.S. embassy in Tokyo in what he thought would be a "quiet" assignment given Japan's reputation for public order and respect for authority.

Then the Tokyo subway system was attacked by terrorists using poison gas, a Philippine airliner was bombed, and the Kobe earthquake killed 5,000 people and destroyed the consul general residence.

"So you can't tell what risks are around the corner regardless of where you are," Rodman says.

That rule holds not just in the real world but everywhere online.

"As a former government employee, I received a notice recently that my personal information was compromised in a hacking incident. So if even the government can't secure our data appropriately, what makes us think we will be able to do it on our own?" he says.

"'You're concerned about your laptop?'" Rodman told him. "They had everything they wanted in physical documents," Rodman recalls. "It's a really good example of how we focus too much on technology than on our own behavior."

The importance of being prepared—expecting the unexpected—is vital, he says.

Rodman says many of the most common-sense safeguards for cybersecurity are obvious once the individual becomes aware of how technology becomes vulnerable.

Rodman has learned over the years that people usually follow three approaches in handling security risk.

[1] *The first is "hope." People live in the moment and hope they remain safe, he says. So if their identity or security is compromised, they hope someone swoops down and saves them. They think they don't need a plan.*

[2] *The second approach is to deal with a problem when it happens. They push the panic button and assume help will arrive. But the speed and effectiveness of that strategy, Rodman says, depends on the availability of the help at the time.*

[3] *"The third strategy and the one we promote is the integrated approach where you combine awareness of your environment, thoughtful plans, training and testing against those plans," Rodman says.*

He highly recommends using credit monitoring services, which will flag whether someone's identity has been stolen. Changing and keeping passwords secret is also key but so is keeping software, especially antivirus software, current.

"Software is the only industry known that's allowed to sell us something that needs to be fixed on a weekly basis," he says. "So we need to keep our software patches current and our antivirus software up to date. New viruses are constantly being developed and deployed."

Criminals will continue to increase their use of social networking sites to identify targets, says Rodman, recalling the kidnapping of hedge fund manager Eddie Lampert in Greenwich. His kidnappers went online first to find the wealthiest people in Connecticut. Lampert was listed and he was then chosen as a target because he was accessible.

Security and awareness while traveling are also important.

"In some countries it's a physical security threat. In other places like China, for example, people are more worried about the security of their digital information while traveling," Rodman says. "So we've designed a program of essentially bringing clean devices to those places—stripped of any proprietary or personal information. When those devices are turned back in they are swiped clean again."

Vigilance is the key for every user of online devices.

"We all rely on the internet and use it for everything. But it creates a lot of vulnerability. We try to help clients understand those vulnerabilities and put some good security practices in place," Rodman says.

Preparedness. Awareness. Vigilance.

The importance of being prepared—expecting the unexpected—is vital.

Security and awareness while traveling is essential.

Vigilance is the key for every user of online devices.

William Blair
222 West Adams Street
Chicago, Illinois 60606

PRESORTED
FIRST CLASS
U.S. Postage
PAID
Oakbrook, IL
Permit #100

CLIENT SERVICE

My William Blair Update

We are entering the final phase of our two-year initiative to transform your client experience. If your assets are held in custody by William Blair, we are changing our custody and clearing platform to National Financial Services LLC (NFS), one of the premier clearing providers in the industry.

Watch your mailbox for *one envelope for each account*

In early April, you will receive one 9"x12" envelope per account from William Blair with important information about the transition to NFS. For many clients, the information in the booklet will be for review only. In other instances, you will need to complete, sign, and return some forms in the booklet by May 6, 2016, to successfully transfer your account to NFS for custody and clearing.

Beginning in mid-May 2016

NFS, at William Blair's direction, will become responsible for certain operational activities, including: clearance and settlement of securities transactions; custody (or safekeeping), receipt, and delivery of funds and securities; and preparing and sending of transaction confirmations and periodic statements for your accounts. These changes will allow us to provide you with enhanced services, technology, and support for your investment account(s).

Our commitment

William Blair and your dedicated advisory team will continue to provide the trusted investment services that you have come to rely on. As always, we remain committed to protecting the safety and security of your account(s). If you have any questions upon receiving your package, please do not hesitate to reach out to your advisor.

You will receive one envelope for each William Blair account in early April.

National Financial Services LLC ("NFS") is an independent company, unaffiliated with William Blair. NFS has not been involved with the preparation of this content supplied by William Blair. 751828.1.0