View this email in your browser

January 15th, 2024

Dear Regina,

Welcome to BioMarketing Insight's monthly newsletter.

Hope everyone had a good holiday and had time to be with their loved ones, family, friends and colleagues .

Welcome to a New Year, 2024 that will be the best year ever.   In order to do this, we must be prepared and do our due diligence to stop cyber attacks. This month I will cover "No Organization is Immune to Cyber Attacks". To find out more, go to the Table of Contents and click on the article link.

If you missed last month's newsletter on "Why There Are Three Holidays in December." Click here to read the article.

enjoy the music from the Berklee School of Music in their song "What the World Needs Now," and ending with Celine Dion and Josh Groban with "The Prayer".

Please read on for other current news in the Table of Content below. The next newsletter will be February 15, 2024.

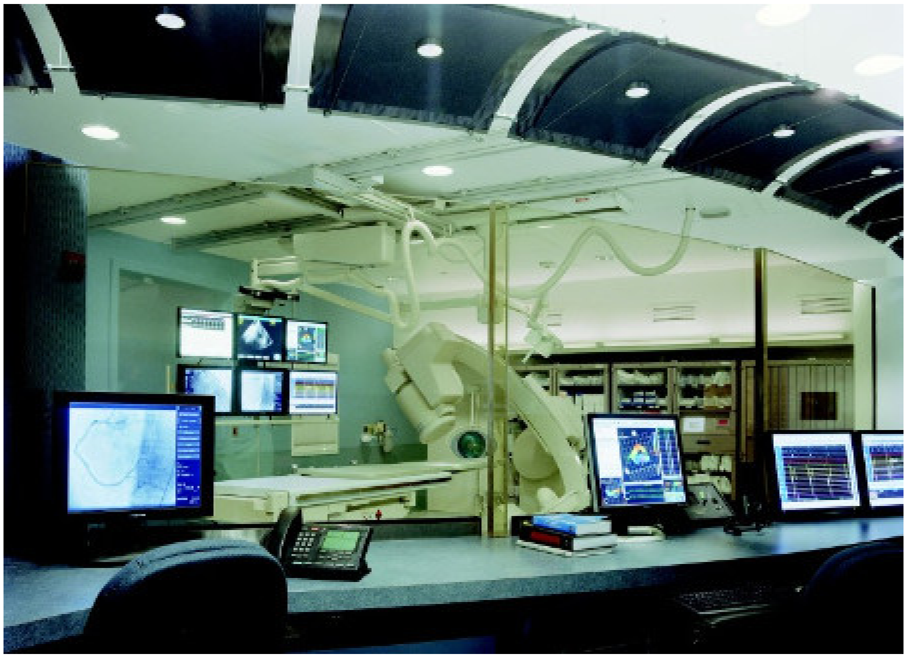
We encourage you to share this newsletter with your colleagues by using the social media icons below, or by simply forwarding this newsletter or use the link below. Should you or your colleagues want to join my mailing list, click on "join my email list" link below.

Sincerely,
Regina Au
CEO, New Product Planning/Strategic Planning
BioMarketing Insight

Share Tweet Forward

Table of Contents

Join my mailing list



Developing a Product? Commercializing a Product?

If you are developing a product and have not conducted the business due diligence to determine commercial viability or success, contact me for an appointment. For successful commercial adoption of your product or looking to grow your business, contact me for an appointment.

For more information on our services, click on the links below:

Product Development
Market Development
Marketing Strategies
Scenario Planning - for more information, email me.

Top

HYBRID EVENT: You can participate in person at Boston, Massachusetts, USA or Virtually from your home or work.

Second round of abstract submission closes on October 12, 2023

3rd Edition of International Vaccines Congress

October 23 -25, 2023 | Boston, Massachusetts, USA

3rd Annual International Vaccine Congress (IVC 2023) Conference on October 23-25, 2023 in Woburn, MA

I am pleased to announce that I spoke at the IVC 2023 Conference in Woburn, MA on October 23 - 25, 2023. The title of my presentation is "Lessons Learned from the Covid - 19 Vaccine and What is Needed When Developing a Vaccine for a Successful Rollout". For more information on my presentation, click here. For more information on the conference, click here.

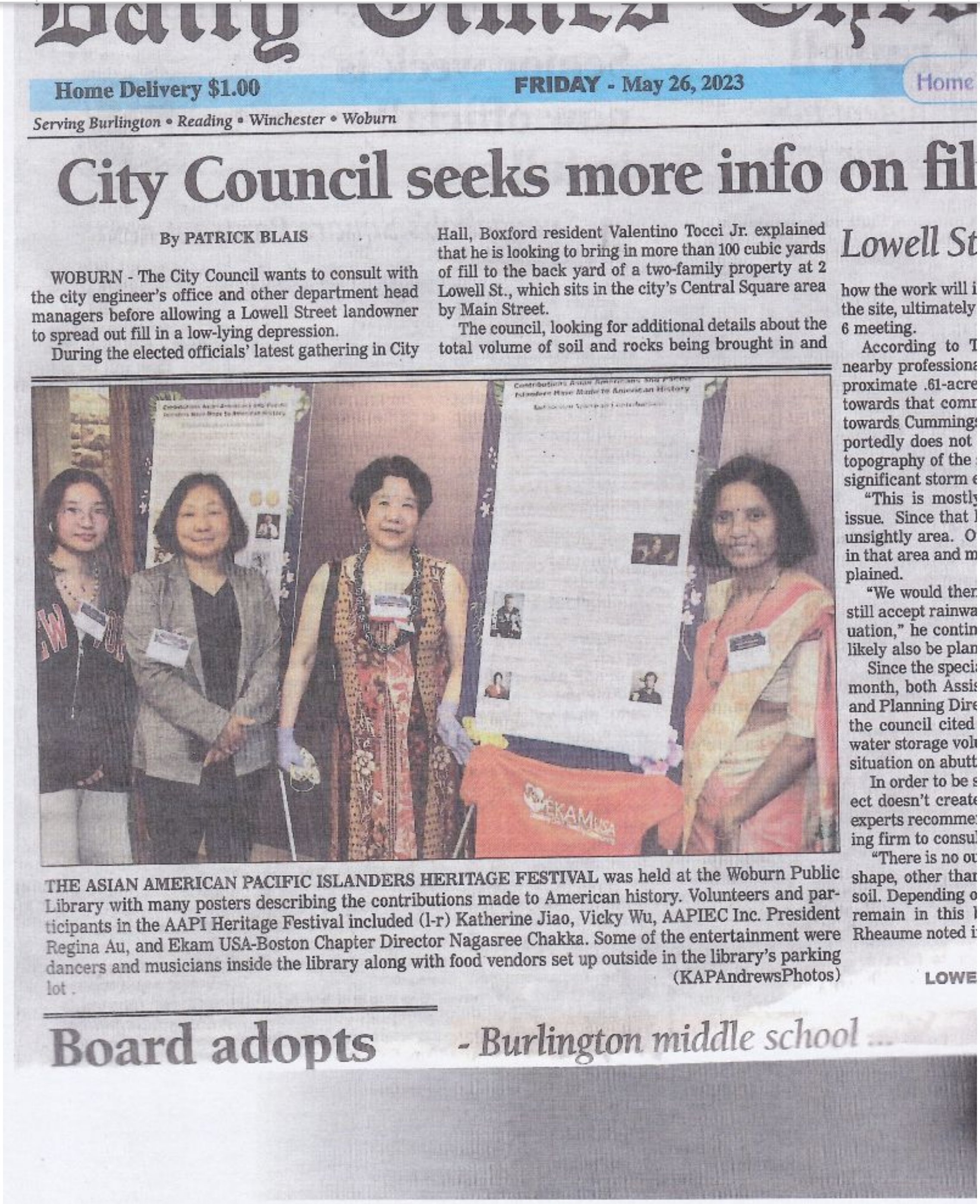
Top

Recap of the AAPI Heritage Festival - Saturday, May 20th, 2023

to build awareness and educate our community on the various cultures and contributions the different Asian and Pacific Islanders ethnic groups have brought to enrich our American History.

Our Festival made the front page of the Daily Times Chronicle. See the article and pictures of our speakers, musicians and performers. In addition, we had our "Contributions AAPI Have Made to American History" Exhibit on display in the lobby and continued on into the program room. More pictures will be revealed next month.

Guest Speakers: Massachusetts State Representative Vanna Howard
Mayor Scott Galvin of Woburn
Special Guest Musician: Kevin So
Guest Musician: Entian Lee, Chinese Zither
Guest Performers: Swasti Bhargava & Aanvi Bhargava, Ekam Boston
Anvee Gudipati, Sreshta Mahavadi, Ekam Boston



Home Delivery $1.00 FRIDAY - May 26, 2023 Home

Serving Burlington • Reading • Winchester • Woburn

City Council seeks more info on fil

By PATRICK BLAIS

WOBURN - The City Council wants to consult with the city engineer's office and other department head managers before allowing a Lowell Street landowner to spread out fill in a low-lying depression.

During the elected officials' latest gathering in City Hall, Boxford resident Valentino Tocci Jr. explained that he is looking to bring in more than 100 cubic yards of fill to the back yard of a two-family property at 2 Lowell St., which sits in the city's Central Square area by Main Street.

The council, looking for additional details about the total volume of soil and rocks being brought in and

Lowell St

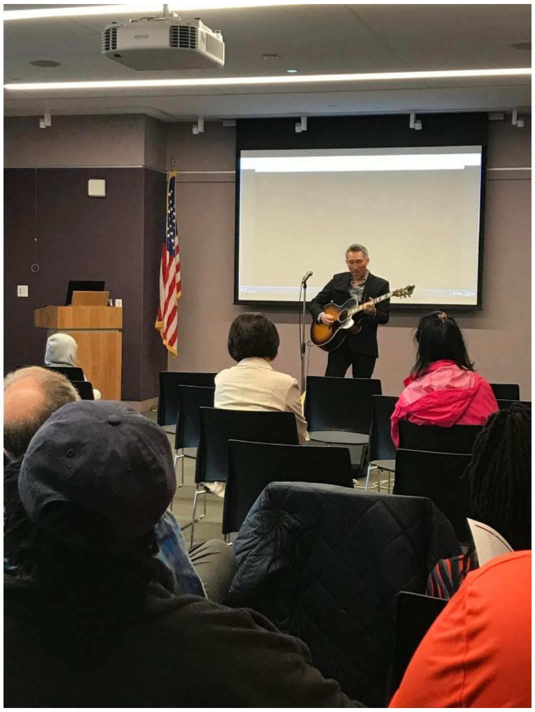
how the work will i
the site, ultimately
6 meeting.
According to T
nearby professiona
proximate .61-acre
towards that comr
towards Cummings
portedly does not
topography of the
significant storm e
"This is mostly
issue. Since that l
unsightly area. O
in that area and m
plained.
"We would ther
still accept rainwa
uation," he contin
likely also be plan
Since the speci
month, both Assis
and Planning Dire
the council cited
water storage vol
situation on abutt
In order to be s
ect doesn't create
experts recomme
ing firm to consul
"There is no ou
shape, other than
soil. Depending o
remain in this l
Rheaume noted i

LOWE

THE ASIAN AMERICAN PACIFIC ISLANDERS HERITAGE FESTIVAL was held at the Woburn Public Library with many posters describing the contributions made to American history. Volunteers and participants in the AAPI Heritage Festival included (l-r) Katherine Jiao, Vicky Wu, AAPIEC Inc. President Regina Au, and Ekam USA-Boston Chapter Director Nagasree Chakka. Some of the entertainment were dancers and musicians inside the library along with food vendors set up outside in the library's parking lot . (KAPAndrewsPhotos)

Contributions Asian Americans and Pacific Islanders Have Made to American History
EKAM USA

Board adopts - *Burlington middle school ...*



HERITAGE FESTIVAL
Thank you to our sponsors!

Asian American
and Pacific Islander
HERITAGE FESTIVAL
Thank you to our sponsors!

Top

Inspirations

Enjoy the song "What the World Needs Now" virtually with the students from the Berklee School of Music.

Practice Good Hygiene Every Day.

Let's End with Celine Dion & Josh Groban Singing "The Prayer"

Top

Lioness

FOR THE FEMALE ENTREPRENEUR

One Biotech Executive's View on the COVID-19 Vaccine

I am pleased to announce that my article on the COVID-19 Vaccine was published in Lioness Magazine. To read my article click on the link here.

Top

No Organization is Immune to Cyber Attacks

In 2023, healthcare organizations experience its worst year ever for cyber attacks. It's not the number of attacks but the attacks have been more damaging and affected more people, says John Riggi, national advisor for cybersecurity for the American Hospital Association.

About 106 million individuals have been affected by cyber attacks involving healthcare organizations, according to federal data on health data breaches says Riggi, compared to about 44 million people affected by health data breaches in 2022.

This translates to nearly 1 in 3 Americans have been affected by a health data breach this year.

This is already a scary number according to Riggi and it will continue to grow since some attacks may not yet been reported to the government. The U.S. Department of Health & Human Services only requires organizations to disclose any breach of health data involving at least 500 individuals.

Riggi estimates there would be about 500 hacks reported in 2023. The average breach is affecting more than 200,000 individuals, Riggi says.

“The bad guys have figured out it's not the number of attacks. It's where you attack,” he says.

“So they're gaining access to data databases that have large volumes of data.”

2023. HCA Healthcare, the nation’s largest for-profit hospital system, said it suffered a “theft” of health data affecting as many as 11 million patients.

Just last month, Ardent Health Services, which operates 30 hospitals in six states and cover more than 200 care sites said it suffered a ransomware attack. The hospitals have had to postpone elective surgeries and temporarily divert services. Electronic medical records were offline, said Ardent where its MyChart services and on-demand video visits were temporarily unavailable.

Health systems and hospitals have also been victimized by attacks on third-party services or breaches targeting their vendors and contractors, Riggi says.

Many healthcare organizations were affected by a breach involving MOVEIt, a well-known file transfer tool, Riggi notes. A Russian ransomware group known as Clop was responsible for the attack. The Centers for Medicare & Medicaid Services was among those affected by the attack, with a contractor suffering a breach, the agency said.

Breaches in 2023 shows that all health systems and hospitals are vulnerable, even large organizations. “It just goes to show one that no organization is immune, that no matter how much money you throw at this problem, we can't defend our way out of this issue,” Riggi says. “There will always be some vulnerability present in any system, including government organizations, which have been victimized this year as well.”

Ransomware groups are infiltrating software and encrypting networks and seeking payments from hospitals to restore access to networks. Some attackers are increasingly going after the health data itself and holding that up for ransom. “They are just contacting the victim and saying, ‘We have your data. Pay us not to publish it on the internet and/or sell it on the dark web,’” Riggi says.

Cyberattackers aren’t succeeding with “zero day” breaches, or finding new, undiscovered vulnerabilities, they are quickly finding existing weaknesses or known published vulnerabilities in software and exploiting them before they can be repaired with a patch, Riggi says.

“...if there's a known published vulnerability, they can develop malware pretty quickly, hours or days to exploit that,” Riggi says. Conversely, it may take a large health system weeks to address all the vulnerabilities in its software because health systems dependent on the third party provider, the developer of that technology, to provide us the patch,” says Riggi.

Healthcare organizations and the federal government are paying greater attention to the risks of cyber attacks to patient safety. Cyberattacks can prevent hospitals from using electronic health records, and in some cases, force health systems to transfer patients to other facilities.

“When they attack a hospital, they are shutting down life critical systems,” Riggi says. “When they encrypt our networks and we have to shut down our network, and our internet connection is lost, that means life critical medical technology is no longer available, which causes an immediate delay and disruption to healthcare, causing the most immediate risk to patient safety and ultimately a threat to life.”

“What we see is an immediate diversion of ambulances, which may be carrying stroke, heart attack and trauma patients. And if some of the hospitals which had been shut down by these despicable ransomware attackers, the next nearest hospital may not be within close proximity, causing a significant delay in urgent treatment,” he adds.

In addition to the risks for patients coming to the hospital, a cyber attack threatens the safety of those who have already been admitted, he notes. “We can't access their electronic medical record. We can't determine quickly what the drug allergies are,” Riggi says. “We can't determine the full history of treatment on this patient.”
For cancer patients who need their treatment, it is even more complicated. “That's not a simple thing to easily ship off all your cancer patients to some other cancer center,” Riggi says.

Riggi had encouraged the federal authorities to treat cyber attacks as “threat to life” crimes. FBI Director Christopher Wray who spoke to CEOs at the American Hospital Association conference reiterated that the justice department will treat ransomware attacks as crimes threatening lives.

Riggi believes that it must be made clear to cyber criminals that if they attack a "hospital or any critical infrastructure that puts lives at risk, the government's coming after you.”

Generative AI

Cybersecurity leaders say they’re concerned with bad actors using AI tools that can probe an organization’s vulnerabilities, and can learn from mistakes.

“There's certainly opportunities for threat actors to use artificial intelligence to advance their own attacks,” said Steve Cagle, the CEO of Clearwater, a cybersecurity firm. “So they can use it to generate code for malware. They can use it to learn the defenses of a security

At the same time, Cagle and cybersecurity experts point out that hospitals and healthcare organizations can utilize AI to improve their own defenses, identify vulnerabilities and repel intruders.

Mike Britton, chief information security officer of Abnormal Security, says he's concerned about cybercriminals using generative AI to go after hospitals. **"**I think the rise of AI and generative AI is absolutely a looming threat, not just for healthcare, but for all organizations," says Britton

Britton says criminals can use AI to send automated emails, and AI-generated responses can pull more information from people or systems that they are targeting. Eventually, those AI-responses can eventually coax victims into providing private information, including bank account information.

"At that point, the live person comes on, takes your money and the scam is over," Britton says.

Many attackers continue to use email-based attacks, which can yield high returns with relatively low effort, he says. "We're not seeing it on a large scale, but we do see generative AI messages being used by attackers," Britton says. "So it's there, it's happening."

At a panel during the HIMSS Global Health Conference & Exhibition in April, cybersecurity experts said hospitals will need to prepare for AI-powered cyberattacks.

Adam Zoller, chief information security officer for the Providence health system, said it's inevitable that criminals will use AI to attack hospitals and healthcare organizations.

"Within the next couple of years, we're gonna see AI-operated ransomware, AI-operated malware that automatically gets into your systems and automatically finds exploitable vulnerabilities," Zoller said.

"Artificial intelligence has been used by cybersecurity vendors and technologies for quite some time now to help in improving defense, by becoming more efficient, more agile," Cagle says.

AI is a double-edge sword, creating new opportunities for improved defenses and more sophisticated attacks. "It's going to be a bit of a battle as time goes on to see who can win the AI race," Cagle says.

Deepfakes

Cybersecurity experts point to the possibility of attackers using “deepfakes” to impersonate executives and leaders. Potentially, bad actors could send fake audio or even video of an executive telling employees to send money to a specific account, among other disturbing possibilities.

The federal government issued a warning about the growing threat of deepfakes earlier this month including a video depicting Ukrainian President Volodomyr Zelenskyy telling his nation to surrender to Russia.

“All these technologies that are able to fake people's voices, and are able to fake people's images and so on, I think that's going to be a major problem,” says Limor Kessem, a senior cybersecurity consultant for IBM Security.

“At this time, there does not appear to be widespread use of deepfakes targeting health care, but we should maintain vigilance and promote awareness in the workforce,” said Riggi.

Lee Kim, senior principal for cybersecurity and privacy at HIMSS, said in a December interview with Chief Healthcare Executive that she sees growing potential for the use of deepfakes, as more leaders meet virtually or connect with their teams via video.

“Deepfakes, I predict, will make a significant entry point into healthcare as well as other industries,” Kim said.

Focusing on records

a hospital or medical group. Some bad actors are focusing on getting access to electronic health records through insurers or other companies that work extensively with health organizations yielding private health information on millions of people.

“They're going to a hospital chain, or a service provider that serves up records, so that they can minimize that effort,” Michael Hamilton, Chief Information Security Office of Critical Insight says. “And they're starting to be very successful doing this. The combination of healthcare and fintech makes those especially juicy targets,” says Hamilton

A cyberattack on MCNA, a dental insurer, affected more than 8.8 million Americans, according to the U.S. Department of Health and Human Services. A pharmacy services firm, PharMerica was hit with a cyberattack in March, and affected more than 5.8 million Americans.

Health systems are vulnerable to attacks aimed at their vendors. Nick Hyatt, the practice manager for Optiv's Global Threat Intelligence Center, says hospitals should be asking their vendors about their cybersecurity capabilities especially “When you're bringing on a new vendor, or when you're bringing on a new piece of software, what does their security look like? I think people forget to ask those questions sometimes,” Hyatt said.

Even if the breach involves a vulnerability outside the hospital’s control, that’s of small comfort. “You're on the hook for whatever happened. So you do have to start asking those tough questions,” Hyatt says.

Other threats

The confluence of state actors, activists and criminal groups is worth watching. “Geopolitically the world is really weird right now. And it's really hard to determine who is cause,” Hamilton says.

Hamilton said recent layoffs in cybersecurity companies could create future problems. “When you create a whole bunch of unemployed people with skills, they might go to the dark side,” Hamilton says. “So you know, that's a situation I think we need to watch.”

Some hospitals and healthcare organizations are struggling to recruit and retain talented cybersecurity professionals, because other sectors offer better pay.
More organizations have defenses aimed at blocking phishing emails and are using multi-factor authentication, such as asking for users to utilize a password and another step, such as a code sent to their phone. So attackers aren’t simply relying on emails, experts say. Some attackers are sending text messages with links, hoping for a response, Hamilton notes.

More than ever, healthcare leaders must be focusing on cybersecurity and ensuring that it is a top priority throughout their organizations, experts say.

Hospital organizations also need to understand that just as bad actors are evolving, they need to constantly look to improve their cybersecurity defenses. Hospitals need to consider the risk to patients and the cost of cyber attacks, both financially and to their reputation.

Scripps Health said that a ransomware attack in 2021 cost the system nearly $113 million. Scripps Health later agreed to pay $3.5 million to victims of the ransomware attack.

Britton of Abnormal Security says defenses that may have proven effective in the past are probably not going to succeed today, or in the future. “What got you here is not what's going to carry you forward because technology tactics have changed.”

Top

Closing Thoughts

The statement; "It's not if you will be hit by a cyber attack, it's a matter of when". When is now and it's only going to get worse. Cyber and ransomware attacks are being used interchangeably but means the same thing. Breach and hacked also has the same meaning.

To put things into perspective, I have been offered and accepted 6 credit monitoring services because of cyber/ransomware attacks or in plain English breached/ hacked.

The statistic that nearly 1 in 3 Americans have been affected by a health data breach in 2023 **is very scary** and if you weren't concerned before, you should be NOW. I was offered a credit monitoring services from my health institution because my data was exposed when MOVEIt a third party vendor was breached.

This statistic is only for health data breaches, we don't know what the statistics are for financial institutions and the biggest breach was when Equifax, a credit monitoring service.

Here are some takeaways from the information above and some of my own for Healthcare institutions:

1) Cybersecurity should be the top priority for their institutions.

2) The cybersecurity team needs to be separate from the IT team as the cybersecurity team needs to be on top of things constantly monitoring for cyber attacks on existing vulnerabilities 24/7.

3) The cybersecurity team needs to implement AI or Generating AI to prevent cyber attacks as these bad actors are using AI to find vulnerabilities quickly.

4) The cybersecurity team needs to make sure that any vendor or third party such as

party. The headline news will be about the institution being attacked, not their vendor.

5) Institutions must make sure all employees and contractors are trained and continuous trained on how bad actors can breach their system and what they should or should not do. This includes not only phishing emails, but texts, deepfake communications. I'm sure there will be more types of threats in the future.

6) Institutions should also keep everyone updated for any breach that may occur even with another department or a sister institution. The more people are aware of the attack and what the company is doing to prevent future attacks gives people confidence in that company. These attacks affects everyone, the individual themselves, friends, family, colleagues and acquaintances. The more people are aware and educated on these attacks the more vigilant they will be in preventing cyber attacks.

For other agencies involved:

1) The U.S. Department of Health & Human Services should require organizations to disclose any breach of health data involved rather than 500 individuals or more. The reason is because sometimes the organization may not know how many individuals are involved until sometimes years later. If all breaches are reports in real time, things can be investigated and implemented quicker rather than after the fact.

2) The FBI should prosecute those who commit these crimes with the severest penalty otherwise, these bad actors are not threatened if it's a slap on the wrist.

Because of all this, I try to be very diligent in taking precautions on not giving people my personal information without a very good reason and even then I try to find an alternative to what people are requesting. I don't do online banking and try not to do things online that require me giving personal information because my information has been breached 6 times. I've been offered credit monitoring services that monitor all your personal and financial information.

It's only going to get worse as bad actors are finding more sophisticated ways to get your personal information. With technology, bad actors are already sending phishing emails from your own email address or people you know and trust. They are also calling you from fake phone numbers or spoofing and areposing as your bank etc asking for personal information. I've had phone calls from my own phone number.

Financial scam should also be a grave concern as they are running ramped using methods mentioned above and more. In 2022, there was 2.4 million fraud report and $8.8 billion lost. This topic is a huge subject of its own and beyond the scope of this newsletter.

that is what these bad actors are counting on to get your personal information. So the next time someone asked for your personal information take a moment to pause and ask why are they asking for this information and if it is not pertinent to what you are doing, don't give it to them. Or try to find an alternative.

Good luck out there because unfortunately it is only going to get worse. Unless all the things I just mentioned is enforced to minimize attacks, we will continue to have major problems that will get worse and worse.

Top

Should you have any questions or need of assistance with your business due diligence, determining your product's value proposition, target product profile and economic value of your product for reimbursement, feel free to contact me at 508-846-9094 or regina@biomarketinginsight.com.