NATIVE ADVERTISING: CONTEXTUAL ADS

PharmaManufacturing.com contextual ad unit is designed for maximum reader relevance and response. The Contextual Ad unit is a native text ad that appears in line with the flow of relevant editorial content (see image) and is ideal for promotion content of high information value, such as white papers.

Because the content archives of *PharmaManufacturing.com* have been painstakingly categorized by technology keyword, advertisers can for the first time have their content marketing messages appear exclusively in the context of relevant articles in seven major technology categories as shown in the accompanying table.

Material requirements

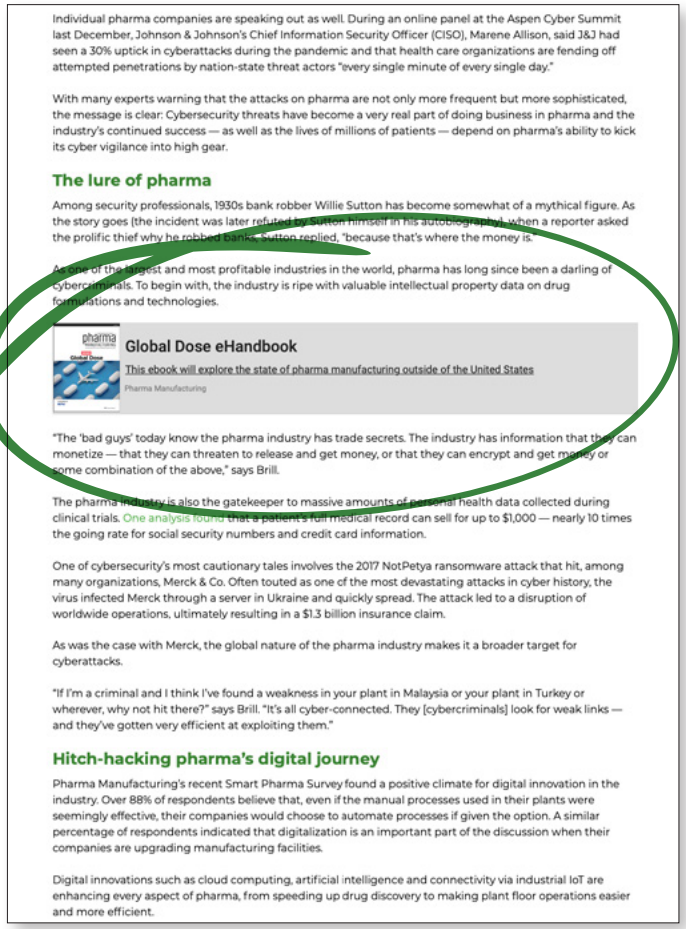
To ensure that your contextual ad is at home in the flow of editorial content, the *PharmaManufacturing.com* production team will create your ad on your behalf. Requirements include an image of the content being promoted, primary headline of up to 35 characters, optional secondary headline of up to 65 characters, and destination URL. Each contextual ad will also include the phrase "Partner with (Your Company Here)" to clearly identify the source/sponsor of the promoted content.

Content Topics

- Production
- Compliance
- Quality and Risk
- Facilities
- Information Technology
- Development

Price:

$1,500 per month
(three month minimum required)



Individual pharma companies are speaking out as well. During an online panel at the Aspen Cyber Summit last December, Johnson & Johnson's Chief Information Security Officer (CISO), Marene Allison, said J&J had seen a 30% uptick in cyberattacks during the pandemic and that health care organizations are fending off attempted penetrations by nation-state threat actors "every single minute of every single day."

With many experts warning that the attacks on pharma are not only more frequent but more sophisticated, the message is clear: Cybersecurity threats have become a very real part of doing business in pharma and the industry's continued success — as well as the lives of millions of patients — depend on pharma's ability to kick its cyber vigilance into high gear.

The lure of pharma

Among security professionals, 1930s bank robber Willie Sutton has become somewhat of a mythical figure. As the story goes (the incident was later refuted by Sutton himself in his autobiography), when a reporter asked the prolific thief why he robbed banks, Sutton replied, "because that's where the money is."

As one of the largest and most profitable industries in the world, pharma has long since been a darling of cybercriminals. To begin with, the industry is ripe with valuable intellectual property data on drug formulations and technologies.

Global Dose eHandbook
This ebook will explore the state of pharma manufacturing outside of the United States
Pharma Manufacturing

"The 'bad guys' today know the pharma industry has trade secrets. The industry has information that they can monetize — that they can threaten to release and get money, or that they can encrypt and get money or some combination of the above," says Brill.

The pharma industry is also the gatekeeper to massive amounts of essential health data collected during clinical trials. One analysis found that a patient's full medical record can sell for up to $1,000 — nearly 10 times the going rate for social security numbers and credit card information.

One of cybersecurity's most cautionary tales involves the 2017 NotPetya ransomware attack that hit, among many organizations, Merck & Co. Often touted as one of the most devastating attacks in cyber history, the virus infected Merck through a server in Ukraine and quickly spread. The attack led to a disruption of worldwide operations, ultimately resulting in a $1.3 billion insurance claim.

As was the case with Merck, the global nature of the pharma industry makes it a broader target for cyberattacks.

"If I'm a criminal and I think I've found a weakness in your plant in Malaysia or your plant in Turkey or wherever, why not hit there?" says Brill. "It's all cyber-connected. They [cybercriminals] look for weak links — and they've gotten very efficient at exploiting them."

Hitch-hacking pharma's digital journey

Pharma Manufacturing's recent Smart Pharma Survey found a positive climate for digital innovation in the industry. Over 88% of respondents believe that, even if the manual processes used in their plants were seemingly effective, their companies would choose to automate processes if given the option. A similar percentage of respondents indicated that digitalization is an important part of the discussion when their companies are upgrading manufacturing facilities.

Digital innovations such as cloud computing, artificial intelligence and connectivity via industrial IoT are enhancing every aspect of pharma, from speeding up drug discovery to making plant floor operations easier and more efficient.