protiviti®
Face the Future with Confidence

Consumer Products and Services Industry Perspectives

Your monthly blog and industry news round-up

March
2017

Building Cyber Resiliency Is the Path to Better Brand Protection for Consumer Products and Services Companies

Last week, I wrote about **customer loyalty**, and how a strong cybersecurity program can help ensure the trust of consumers. Here are some fresh stats about the business impact of cyber threats that consumer products and services executives should know about: In 2016, one in five businesses lost customers due to a cyber attack. Nearly 30 percent lost revenue. About one-quarter lost business opportunities. And when a breach occurred, brand reputation was one of the top areas of the organization to be affected, right behind operations and finance.

These unsettling findings are from the Cisco 2017 Security Capabilities Benchmark Study, featured in Cisco's latest **cybersecurity report**. Combine these data points with all the news about recent hacks and breaches involving major retailers, restaurants, hotels, and other consumer products and services companies, and it becomes crystal clear why industry executives are extremely concerned about cyber threats.

In the latest **Executive Perspectives on Top Risks Survey** from Protiviti and North Carolina State University's ERM Initiative, which I referenced in my recent post, respondents from consumer products and services businesses also cited the following risk among the top five for their industry group in 2017:

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand.

The research also shows that the risk score for this concern increased significantly from the 2016 survey.

Consumer respect and trust are at stake

For consumer products and services companies that spend millions of dollars annually to cultivate and promote their brand image, a hack or a data breach can be devastating to their reputation — and their bottom line. These events can lead not only to long-term brand damage, but also the loss of the public's respect and trust. This is especially true if customer data is compromised or stolen, leaving people at risk for financial loss and identity theft. Even if a company can recover quickly from such an event and make things right with its customers, its image will likely remain tarnished for some time to come.

Unfortunately, cyber threats (and privacy concerns) will become only more severe as businesses and consumers increase their reliance on technology in all aspects of their lives; digital commerce and mobile payments continue to grow; and the emerging **Internet of Things (IoT)** expands. Over time, consumer products and services companies will need to significantly increase the data they collect to provide highly customized products, services and experiences to their customers.

These trends underscore why consumer products and services businesses must make improving cybersecurity and building cyber resiliency even higher priorities — starting now.

Developing a world-class response to a high-profile crisis

Most executives today understand that a cyberattack is not a matter of if, but when, for their organization. Taking steps to prevent hacks or breaches should always be a high priority for any business, of course. But what is even more important is creating a well-thought out and tested action plan that will allow the company to respond swiftly to a cyber incident, mitigate the impact of that event on the business and its customers, and protect the brand.

A recent issue of Protiviti's ***Board Perspectives: Risk Oversight*** offers some insight that can help consumer products and services companies better protect their brand reputation in an increasingly treacherous cyber threat landscape. One of the "10 essential keys" to risk management outlined in the document —developing a "world-class response to a high-profile crisis"— is particularly relevant to the cyber threat discussion.

Creating a world-class response requires that the board of directors and executives ensure, long before a crisis hits, that:

- The risk assessment process has been designed to identify areas where preparedness is needed.
- A crisis management team is in place and prepared to address a specific sudden crisis scenario; otherwise, a rapid response will be virtually impossible.
- Response teams are supported with robust communications plans that emphasize the importance of transparency, straight talk and effective use of social media.
- Response teams update and test their rapid response plans periodically.

These actions can strengthen organizational resiliency. When developed with cyber threats specifically in mind, they help to build cyber resiliency. Preparing to reduce the impact and proliferation of a cyber event is paramount for any modern business. For consumer products and services companies, it can make all the difference in maintaining their customers' trust, preserving the long-term health of their brands, and being able to confidently face the future.

Customer Loyalty Through Better Security — and How to Achieve It

Customer loyalty programs are among the basic building blocks of successful consumer products and services companies today. These programs are not only competitive differentiators, but also key drivers of revenue and profits for retailers, restaurants, hotels, airlines and many other businesses. The success of loyalty programs, however, hinges on more than inspiring customers to opt in and offering them rewards that they find compelling. Consumer trust is also essential.

Consumers want to be assured that the companies they interact with through various touch points — online, offline and through mobile applications — are doing everything possible to protect their personal data and privacy. Even millennial consumers, who are generally more willing than customers in other demographic groups to share personal information with businesses in exchange for rewards, have high expectations that companies will keep their data secure and respect their privacy. And if the companies don't, they are quick to hold them accountable.

Privacy concerns are weighing on the minds of executives in the consumer products and services industry this year, according to a survey, ***Executive Perspectives on Top Risks for 2017***, from Protiviti and North Carolina State University's ERM Initiative. Representatives of this industry group who took the survey ranked the following concern third among the top five risks: *Ensuring privacy/identity management and information security/system protection may require significant resources for us.*

Digitalization, the IoT and cyberthreats add to the challenge

Like most things related to information security in a digital world, privacy, customer identity management and information security are all easier said than done. In fact, they are becoming only more challenging for consumer products and services companies as these businesses:

- Introduce more mobile and digital offerings to their customers
- Collect, store and analyze more and more customer data from applications and devices
- Develop and use applications and devices designed for the rapidly emerging and highly interconnected **Internet of Things** (IoT)
- Embrace digitalization and migrate "analog" approaches to customers, products, services and operating models to an "always-on," real-time and information-rich marketplace

It is hardly surprising then that consumer products and services businesses face a constant barrage of sophisticated and stealthy cyberthreats designed to target customer and payment information.

Recent high-profile data breaches and targeted hacks involving major retailers, fast food chains and hotels are just the latest headache-causing wrinkle as consumer products and services companies are scrambling to evaluate their ability to protect customer and payment information. (Executives no doubt had these incidents on their minds when responding to the latest risk survey: they also ranked cyberthreats among the top five risks for their industry in 2017.)

Drive results through strategy and collaboration

Certainly, there is no getting around the need for consumer products and services companies to devote more resources toward ensuring privacy, addressing identity management issues, and protecting information and systems. This is an imperative for any business that handles customer and financial data in a digital world. But organizations also must be **very strategic** when aligning and deploying these resources if they want to see results.

Developing the right strategy requires effective collaboration between the business and IT. If they are not doing so already, business executives in consumer products and services organizations should resolve to reach out to their counterparts in IT sooner rather than later.

Another party to include in discussions about privacy risk and cyberthreats this year: internal audit. We are seeing more organizations increasing business, IT and internal audit collaboration not only to address known risks, but also to help the business prepare for new challenges related to digitalization and the IoT. As Protiviti's white paper, ***The Internet of Things: What Is It and Why Should Internal Audit Care?***, explains, "Businesses developing and using applications and devices within the IoT must be aware of how the data they are collecting, analyzing and sharing impacts user privacy."

Engaging business, IT and internal audit leaders to share their perspectives on these risks will help consumer products and services companies to ensure they are doing everything necessary to protect their customers' privacy and information in a digital and hyperconnected world. It will also give them more confidence to interact with consumers through more channels, and to innovate programs and other offerings that will earn — and keep — their business.

Store Audit Technology Update: The Move to Mobile

As retailers cut costs and drive efficiencies across their organizations, internal audit functions are turning to technology to streamline processes, increase analytic capabilities, and supplement traditional store audits with continuous monitoring and standardized store self-audits.

This **paper** revisits recommendations from Protiviti's *The Retail Store Audit: Using Technology to Optimize the Audit Process*, updating them to reflect the emergence of big data analytics, cloud connectivity, and smartphone and tablet technology.

Who's Minding the Store? Managing Retail Risk From the Inside Out

Store-level control self-assessments (CSAs) provide a structured means for stores to evaluate their own operations, then submit the results to corporate headquarters where they are analyzed for anomalies.

This **paper** recommends a two-tiered approach for CSAs. This combines annual self-assessments for all stores, with rotating audits and data analytics to benchmark and validate store-generated reports.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contact

Richard Childs
Managing Director
Leader, Consumer Products and Services Industry Practice
+1.916.830.0107
richard.childs@protiviti.com

protiviti®