Why CMOs should care about cyber risk
Contents

Executive summary 3
Innovative technologies could open the door to cyber risk 4
CMOs are typically not involved in cyber risk, but should they be? 5
Innovative technology platforms are not necessarily secure 6
Connected products could lead to cyber risk 8
CMOs' use of third-party vendors can open the door to cyber risk 10
Customer trust can be at risk when deploying innovative technologies 11
How CMOs can become more involved with cybersecurity risk 12
Endnotes 14
Contacts 15
Acknowledgments 15
Executive summary

Cyber risk has become a high priority to both corporations and consumers who are concerned about theft of personally identifiable information (PII). While cyber risk has typically been the concern of CIOs, CISOs, and CTOs, the time has likely come for CMOs to also focus on cyber risk. Here’s why . . .

CMOs traditionally have been responsible for creating their company’s brand image while building loyalty and consumer trust. But in today’s digital marketing environment, the focus can also include protecting that image. In addition to traditional brand-building activities, many CMOs are expected to play a leadership role in deploying innovative technologies. These technologies are an integral part of their marketing toolkit, which can include:

- data analytics
- customization
- personalization
- overall campaign optimization
- sophisticated, digital-led campaigns and activities

In addition, while implementing new marketing strategies, CMOs and their marketing teams are commonly collecting more PII. PII exposure as a result of some investment in newer marketing strategies is potentially another direct threat that CMOs may be unknowingly contributing to. The deployment of new marketing tools may be going unnoticed by cybersecurity teams, adding another potential “silent” cyber threat that’s growing. Thus, protecting PII is no longer just the responsibility of cyber executives, but CMOs as well, who oversee the collection of information through their marketing initiatives. CMOs could benefit from working with their cyber counterparts to help ensure their companies are implementing security measures to mitigate cyber risk.

Today’s CMOs often require more than just a basic understanding of cybersecurity risk. CMOs could benefit from taking a more collaborative approach and engaging in deeper conversations with both senior leadership and their cybersecurity counterparts to increase their knowledge of cyber risk. Doing so could ensure that marketing activities facilitated by innovative technologies are secure, vigilant, and resilient.

Research methodology

Insights reported in this paper are drawn from two major sources: Deloitte’s Cyber Risk in Consumer Business Study and the CMO Survey.

Deloitte launched the Cyber Risk in Consumer Business Study to assess current challenges faced by companies in the consumer products, retail, restaurant, and agribusiness sectors. Using a combination of an online survey and in-depth interviews, opinions were gathered from over 400 CIOs, CISOs, CTOs, and other executives in these sectors. Insights reported in this paper are drawn from a subset of 150 interviews with executives from the consumer products sector.

The CMO Survey was conducted by Christine Moorman in conjunction with Duke University’s Fuqua School of Business, Deloitte, and the American Marketing Association. Insights reflects data from interviews with 388 CMOs from the top US marketers at for-profit companies. Interviews were collected online.
Innovative technologies could open the door to cyber risk

Many of today’s businesses are going through a period of digital transformation. Harnessing emerging technologies in order to redefine products, services, and consumer experiences is commonly the new cost of doing business. As a result, many consumer businesses are investing in technologies such as customer analytics, cloud integration, connected devices, and digital payment technology. However, these technologies are likely leaving consumer businesses increasingly exposed to cyber threats as discussed in Deloitte’s recent publication, Cyber Risk in Consumer Business.

As consumer products companies increase their investments in innovative technologies, CMOs anticipate deploying the very same technologies to execute their marketing strategies that may lead to cyber risk. The CMO Survey indicates that CMOs plan to substantially increase spend in the next three to five years on social media (an anticipated increase of 90 percent), mobile marketing (+127 percent), and marketing analytics (+375 percent). This represents substantial investment on the part of marketing organizations.

These investments are typically critical to maintaining relevance and presence with today’s digitally savvy consumer. Since CMOs tend to lead these and other related activities, they could benefit from taking a more active role with their executive counterparts (CIOs, CISOs, and CTOs) to ensure the proper precautions to mitigate cyber risk are in place when deploying these technologies to execute their marketing strategies. For example . . .

- **When collecting PII over social media, ensuring the communication channels are secure is essential, so that hackers cannot steal proprietary consumer information.**

- **Consumer privacy concerns are raised when using mobile marketing to “push” coupons, recipes, and suggestions for related products to consumers. There can be potential negative consequences to consumers if information about where and when they shop falls into the wrong hands, particularly if the consumer is part of a vulnerable target segment, such as children, young adults, and senior citizens.**

- **Marketing analytics often involves merging sales and behavioral data with PII. It’s essential that data is stored securely and that access to the information is granted only to essential personnel.**

**Investment in newer marketing strategies dependent on innovative technologies**

- **Social media:** 77 percent of social media programs are led by CMOs who report using social media for: brand awareness and brand building (46 percent); acquiring new customers (31 percent); introducing new products (29 percent); and retaining current customers and brand promotions such as contests and coupon distribution (both at 28 percent).

  - Social network ad spending is expected to be at $20.31 billion in 2017 and grow by 2019 to $29.68 billion.

- **Marketing analytics:** 58 percent of marketing analytics falls within the purview of the CMO and is used for: search engine optimization (SEO), email marketing, customer segmentation, loyalty and rewards programs, and overall marketing strategy. IDC predicts that by 2019, the US market for big data and business analytics solutions will reach more than $98B.

- **E-commerce:** 28 percent of CMOs lead e-commerce activity, while they report that, on average, 12 percent of their sales are through the Internet. Similarly, the National Retail Federation estimates 8–12 percent US e-commerce growth in 2017.

- **Mobile marketing:** Mobile marketing involves either sharing ads via mobile phones or “pushing” information to consumers on their smartphones using location-based targeting. Both are expected to grow substantially: Mobile ad spending is expected to be at $58.37 billion in 2017 and increase to $102.3 billion by 2021. Location-targeted mobile ad spend is projected to grow from $12.4 billion in 2016 to $32.4 billion in 2021.

- **Customer relationship management:** In addition, 41 percent of CRM is led by CMOs. CRM also represents a substantial amount of marketing spend: IDC predicts that by 2018 spending on CRM applications will reach $31.7 billion attaining a CAGR of 6.9 percent. CRM is typically used by CMOs for marketing campaign issues such as: insufficient or inaccurate reporting, low customer retention, and competitive tracking.
CMOs are typically not involved in cyber risk, but should they be?

Consistent with the traditional role of the CMO, cybersecurity executives indicated that only 22 percent of consumer products companies include CMOs on incident response teams in the event of a cyber breach. This seems low given the importance of marketing to consumer facing businesses, particularly since CMOs are often the stewards of brand reputation and customer trust, which can be severely impacted during a cyber breach. But, brand reputation and its impact on consumer trust and loyalty are not high on the list of concerns of cybersecurity executives. Only 16 percent of food and beverage cyber executives report being concerned with tarnishing perceptions related to brand trust. Their focus is on issues that disrupt production (48 percent) and theft of proprietary information (42 percent).

While one might expect incident response teams to be led by cyber executives, the involvement of the CMO is likely critical as well, especially now that many marketing companies are starting to sell directly to consumers and collect PII data such as credit card information, cell phone numbers, and online and offline addresses and birth dates. Further, CMOs report information they collect is shared both vertically across different levels of their organizations all the time (by 17 percent of CMOs) and horizontally across different functions and business units all the time (by 15 percent of CMOs). Thus, protecting PII is no longer just the responsibility of cyber executives, but CMOs as well, who oversee the collection of information through their marketing initiatives.
Innovative technology platforms are not necessarily secure

Many CMOs most likely rely on their cyber executive counterparts to protect the consumer data collected through various marketing programs, but CMOs should become more involved in the process than in the past. The Cyber Risk in Consumer Business study revealed that investments in technology, particularly the ones CMOs are concerned with, are not necessarily secure.

Less than half of the cyber executives at consumer products companies that were interviewed indicated that they had a “mature” program in place to protect technologies (figure 1). For example, of those investing in connected products, only 46 percent have a “mature” program in place to protect them.21

Figure 1: Percentage of consumer products companies with mature programs in place for safeguarding specific technologies

Source: Cyber Risk in Consumer Business, Deloitte 2017
Many consumer products companies appear to be operating with a false sense of security regarding cyber risk. This is suggested by the fact that even though 76 percent of consumer products companies perceive themselves to be adequately prepared for a cyber breach, a full 87 percent do not have an incident response plan that has been documented and tested in the past 12 months.  

Consumer products executives can face numerous cyber risk challenges such as inadequate funding and lack of alignment on roles and responsibilities (figure 2). Solving these challenges is paramount to effective cyber risk management and CMOs need to be involved in the process.

Figure 2: Percentage of consumer products executives facing challenges on cyber risk

27% Lack of clarity on roles and responsibilities
21% Lack of understanding of where cyber risks relates to the business
19% Lack of understanding of where the organization's data is located

Source: Cyber Risk in Consumer Business, Deloitte 2017
Why CMOs should care about cyber risk

Connected products could lead to cyber risk

The adoption of connected products is expected to grow dramatically in the coming years. Though estimates of connected devices vary considerably, Gartner suggests that by 2020 there will be an estimated 20.8 billion, but others suggest it could be as high as 31 billion. CMOs are involved with managing the customer experience around connected products and indeed may be spearheading some of this growth.

The rapid growth of connected products not only presents numerous benefits to consumer businesses and their customers, but it also can increase cyber risk. That’s because many connected products rely on advanced technologies, such as the cloud to store information and mobile payments to facilitate transactions. With ever-increasing connectivity, there are commonly growing cybersecurity vulnerabilities as companies increase the points of entry, opening the door to cyber breaches that can arise anywhere across the entire connected ecosystem—from consumers to third-party vendors.

Still, 30 percent of consumer products companies do not believe their cyber risk management program is effective at maintaining their strategy to develop and market connected products.

Consumer products executives have five key concerns related to connected products (figure 3).

Figure 3: Percentage of consumer products executives with specific concerns on risk related to connected products

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of IP</td>
<td>69%</td>
</tr>
<tr>
<td>Theft of customer information</td>
<td>68%</td>
</tr>
<tr>
<td>Product disruption</td>
<td>61%</td>
</tr>
<tr>
<td>Tarnishing brand image</td>
<td>60%</td>
</tr>
<tr>
<td>Product safety</td>
<td>53%</td>
</tr>
</tbody>
</table>

Source: Cyber Risk in Consumer Business, Deloitte 2017
Why CMOs should care about cyber risk
CMOs indicated that 55 percent use channel partners to execute marketing activities. More specifically as it relates to social media, 17 percent of CMOs indicate their social media activities are performed by an outside agency. This can raise the issue of third-party risk, which emerged as a concern in the Cyber Risk in Consumer Business study.

While third-party vendors can help companies integrate new technologies such as cloud, mobile payment, and e-commerce solutions into their businesses, they can open new possibilities to cyber risk from onboarding if relationships are not managed correctly through frequent assessments. Of concern is that frequency of third-party risk assessment is low with only 7 percent of consumer products executives surveyed indicating they conduct third-party risk assessment quarterly and only 34 percent do so semiannually.

It’s imperative that CMOs ensure that the vendors they use to execute marketing programs, particularly the ones that involve collecting PII, are continually vetted so collected information is secure and processes meet the highest standards of cybersecurity management.
Customer trust can be at risk when deploying innovative technologies

It’s critical for consumer products companies to maintain the trust of their consumers to maintain brand loyalty and a solid reputation. CMOs believe trust is critical to successful consumer relationships as observed in the CMO Survey: 24 percent cite trusting relationships as a top priority in the next 12 months. This dimension has grown 41 percent since 2016, a larger increase than any other priority.

Even so, consumers are typically cautious and skeptical about companies protecting their PII. Longitudinal research across thousands of US consumers reveals a heightened state of uncertainty around data security over the past decade. In 2016, roughly 80 percent of US consumers felt they have lost control over how their personal information was being used by companies.

Today’s consumers already demonstrate they can be unforgiving with businesses that neglect their data. In this heightened state of unease, many customers remain vigilant, and efforts to mitigate their own risk often translate to cautionary, or even punitive, actions and behaviors. Over the past 12 months, 31 percent of US consumers deleted specific apps on their smartphones and 27 percent avoided specific websites to mitigate their own cyber risk. Further, 16 percent of men and 6 percent of women are likely to switch to a competitor following a data breach.
CMOs typically require more than just a basic understanding of cyber risk now that they’re deploying many of the same technologies as part of their marketing toolkits that potentially leave companies vulnerable to a cyber breach. CMOs should consider taking a more collaborative approach with their cyber executive colleagues, engaging in conversations that increase their knowledge about cyber risk, and potentially educating their consumers on the steps they’re taking to secure consumers’ PII.
Important questions for CMOs to discuss with their cyber colleagues

To understand the potential cyber risks associated with the innovative technologies now being deployed by CMOs as part of their marketing toolkits, there are numerous questions CMOs should consider discussing with their cybersecurity colleagues, such as . . .

• How prepared is the organization for a cyber breach?

• Where is the company most vulnerable to attack?

• How often are incidence response plans tested and documented?

• What innovative technologies deployed in marketing toolkits are vulnerable? What can be done to secure them? How can security measures be part of the design process?

• For PII data collected: Where is the information stored? How secure is it? Who has access to the information?

• For connected products: How secure is the connected products ecosystem?

• For partners/third-party vendors: How often are partners/third-party vendors vetted and trained on security best practices?

• In the event of a cyber breach, how can marketing respond in a way that supports the incidence response team and protects brand reputation as well as consumer trust and loyalty?

This dialogue, as well as applying the lessons learned in the Cyber Risk in Consumer Business report, can help CMOs and their companies:

**Be secure:** Take a measured, risk-based approach to what is not secured and how to secure it. This includes managing cyber risks as a team and increasing preparedness by building cyber risk management strategies in the enterprise and emerging technologies as they are deployed.

**Be vigilant:** Monitor systems, applications, people, and the outside environment to detect incidents more effectively. This includes developing situational awareness and threat intelligence to understand harmful behavior and top risks to the organization, and actively monitoring the dynamic threat landscape.

**Be resilient:** Be prepared for incidents and decrease their business impact by improving organizational preparedness to address cyber incidents before they escalate. This also includes capturing lessons learned, improving security controls, and returning to business as usual as quickly as possible.
Endnotes

4. Ibid.
19. Ibid.
22. Ibid.
23. Ibid.
27. Ibid.
31. Ibid.
Contact

Barb Renner  
Vice Chairman & US Leader  
Consumer Products  
Deloitte LLP  
brenner@deloitte.com

Curt Fedder  
Senior Manager  
Consumer Products Research Team Leader  
Center for Industry Insights  
Deloitte Services LP  
cfedder@deloitte.com

Acknowledgments

We wish to thank:

Paula Spoto, marketing senior manager (Deloitte Services LP)  
Ryan Robinson, research lead (Deloitte Canada)  
Marcello Gasdia, manager (Deloitte Consulting LLP)  
Courtney Flaherty, public relations manager (Deloitte Services LP)  
Jagadish Upadhyaya, assistant manager (Deloitte Support Services India Pvt. Ltd.)  
Shweta Joshi, senior analyst (Deloitte Support Services India Pvt. Ltd.)

We would also like to thank the rest of the survey team, and the many others who contributed their ideas and insights to this paper.
About the Deloitte Center for Industry Insights

The Deloitte Center for Industry Insights (the Center) provides premier insights based on primary research on the most prevalent issues facing the consumer business and manufacturing industries to help companies run effectively and achieve superior business results. The Center is associated with the Deloitte US firms’ Consumer & Industrial Products practice, which benefits from the insights of over 12,000 multi-disciplined professionals with a wide array of deep, hands-on industry experience.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

This publication contains general information only and Deloitte is not, by means of this publication, rendering business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2017 Deloitte Development LLC. All rights reserved.