



THE FORCE  
MULTIPLIER

MARKETING AND DATA SECURITY:

# The Unlikely Brand Building Partnership

Can Marketing and Security Safeguard  
Brand Trust Amid the Data Storm?



# TABLE OF CONTENTS

## SECTION 1: COLLABORATION & ALIGNMENT

- 3** Introduction
- 5** How Marketing Sees Threats
- 6** Initiatives, Campaigns, MarTech
- 8** Capabilities: Brand, Data, CX, EX
- 11** Marketing-Security Relationship Strength by Industry
- 12** Overcoming Obstacles

## SECTION 2: SOUND OFF

- 14** KPMG Expert Commentary
- 17** PSEG Long Island: John Kupcinski
- 18** Teradata: Aditi Uppal
- 19** The Doctor's Company: Jesmine La Russa
- 20** Veteran Product Marketing Leader: Harsh Singh
- 21** Trustwave: Jodie Hoare (formerly)

# INTRODUCTION

Marketers are looking to acquire more customer data from more sources with the sunset of cookies. Data-hungry artificial intelligence (AI) technology, such as ChatGPT, leverages data in whole new ways. Personalized messaging and targeted campaigns mean more information flowing through the data supply chain.

Breaches and incidents are likely, if not imminent in some cases, and will take a sledgehammer to brand trust. The unexpected line of defense: the Chief Marketing Officer (CMO)-Chief Information Security Officer (CISO) partnership. Is your partnership strong enough to keep your brand safe during the coming data storm?

In this study, conducted by the CMO Council and KPMG, we found that a third of marketing-security partnerships are not collaborating effectively to acquire, maintain, and secure customer data for competitive advantage. The jury is out on the other two-thirds.

***33% of marketers say security orgs are hesitant, even unwilling, to collaborate.***

(Source: CMO Council)

The good news is that the vast majority of marketing leaders understand the importance of the marketing-security partnership to preserve brand reputation amid rising data privacy and security concerns. For many, changes are already underway.

“The relationship between marketing and information security absolutely has to evolve because of the unknown territories we’re in, such as the influx of GenAI and the role of trust and privacy,” says Aditi Uppal, vice president of digital marketing and demand generation at Teradata.

## What’s at Stake

It’s critical to shore up this partnership because it’s about to be tested in a big way. The top three marketing initiatives posing the greatest security risks are AI and machine learning, customer behavior data, and Internet of Things, our study found.

Much is riding on marketing and security to keep data safe as these initiatives take flight. When security is willing to collaborate with marketing, companies stand to enjoy a higher level of performance in four critical areas:



**Brand Reputation**



**Data Insights**



**Customer Experience**



**Employee Experience**

A strong marketing-security partnership preserves brand reputation in an environment rife with privacy concerns; showcasing a strong security commitment can also help build the brand. Working together, marketing and security can better acquire and protect customer data for actionable insights and enrich both the customer and employee experiences.

Conversely, a weak marketing-security partnership can lead to data disasters, which will erode brand reputation as well as customer and employee trust.

## Challenge: Failure to Communicate

How can marketing and security strengthen their partnership? Personal relationships are built on communication, collaboration, and mutual respect, and this is no different with marketing and security.

In our study, marketers cited the following areas where deeper collaboration is needed:



#### Misaligned Goals



#### Inadequate Understanding of Roles



#### Lack of Communication

It's important for marketing and security to engage early and often on how to balance derivation of business value of data with data protection and handling. Problematic partnerships happen when communication occurs only during a crisis. The goal is to build fluid security guardrails and mechanisms up front in a natural manner, not bolt them on at the end.

“Cyber is not a shop of ‘No,’ rather how can we get to ‘Yes,’” says John Kupcinski, CISO at PSEG Long Island. “Because of this, it’s important to engage cyber early in the process to ensure there are no gotchas before the work is about to commence. We want to partner and enable the business in a secure and safe fashion.” (Kupcinski’s personal opinions in no way reflect the opinions or positions of PSEG Long Island.)

### What You’ll Learn

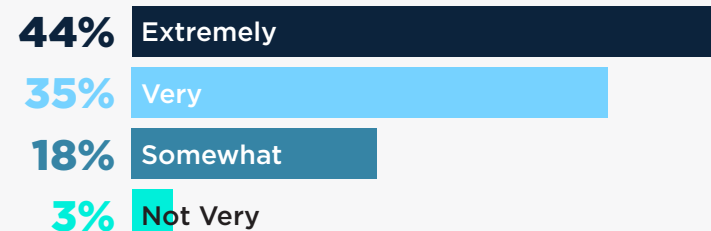
As marketers compete on customer data insights and leverage emerging AI technology, the marketing-security partnership will continue to be under the spotlight. The CMO Council and KPMG embarked on an extensive study to understand how marketing and security can redefine their working relationship to get ahead.

We explore areas of alignment such as communication practices, joint initiatives, technology assessments, etc. We unearthed significant performance gaps, in safeguarding brand reputation, driving actionable data insights, ensuring personalized and protected customer interactions, and fostering a secure and collaborative work environment, between marketing-security partnerships showing a willingness to collaborate and those that don’t.

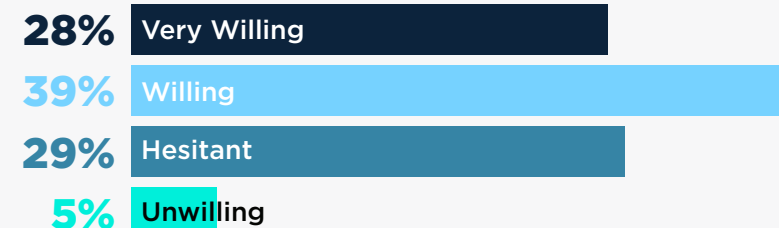
### Our Methodology

Our findings are based on a survey of 256 marketing leaders across industries and geographies. Additionally, we conducted in-depth interviews with marketing or security executives from Teradata, CDW, The Doctor’s Company, and PSEG Long Island.

### IS THE MARKETING-SECURITY RELATIONSHIP IMPORTANT?



### IS SECURITY WILLING TO COLLABORATE WITH MARKETING?



\*Amounts do not add to 100% due to rounding

# HOW MARKETING SEES THREATS

Marketing wants to acquire and use data for more personalized interactions with customers, but this leads to more opportunity for bad actors to steal data, create attack profiles, and compromise systems and services.

Brand hijacking, unseemly online ad placement, and customer data breaches are just a few of the security incidents on the rise. There's no shortage of alarming stats:

- ◆ **77% of security decision-makers experienced at least one data breach over the past 12 months (Source: Forrester)**
- ◆ **8.2 billion breached records worldwide in 2023 (Source: IT Governance)**
- ◆ **20% increase in data breaches in the US from 2022 to 2023 (Source: Identity Theft Resource Center)**

Marketers haven't missed the warning signs either. Two-thirds of marketers say security breaches of customer data are top of mind when planning initiatives, making investments, and executing campaigns, our study found.

Better collaboration can reduce risk — but it's a two-way street. Marketing leaders need to understand, at a high level, how to protect data. Security leaders need to consider how to structure data management and protection thoughtfully to avoid limiting business agility.

## The Looming AI Threat

The top marketing initiative posing the greatest security threat is the use of AI, followed by customer behavioral data and Internet of Things, according to our survey. Gartner also cites generative AI (GenAI) as a driving force behind top cybersecurity trends in 2024.

AI has the potential to optimize data utilization, transform the marketing department, increase productivity, and lower costs, but it carries its fair

share of risks. Data privacy and protection, adversarial attacks and model integrity, bias and fairness in AI algorithms, AI supply chain risk and third-party integration, insider threats and unauthorized access are just a few of the ways in which AI can induce harm to a business.

In sum, the partnership between the CMO and the CISO helps organizations address these challenges of AI and mitigate its risks. Active collaboration, clear division of roles, and consistent communication between these two officers can greatly enhance the organization's security posture.

---

**Key Recommendation:** *Prepare your business to be at the forefront of AI technology in your industry by acutely examining your data collection, storage, and usage across functions.*

*“With the proliferation of AI, specifically around chatbots like ChatGPT, it's imperative that TDC employees remain diligent in our efforts to safeguard sensitive data.”*

— Jesmine La Russa, VP, Marketing,  
The Doctor's Company



# INITIATIVES, CAMPAIGNS, MARTECH

A stronger connection is evolving between CMOs and CISOs, especially in regard to current and future regulations related to customer consent and preference management. Regulations impact everything from incident response plans and data privacy policies to cookieless websites and social media platforms.

Marketing and security should be collaborating on these and other initiatives — and they should do so early and often. “The relationship has to be a lot more proactive and strategic in nature,” Teradata’s Uppal says.

***In 65% of campaigns, security isn’t actively engaged by marketing during conceptualization and planning.***

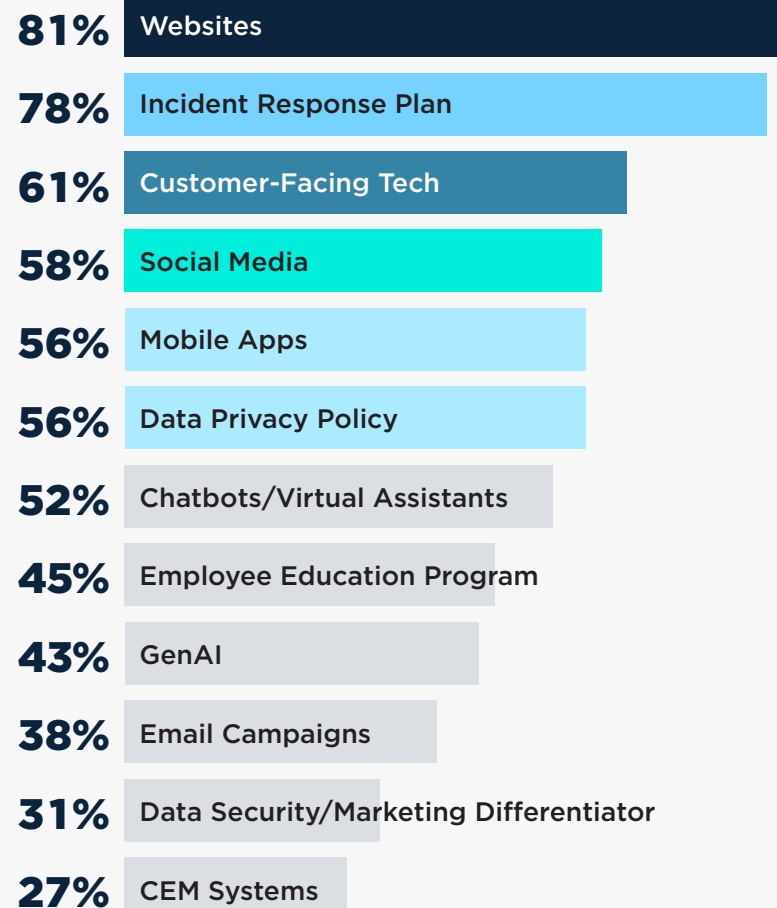
(Source: CMO Council)

Yet this isn’t always the case.

Our survey found a collaboration blind spot with marketing campaigns. Only 35% of marketing-security partnerships collaborate during campaign conceptualization and planning. For the vast majority of campaigns, security isn’t actively engaged by the marketing team until after they’re already in motion. Among less-evolved marketing-security partnerships, more than half (53%) don’t collaborate on campaigns at all.

It’s important for security to understand marketing’s intentions with data in a campaign before launch. A campaign on a social media platform, for instance, might have underlying terms and conditions that can result in marketing leaving digital breadcrumbs for third parties to find.

## CMO-CISO JOINT INITIATIVES



### What Should Marketing and Security Talk About?

PSEG Long Island's Kupcinski says companies have a risk appetite — tolerance and exposure — and the job of cyber is to draw tolerance down through corrective means and limit exposure as much as possible.

Cybersecurity can be an effective partner to collaborate on innovative security features, Kupcinski says. (For more, see “Featured Perspective: John Kupcinski,” page 17.)

**Key Recommendation:** *Data protection starts with an understanding of what data is collected, purposes for which it's used, and with which third parties it's shared. Proactive collaboration between security and marketing teams can streamline this process and make the job easier for each respective team.*

*“From a cyber or data governance perspective, we need to know we're not designing a campaign that could increase the risk to the firm. The earlier we can have those conversations, the better tailored the output.”*

— John Kupcinski, CISO, PSEG Long Island



### CAMPAIGN COLLABORATION

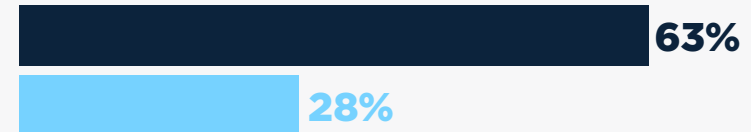
#### Conceptualization and Planning



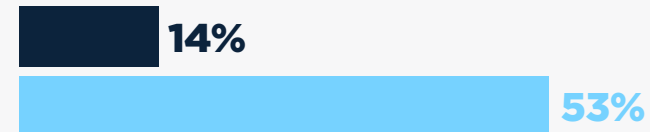
#### Campaign Implementation



#### Post-Launch Adjustments



#### Don't Collaborate on Campaigns



■ Willing to Collaborate    ■ Not-so-Willing to Collaborate

# CAPABILITIES: BRAND, DATA, CX, EX

Organizations where marketing and security collaborate on acquiring, maintaining, and securing customer data for competitive advantage enjoy performance boosts in brand reputation, actionable data insights, customer experience and employee experience.

The gap between partnerships willing to collaborate and those not so willing is very apparent.

Our study split survey respondents into two groups depending on how marketers rated their security counterparts' willingness to collaborate. Respondents who answered "very willing" or "willing" were put in one group, and those who answered "hesitant" or "unwilling" were put in another.

We then asked each group how they ranked their performance in four marketing-security capabilities: brand reputation, data insights, customer experience, and employee experience. We've highlighted the starkest differences below.



## Brand Reputation

*We define brand reputation as the ability for marketing and security to safeguard a company's image.*

By demonstrating trustworthiness, protecting customer data, practicing proper data acquisition and governance, and addressing issues promptly and efficiently, marketing and security can better preserve brand reputation.

Our study found that 46% of marketing-security partnerships that are willing to collaborate were "very satisfied" in their ability to preserve brand reputation. Only 1% of marketers in a partnership that is less willing to collaborate said the same thing.

*"Because of the nature of the work we do and our openness to marketing transactions and customer interactions, it's no longer in our control to even assess what can lead to a risk."*

— Aditi Uppal, Senior Director,  
Digital Marketing at Teradata



## CMO-CISO PARTNERSHIP PERFORMANCE SCORECARD

### BRAND

|            |                   |            |
|------------|-------------------|------------|
| <b>46%</b> | Very Satisfied    | <b>1%</b>  |
| <b>51%</b> | Satisfied         | <b>63%</b> |
| <b>2%</b>  | Dissatisfied      | <b>34%</b> |
| <b>1%</b>  | Very Dissatisfied | <b>2%</b>  |

■ Willing to Collaborate    ■ Not-so-Willing to Collaborate

\*Amounts do not add to 100% due to rounding



### Data Insights

*We define data insights as the ability for marketing and security to acquire and protect customer information for data-driven decision-making.*

Through flexible and business-centric security controls, marketing and security can drive data-driven decision-making and targeted marketing strategies. According to a CMO Council pulse poll, nearly 80% of marketing leaders say data, analytics, and insights are very important to winning and retaining customers.

Our study found that only 4% of marketing-security partnerships that are willing to collaborate were “dissatisfied” (3%) or “very dissatisfied” (1%) in their ability to acquire and protect customer data for actionable insights. A whopping 62% of marketers in partnerships that are less willing to collaborate were “dissatisfied” (59%) or “very dissatisfied” (3%).



### Customer Experience

*We define customer experience as the ability for marketing and security to ensure seamless, personalized, and protected customer interactions.*

By collaborating on data security and marketing strategies, marketing and security can deliver a better customer experience. It’s an area in need of improvement. According to the KPMG’s 2023 US Customer Experience Excellence report, satisfaction with customer experience delivery has fallen across all industries.

Our study found that 89% of marketing-security partnerships that are willing to collaborate were either “very satisfied” (32%) or “satisfied” (57%) in their ability to enrich the customer experience. Only 23% of marketers in partnerships that are less willing to collaborate said they were “satisfied.” None were “very satisfied.”

## CMO-CISO PARTNERSHIP PERFORMANCE SCORECARD

### DATA INSIGHTS

|            |                   |            |
|------------|-------------------|------------|
| <b>46%</b> | Very Satisfied    | <b>2%</b>  |
| <b>51%</b> | Satisfied         | <b>35%</b> |
| <b>3%</b>  | Dissatisfied      | <b>59%</b> |
| <b>1%</b>  | Very Dissatisfied | <b>3%</b>  |

### CUSTOMER EXPERIENCE

|            |                   |            |
|------------|-------------------|------------|
| <b>32%</b> | Very Satisfied    | <b>0%</b>  |
| <b>57%</b> | Satisfied         | <b>23%</b> |
| <b>10%</b> | Dissatisfied      | <b>60%</b> |
| <b>1%</b>  | Very Dissatisfied | <b>16%</b> |

■ Willing to Collaborate ■ Not-so-Willing to Collaborate

\*Amounts do not add to 100% due to rounding



### Employee Experience

*We define employee experience as the ability for marketing and security to foster a secure and collaborative work environment.*

By combining marketing innovations with robust cybersecurity measures, marketing and security can do a better job of empowering employees with a great experience, especially those working remotely who rely on a digital experience. A recent *Forbes* article citing multiple sources revealed that happy employees are as much as 20% more productive, and highly engaged teams are 21% more profitable.

Our study found that 84% of marketing-security partnerships that are willing to collaborate were either “very satisfied” (18%) or “satisfied” (66%) in their ability to enrich the employee experience. Only 22% of marketers in partnerships that are less willing to collaborate said they were “satisfied.” None were “very satisfied.”

**Key Recommendation:** *Understand the widespread impact that your marketing-security partnership has on your business, both internally and externally.*

### CMO-CISO PARTNERSHIP PERFORMANCE SCORECARD

#### EMPLOYEE EXPERIENCE

|     |                   |     |
|-----|-------------------|-----|
| 18% | Very Satisfied    | 0%  |
| 66% | Satisfied         | 22% |
| 15% | Dissatisfied      | 66% |
| 1%  | Very Dissatisfied | 12% |

■ Willing to Collaborate ■ Not-so-Willing to Collaborate

\*Amounts do not add to 100% due to rounding

*“From a marketing perspective, you can support the CISO by helping his team get its message out internally about what they’re doing and how everyone’s involved. The CISO can help marketing externally by showing customers how the brand is addressing security issues through blogging and in your marketing programs.”*

— Jodie Hoare, formerly Head of Marketing, EMEA, Trustwave



# MARKETING-SECURITY RELATIONSHIP STRENGTH BY INDUSTRY

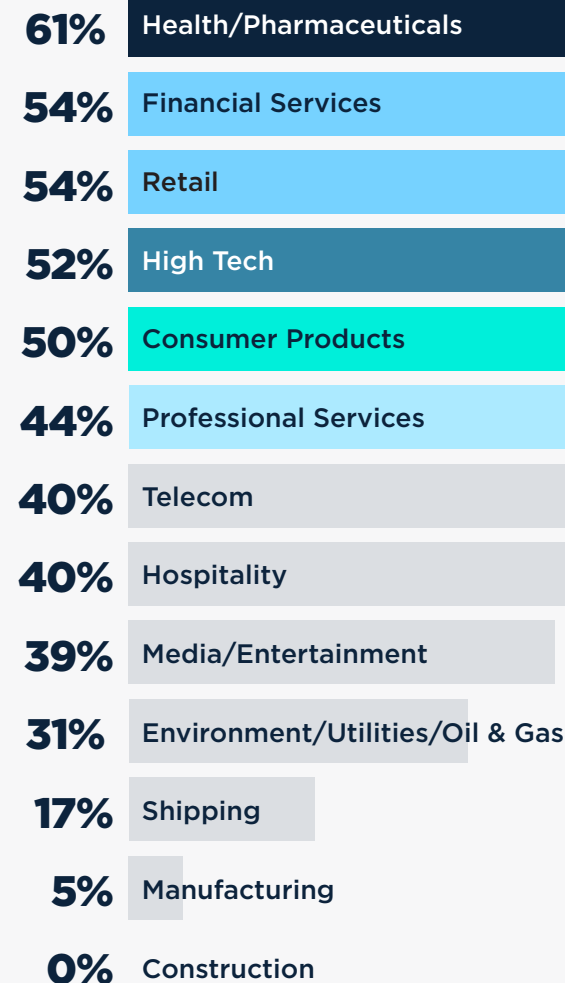
Industries vary widely in their use of marketing data, regulatory concerns, risk tolerance, and exposure. This was reflected in our survey results, and we've surfaced the following industry-specific themes:

- ◆ Financial Services, Health/Pharmaceuticals, and High Tech place strong emphasis on the marketing-security relationship to preserve brand reputation.
- ◆ Financial Services, Health/Pharmaceuticals, and Media/Entertainment show a high willingness to collaborate.
- ◆ Manufacturing and Professional Services have big barriers to collaboration.
- ◆ Media/Entertainment and Telecom show a higher inclination toward joint initiatives for employee education programs on data security and marketing's role.
- ◆ Health/Pharmaceuticals and Telecom lead in leveraging data privacy and security as a marketing differentiator.

---

**Key Recommendation:** Tailor the marketing-security partnership to the specific needs and concerns of your industry to maximize its effectiveness.

## IS THE MARKETING-SECURITY RELATIONSHIP "EXTREMELY IMPORTANT"?



# OVERCOMING OBSTACLES

Shoring up the marketing-security partnership will require a collective effort and willingness to collaborate on behalf of both parties. Chief among the challenges to overcome is misaligned priorities, our survey found.

Herein lies the crux of the marketing-security partnership. The more marketing becomes accessible to customers through data insights, the more opportunity for adversaries to create attack profiles based on data in the public domain and target specific organizations.

“Accessibility is inversely proportional to security. The more ways the business looks to provide services — internally and externally — increases the potential exposure and attack surface,” CISO Kupcinski says.

***32% of less collaborative partnerships communicate only during a crisis.***

(Source: CMO Council)

Regular communication about marketing’s intentions with data can help ease tensions. Kupcinski says security should be involved in marketing meetings early and often in order to tailor the marketing output while drawing down risk. (For more, see “Featured Perspective: John Kupcinski,” page 17.)

Marketing-security partnerships willing to collaborate tend to have regular joint meetings (44%) or regular communications over email and other channels (27%) more so than partnerships less willing to.

## COLLABORATION CHALLENGES



Misaligned  
Priorities  
**61%**



Inadequate  
Understanding of Roles  
**57%**



Lack of  
Communication  
**51%**



Limited  
Resources  
**38%**



No Significant  
Challenges  
**15%**



Other  
**1%**

The goal of meeting early and often is to get to a shared vision and avoid conflict down the road. Adversarial partnerships develop when either party takes actions without discussing them first.

**Key Recommendation:** Invest in training and education to improve understanding of roles and responsibilities between marketing and security to make communicating easier and more frequent, adopting a proactive rather than reactive approach.

*“Where do you draw the boundaries? If you want to take customer data, what are the permissions? If you want to keep the data, who’s responsible for its safety? The CISO understands compliance and regulations much more than any CMO.”*

— Harsh Singh, Veteran Product Marketing Leader



## COMMUNICATION GAP

### Regular Joint Meetings



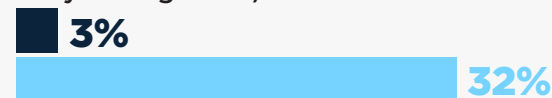
### Regular Email/Platforms



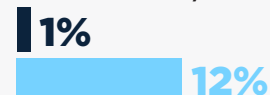
### Ad Hoc Discussions



### Only During Crisis/Incidents



### Do Not Share/Communicate



### Marketing Campaign Planning



■ Willing to Collaborate    ■ Not-so-Willing to Collaborate

## EXPERT COMMENTARY FROM KPMG

**BRET SANFORD-CHUNG**

Managing Director

Marketing Advisory Services

KPMG, LLP

**ORSON LUCAS**

Principal

Cyber Security Services

KPMG LLP



### HOW IMPORTANT IS THE MARKETING-SECURITY PARTNERSHIP? WHY DOES IT MATTER?

**BRET SANFORD-CHUNG:**

The marketing-security partnership is the foundation of your customer and employee experience, and by extrapolation, your brand. When a customer invites your product into their home or their life and shares private, personal data with your organization, they do so with the expectation that the data is protected and they will receive value in exchange. Marketing and security need to be in lockstep to meet those expectations and build brand strength in a market that increasingly scrutinizes the collection, handling, and protection of data.

**ORSON LUCAS:**

I couldn't agree more. Marketing is frequently the front line of consumer engagement relative to sensitive personal information. It's important that Chief Marketing Officers are enabled to drive business growth, but also important that appropriate guardrails are in place to do that in a way that ensures trust as a priority. Certainly, the CISO relationship is a key partnership in that respect, as are strong relationships with the Chief Privacy Officer, Chief Data Officer, and senior business stakeholders and the Board.

***48% of American workers don't trust their companies to use their personal data ethically.***

(Source: CMO Council)

## WHAT STEPS CAN CMOs TAKE TOWARD A BETTER MARKETING-SECURITY RELATIONSHIP?

### BRET SANFORD-CHUNG:

CMOs need to build trust with their security counterparts by fostering open and early communication. It's all about providing context — historically, the two functions have been focused on very different things — so CMOs must provide CISOs with the understanding of why they seek to do things, not just what they want to do. This will help get everyone on the same page strategically. Operationally, establishing a focus on security within the marketing team, involving security early and often, and collaborating on incident response and prevention across functions will reap dividends over time.

## HOW CAN MARKETING AND SECURITY OVERCOME THEIR CULTURAL DIFFERENCES?

### BRET SANFORD-CHUNG:

It is important for them to both realize they have the same end goal: build a strong brand with minimal risk. Today, a huge part of this is protecting data and demonstrating that you are protecting it. From there, the functions can work backwards on shared goals. Start with one source of truth — use collaborative metrics that both teams derive value from. Communication becomes easier when everyone speaks the same language. While both functions must still focus on different aspects of the business, with shared trust, common goals, and one source of truth, their diversity of thought becomes an asset to be leveraged rather than an obstacle to overcome.

### ORSON LUCAS:

In my experience, establishing common ground and goals at the outset is a critical success factor in successful CMO-CISO partnerships. This may challenge CISOs to be more business centric in finding solutions that protect personal information while enabling the business and may also challenge CMOs to consider and address risks they may not have otherwise considered. Ultimately though, there is a very real opportunity for joint wins through a common strategy that allows for deeper, richer interactions with consumers while helping to get them comfortable their data is appropriately secured.

### ORSON LUCAS:

I'd echo Bret's comments: first and foremost, find common ground and joint wins. Effective cybersecurity means balancing protection of sensitive information with business enablement.

## WHAT ARE SIGNS THAT THE MARKETING-SECURITY BALANCE HAS BEEN ACHIEVED?

### BRET SANFORD-CHUNG:

Unfortunately, there isn't a clear metric here, but remember the symbiotic nature of the relationship — fewer data issues, more transparent communication, and quicker response and resolution are all products of a strong data/marketing tie. Fortunately, these are also the markers of a strong brand able to differentiate from the competition. A win-win all around.

### ORSON LUCAS:

It's hard to prove a negative. That's one of the big challenges that CISOs often face — if there are no breaches, lawsuits, etc. related to unauthorized access, disclosure or loss, presumably the CISO is doing their job. However, as CISOs think about metrics they report, they should consider augmentation of metrics that speak to business enablement and that tie into CMO success factors, including increased and/or richer customer engagement and customer trust. Additionally, while qualitative and may not make the cut for data-driven dashboards, one of the most important areas of sentiment to monitor for CISOs is the degree to which business partners are proactively engaging security for consultation and partnership on key initiatives.

## EXECUTIVE PERSPECTIVE



**JOHN KUPCINSKI**

Title: Chief Information Security Officer

Company: PSEG Long Island

Industry: Energy



**“** *Cyber is not a shop of ‘No,’ rather how can we get to ‘Yes.’ Because of this, it’s important to engage cyber early in the process to ensure there are no gotchas before the work is about to commence. We want to partner and enable the business in a secure and safe fashion.* **”**

“Accessibility is inversely proportional to security. The more ways the business looks to provide services — internally and externally — increases the potential exposure and attack surface,” says John Kupcinski, chief information security officer at PSEG Long Island. (Kupcinski’s personal opinions in no way reflect the opinions or positions of PSEG Long Island.)

Conversely, cybersecurity can also be a marketing differentiator. Cybersecurity is beginning to be seen by consumers as a dimension of quality that buyers are looking to invest in. Consumers want secure products and services. Companies are expected to protect consumer data and privacy. Additionally, investors take into account cyber controls as part of regulatory filings.

Put simply, customers are more aware of security risks. A product that guarantees data security and privacy enhances customer satisfaction and loyalty. Failure to properly manage cybersecurity can drive customers away, lower investment outlook, and increase regulatory scrutiny.

As part of the CISO-CMO conversations, cybersecurity can help drive product features, enhance elements of reliability, highlight its operating characteristics, and be an important consideration regarding reliability.

Cybersecurity can partner with marketing. “From a cyber or data governance perspective, we need to know we’re not designing a campaign that could increase the risk to the firm,” Kupcinski says. “The earlier we can have those conversations, the better tailored the output.”

Here’s a sampling of considerations when marketing is looking to partner with cybersecurity:

1. Is there a place for cyber within marketing and product development? What are my customer insights, concerns and expectations regarding security of our products and services? Is there a way to integrate customer feedback collected by marketing to improve security features? Cyber can be an effective partner to collaborate on innovative security features that can be highlighted in marketing campaigns to differentiate products in the marketplace.
2. Cybersecurity teams should be involved from the initial stages of marketing campaigns and product development to ensure security is built in upfront. Marketing and product teams can work with cybersecurity experts to communicate security features and practices transparently, enhancing customer trust.
3. Marketing should engage cybersecurity and develop joint strategies for communicating effectively during and after a security incident to manage public perception and maintain trust.
4. Internal and external collaboration: Marketing can assist in creating engaging security awareness campaigns for both customers and employees by leveraging their expertise in communication, which includes joint efforts to educate customers on safe practices, enhancing overall product experience and satisfaction.

## EXECUTIVE PERSPECTIVE



### ADITI UPPAL

Title: Vice President, Digital Marketing and Demand Gen

Company: Teradata

Industry: Technology

teradata.

**“** *The relationship between marketing and information security absolutely has to evolve because of the unknown territories we're in, such as the influx of GenAI and the role of trust and privacy. The relationship has to be a lot more proactive and strategic in nature.* **”**

What customer interactions lead to risk? What are the dos and don'ts with generative AI? When should marketing reach out to security? These are just a few of the questions spurring a reevaluation of marketing and security working together.

“The relationship between marketing and information security absolutely has to evolve because of the unknown territories we're in, such as the influx of GenAI and the role of trust and privacy,” says Aditi Uppal, vice president of digital marketing and demand generation at Teradata. “The relationship has to be a lot more proactive and strategic in nature.”

For far too long, far too many marketers have relied on ad hoc conversations with security usually after launching campaigns and executing other data-related marketing activities. This is because marketing often moves at faster speeds than does security.

But this is no longer good enough.

“Ad hoc communication usually comes down to a lack of awareness of security's role, vision, and charter and how marketing and security teams should work together,” Uppal says. “The onus is not only on marketing but on security to educate and inform their role and

how a strategic partnership can add value to both sides and more importantly to the organization and customers. Because of the nature of the work we do and our openness to marketing transactions and customer interactions, it's no longer in our control to even assess what can lead to a risk.”

Uppal says marketing and security need to get ahead of risk by being proactive when it comes to new data sources, data-related technologies, data collection methods, etc. Both marketing and security professionals need to know how to engage with each other early and often with regard to operating principles, priorities, approval processes, and governance models.

“This is especially true for tech companies dealing with a lot of data and analytics,” Uppal says. “It's too late when you're running a campaign, in front of a customer, and starting to get all the information. The ball is already out.”

At Teradata, the CISO org reports directly to the C-suite and not to any subteams. Fewer go-betweens mean marketing and security can have a more direct relationship. Together, the information security org and marketing org can share a common goal to show the market that their organization is a trusted one.

## EXECUTIVE PERSPECTIVE

**JESMINE LA RUSSA**

Title: Vice President, Marketing  
Company: The Doctor's Company  
Industry: Insurance



**“** *With the proliferation of AI, specifically around chatbots like ChatGPT, it's imperative that The Doctors Company employees remain diligent in our efforts to safeguard sensitive data.* **”**

When Jesmine La Russa, vice president of marketing at The Doctors Company, visited <https://chat.openai.com/>, she received a comprehensive warning from her company.

The warning starts with this: “With the proliferation of artificial intelligence, specifically around chatbots like ChatGPT, it is imperative that TDC Group employees remain diligent in our efforts to safeguard sensitive data. The bottom line is information you input into ChatGPT and like tools is not confidential and sensitive TDC Group data should not be used in connection with ChatGPT or like tools.”

The warning goes on to describe the risk: “Rapidly developing AI technology and security errors on the part of these platforms are still common. It is also a common practice for these solutions to save data entered in them to make that data available to others.”

Then the warning ends with consequences: “Violation of the confidentiality requirements found in the employee handbooks across the TDC Group could include consequences up to and including termination. Violations involving medical records could violate HIPAA, expose the employee to criminal sanctions and the TDC Group companies to penalties.”

If all of this sounds overly harsh, it's not. This kind of message is critical, especially in the heavily regulated insurance industry, and shows that the

security team at The Doctors Company takes a proactive approach to the latest risks.

This doesn't mean marketing is prohibited from using AI. The team is prioritizing data security while creating steps for responsible use.

“One of the things that we're doing between now and next year is working with IT to develop the digital and marketing technology roadmap, which will certainly include the application of AI tools and resources,” La Russa says. “From a marketing perspective, there's a lot we would like to do with personalized data, too.”

It's important to note The Doctors Company understands marketing's impact on the business, La Russa says. Case in point: Marketing recently integrated analytics capabilities within a new direct to consumer platform yielding meaningful customer journey metrics and identifying needed improvements for future development. Innovation in support of improved customer experience is a strategic priority for the company.

“Data metrics connect what we do for lead generation to business conversion,” La Russa says. “We can now deliver actionable insights and metrics that demonstrate how marketing supports and aligns with the overall corporate strategy.”

## EXECUTIVE PERSPECTIVE



### HARSH SINGH

Title: Veteran Product Marketing Leader

Industry: Technology

“ If you want to take customer data, what are the permissions?  
If you want to keep the data, who’s responsible for its safety? ”

Harsh Singh, a veteran product marketing leader in the technology industry, understands customers are full of angst about companies acquiring and sharing their personal data. They wonder how their data is being used, when they gave their permission, and under what conditions.

“Where do you draw the boundaries?” Singh says. “If you want to take customer data, what are the permissions? If you want to keep the data, who’s responsible for its safety? This is where the relationship comes into play because the CISO understands compliance and regulations much more than any CMO.”

Even though marketers intend to do right by customers — no one wants to breach trust — they just don’t know enough about acquiring and keeping data safe. Using the data is another sticking point. Personalization can lead to more meaningful interactions, but leveraging customer data to tailor content can be tricky.

“I’m not sure anyone has fully solved it because it’s an evolving problem,” Singh says.

For these reasons, Singh advises marketers to acquire and use data for a specific purpose. Marketers need to be transparent about this purpose when seeking permission.

Before collecting data, marketers should reach out to security to explain what they’re trying to achieve and why they need specific data. It’s a discussion, Singh says, that allows for security professionals to push back — are you collecting more data than you need?

The goal is to get to a shared vision and avoid conflict down the road. An adversarial relationship happens when actions are taken from either party without first discussing them. The attack surface grows when marketers acquire, use, and store data in silos.

“We are in an age of data abundance, and so there’s more importance being given to this partnership,” Singh says.

## EXECUTIVE PERSPECTIVE

**JODIE HOARE**

Title: Head of Marketing, EMEA (formerly)

Company: Trustwave

Industry: Technology



**“** *The CISO can help marketing externally by showing customers how the brand is addressing security issues through blogging and in your marketing programs.* **”**

Jodie Hoare has unique insight into the CISO mindset. After all, the former head of marketing for EMEA at Trustwave used to market to them daily and talk to them regularly. Hoare knows their aspirations, challenges, and modus operandi.

“From a marketing perspective, you can support the CISO by helping his team get its message out internally about what they’re doing and how everyone’s involved,” Hoare says. “The CISO can help marketing externally by showing customers how the brand is addressing security issues through blogging and in your marketing programs.”

A mutually beneficial relationship helps marketers and security professionals understand each other’s point of view, strengths, and weaknesses. This will be increasingly important as emerging technologies such as AI race toward the intersection of marketing and security.

Hoare says CMOs can make the relationship even more personal by helping CISOs advance in their careers.

For instance, Hoare has seen more boards of directors looking to add a CISO to their ranks due to growing concerns around customer data. Boards don’t know the right questions to ask the business to ensure it’s doing due diligence with data security, customer privacy, and regulations.

At the same time, many CISOs are in uncharted waters; they’ve never been on a board of directors before. CISOs are unsure about how to promote themselves and become board candidates and what exactly a board expects of them.

Working with CISOs, Hoare cocreated a report with an alliance group in the UK about CISOs engaging with boards of directors and having those conversations. To this end, she says CMOs can help CISOs raise their profiles in blogs and on social media.

“Elevating them into a different career route, say, a director on a board, is definitely a win for the relationship,” Hoare says.



The Chief Marketing Officer (CMO) Council is the only global network of executives specifically dedicated to high-level knowledge exchange, thought leadership and personal relationship building among senior corporate marketing leaders and brand decision-makers across a wide range of global industries. The CMO Council's 16,000-plus members control approximately \$1 trillion in aggregated annual marketing expenditures and run complex, distributed marketing and sales operations worldwide. In total, the CMO Council and its strategic interest communities include more than 65,000 global executives in more than 110 countries covering multiple industries, segments and markets. For more information, visit [www.cmocouncil.org](http://www.cmocouncil.org).



KPMG LLP is the U.S. firm of the KPMG global organization of independent professional services firms providing audit, tax and advisory services. The KPMG global organization operates in 143 countries and territories and has more than 273,000 people working in member firms around the world. Each KPMG firm is a legally distinct and separate entity and describes itself as such.

KPMG is widely recognized for being a great place to work and build a career. Our people share a sense of purpose in the work we do, and a strong commitment to community service, inclusion and diversity and eradicating childhood illiteracy. Learn more at [www.kpmg.com/us](http://www.kpmg.com/us).

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.