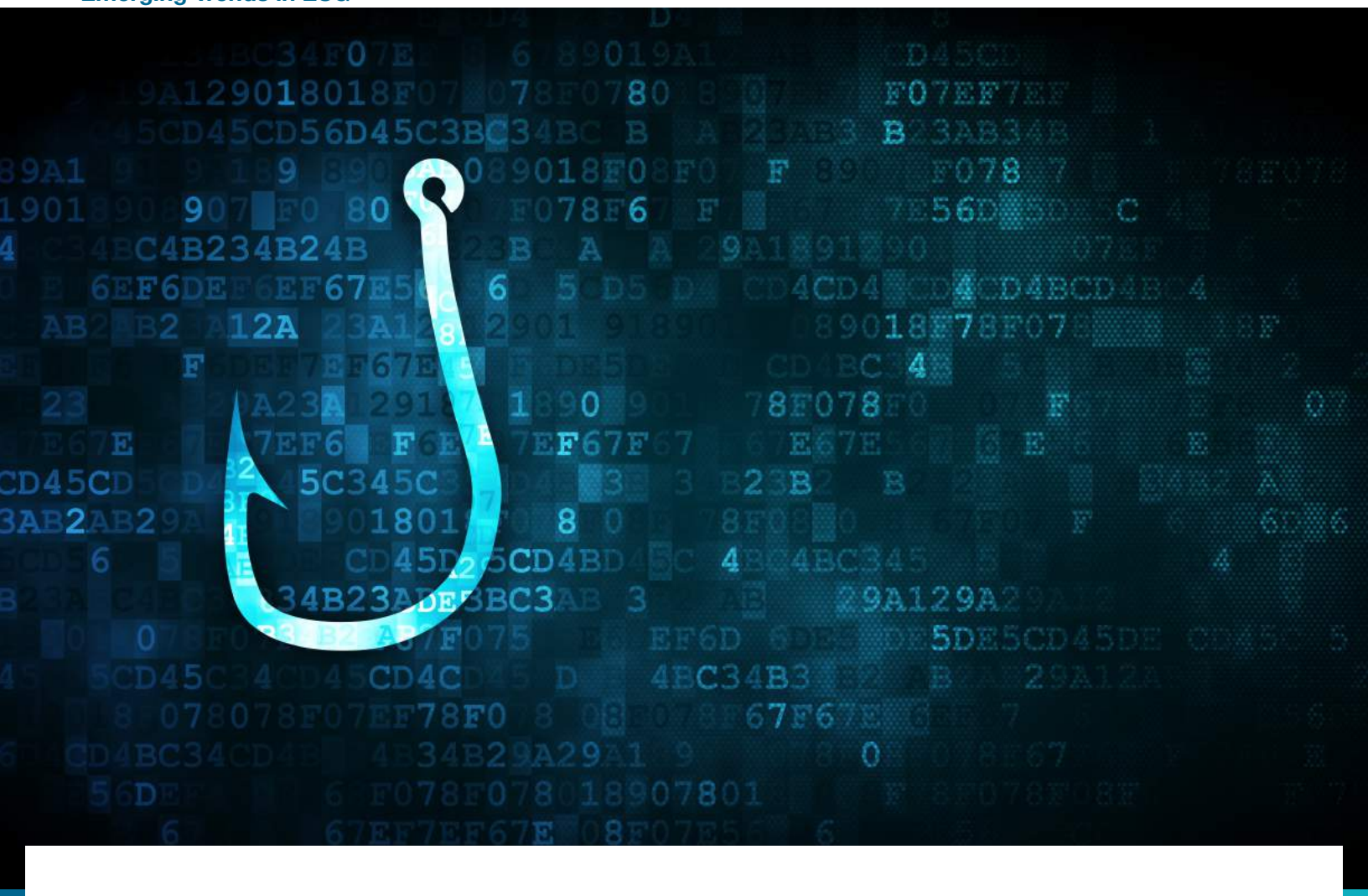


JUNE 2021

Inside this Issue

Seafood Industry Cyberattacks on the Rise

The world's largest corporations are under attack and frequently at that.

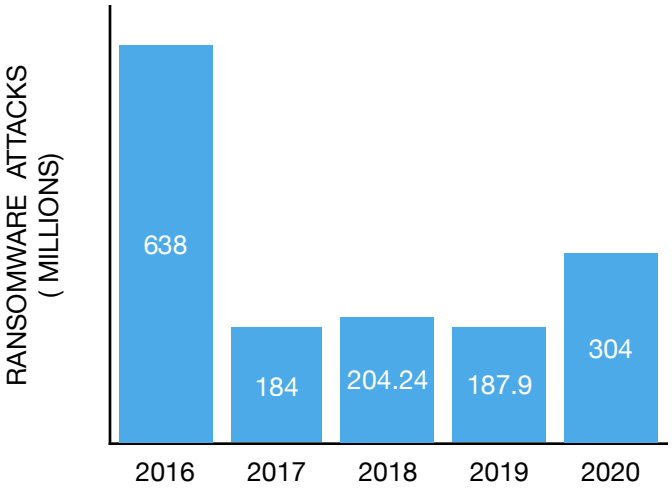
Using ransomware, a type of malicious software that blocks users from accessing their own data, digital extortionists are encrypting files, adding extensions to attacked data and holding it "hostage" until the demanded ransom is paid.[1]

According to an annual report on global cybersecurity, there were a total of 304 million ransomware attacks worldwide in 2020. This was a 62 percent increase from a year prior, and the second highest figure since 2014 with the highest on record being 638 million attacks in 2016.[2]

The seafood sector could be a particularly attractive target for hackers mainly because of the lack of IT investment in cybersecurity.

Unlike the financial services sector where hacking poses an obvious threat to depository, investment, and other financial accounts, in the food industry, the threat seemed less ominous.

Annual Ransomware Attacks Worldwide



Source: Statista

"Part of the problem is the [food] sector believes it's immune," writes one business solutions blog. "Why would anybody attack a food company? National and international crime organizations frequently target the food chain to commit large scale adulteration, counterfeiting, fraud, theft and smuggling; even hacking into storage and distribution company systems to uplift counterfeit products and insert them into the legitimate supply chain."[3]

Even in comparison with the far more mature agriculture and protein industries such as chicken, pork, and beef, the aquaculture industry is in the early innings of integrating and utilizing Big Data, data science, and automation for its production.

Adding cybersecurity to an already substantial list of major concerns that include changing water conditions, diseases, algae blooms, and sea lice, would add margin pressure to a sector already beset by significant challenges.

THE JBS HOSTAGE SITUATION

In May 2021, the world's largest meat packer, JBS, fell victim to an organized cyberattack that severely disrupted operations throughout North America and Australia. The attack was so severe that the U.S. Department of Agriculture (USDA) was unable to release wholesale prices of beef and pork, and there was unease on longer term commodity pricing if the stoppage continued.[4]

It took the company approximately four days to fully restore operations, and it was later revealed that JBS paid USD 11m in ransom via Bitcoin to resolve the situation.[5]

The FBI attributed the JBS attack to Russia-linked hacking group REvil, a notorious criminal cyber gang that previously targeted Apple and Quanta Computer among others.[6]

But JBS had full and fair warning to bolster its cybersecurity efforts years ahead of this attack, according to former employees. Following an intensive audit over 2017/18, it was recommended that the company invest in specialist monitoring technology to detect possible intrusions; this recommendation was rebuffed as it was deemed too costly by management. [7]

SEAFOOD/AQUACULTURE ALREADY IN THE CROSSHAIRS

The attack is one of more than 40 ransomware attacks against food companies since May 2020 tracked by cyber intelligence analyst Allan Liska at Recorded Future. Including a business and personal data breach at Peter Pan Seafoods that affected nearly 9,000 employees, Liska's database includes a large, privately held Saudi shrimp farmer, a seafood processor with operations in Washington and Alaska, and an East Coast lobster and scallop distributor serving clients globally. [8]

While "publicly reported attacks only make up a fraction of all ransomware attacks...broadly speaking, the food industry, especially food processing plants have under-invested in security. As food plants have modernized and become more dependent on computers and networking, they have been slow to add in proper security controls," said Liska.

Underreporting of cyberattack incidents within the seafood sector remains a significant issue; unless a company has been directly affected, management may not appreciate how rampant the problem is until it's too late. In speaking to one senior seafood processing executive that dealt with a breach, he pointed to two other seafood companies whose attacks were never publicized.

"The world's largest corporations are under attack and frequently at that."

INDUSTRIAL CONTROL SYSTEMS VULNERABLE

Internet-enabled automated industrial control systems such as those at food processing plants are of particular concern to security experts.

In 2016, the FBI issued a security bulletin in coordination with the USDA detailing the threat of increasing digitization on the nation's food systems and noted lessons learned from the healthcare industry: manufacturers' prioritization of user-friendly, interoperable devices over security rendered them vulnerable to attack. [9]

Large parts of the food industry also rely on decades-old, custom-written software that is essentially impossible to update, running on outdated operating systems like Windows 98.[10]

While all of this may sound like a significant IT headache, experts stress greater potential dangers could result from cyberattacks in the future; "sale of tainted food, financial ruin for producers, and even injury or death of plant workers."[11]

"Maybe your product advantage is neutralized because a competitor just launched a copycat product using stolen intellectual property gained by hackers. Or maybe a hacker has stolen sensitive commercial and supply chain information belonging to one of your major retail clients and is demanding a huge ransom."[12]

Attackers are increasingly targeting industrial sectors because these companies are more willing to pay up to regain control of their systems, downtime for which can cost millions, experts say.[13]

In 2017, Mondelez International reported a global computer outage via malware that may have impacted its bottom line by as much as USD 100m. [14]

ECO-TERRORISM ANGLE

While much attention has been paid to cyber vulnerabilities at the processing stage, any part of the seafood production chain using "smart" or precision farming technology, on land or at sea, can be exposed to hacking.

Ransom-seeking cyber criminals will follow any money-making opportunity, but it would be naive to assume that climate or animal right's activists couldn't also seek to use hacking as a cudgel to enforce their viewpoints.

Inflammatory, one-sided documentaries like *Artifishal*, backed by consumer brand Patagonia, and Netflix's *Seaspiracy* have given industry opponents unprecedented reach in spreading the gospel against commercial fish farming.

Consider the potential threat of radicalized industry opponents turning into full-on eco-terrorists, remotely disrupting biomass tracking, feed delivery control, parasite sensors, etc. With effectively "live" hostages at stake, the implications for widespread and long-term catastrophic damage have increased significantly.

COMING TO TERMS

A recent article in *The Economist* perhaps said it best: Dealing with cyber-insecurity is hard because it blurs the boundaries between state and private actors and between geopolitics and crime....A cloud of secrecy and shame surrounding cyberattacks amplifies the difficulties. Firms cover them up."[15]

It will be imperative for companies small and large to ensure their investors and consumers that steps have been taken *proactively* to deter future cyber intrusions that derail operations. There is simply too much money and invested time at stake for an industry with already tightening margins, facing more scrutiny than ever before.

SOURCES

1. Unitrends. "How Ransomware Works." https://www.unitrends.com/solutions/ransomware-education.
2. SonicWall, Statista. Annual Number of Ransomware Attacks Worldwide from 2014 to 2020 (in millions). 2021. Statista, https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/.
3. BSI Group. "The silent assassin: Nine reasons why cybersecurity for food matters." BSI Blog, https://www.bsigroup.com/en-GB/blog/food-industry-blog-news/cybersecurity-for-the-food-industry/.
4. Bloomberg. "No One Knows How Much U.S. Meat Costs After Cyberattack Jams Report." 1 June 2021, https://www.bloomberg.com/news/articles/2021-06-01/no-one-knows-how-much-u-s-meat-costs-as-cyberattack-jams-report?sref=JAemJnte.
5. The Wall Street Journal. "JBS Paid $11 Million to Resolve Ransomware Attack." The Wall Street Journal, 9 June 2021, https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.
6. Reuters. "JBS meat plants reopen as White House blames Russia-linked group over hack." Reuters, 2 June 2021, https://www.reuters.com/world/us/russia-linked-hacking-group-is-behind-cyberattack-against-jbs-bloomberg-news-2021-06-02/.
7. Bloomberg. "JBS Rebuffed Call to Boost Cyber Spending, Ex-Employees Say." Bloomberg, 8 June 2021, https://www.bloomberg.com/news/articles/2021-06-08/jbs-rebuffed-call-to-boost-cyber-spending-ex-employees-say.
8. Peter Pan Seafoods. Legal Notice. David Wright Tremaine LLP, 4 Jan 2021, https://www.doj.nh.gov/consumer/security-breaches/documents/peter-pan-seafoods-20210111.pdf.
9. Federal Bureau of Investigation, Cyber Division. Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector. 31 March 2016, https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf.
10. Politico. "Cyberattack on food supply followed years of warnings." 5 June 2021, https://www.politico.com/news/2021/06/05/how-ransomware-hackers-came-for-americans-beef-491936.
11. Politico. "Cyberattack on food supply followed years of warnings." 5 June 2021, https://www.politico.com/news/2021/06/05/how-ransomware-hackers-came-for-americans-beef-491936.
12. BSI Group. "The silent assassin: Nine reasons why cybersecurity for food matters." BSI Blog, https://www.bsigroup.com/en-GB/blog/food-industry-blog-news/cybersecurity-for-the-food-industry/.
13. The Washington Post. "Ransomware attack leads to shutdown of major U.S. pipeline system." The Washington Post, 8 March 2021, https://www.washingtonpost.com/business/2021/05/08/cyberattack-colonial-pipeline/.
14. Food Processing. "Malware May Have Cost Mondelez $100 Million." FoodProcessing.com, 6 November 2017, https://www.foodprocessing.com/articles/2017/malware-may-have-cost-mondelez-millions/.
15. The Economist. "To stop the ransomware pandemic, start with the basics." 2021, https://www.economist.com/leaders/2021/06/19/to-stop-the-ransomware-pandemic-start-with-the-basics.

PERITUS CAPITAL

Peritus Capital LLC is a minority-owned and operated boutique investment firm that invests in, supports, and finances the global development of early-stage and established companies that integrate Environmental, Social, Governance (ESG) principles into their business models. We are a global team with an extensive network of international investors able to invest across multiple geographies.

535 FIFTH AVE 4/F
NEW YORK, NY 10017
(646) 360-3102

HELLO@PERITUSCAP.COM