	CATEGORY	DATE OF ISSUE
KraftHeinz	**Risk Management**	**06/26/2019**
TITLE		
CYBERSECURITY RISK		

Risk Description

As a Company, we are significantly dependent on information technology. We therefore are subject to risks to the security of information technology (IT) systems and the protection of sensitive assets and/or data against unauthorized internal and external access and/or misappropriation. These IT systems, some of which are managed by third parties, may be susceptible to damage, invasions, disruptions, or shutdowns due to hardware failures, computer viruses, hacker attacks and other cybersecurity risks, telecommunication failures, user errors, catastrophic events, or other factors.

Potential Business Impact

If our information technology systems suffer severe damage, disruption, or shutdown, we could experience business impacts including, but not limited to:

- business disruptions,
- reputational damage,
- processing inefficiencies,
- the leakage of confidential information,
- and the loss of customers and sales.

These impacts could potentially adversely affect our product sales, financial condition, reputation, and operating results.

Approach to Mitigate Risk

To mitigate cybersecurity risk, Kraft Heinz has implemented certain management action plans. This includes establishing a cybersecurity program that benchmarks against the industry and maintains a security plan to continually improve protections and resiliency. The cybersecurity program is managed by the Information Risk Executive Steering team, and reports twice a year to the Kraft Heinz Board of Directors' Audit Committee.

# # #