



Gallagher

Insurance | Risk Management | Consulting

Food & Agriculture

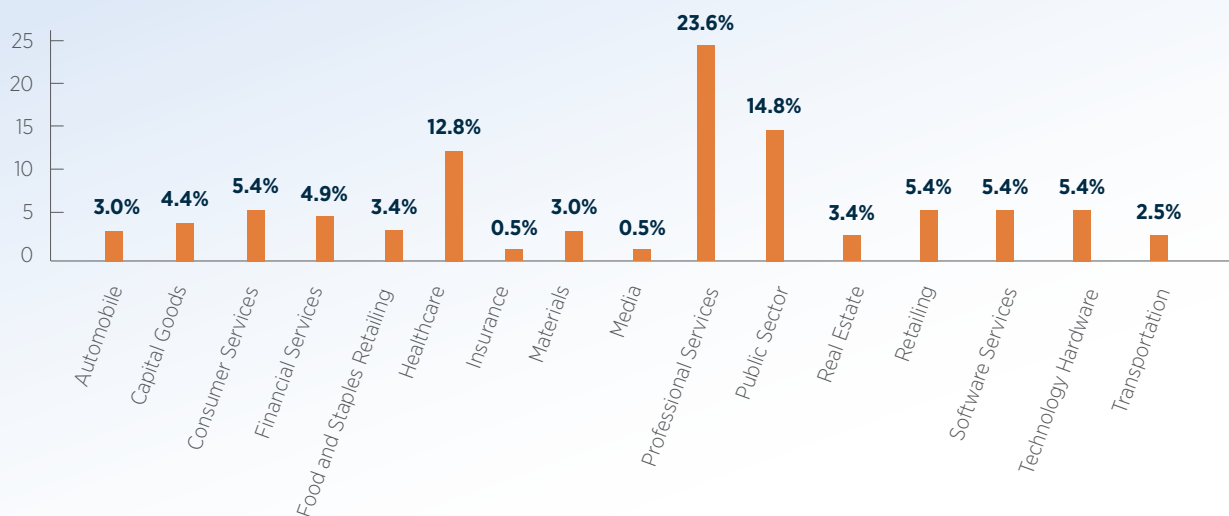
Ransomware Crops Up in the Food & Agriculture Industry

John Farley, Managing Director, U.S. Cyber Practice

Those that manage risk in the food and agriculture industry traditionally focused on perils associated with natural disasters, physical safety, contractual liability and other forms of risk. However, a comprehensive enterprise risk management approach that reflects today's changing risk landscape calls for a reassessment of what is now impacting the bottom lines of those in this sector. Cyber risk has emerged as one such threat that cuts across all sectors, and there is clear evidence that cybercriminals are now targeting food and agriculture.

Today's cyberthreat actors favor ransomware as the attack method of choice, where they deploy a form of malicious software, often via phishing emails. Once inside a network, it often spreads quickly to lock down all data throughout the victim's entire ecosystem, impacting devices, servers, phones and many other integral parts of the organization, effectively ceasing operations. Demands in the six and seven figures are often made in exchange for the release of data. Refusal to pay often results in threats to destroy data or release sensitive data to the public. Coveware issued a recent report¹ that documents bottom-line costs to victims of ransomware attacks. They found that the average ransom payment was \$139,739. Even more concerning, business interruption costs could be even greater than the amount of the ransom paid, with the average downtime being 22 days.

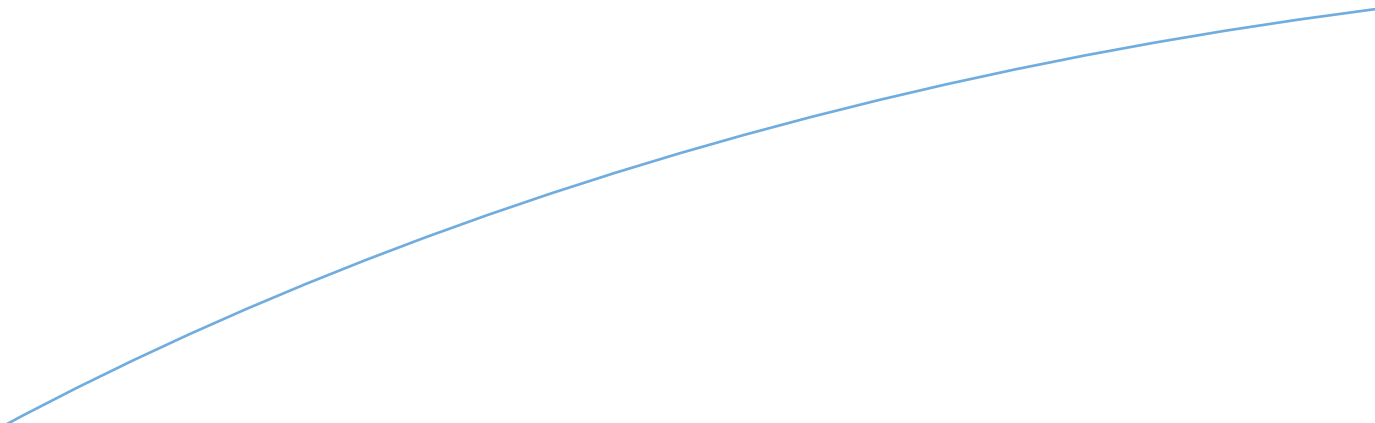
COMMON INDUSTRIES TARGETED BY RANSOMWARE Q3 2021



Trends of rising ransomware risk in the food and agriculture sector became clear when the FBI released a [report](#)² on September 1, 2021, citing several attacks where food and agriculture businesses were victimized, including the following.

- In July 2021, a U.S. bakery company lost access to their server, files and applications, halting their production, shipping and receiving as a result of Sodinokibi/REvil ransomware, which was deployed through software used by an IT support managed service provider (MSP). The bakery company was shut down for approximately one week, delaying customer orders and damaging the company's reputation.
- In May 2021, cyber actors using a variant of the Sodinokibi/REvil ransomware compromised computer networks in the U.S. and overseas locations of a global meat processing company, which resulted in the possible exfiltration of company data and the shutdown of some U.S.-based plants for several days. The temporary shutdown reduced the number of cattle and hogs slaughtered, causing a shortage in the U.S. meat supply and driving wholesale meat prices up as much as 25%, according to open source reports.
- In March 2021, a U.S. beverage company suffered a ransomware attack that caused significant disruption to its business operations, including its operations, production and shipping. The company took its systems offline to prevent the further spread of malware, directly impacting employees who were unable to access specific systems, according to open source reports.
- In January 2021, a ransomware attack against an identified U.S. farm resulted in losses of approximately \$9 million due to the temporary shutdown of their farming operations. The unidentified threat actor was able to target their internal servers by gaining administrator-level access through compromised credentials.
- In November 2020, a U.S.-based international food and agriculture business reported it was unable to access multiple computer systems tied to their network due to a ransomware attack conducted by OnePercent Group threat actors using a phishing email with a malicious zip file attachment. The cybercriminals downloaded several terabytes of data through their identified cloud service provider prior to the encryption of hundreds of folders. The company's administrative systems were impacted. The company did not pay the \$40 million ransom and was able to successfully restore their systems from backups.

Cyberthreats have grown exponentially for food and agriculture due to risks associated with the rapid adoption of recent technology advances. Specifically, the concept of precision agriculture evolved as a critical business strategy, where farming and livestock operations have come to rely on a vast ecosystem of technology-dependent tools. These include global positioning systems, remote sensors and vast communication networks that are now considered critical to the success of the efficiency and success of the sector. However, these new technologies rely on a secure internet to perform properly, and any disruption to even one device could cause a domino effect, leading to a significant negative impact to the bottom line. In today's world of hacking, system glitches and insider threats, it's no surprise that this industry is starting to understand the need to take cyber risk management and cyber risk transfer to an enhanced safety level. The U.S. Department of Homeland Security report raised this very concern in their [Threats to Precision Agriculture](#) report.





PREVENTING AND MITIGATING RANSOMWARE ATTACKS

Implementing an effective cyber risk management program always starts with obtaining a comprehensive understanding of your environment with insight into security gaps specific to the organization.

The FBI offered advice on preventing and mitigating ransomware attacks, including the following.

- Regularly back up data, air gap, and password protect backup copies offline. Ensure that copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software and firmware as soon as they are released.
- Use multifactor authentication with strong pass phrases where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access/RDP ports, and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges, and configure access controls with least privilege in mind.
- Install and regularly update antivirus and anti-malware software on all hosts.
- Only use secure networks, and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on cybersecurity awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (e.g., ransomware and phishing scams).

TRANSFERRING CYBER RISK

The cyber insurance marketplace offers solutions to transfer risks associated with ransomware and other cyberthreats. Policy terms and conditions vary and can be negotiated. Most policies cover both first- and third-party costs, including but not limited to:

- Legal counsel to meet compliance obligations
- Forensic investigation firms to investigate and remediate attacks
- Access to cyber extortion negotiators with immediate access to cryptocurrency
- Business interruption and extra expense costs
- Data recovery costs
- Costs to notify affected individuals and regulatory authorities
- Credit monitoring services
- Costs to hire a public relations firm to reduce reputational harm
- Costs to defend and settle third-party lawsuits and regulatory investigations

Those that seek cyber insurance coverage need to be prepared for a market that is laser-focused on data security controls, with a particular focus on those designed to prevent ransomware attacks. Without these in place, applicants may be subject to higher insurance rates, reduced policy limits, greater retentions and policies that restrict coverage. There is also a distinct possibility that a cyber insurance underwriter will decline to offer terms at all if they are not satisfied that specific protections are in place. Questions regarding multifactor authentication, remote desktop protocol, privileged access management, data backup practices, email hygiene, incident response planning and employee training will need to be answered.

It is advisable to work closely with your cyber insurance broker prior to entering the cyber insurance market. Doing so may help you understand where your security controls may be lacking and can provide a road map to remediation. Ultimately, the goal is to be viewed as a best-in-class risk by the underwriting community when applying for cyber insurance.

Sources

1 Coveware: *Industry Segments that succumb to a Ransomware Attack in Q3 2021*

<https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>

2 FBI Private Industry Notification

<https://s3.documentcloud.org/documents/21053966/fbi-bc-cyber-criminal-actors-targeting-the-food-and-agriculture-sector-with-ransomware-attacks.pdf>



ajg.com The Gallagher Way. Since 1927.

The information contained herein is offered as insurance industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer legal advice or client-specific risk management advice. Any description of insurance coverages is not meant to interpret specific coverages that your company may already have in place or that may be generally available. General insurance descriptions contained herein do not include complete insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis.

Gallagher publications may contain links to non-Gallagher websites that are created and controlled by other organizations. We claim no responsibility for the content of any linked website, or any link contained therein. The inclusion of any link does not imply endorsement by Gallagher, as we have no responsibility for information referenced in material owned and controlled by other parties. Gallagher strongly encourages you to review any separate terms of use and privacy policies governing use of these third party websites and resources.

Insurance brokerage and related services to be provided by Arthur J. Gallagher Risk Management Services, Inc. (License No. 0D69293) and/or its affiliate Arthur J. Gallagher & Co. Insurance Brokers of California, Inc. (License No. 0726293).

© 2021 Arthur J. Gallagher & Co. | GGB40581