July 15th, 2021

Dear Regina,

Welcome to BioMarketing Insight's monthly newsletter.

Everything today is digital and we are all connected by the internet. While this may make things easy there is always the risk of being hacked and having your identity, financial information, and data stolen. Cybersecurity measures must be taken to stop ransomware and viruses in protecting yourself. This month's newsletter will cover "Why Ransomware Attacks are on the Rise and Are Life Sciences Companies Prepared?"

Last month's topic was "How do we convince people to get vaccinated?" If you missed last month's newsletter titled "Getting to Herd Immunity, Greater than 70% Fully Vaccinated Has Slowed: What Approaches Needs to be Taken", click here to read my article.

Lioness Magazine for entrepreneurs. To read my article, click here to go to the Table of Content.

If you need a little inspiration or something to make us laugh to get us through this difficult time, click on the "Inspiration" link to give yourself a few minutes to relax and enjoy the music from the Berklee School of Music in their song "What the World Needs Now," other inspirations 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 published on August 15th, 2021.

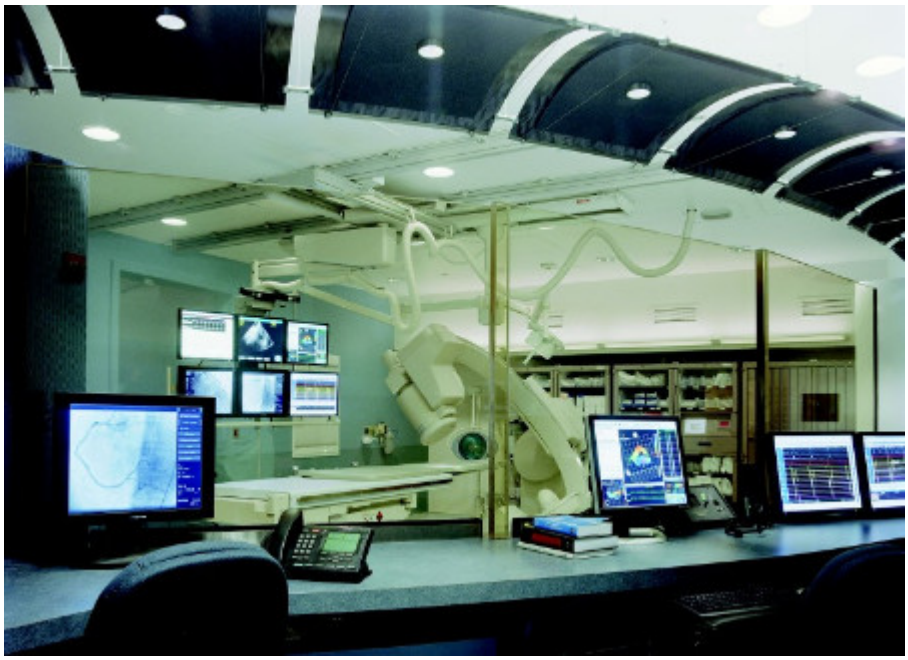
We encourage you to share this newsletter with your colleagues by using the social media icons below, or by simply forwarding this newsletter or use the link below. Should you or your colleagues want to join my mailing list, click on "join my email list" link below.

Please email me, Regina Au, if you have any questions, comments, or suggestions.

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

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:

Marketing Strategies

Scenario Planning - for more information, email me.

Top

Fresh Thinking in the Next Normal

I am pleased to announce that I will be presenting at the Institute of Management Consultants event on "What Will the “Next Normal“ Be for Productivity, Motivation and Retention of Employees? Four Things Employers Need to Consider." on July 20th, 2021 at 2 pm. For more information and to register click here.

Top

Inspirations

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

We Will Get Through It Together

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

February 20, 2021 - Chinese BioPharmaceutical Association: Innovation 2021

Association USA on Feb. 20, 2021. The theme of the event is "Innovation 2021: Lessons Learned in the Pandemic and the Opportunities Afterwards". My presentation will be on COVID-19 Testing and Vaccination Market Insights in US. For more information click on this link.

Top

Another Crisis is Brewing

I am pleased to announce that my article "Another Crisis is Brewing" has been published in the European Biopharmaceutical Review's October 2020 issue. To read this article click here and go to page 16.

Top

Why Ransomware Attacks are on the Rise and Are Life Sciences Companies Prepared?

On May 7th, 2021, American Colonial Pipeline Company (Colonial Pipeline) network, which operates the largest fuel pipeline in the US, was shut-down by a cyber-attack for several days causing fuel shortages and the highest fuel prices in years. Four US states declared a state of emergency.

It was reported that the Russian-based cybercriminals called the "DarkSide" was responsible for gaining access and scrambling the data held on Colonial Pipeline's network. Colonial Pipeline paid US$5 million to regain control of its systems and restart its operations.

The FBI and the Australian Cyber Security Centre (ACSC) maintain that victims of ransomware should not pay cyber criminals; as it only reinforces their criminal behavior and there is no guarantee that if you pay the ransom the criminals you will get back control.

On June 1st, 2021, A Russian cyber-criminal group called REvil, aka Sodinokibi , one of the most prolific and profitable cyber-criminal groups in the world hacked JBS, the world's largest meat supplier and shut down some operations in the US, Canada and Australia. JBS in Brazil controls about 20% of the slaughtering capacity for U.S. cattle and hogs, so the plants' reopening should prevent a severe supply-chain disruption. JBS paid $11million to REvil.

It is the third major attack this year tied to Russia, the first being Quanta Computer Inc. a supplier to Apple Computers who paid $50 million. White House press secretary Jen Psaki said the JBS hack was expected to be discussed at President Joe Biden's mid-June

In 2020, SolarWinds Orion was hacked by Russian cybercriminals who was believe to be sponsored by the Russian government managed to inject malware into Orion updates released between March 2020 and June 2020. The Russians targeted SolarWinds because the range of U.S. government customers is vast.

The Pentagon is SolarWinds' biggest customer, followed by the Army and the Navy as big users. The Department of Veterans Affairs, which is heavily involved in the U.S. response to Covid-19, is another customer who spent $2.8 million for a renewal license. The National Institutes of Health, the Department of Energy, the DHS and the FBI are also amongst the many branches of the U.S. government that have previously bought the tool.

SolarWinds, a publicly-listed Austin, Texas-based company also has private sector customers that includes more than 425 of the Fortune 500, all major US telecoms providers, the top five U.S. accounting firms, hundreds of global universities, the NSA and the White House.

Due to these attacks, President Biden has signed an executive order to boost the country's cybersecurity, a Software Bill of Materials (SBOM) in an electronically readable format designed to provide an inventory of third-party components in devices, a requirement amid efforts to improve cybersecurity across the federal government and private sector.

An SBOM was included in the executive order signed by President Joe Biden to bolster the nation's cybersecurity posture by, among other actions, enhancing software supply chain security, according to ," Kevin Fu, acting director of device cybersecurity at the Center for Devices and Radiological Health, at the Food & Drug Law Institute annual conference. "That highlights the degree to which [SBOM] has reached".

The most targeted sectors include critical infrastructure sectors like health, state and territory governments, education and research, transport and retail.

All organizations are at risk of ransomware attacks, it's not if an organization will be hacked but when. It's far better to minimize vulnerabilities than to face the consequences of an attack. It's clear from these attacks that even companies that run critical infrastructure for other companies and organizations are also just as much at risk.

The Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) have advised all the normal precautions such as using multi-factor authentication, performing regular backups and turning on ransomware protection – but this isn't always enough, so having robust incident and data breach response plan in place is a must! Whether or not you should pay a hacker's ransom is debateable and there may be a number of legal, policy and commercial considerations to content with; however, in this

Why are companies getting hacked if they have cybersecurity software protection?

There are four major reasons companies and government agencies are getting attacked:

1. Cyber Failures
    - Failure to keep software update
    - Failure to train employees on not clicking on phishing emails
2. Ransomware has become more lucative
    - Average payment in Q1 2021 ranged from $200K - $225K
3. Ransomeware as a service - hackers are reinventing the process
    - Hackers steal sensitive date before encrypting it and then threaten to go public of victim refuse to pay
    - Hackers will also sell or lease their ransomware software to other affiliate groups and these affiliate groups share the profits with the hacker.DarkSide is an example of it.
4. Russia Factor - Russia and Eastern Europe

How to Protect Your Company by Eric Goldstein, Executive Assistance Director for Cybersecurity, Cyber Infrastructure Security Agent (CISA)

1. Keep your software updated
2. Use multi-factor authentication

4. Rework server backup system
5. Protect all data and information with a robust firewall
6. Security Directive Pipeline-2021-01, enhancing pipeline cybersecurity
    - Report cybersecurity incidence to Homeland Security, CISA
    - Designate a dedicated Cybersecurity Coordinator who is required to be available 24/7 to TSA and CISA to coordinate cybersecurity practices and address any incidences that arise.
    - Requires owner to review their current activities against TSA'a recommendations for pipeline cybersecurity to assess cyber risks, indentify any gaps, develop remediation measure and report the results to TSA and CISA.

Possible legislation that propose to have companies to report when they pay their hackers.

Are Life Sciences Companies Prepared?

Any organization in health care or the medical field, especially the companies developing vaccines against COVID-19 will likely draw the attention of bad actors. What is surprising is how well – or how poorly – pharma manufacturers score when it comes to indicators that gauge how vulnerable they are to attack.

In the 2021 Ransomware Risk Pulse: Pharmaceutical Manufacturing report, Black Kite reports that 9.5% of the top 200 global pharmaceutical manufacturers and 12.2% of pharmaceutical industry IT solutions providers scored above 0.6, which Black Kite identified as the critical threshold. Forty-two percent of the pharmaceutical data management vendors, scored a Ransomware Susceptibility Index (RSI) above that threshold. The lesson here is mind who you do business with – insist that they contractually meet certain security thresholds and cut them loose if they don't.

attention to my supply chain,' and they're struggling to find their way in a very complicated area – supply chain third-party risk – especially around cyber," said Bob Maley, CSO at Black Kite.

In fact, Black Kite found that data management vendors pose the most significant annual financial risk, $6.2 million. While the vendors bear responsibility for locking down their solutions, "ultimately, the burden is on the company that uses the vendor," Maley said.

"A lot of times, vendors don't have the wherewithal or the finances to recover from that, and it falls back to you," he explained. "If there are indicators and signals that a vendor is susceptible; if that company is not willing to change and the financial impact to your corporation is bigger, well, maybe it's time to move to new vendors."

What will make the C-suite stand up and take notice is Black Kite's research on the financial impact (risk) calculated for each pharmaceutical company. First, deriving a Loss Event Frequency (LEF) – the likely cybersecurity event frequency for a company within a year – then multiplying that by the probable cost of a ransomware attack, Black Kite found the average annual cybersecurity financial risk for pharmaceutical companies is more than $31 million.

"Best practices, essentially, aren't being followed," said Maley. "They're the basic hygiene themes of your program that are being missed. These are not new controls, these are paying attention to the details."

New York City trying to become the next Life Science hub like Boston, become the first major American metropolitan area to open a real-time operational center to protect against cybersecurity threats, regional officials said.

Based in lower Manhattan skyscraper building, the center is staffed by a coalition of government agencies and private businesses, with 282 partners overall sharing intelligence on potential cyber threats. Its members range from the New York Police Department to Amazon.com Inc. and International Business Machines Corp. to the Federal Reserve Bank and several New York healthcare systems.

Known as New York City Cyber Critical Services and Infrastructure open July 1st after two years of planning. The cyberdefense center was developed as attacks against government and business infrastructure increase across the country such as the cyber attacks against, JBS, Colonial and Quantas Computer and SolarWind.

Top

Closing Thoughts

Ransomware is on the rise whether we like it or not because it is lucrative for hackers. It's not a matter of if a company, organization or government will be hacked, it is when. Hackers don't discriminate and will attack anyone and everyone.

If companies don't invest in cyber security to protect themselves, the risk of being attacked not just once but multiple times is greater. Although Homeland Security, FBI and CISA have said not to pay the ransom, ransomware can shut a company or hospital down for days and the lost revenue to a companies or hospitals is far more than paying the ransom.

Most hackers will attack the infrastructure of a company or hospital because there is multiple points of vulnerabilities:

1. The company infrastructure is unprotected;
2. Any affiliate or vendor that support the infrastructure or protects the company from cybersecurity is not securely protected themselves;
3. Employees who are not trained to be on alert for phishing emails or bringing in their own devices
4. Companies that don't have a separate network for the company and one for employees/guests
5. Using the cloud but doesn't have security at all points to the cloud
6. Using, receiving and sending data that is not encrypted
7. Using devices that are not secure.

There are seven (7) common types of cyber attacks according to Cisco: You can read more about each at this link.

1. **Malware**
2. **Phishing**
3. **Man-in-the-middle attack**

5. **SQL injection**
6. **Zero-day exploit**
7. **DNS Tunneling**

Cybersecurity is very complex and requires a separate team from IT because IT doesn't have the bandwidth to do everything. Cybersecurity is very specialized where not all IT personnel knows cybersecurity. Part of the cybersecurity team should include an internal hacker to make sure that a company has no vulnerabilities. By covering all the things mentioned in this article, a company can rest peacefully knowing that their company is as protected as one can possibly be.

Following this protocol can be expensive but having just one incident of being hacked cost more than all the precautions put in place. Quoting an old cliche, you can spend a little more money now or chance a $31 million financial risk annually according to Black Kite should you get hacked and not to mentioned the bad publicity associated with getting hacked with your clients and the public.

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 781-935-1462 or regina@biomarketinginsight.com.
