Grocery Industry's Cybersecurity Challenges: Harbinger Of Threats To Corporate America

Richard Levick Contributor
I write about the intersection of business and public affairs.

Button up your overcoat; it's about to rain cyberthreats

Few businesspeople have as much on the line every moment of every day as grocers. When disquieting events happen at a grocery store, customers can be more than just inconvenienced. In extreme circumstances, grocery products can be the cause of illness, even death.

What makes the grocery industry so susceptible to calamities is that food is a necessity, not a luxury. Threats to food safety have the potential to create panic. If a company is the sole retailer affected, there's a sobering chance it could lose customers — but perhaps only temporarily. The length of customers' disaffection all depends on the effectiveness of the company's response.

What constitutes an effective response? When it comes to cybersecurity, it's not always easy to say. It's scary, but data breaches, ransomware, malware, phishing and other cybersecurity issues are all still in their infancy. There are no widely accepted industry standards for incident response, leaving "reasonable" action in the eye of the beholder. One thing is for sure — the miracle of the Internet is being turned into weaponization by a myriad of bad actors.

The specter of malicious product tampering or computer hacks that prevent items from being properly refrigerated are among the risks that keep grocers awake at night. In many ways, they're a microcosm of the pressures faced these days by

corporate CEOs, communications executives, and their legal counsel. Fears surrounding cybersecurity and attendant liability nightmares have become Corporate America's #1 risk management concern. For the past decade, the threat of hacking was largely limited to information. Now, life, health, and safety are becoming the real exposure, and few companies are ready, though all will face attacks. If a company thinks its prophylaxis is sufficient, it is wrong. If it thinks free credit reporting is still a satisfactory response, it is more unprepared than it realizes.

In early June, I was among the crisis response specialists invited to participate in a crisis management conference organized by Pillsbury Winthrop Shaw Pittman LLP. The panel was given a cybersecurity scenario that involved a ransomware breach disrupting customer transactions in dozens of stores across a nationwide chain.

The scenario cut right to the heart of the grocery industry's biggest fear: the reputational impact of a liability or injury lawsuit stemming from a single incident, an episode whose repercussions could overwhelm decades of conscientious customer and community service.

Here's the strategic premise I shared for grocery industry executives caught in the klieg lights: from the moment the crisis hits, their brand reputation hinges on empathetic communications that keeps their customers front and center. Yes, regulatory and legal liability will provide a threshold for them to respond, but their efforts to go above and beyond mere compliance will be what customers remember. As cybercrime gets more sophisticated, audiences from customers to shareholders expect a more fulsome response. "Hey, we are a victim, too," will only get you so far, and less and less each day.

A company should frame its response through the prism of its customers — a young mom trying to get food for her children, or a son that needs to pick up medicine for his sick father, or a family living paycheck to paycheck.

Always act out of an abundance of compassion and caution, I counseled. Anticipate the health-and-safety questions customers are likely to have and develop emotionally resonant answers. Identify resourceful ways to make their lives easier. A response that surmounts basic regulatory requirements will cultivate good will and could win over lifelong customers.

With that in mind, I advised industry executives to use all channels available to communicate with consumers — from signage at store shelves to social media and online postings. They should also consider having employees outside each affected retail location to talk with customers as they arrive. Employees that are the face of the company are often best equipped to explain facts, answer questions, and collect insight about customer concerns.

Not only do grocery stores face the same cyberthreats that other retailers face, but they also have tremendous financial capital at risk if a significant event disturbs refrigeration or inventory systems. These additional operational systems must be considered in a company's Incident Response Plan, just as they would be in Business Continuity planning for bad weather power outages.

It is imperative companies establish Business Continuity Plans, Incident Response Plans, and Crisis Communications Plans. Those plans should be examined against detailed risk assessments and help guide employee training. Plans should be validated through simulated exercises. This builds a culture where cybersecurity is a priority and employees understand their role in protecting the brand.

Tom Campbell, the head of Pillsbury's crisis management practice and the host of the conference, warns that, "Failing to prevent a cyber breach will injure a company but failing to rapidly respond to the crisis that follows can kill it."

Brian Finch, co-chair of Pillsbury's Privacy, Data Protection, and Cybersecurity team, adds that, "Businesses of all stripes have to understand that today's

cyberthreats go well beyond simple 'smash and grab' data thefts. Their preparation, and by extension their legal exposure, most be attuned to stopping or minimizing the impact of cyberattacks that could slow or stop their revenue intake."

Cyberattacks, data breaches, and information security issues have become so pervasive that people may generally forgive companies for a breach — but not for slipshod communications about it. And not for failing to take proactive measures to protect information and assets in the first place, whether it's installing the latest patches or conducting security penetration tests.

Cybersecurity is not just a technology issue. It's a risk management issue. Everyone in the company should understand the company's objectives when it comes to cybersecurity and incident response. Employees are a critical first audience for security messaging and communications; it is inevitable that they will receive questions when an incident occurs.

When it comes to messaging to external stakeholders – from investors to industry analysts to consumers — the critical component is quick and consistent messaging. Telling key audiences what happened, what the company is doing to fix it, and what it is doing to prevent the episode from happening again is paramount.

The fact is that a company's risk will never be zero. When it comes to cybersecurity and data breaches, the old axiom "Not if, but when" has never been more true.

Richard Levick, Esq., @richardlevick, is Chairman and CEO of LEVICK. He is a frequent television, radio, online, and print commentator.

Richard Levick Contributor

I am chairman and CEO of LEVICK, which provides strategic communications counsel on the highest-profile public affairs and business matters globally. I have been named f... **Read More**