2018

CMO CYBERSECURITY SURVEY

Key Findings

TABLE OF CONTENTS

FOREWORD

Marketing as a discipline has never before been as effective and enabled as it is today, thanks to the proliferation of technologies designed to help us learn more about our prospects' needs; communicate our value propositions clearly and compellingly; and measure our effort, from reach to reaction.

But much like other business functions, marketing teams today are coming to recognize and accept the responsibility that accompanies the power of the modern marketing technology "stack." Out of necessity in most cases, this has made marketing and IT teams critical partners in helping the organization manage digital risk.

The coalition of cybersecurity companies behind the 2018 CMO Cybersecurity Survey are committed to better understanding the shared responsibility between marketing and IT, and finding the best ways to enable these teams in their respective and common missions.

2018 SURVEY SPONSORS

CISCO

IBM

RSA®

Secureworks®

splunk>

Symantec™

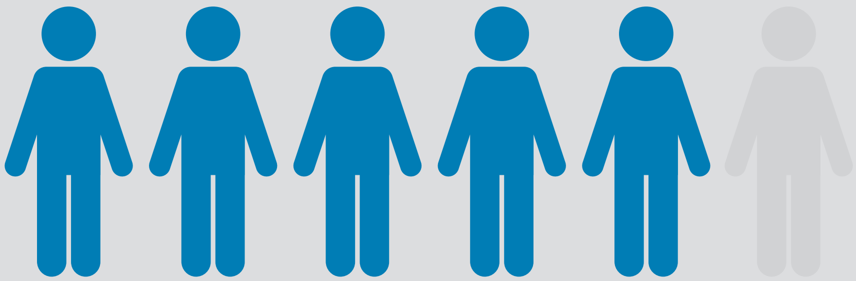
EXECUTIVE SUMMARY

The CMO Cybersecurity Survey is designed to better understand how—and how well—IT and marketing teams work together in terms of cybersecurity.

This data can be valuable to IT and marketing team members and leadership who want to work more effectively together to help manage the organization's digital risk. Likewise, the perspectives contained in the survey findings can help these teams better understand one another's priorities and challenges in pursuit of this common goal.

KEY FINDINGS FROM THE 2018 SURVEY INCLUDE:

Five of six of all respondents agree that marketing complies with IT security policies, protocols, and procedures.



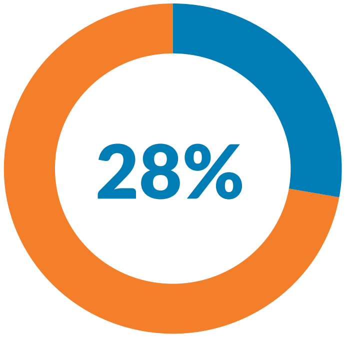
However, IT employees are almost twice as likely than marketing employees to think that marketing employees use "workarounds" – **whether intentionally or unintentionally.**

Marketing is **less likely** than IT to think that their companies' security functions regularly review, lead, or decide on marketing applications and/or cloud service providers.

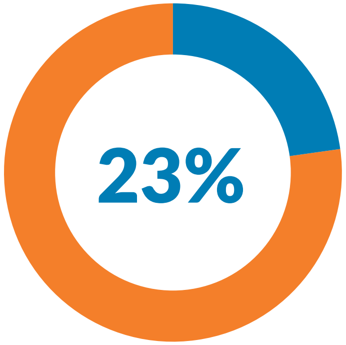
KEY FINDINGS

MARKETING & SECURITY COLLABORATION

Marketing employees are often unaware of the *frequency* of their team's engagement with IT.



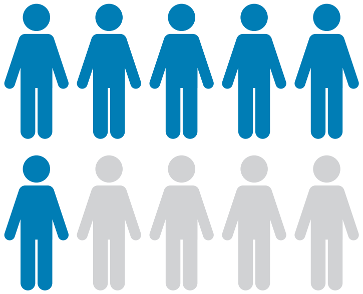
More than one-quarter of marketing employees do not know how often IT **inspects** marketing-related infrastructure applications.



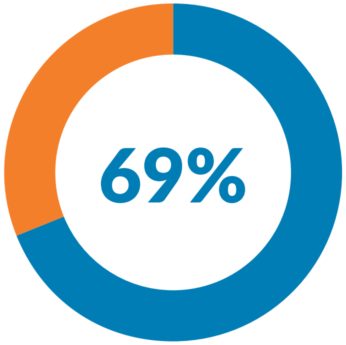
Almost one-quarter of marketing employees do not know how often their team **collaborates** with IT to ensure marketing infrastructure meet security guidelines.

Only 4% of IT employees do not know how frequently the two teams engage.

Marketing and IT employees view the *effectiveness* of collaboration similarly, but there are differences by job level.



About six in ten of both marketing and IT employees describe collaboration as **very/extremely effective.**



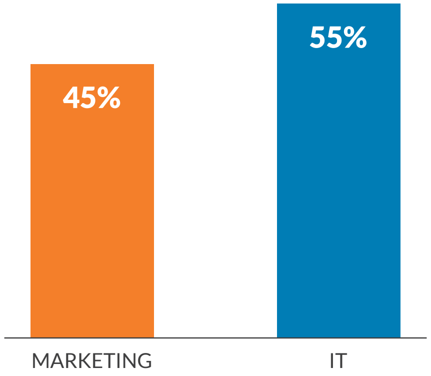
At 69%, **upper management employees** are more likely than managers and other job roles to consider collaboration to be **very/ extremely effective.**

KEY FINDINGS

MARKETING & SECURITY COLLABORATION

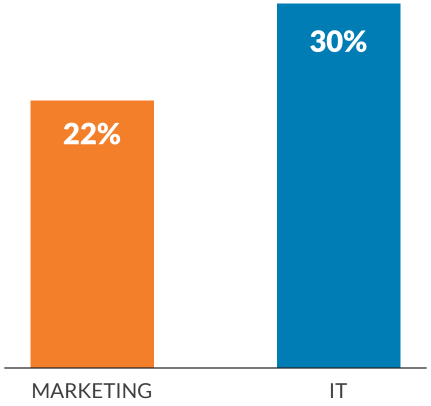
INVOLVEMENT

Marketing is **less likely** than IT to think that their companies' security functions regularly review, lead, or decide on marketing applications and/or cloud service providers.



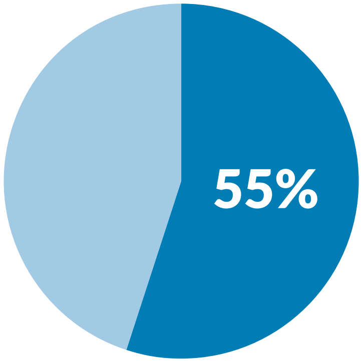
BURDEN

IT is **more likely** than marketing to describe the security review process of marketing technology as very / extremely **burdensome.**



MONEY MATTERS

At companies with $1 billion + annual revenue, 55% of security functions regularly lead and decide on marketing applications and / or cloud services.

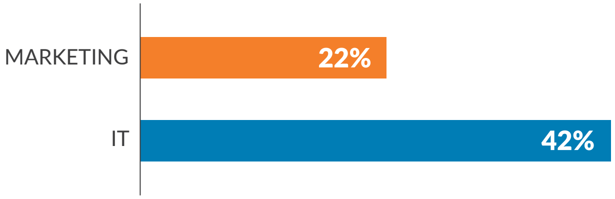


KEY FINDINGS

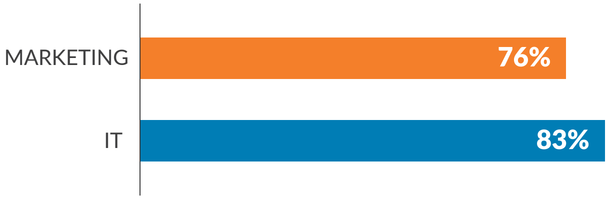
RISK

2X

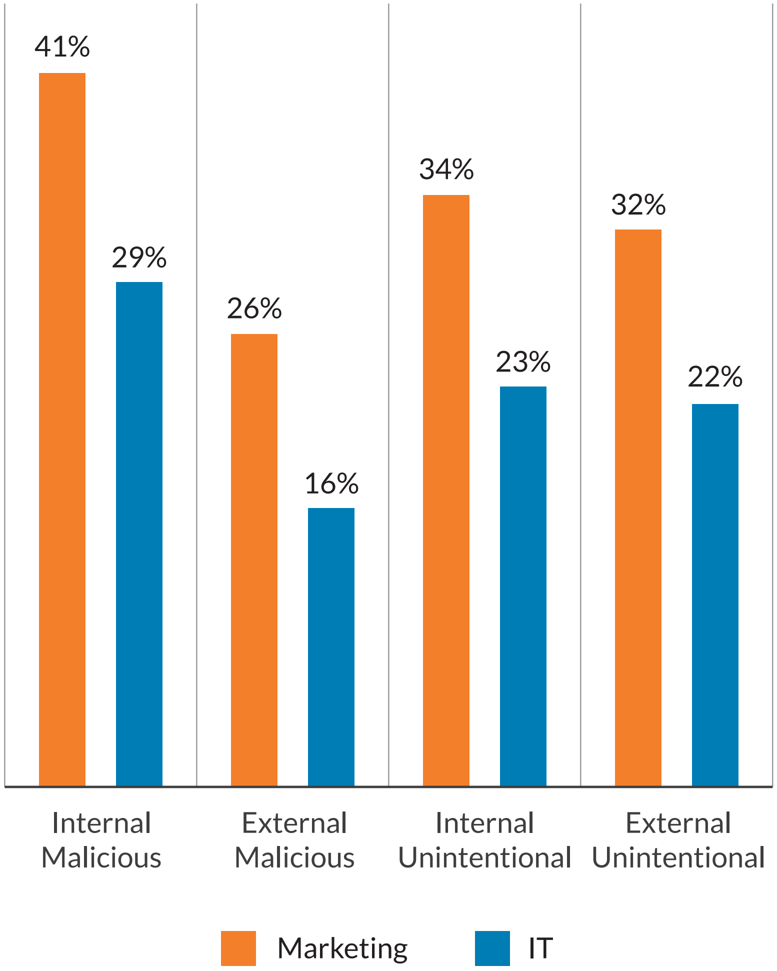
IT is almost **twice as concerned** as marketing that marketing is **exposing** the organization to cyber security incidents.



IT is **more confident** than marketing that marketing understands its **responsibility** to minimize the risk of cybersecurity incidents.



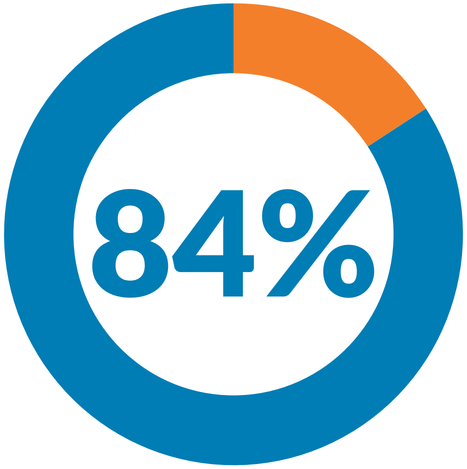
Marketing is **more likely** than IT to have **low concern** for cyber threats.

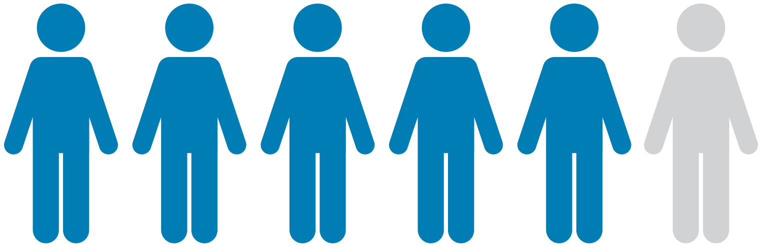


KEY FINDINGS

FOLLOWING PROCEDURES

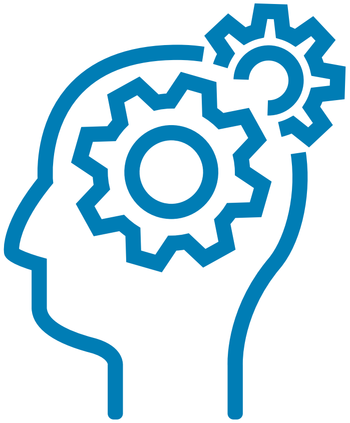
Five of six of all respondents agree that marketing complies with IT security policies, protocols, and procedures.





However, IT employees are almost twice as likely than marketing employees to think that marketing employees use “workarounds” – **whether intentionally or unintentionally.**

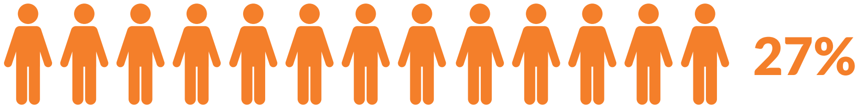
2X



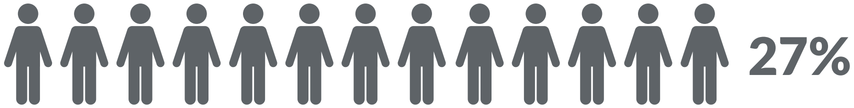
KEY FINDINGS

“SHADOW IT” & TECHNOLOGY SPEND

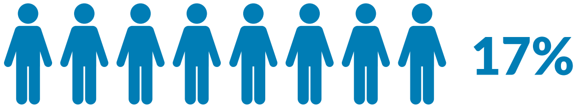
IT believes that R&D and customer service are most likely to use “Shadow IT.”



Research and Development

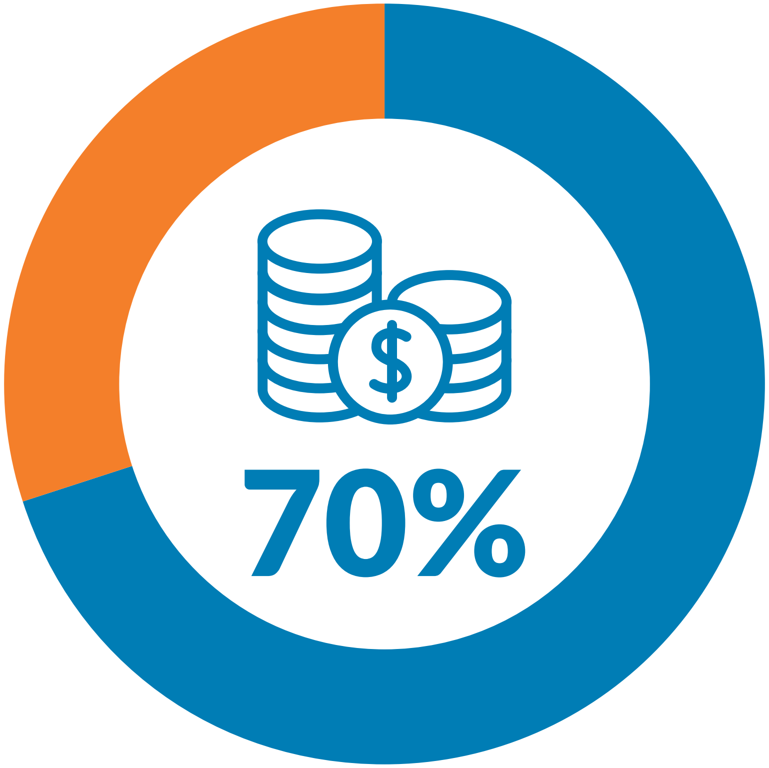


Customer Service



Marketing

The IT department is cited as receiving the highest share of technology spend.



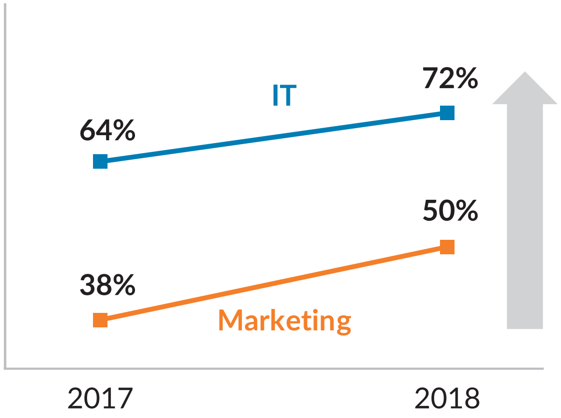
Almost three-quarters of respondents indicate that IT is allocated at least 3% of company revenue.

KEY FINDINGS

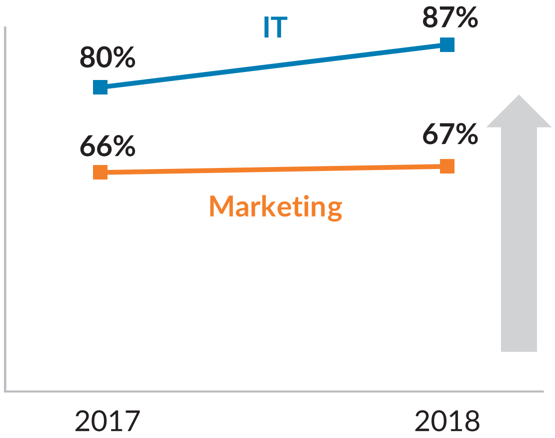
YEAR-OVER-YEAR

Overall, IT concern about cyber threats has increased more substantially from 2017–2018 than marketing concern.

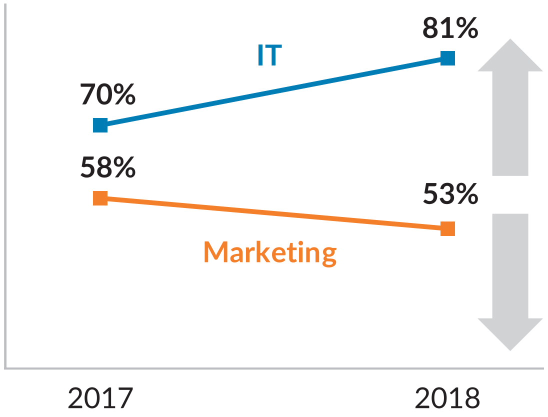
INTERNAL MALICIOUS
Medium + High



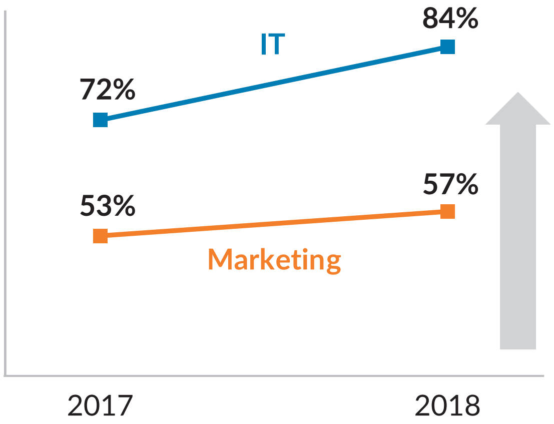
EXTERNAL MALICIOUS
Medium + High



INTERNAL UNINTENTIONAL
Medium + High



EXTERNAL UNINTENTIONAL
Medium + High



KEY FINDINGS

YEAR-OVER-YEAR

From 2017 to 2018, there is an increase among IT and marketing respondents that marketing *understands* its responsibility to minimize cyber risk.

RESPONSIBILITY

More IT and marketing employees believe that marketing understands its *responsibility* to minimize cyber risk.

PROCESS

More marketing employees indicate that it knows *how* to minimize cyber risk, but IT's view of marketing's understanding remains steady from 2017-2018.

COMPLIANCE

More IT and marketing employees think that marketing *complies* with IT security policies, protocols, and procedures.

CONCLUSIONS

Today, both marketing and IT organizations agree that marketing better understands its responsibility to minimize cyber risk. However, there are areas that still need to be addressed in order to achieve a more effective working relationship to benefit each group and the organization's cybersecurity posture as a whole.

Both Marketing and IT are **often not on the same page** when it comes to working together in terms of cybersecurity, citing differences in understanding of collaboration, involvement, and review processes.

Marketing teams are **not overly concerned about specific cyber threats**, frequently describing their concerns for various threats as "low," an indication that they may not be fully aware of the potential implications of those threats.

Marketing groups may be **unknowingly putting their organizations at risk** by using unintentional or intentional "workarounds".

RECOMMENDATIONS

1

NURTURE THE IT-MARKETING RELATIONSHIP

Bringing Marketing and IT closer, and working to understand the other's perspective, is a win-win for both teams, and for the organization's risk posture, too. For example, Marketing should work closely with IT when selecting new marketing tools and technologies.

2

TEACH MARKETING ABOUT SECURITY, AND SECURITY ABOUT MARKETING

IT teams who take the time to educate marketing teams about security can realize real benefits, so long as they keep the conversation relevant and contextual. Likewise, these teams need to have a common understanding of Marketing's business goals and priorities. With this context, these teams can start to move beyond talking about cyber threats, and start talking about digital risk.

3

BECOME CYBER AWARE

Everyone needs to get and stay smart on cybersecurity. Cybercrime won't go away so keeping current is key. Security is not an IT problem, it's a business risk problem.

4

TAKE ACCOUNTABILITY

Marketers must build modern marketing infrastructure with security in mind, partnering directly with the CIO or CISO on it. Marketers are effectively in IT if they are modernizing your marketing engine.

5

INSIST VENDORS PROVE THEY ARE SECURE

Marketing and IT teams must insist that vendors undergo security audits related to their ability to protect and defend data. These reviews can also identify any possible vulnerabilities or entry points that can affect other parts of the business. Start with making sure your marketing ecosystem and third parties undergo proper security reviews and have proper data privacy controls in place.

6

PARTNER WITH IT ON THE MARKETING ROADMAP AND MONITORING PLAN

Marketers should drive a conversation about how the IT security teams can better protect the marketing infrastructure and respond in the event of a breach. Ask questions about identity management and threat detection strategies. If marketing isn't working with the IT security team, they are working against it.

7

ADVOCATE FOR A BREACH COMMUNICATION PLAN

Marketing should work to build a crisis communication plan for a breach, even if it's not their job. Plan and stage breach-response simulations, and start a discussion about disclosure policies to align all players on the definitions and protocol for breach communication. If nothing else, retain a good crisis communication firm; remember, though, that not all crisis communication firms know how to handle breaches!

METHODOLOGY & SAMPLE SIZE

The 2018 CMO Cybersecurity Survey was administered in five languages in 10 countries:

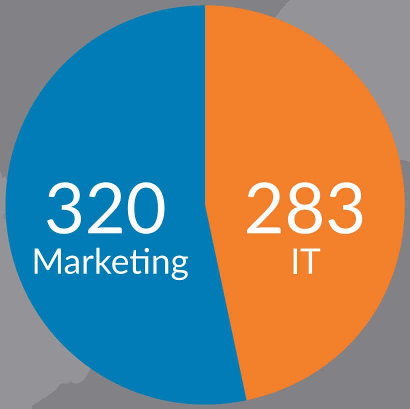
United States, Canada, Australia, Singapore, India, United Kingdom, France, Germany, Italy, Japan

SAMPLE:

MORE THAN

600

Marketing & IT Employees



IN ORGANIZATIONS WITH REVENUE **of at least**

$50 MILLION **in 2017**