MAZARS USA LLP

ONLINE INSIGHTS WEBCAST

As one of the nation's leading accounting firms, Mazars USA provides the resources, experience and global expertise to help you adapt in a dynamically changing business landscape.

CONSUMER PRODUCTS INDUSTRY TRENDS AND CYBERSECURITY ISSUES

Mazars USA's Consumer Products annual benchmarking study identified key financial benchmarks and critical industry trends and issues. We conduct this annual study to provide financial managers with information from which they can develop goals, standards and expectations for their companies. The 2017 study was conducted on high performing companies defined as those with sales between $70 million and $200 million, importing from overseas and EBITDA of at least 7%. Some key trends identified and presented were as follows:

- 2016 sales growth – 10%
- Gross margin on net sales: 30% - 35%
- Shipping and warehousing as a percentage of sales: 2%-4% and most use a 3rd party facility
- Anticipated 2017 sales growth: 5% - 10%
- Very little production movement away from China
- Most recent healthcare cost increases: 5% - 10%
- Key business concern: The changing retailer ie. from brick and mortar to ecommerce

Cyber-attacks continue to make headlines year after year, as professional criminals become better organized and find new ways to monetize their activities. Mazars USA promotes awareness of industry-specific cyber risks, and proactive steps to manage them. The threat landscape for the Consumer Products industry in 2017 is characterized by evolution rather than revolution. Some highlights for this year include:

- Phishing / social engineering attacks still dominate in 2017. Hacking, malware and social are the primary threat actions, and User Devices / Persons are the main targets.
- Top attacks include crimeware and cyber-espionage, and the most commonly breached data type was company secrets.
- Attack impacts, in both direct and indirect cost, are increasing year over year.
- Contributory factors to breaches include insufficient employee awareness training and social engineering testing, lack of dedicated IT security management oversight, lack of monitoring and detection capabilities, poorly-controlled third party (vendor / partner) remote access, out of date or unpatched computer systems, misconfigurations and unchanged default passwords.

We would like to thank you for attending this webcast, and encourage you to reach out to us if you would like to discuss cyber risk as it relates to your organization.

CONTACT

Stuart A. Nussbaum, CPA
Partner
212.375.6828
Stuart.Nussbaum@MazarsUSA.com

Brian Browne
Principal
267.532.4368
Brian.Browne@MazarsUSA.com

Tony Antonaccio
Manager
267.532.4440
Anthony.Antonaccio@MazarsUSA.com

WWW.MAZARSUSA.COM

MAZARS