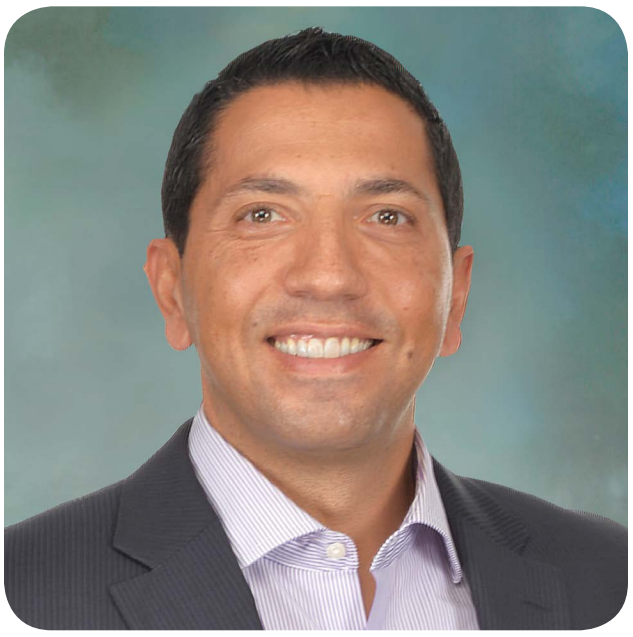
The Cybersecurity Threat in New York City



Jerry Ravi
Partner at EisnerAmper, LLP

EISNERAMPER
ACCOUNTANTS & ADVISORS

Michael Nizich, Ph.D.
Director, Entrepreneurship and Technology Innovation Center at New York Institute of Technology

NYIT

With cyber breaches at the SEC and Equifax making headlines, many New York City business leaders are concerned about the risks their companies could face. The number of data breaches in the U.S. hit a half-year record high of 791 in the six months ending June 30, 2017, according to recent figures from the Identity Theft Resource Center and CyberScout, the identity protection and data risk services firm.

As the financial capital of the world and hub of leading health care institutions, New York City holds a trove of the kind of data cybercriminals love. This realization isn't lost on government leaders. Earlier this year, New York State finalized regulations that require banks and insurance companies to meet specific security standards and report breaches. And this past summer, Mayor Bill de Blasio announced a plan to invest $30 million to turn New York City into a cybersecurity hub. The plan seeks to create 3,500 cybersecurity jobs.

While such efforts may serve as a deterence, cybercriminals aren't likely to slow their efforts anytime soon. So what can New York City's business leaders do to protect their organizations? Crain's Custom recently spoke with Jerry Ravi, partner at the full-service accounting and advisory firm EisnerAmper, and Mike Nizich, director of the Entrepreneurship and Technology Innovation Center at New York Institute of Technology, for their insight on the current cyberthreat facing New York City companies and how companies can protect themselves.

Crain's: What are the most pressing cybersecurity issues you are seeing right now among New York City firms?

EISNERAMPER **Jerry Ravi:** The most pressing issues around cybersecurity are two-fold: failure to perform a proper and continuous information security risk assessment, and failure to monitor ongoing risk exposure. We see firms starting to move in the right direction. However, establishing and monitoring key internal controls is the cornerstone of good security posture.

Just recently, and once again, we heard of a major breach—Equifax. This is just another case in which a company failed to properly patch a vulnerability in its system. Patching is fairly simple and can be monitored via the performance of a vulnerability assessment. Most firms perform vulnerability assessments at least annually, and oftentimes they are notified of vulnerabilities through their software vendors and consultants.

My recommendation is to move to a continuous vulnerability assessment, thus allowing for early detection of risks. At the end of the day, it is so important to be vigilant and know the context of the issues we face when it comes to cybersecurity. For example, there are patching vulnerabilities with our mobile phones. Just recently, Google pushed out a significant patch fix for some of its mobile devices. This patch closed the doors for hackers who could potentially access information, such as your credentials and data on your phone. Again, the simple fix was to install the patch.

NYIT **Mike Nizich:** I think some of the most pressing cybersecurity issues right now among New York City firms are both an incomplete understanding of cybersecurity threats and vulnerabilities among executives and decision makers, and a shortage of skilled workers to combat and address those cybersecurity threats and vulnerabilities. High-level executives need to have a clear understanding of the cybersecurity

landscape in order to address the planning and budgeting needed to build a holistic security plan and meet specific protocols required by the government, such as the National Institute of Standards and Technology (NIST) cybersecurity framework. NIST establishes the policies that companies and organizations should follow in order to protect their critical infrastructure. In addition, there may be other security-oriented regulatory protocols that must be followed, including HIPAA and Sarbanes-Oxley that could greatly increase the risk of a breach if not adhered to.

In general, I believe there is a less than optimal level of understanding regarding the U.S. cybersecurity workforce, and the challenge of finding talented personnel to fill cybersecurity positions. As per the National Security Agency, there are currently 240,000 unfilled jobs in the field of cybersecurity, which means that even if every computer science student in the country were hired for this field of work, the workforce would continue to fall short by three-quarters of the gap. This especially poses an enormous challenge to corporations, which compete with the government to hire their own cybersecurity specialists.

Crain's: Cybersecurity challenges change quickly from year to year. What are the latest threats—and do you see these threats in local businesses?

EISNERAMPER **Jerry Ravi:** Two threats continue to be top of mind. First, insider negligence is still a growing issue. Employees are not well trained on what to do when they see something suspicious. In addition, they are also not well trained on what not to do (such as click on the malicious link).

The second threat is ransomware. Ransomware continues to hit firms of all sizes. In essence, it starts with malicious software that's installed on your system which is designed to block access until a sum of money is paid, usually in Bitcoin. Local businesses are absolutely a target, and, for the most part, hackers target areas where they feel the success rate is high. Local businesses can find ways to stay informed on key vulnerabilities impacting their area, through threat intelligence groups, peer groups and local government agencies.

"Insider negligence is still a growing issue. Employees are not well-trained on what to do when they see something suspicious."

— Jerry Ravi, Partner at EisnerAmper, LLP

NYIT **Mike Nizich:** I agree about the serious threat that ransomware poses to information security. Unfortunately, many programmers, even at the student level, are able to create the code for this dangerous software. Once the code infiltrates the network, it can run rampant, locking the user out and encrypting all data. The only way to get access to the system is to pay the ransom. Hospitals and banks were recently targeted by what's known as the 'WannaCry' virus, which targeted large organizations, among many others, that had the resources to pay the ransom—and prevented them from accessing necessary data.

As threats become more commonplace, businesses have become more familiar with the technological tactics of cybercriminals, such as phishing, where users click on a link that requests their data, unknowingly handing information over to the criminals; or pharming, where users enter the address of the desired website, only to be redirected to a duplicate fake website which steals user names and passwords.

However, many companies and their professionals may be unaware of other types of social-engineering tactics. In these instances, criminals may simply communicate with an individual to collect private information that allows them to hack into the system. New York City business professionals, who often find themselves in densely populated environments and tend to rely on mass transit, may be more exposed to these types of criminal behaviors. Populous environments create the ideal situation for criminals to capture information, allowing them to obtain information simply by overhearing a discussion between employees or prompting an individual to inadvertently reveal information through casual conversation.

We're also seeing more companies taking advantage of trends such as cloud-based storage systems and the Internet of Things (IoT). Cloud-based systems provide a more affordable option for storing data, but they also present new threats and vulnerabilities that many businesses and executives may be unaware of. For example, many executives may be unaware that most cloud-based software is actually centralized and stored with the data of thousands of other companies. While this helps to save on costs, a hacker now only has to make one successful attack to gain access to data from thousands of companies.

Many of today's devices are taking the form of more convenient 'smart devices,' thanks to IoT. Even a piece of equipment as simple as a commercial air-conditioning unit could provide cybercriminals with access to an organization's network. While the HVAC technician may no longer need to visit the site to fix the AC unit, thanks to the unit's smart technology, this solution has exposed the business to a series of vulnerabilities that no one knows exists—except the bad guys.

Crain's: How do cyberthreats against large organizations differ from those faced by midsize and smaller organizations?

EISNERAMPER **Jerry Ravi:** Actually, smaller organizations could be more vulnerable than larger. It depends on the overall risk profile and type of business, and the type of information and data held by the company (for example, protected health information or personally identifiable information).

With that said, there are two main differences between larger and smaller organizations. First, it starts with their ability to utilize and attract the resources needed to combat these risks. Typically, larger organizations can attract a better pool of talent. Second, larger companies, by their very nature, have more employees and can be more complex. More employees translates into more risks. Cybersecurity starts with the employees and is a human/behavioral issue, rather than a purely technical one. Smaller and midsize companies can take advantage as they're able to monitor and respond to risks quickly.

NYIT **Mike Nizich:** Similar to the way that a burglar would target rich neighborhoods, a cybercriminal will target the bigger companies that may have the most valuable data. These larger companies could experience a loss of revenue from customer loss or even a loss in stock value simply from the news of being hacked. Whereas a small business could lose its entire life savings, often times the larger corporations experience the greater loss of public trust and have a difficult time regaining their footing once they've been hacked.

Crain's: Which New York City industries are most likely to be affected by cybersecurity threats—and what types of threats are they seeing?

EISNERAMPER **Jerry Ravi:** I typically see more activity in areas where there's more risk. These industries include both financial services and health care, which have access to and hold sensitive data that is well worth it to hackers. Some retailers are also popping up with more vulnerabilities than in the past, particularly around the loss of data or data theft. The means in which this occurs are mostly phishing and social engineering.

I would like to elaborate on the 'loss of data or data theft' threat. More and more, this threat is becoming a major issue. Often firms are failing to monitor their environment, which includes access to their files and systems by both employees and third-party vendors. The continuing increase in data loss and theft is due in large part to two factors. One is compromises in insider accounts, increased by far wider employee and third-party access to sensitive information than is necessary to do their jobs. The other is a failure to monitor. Access and activity around email and file systems where most confidential and sensitive data moves and lives are not monitored thoroughly.

Technology can help with this problem as many cost-effective software products and tools such as End Point Security and Data Loss Prevention are at our disposal. Firms can solicit advice from their third-party consultants for recommendations on what tools to select and implement. In addition, accounts can be better protected by implementing two-factor authentication across key areas and systems. Technology tools are available to enable this feature, thus lowering the risk that a user's credentials are stolen.

NYIT **Mike Nizich:** Any company that has valuable data could be targeted, especially those entrusted with data relating to health care, finance or e-commerce. There have even been instances where health care data has been stolen in hopes of being sold to companies that target individuals with specific illnesses.

"Any company that has valuable data could be targeted, especially those entrusted with data relating to health care, finance, or e-commerce."

— Michael Nizich, Ph.D., Director, Entrepreneurship and Technology Innovation Center at New York Institute of Technology

Both businesses and individuals are still adjusting to the fact that there's a market for information right now on the dark web, and because we're overcoming that learning curve, it seems that criminals have the upper hand.

Leading law enforcement agencies are now beginning to establish cybersecurity task forces and formalize cybercrime investigation procedures, in the hopes of better understanding how these criminals operate. Highly specialized, trained law enforcement officers will be required to catch these savvy criminals who understand the ramifications and penalties associated with their actions.

Crain's: Hacking was the top type of cybersecurity breach in Verizon's 2017 Data Breach Investigations report. Most organizations are aware of the threat of hacking, so why are they so vulnerable? What can New York City firms do to protect themselves?

EISNERAMPER **Jerry Ravi:** I agree that firms are aware and know of the issue. Where they are lacking is [in creating] a security program and overall plan to deal with the issues. When advising my clients, I try to start by focusing on three things, as follows: (1) Be proactive. Offense is the best defense. (2) Promote cybersecurity awareness across the firm every day to build a risk-aware culture. (3) Continuously identify and monitor your risks.

There are many things that a small to midsize company can do to combat this ever-growing, ever-changing risk. We just need to stay in front and make it a priority to manage the risks going forward.

NYIT **Mike Nizich:** A company's vulnerability will often stem from its software, rather than its hardware. Every software has a patch program in place, which is designed to install updates, fix bugs or improve the program's performance. With these patch programs, users of an organization are unwittingly exposed to security vulnerabilities. Criminals can use free, downloadable programs to detect whether a business has updated its software with new patches. A criminal with knowledge of the software and the patch's vulnerabilities can then exploit these weak spots and gain access to the system and its data. By patching security vulnerabilities, companies can avoid this scenario.