RSA

RSA DATA PRIVACY & SECURITY SURVEY 2019:

The Growing Data Disconnect Between Consumers and Businesses

BUSINESS-DRIVEN SECURITY™

CUSTOMER DATA IS CREATING DIGITAL RISK

As competition increases across every marketplace, companies are rapidly evolving digital business models and services in an ongoing effort to give consumers better, more tailored, and more purchase-worthy digital experiences.

But there is a growing disconnect between how companies capitalize on customer data and consumer expectations around how their data should be used and secured. 2018 was host to a myriad of high-profile data breaches that compromised billions of accounts. In these incidents, businesses suffered financial damages in the form of breach-related expenses and regulatory fines, and they also suffered a potentially irreparable loss of customer trust. Consumers realized that their data had been exposed, and that it had been used in ways they had not considered and approved. This loss of trust represents one of the biggest hidden risks of digital transformation. Cyber breaches could potentially become market-making events heralding the decline and eventual demise of big brand names if consumers flee to competitors.

It is against this backdrop that we conducted our second annual RSA® Data Privacy & Security Survey, focusing on a topic increasingly relevant to today's business environment: ethical use of data.

EXECUTIVE SUMMARY

The steady drumbeat of data-misuse and breach disclosure-related headlines of recent years is rapidly evolving consumers' data-privacy attitudes. While consumers believe there are ethical ways companies can use their data, they harbor heightened concerns about their privacy, distrust trends such as personalization and device tracking, and blame companies when hacked. Somewhat paradoxically, consumers also believe that their responsibility to protect their own data is minimal, leading to lax password and information-handling practices. As a result, companies need to educate consumers about how data is shared, gain their consent and trust, and lead by example. Those who do will forge their brand around the ethical use of data, while those who delay or defer may experience a backlash in the media-driven marketplace.

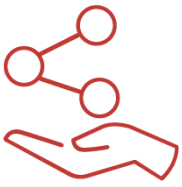
RSA® DATA PRIVACY & SECURITY SURVEY AT A GLANCE

Our second annual survey focuses on ethical data use. It provides:

- An analysis of consumer expectations in France, Germany, the United Kingdom (U.K.), and the United States (U.S.), as evidenced by survey respondents
- An understanding of country-by-country differences and why they matter
- A look at generational differences, including Gen Z, younger and older Millennials, Gen X, and Baby Boomers
- Insight into consumers' attitudes toward how different types of personal information, such as online passwords, contact information, browsing data, medical data, and more, should be protected
- Recommendations for companies who want to create sustainable ethical data policies

As RSA probed consumer perspectives on data collection, usage, and sharing, we uncovered the following insights for businesses to take away from the report:

1. **Context matters:** Individuals across all countries surveyed are concerned about their financial/banking data, as well as about sensitive information such as passwords. Other areas of concern vary dramatically by generation, nationality, and even gender. Companies must consider their users' personal context when establishing and communicating their data policies and practices.
2. **Privacy expectations are cultural:** While the EU General Data Protection Regulation (GDPR) spans all member states of the European Union, consumers respond to data privacy differently based on their nationality due to cultural factors, current events, and high-profile data breaches in their respective countries. Businesses need to consider how regulations and other data-sharing violations are shaping—and hardening—public opinion across all their markets.
3. **Personalization remains a puzzle:** Countless studies have demonstrated that personalized experiences increase user activity and purchasing. However, at the same time, consumers disagree with the statement that companies having more data allows them to offer better and more personalized products and services. Last year, we witnessed both a media and consumer backlash when big brands revealed far-reaching data collection and sharing practices, as well as data breaches. It's imperative for companies to communicate why and how they are using customer data to mitigate future business risk.



When asked, "There are ethical ways in which a company can use my personal information/data," 48% of survey respondents on average agreed.

HOW ATTITUDES TOWARD THE ETHICAL USE OF DATA VARY

RSA

- **The U.S. leads the countries surveyed in consumer acceptance:** In the U.S., 60% agreed, but only 48% in the U.K., 45% in France, and 43% in Germany agreed.
- **Digital-born consumers are the most comfortable with data sharing:** 54% of Gen Z (ages 18–24 in this survey) and 54% of younger Millennials (ages 25–34 in this survey) agreed, while only 49% of older Millennials (ages 35–44 in this survey), 47% of Gen X (ages 45–54 in this survey), and 44% of Boomers (ages 55+ in this survey) agreed.

As consumer attitudes vary across generations, regions, and time, it is critical that companies' policies are sustainable. To achieve this goal, companies must acknowledge and protect consumers' right to privacy while considering the impact of emerging technology. It is our hope that companies can use this survey information to craft and refine their own ethical data policies and standards. By so doing, they can forge deeper connections with customers to grow their business while addressing very real concerns about data protection and privacy.

ABOUT THIS SURVEY

This is the second year of the RSA® Data Privacy & Security Survey. The purpose of the annual survey is to understand global consumer values about data privacy and security, and chart year-over-year changes. By so doing, we seek to understand critical data collection, usage, storage, compliance, and security trends that can impact businesses in their fast-moving marketplaces.

OUR METHODOLOGY

A TOTAL SAMPLE SIZE WAS

6,387

ADULTS IN FRANCE, GERMANY, THE U.K., AND THE U.S.


FRANCE


GERMANY


U.K.


U.S.

- The survey was conducted online by YouGov Plc.
- All figures, unless otherwise stated, are from YouGov Plc.
- The survey was conducted in the period of December 18–27, 2018, for a true year-end look at consumer attitudes.
- Figures have been given an even weighting for each country to produce an "average" value.

RSA

ASSESSING DATA USE ACROSS THE GENERATIONS

Respondents were surveyed across several age brackets:

- Ages 18–24 (Gen Z)
- Ages 25–34 (younger Millennials)
- Ages 35–44 (older Millennials)
- Ages 45–54 (Gen X)
- Ages 55 and above (Boomers)

PERSONAL INFORMATION TYPES CONSUMERS CONSIDER PROTECTING

Consumer attitudes vary on personal information they view as private. For the purpose of this report, we are defining personal information as:

- Financial/banking data
- Security information
- Identity papers
- Medical records
- Contact information
- Biometrics
- Genetic data
- Browsing data
- Location data
- Political party affiliation

KEY INSIGHT #1
WHEN IT COMES TO DATA, CONTEXT MATTERS

While consumers recognize that they create and share vast amounts of digital data, they view different types of data differently. Because of this, not all personal information is created or protected equally.

THE TOP 5 TYPES OF PERSONAL INFORMATION CONSUMERS CARE ABOUT

We asked survey respondents, “Overall, which, if any, of the following types of personal information/data do you generally feel protective of?” The answer was: Any data that could be used to steal their identities or commit fraud. Here’s a short list of the data types consumers fear losing control over.

78%
FINANCIAL/ BANKING DATA

75%
SECURITY INFORMATION

70%
IDENTITY INFORMATION

61%
MEDICAL INFORMATION

57%
CONTACT INFORMATION

RSA

Boomers in all markets surveyed care more about these top five pieces of personal information than the other age groups, as the general comfort around data use increases in younger age groups. However, Gen Z's expressed greater concern around their digital footprint (location, photos, and videos) compared to the other data types, bringing their concerns more in line with the older demographics.

PLEASE SAFEGUARD MY RECYCLED PASSWORD

According to another survey, despite user sensitivity around password loss, up to 73% of users reuse the same passwords across their online accounts, increasing the risk of password theft and credential misuse.

Consumers' desire to protect these types of personal information is understandable, given that this data can be used to commit identity theft and worse. With repeated data exposures, cybercriminals find it easier than ever to construct digital identities, typically to commit financial fraud, but also to impersonate victims. In recent years, cybercriminals have taken over children's identities since they lack credit histories—committing financial fraud that often takes years to detect.

In addition, hacking techniques, such as credential stuffing, automate attacks using stolen credentials, gaining faster access to a network through one or multiple accounts. This technique enables hackers to commit greater data theft before they are identified and boxed out of networks by security teams.

Males and females in all markets surveyed feel similarly about protecting their personal information, with one important exception: Women are more protective than men of photos and video.

WOMEN ASSERT THEIR RIGHT TO DIGITAL PRIVACY

As a result, a company's loss of control of this data is viewed by women as an intense violation of personal privacy. As we've seen in the past, it is the company who is blamed for these incidents, despite consumers creating these risks by responding to spear phishing attacks or using weak passwords. Thus, adopting technologies like multi-factor authentication and user behavioral analytics is particularly important for businesses that store sensitive information.

> ***Women are more protective of photos and videos than men are: 54% to 47%.***

RSA

KEY INSIGHT #2
DATA PRIVACY EXPECTATIONS ARE CULTURAL

The GDPR came into effect on May 25, 2018. France, Germany, and the U.K. all passed data privacy legislation to harmonize with the GDPR and adapt it to their countries' needs. Since then, data privacy complaints have increased in these three countries.

What's interesting is European attitudes toward data privacy are not monolithic. As a case in point, our survey found that the French were less protective of their personal data than their German and U.K. counterparts across almost all categories of data surveyed.

DATA PRIVACY SURPRISE: WHAT CONSUMERS DON'T CARE TO PROTEECT

French and U.S. consumers feel freer about sharing data than their German and U.K. counterparts. Who's concerned?

ONLY
43%
OF FRENCH FEEL PROTECTIVE OF THEIR MEDICAL DATA

ONLY
37%
OF FRENCH AND U.S. FEEL PROTECTIVE OF THEIR BROWSING DATA

ONLY
42%
OF U.S. FEEL PROTECTIVE OF THEIR COMMUNICATIONS (MESSAGES, EMAILS, ETC.)

France was the least concerned nation surveyed, with regard to the privacy of their medical records (however, their concern increased 10% year-over-year).

Germans are generally less comfortable sharing data, and it is possible that the recent passage of the GDPR has propelled national awareness and concern about data sharing to new heights. As the chart below indicates, Germans have become more protective of their data, with the greatest increase seen in their desire to protect location-tracking data.

DATA PRIVACY IS A GROWING CONCERN REGIONALLY

RSA

GERMANS ARE FIERCELY PROTECTIVE OF DATA PRIVACY

Here's how German attitudes about data privacy changed within months of the GDPR's implementation:

	2018	vs. 2017
FEEL PROTECTIVE OF MEDICAL DATA:	70%	63%
FEEL PROTECTIVE OF COMMUNICATIONS:	62%	52%
FEEL PROTECTIVE OF LOCATION DATA:	42%	29%

Germans are also increasingly protective of their children's privacy, banning the sale of IoT toys and smart watches which can be used to monitor and track children's behavior.

CONSUMERS ARE MORE CONCERNED ABOUT IDENTITY THEFT THAN EVER

When it comes to stolen data, consumers worldwide are worried about identity theft resulting in financial loss. All respondents expressed concern about monetary loss—the U.K. especially so.

> *U.K. respondents were the most concerned about identity theft resulting in financial loss. Some 78% were concerned versus an average of 72% of all countries surveyed*.

Blackmail is also a worry, but not for all. Gen Z is disproportionately concerned (with 42% worried), compared to older generations. This is likely because Gen Z is the most digitally wired of all generations, using social networking and messaging compulsively and consuming online content in bite-sized chunks throughout the day. As such, Gen Z has the largest digital footprint to protect.

Beginning with younger Millennials, blackmail worries fade. Just 35% of younger and older Millennials, 32% of Gen X, and 31% of Boomers are concerned.

This is likely because older generations are more hesitant to share personal information and thus post less information that would be blackmail-worthy. In addition, Gen Xers and Boomers who are preparing for—or entering—retirement could be less concerned with professional risk than their younger counterparts.

RSA

Gen Z is more worried about blackmail than other generations. Some 42% in 2018 feared blackmail. On average, only 34% of all respondents were concerned.

THE BLAME GAME: POINTING FINGERS AFTER A BREACH

In the aftermath of a data breach, it's easy to point fingers: at a CEO for a culture of noncompliance, at a CMO for aggressive marketing, at a CIO for not addressing vulnerabilities—or at the hackers themselves.

U.K. and U.S. respondents tend to blame companies instead of hackers, while French and Germans disagree. This may be due to the recent high-profile breaches in the U.K. and U.S., fresh in the memory of our respondents.

What's clear, though, is consumers do not blame themselves. Most feel they would not get in trouble if they lost confidential data on the job. Similarly, when companies get hacked due to employees' poor username and password practices, companies are blamed. Often, these hacks can be traced to third-party and social media sites, where employees have reused usernames and passwords, effectively opening the door for hackers at their places of business.

To date, data breaches in Germany and France have been smaller scale, and both countries have tough new legislation aligned with the GDPR. For these reasons, consumers in these countries may be more willing to blame hackers, rather than companies.

AFTER THE HACK: WHO'S TO BLAME

When their data is hacked, consumers usually say companies are to blame. In answer to the question, "If a company loses my personal data/information I feel inclined to blame them above anyone else, even the hacker":

U.S. RESPONDENTS AGREE

64%

U.K. RESPONDENTS AGREE

72%

FRENCH ARE ON THE FENCE WITH HALF AGREEING

50%

FEWER GERMANS AGREE

41%

RSA

It's you, not me: Most respondents are not concerned about getting into trouble at work for losing confidential data. Here's who's concerned:

22%  FRENCH

16%  GERMANS

15%  U.K.

8%  U.S.

Companies bear the responsibility for educating employees: Information security training and risk awareness campaigns can help build a risk culture. Generally, employees are not held responsible for information risk incidents across all geographies, except in cases of extreme negligence or policy-violating behavior. European labor laws are generally protective of employees' rights, so it makes sense that respondents in these geographies are not concerned about being dismissed. What is surprising is that employees the U.S., who can be dismissed at will, don't fear repercussions from losing company data.

KEY INSIGHT #3
CONSUMERS ARE AT ODDS WITH BUSINESSES ON PERSONALIZATION

Over the past 20 years of digital transformation, consumers and companies have made a pact: Many consumers agreed to share data in return for free or discounted goods, and companies agreed to use data to personalize experiences and innovate their products. Personalization is a key part of consumers' digital lives. They browse online retailers, using "recommended for you" or "people who purchased this also bought" suggestions to filter and make purchase decisions. They collaborate with streaming platforms and news site aggregators to filter content and enjoy newsfeed stacking across social networks. And the list goes on.

But now consumers' view—or at least their understanding—of that shared benefit has changed. Due to constant media coverage, users are well-aware that technology's tracking of their behavior has been more pervasive than they assumed, and that their personal data has been shared with third (and sometimes fourth) parties in ways that feel violating. So it's no surprise that individuals are increasingly cynical about companies' data protection claims, promises, and policies.

Companies need to find a bridge across this to connect with consumers that meet both shared and felt needs, while respecting privacy. That challenge will become even more difficult as the Internet of Things (IoT) becomes prevalent in the workplace and enables smart homes, connected cars, and smart cities. In the near future, IoT, device use, and artificial intelligence will grow to the point that technology knows consumers even better than they know themselves.

Ethical data use is when a company only takes the personal information needed to deliver the service customers are receiving and nothing more—52% of all survey respondents agree.

Does providing more data lead to better products and services?

	2018	2017
SURVEY RESPONDENTS AGREED	29%	31%

IOT IS EVERYWHERE—AND THAT'S PARTLY A PROBLEM

60% of all consumers surveyed on average find wearables creepy. However, early adopters love them for their ability to help optimize diet, fitness, productivity, and other goals.

When it comes to the ethical use of data, there are notable regional differences. Respondents in the U.S. are more comfortable sharing data, so it's no surprise they feel more optimistic about how companies use their data.

THE U.S. IS THE MOST ACCEPTING OF THE ETHICAL USE OF DATA

CAN WE AGREE ON ETHICAL DATA USE?

When asked if there are ethical ways in which a company can use personal information, 48% of respondents say yes. Gen Z and younger Millennials lead the way with 54% of both groups believing data can be ethically used by companies.

45% FRENCH | 43% GERMANS | 48% U.K. | 60% U.S.

From these statistics, it's clear that companies face an uphill battle when it comes to convincing consumers that data sharing benefits them. There are specific parameters to what consumers consider ethical about data sharing: It must provide convenience or help protect their identities. For example, modern fraud engines now use location data to authenticate travelers and their transactions as they move from country to country.

RSA

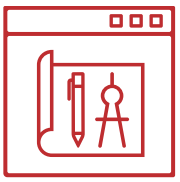
The same fraud engine would pick up anomalies, such as atypical transactions in nonrelevant countries, and deny these transactions. However, it needs permission to access consumers' location data to provide this convenience.

THE ETHICAL USE OF DATA ACCORDING TO CONSUMERS

What do consumers want? Our survey delved deep into specific use cases to understand how consumer expectations are changing.

We asked a series of questions to probe respondents' attitudes about digital marketing and content personalization, which are used pervasively by companies. Are consumer attitudes toward personalization a case of "Do as I say, not as I act?" The evidence would seem to suggest yes.

HOW WESTERN CONSUMERS FEEL ABOUT DIGITAL PERSONALIZATION



Consumers are pushing back on personalization, despite enjoying its benefits on a daily basis. Across all geographies surveyed, they increasingly perceive personalization as intrusive and unethical.

- *Tailored newsfeeds*: A mere 24% of total respondents feel it's ethical (31% in the U.S.), compared to 59% who feel it's unethical.
- *Recommendations based on purchase/browsing history*: 25% of all surveyed feel it's ethical (37% in the U.S.), compared to 59% who find it unethical (67% in the U.K.).
- *Using a "like" history to recommend content*: 28% feel it is ethical versus (38% in the U.S.), compared to 55% who feel it is unethical.
    - Sentiment is stronger abroad: 61% in U.K. and 60% in France find it unethical. But there's an important caveat—averaged across all countries surveyed, more Gen Zs viewed this use as ethical, with 41% viewing it as ethical versus 38% who find it unethical.
- *Tracking online activity to tailor advertisements*: 17% of those surveyed viewed it as ethical, and 68% find it unethical.
- *Tracking devices and locations to identify unauthorized access*: Some 36% overall feel this is ethical, versus 46% in the U.S.
    - Of note: in France, only 27% view it as ethical, with 58% viewing it as unethical.
- *Tracking shopping habits and locations to monitor fraud*: 45% of respondents view it as ethical. By region: 56% of U.S. respondents view it as ethical, while only 28% in Germany and 34% in France do. Averaged across all countries, just 39% of respondents view it as unethical, versus 52% in France.
- *Commuting habits*: Some 42% of those surveyed view this type of tracking as ethical, notably that's 47% in the U.S. and 50% in the U.K. Only 40% overall view it as unethical, but Germany and France were higher, with 42% of Germans and 48% of French finding it unethical.

GEN Z LIKES THEIR "LIKES"

When it comes to individual findings, it's not surprising that Gen Z finds using "likes" to tailor content more ethical than any other age group surveyed. Many Gen Zs are avid users of social sites, such as Instagram, Snapchat, and Twitter—all of which use "likes" to shape the experience. In fact, some Gen Zers operate multiple accounts, such as public and private Instagram accounts, to restrict some content sharing to select groups of friends.

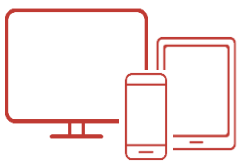
EVERYONE DISLIKES ADVERTISING

Nobody likes advertising (a finding that aligns with last year's analysis), as it interrupts digital browsing and content consumption. Consequently, many consumers feel misled when they read ads masquerading as articles. Our survey results reflect consumers' view that targeted advertising is an unethical use of data.

DEVICE TRACKING IS CONTROVERSIAL

Device tracking is one of the topics that best underscores the disconnect between consumer expectations and the reality of data use—and opens companies up to potential digital risk if their policies aren't communicated in a transparent way. While consumers appreciate the ability to protect and locate their devices, they're well aware that device tracking can be used to create continual situational awareness about them. In the U.S., the top telecommunications companies have been selling mobile device location data, which can be used by bounty hunters to track consumers' real-time location.

Device-tracking information is used legitimately by advertisers, financial and medical service providers, and public safety officials. Device tracking can authenticate users, enable real-time marketing offers and transactions, prevent fraud, and assist in medical and police service delivery such as emergency response. While device tracking is part of consumers' daily lives, it is conceivable that its negative applications have gained additional air time at the expense of its benefits.



The French felt especially strongly, with 58% believing that device tracking was unethical, noticeably higher than other regional counterparts. It's possible that the late-2018 clashes of the "gilet jaunes" ("yellow vests") with police in France were on French respondents' minds as we surveyed them about their data-tracking perspectives.

RSA

ANTI-FRAUD BEHAVIOR AND LOCATION TRACKING A WIN

While consumers do not want their behavior or devices to be tracked, they are willing to make an exception when it comes to anti-fraud protection. Shopping and location tracking to prevent fraud is ethical to most U.S. consumers. Since most consumers are afraid of digital financial theft or unauthorized purchases, this is understandable.

Except for fraud prevention, the disconnect between consumers' data preferences and today's digital reality represents a significant amount of digital risk—potentially exposing companies to backlash, boycotts, or divestments.

CONCLUSION—ADDRESSING THE DIGITAL DISCONNECT PROACTIVELY

Companies should be aware that having and communicating an ethical use of data policy will become the new normal. While consumers want to understand how their data is being collected, stored, managed, and shared, it's clear they don't have a full understanding today. After a year of several high-profile data breaches and negative media coverage about company practices, consumers have stronger opinions about the ethical use of data. It's likely, too, that the GDPR has raised the stakes for all companies when communicating about data collection, usage, and sharing.

Consequently, many now feel uncomfortable with companies' collection processes and are pulling back from data sharing. This year's survey revealed:

75% Of respondents now limit the amount of personal information they share online.

57% More U.K. respondents (57% versus 43% on average across the countries we surveyed) have noticed an increase in data-consent pop-ups compared to a year ago.

29% U.S. respondents are significantly more likely than Europeans to say they've felt pressure from their employer to provide personal health data to receive a health benefit discount or other monetary incentive. (Some 29% in the U.S. cited pressure versus 20% overall.)

RSA

As data breaches soar, we wanted to understand how consumers are being affected. We asked, “Has your personal information been compromised online by a data breach in the last five years?

HAVE YOU BEEN THE VICTIM OF A DATA BREACH?

36%
OF ALL RESPONDENTS AGREED

45%
OF U.S. RESPONDENTS AGREED

39%
OF ALL RESPONDENTS DIDN’T KNOW

21%
OF ALL RESPONDENTS DISAGREED

With billions of data records breached to date, we estimate the real number of people impacted by breaches is likely much higher, exposing the brands who may be yet unaware of their breaches to more digital risk.

WHAT OUR FINDINGS MEAN FOR BUSINESS

As our survey findings indicate, companies can lead on—and learn from—the important topic of the ethical use of data. Setting policies is ongoing, since consumer expectations and behavior are constantly changing.

However, companies should be wary of aggressively collecting unnecessary data, using it in intrusive ways, or sharing it with partners in ways consumers would not approve. Companies can use their stance on how they use data ethically to build customer trust and loyalty to their brand, much the way outdoor retailers have with environmental sustainability to communicate values and build brand.

All of this—excessive data collection, invasive personalization, unapproved sharing, faulty controls, and breach notification delays—can and does hurt companies. Aggressive data collection policies can lead to a media and public backlash, with consumers deleting apps or decreasing usage and data sharing. Meanwhile, faulty controls and data breaches create risk to companies’ reputations, spurring negative media coverage, high-profile boycotts (such as technology journalist Walt Mossberg’s decision to quit Facebook and Messenger), regulatory censure, fines, and lawsuits.

The situation creates an inescapable ethical data conundrum. Consumers may feel coerced and refuse personalized services. Only 22% agree that they would willingly hand over data to improve experiences, and some 41% disagreed. The reality is consumers use personalized services all the time, and numerous studies have demonstrated that consumers are more likely to buy and spend more when the experience is personalized.

Also, consider the fact that many companies delay announcing data breaches (something that is no longer possible as mandated by the GDPR), as they assess the scope of the data loss and formulate their media and consumer responses. While only a third of all respondents believe their personal information has been compromised in a data breach, the billions of records breached last year suggest the number is likely much higher.

RSA

Half of all consumers surveyed (58% of U.S. respondents) said they'd consider divesting from companies that show they have no regard for protecting customer data.

Nearly every business on the planet touches consumer data, yet digital leaders and data aggregators are held to the highest standards in terms of protecting personal information. As our survey results indicate, most consumers blame companies over hackers in the event of a data breach, and employees don't hold themselves responsible if they lose confidential information on the job.

Companies must embrace their combined responsibilities of using customer data in an ethical way and securing it properly. Proper data hygiene and security need to complement each other, and companies must demonstrate a strong commitment to both to earn and keep consumers' trust.

Companies that define and communicate ethical data practices to their customers will create stronger relationships with them—by clearly articulating and developing experiences that provide an authentically mutual benefit.

How will your company lead on—and learn from—ethical data use in 2019?

Join the conversation online @RSAsecurity.

Contact RSA for help managing digital risk: rsaglobalcomms@rsa.com

RSA