

FEI Professional Development Session

Presented by RSM

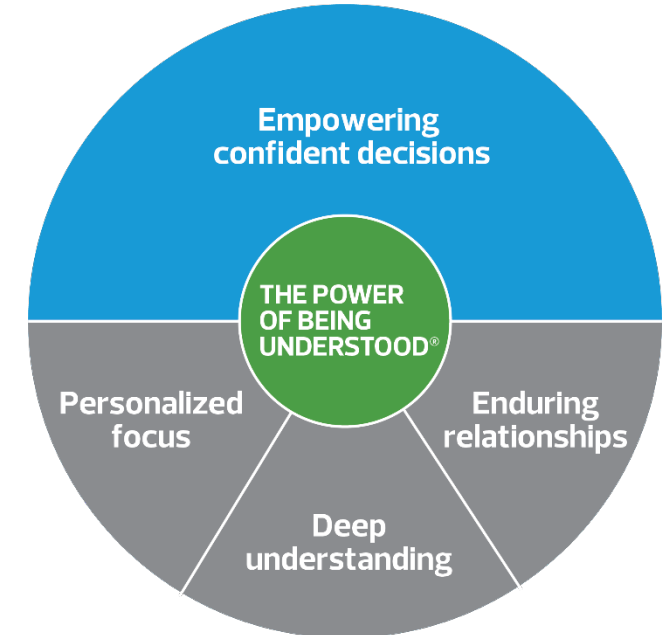
7/24/2019



RSM overview

First-choice advisor to middle market

- Leading provider of audit, tax and consulting services focused on the middle market
- Fifth largest audit, tax and consulting firm in the United States
 - Over \$2.4 billion in revenue
 - Nearly 11,000 employees in 87 cities and four locations in Canada
- U.S. member of the sixth largest independent network of audit, tax and consulting firms globally*
 - Presence in more than 116 countries
 - More than 41,000 people in over 750 offices
 - More than \$5 billion (U.S.) in worldwide revenues



* RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/about-us for more information regarding RSM US LLP and RSM International.

Your presentation team



Chris Hannifin

Manager, Technology Consulting

chris.hannifin@rsmus.com

+1 210 253 1569

Chris provides cybersecurity consulting services to a wide variety of industries, focusing on reducing cybersecurity risks. He has more than 10 years of experience within the cybersecurity industry, helping organizations identify, prioritize and manage cybersecurity risks.

Qualifications

- Manager - Security, Privacy and Risk Consulting
- San Antonio Leader for SPRC
- Located in San Antonio, TXCurrent USAFR Cyber Threat Intelligence Officer (19 years)
- MBA, GSEC, CISSP



Rob McGee

Manager, Management Consulting

robert.mcgee@rsmus.com

+1 210 885 2468

Rob is an innovative human resources and total rewards practitioner with over 15 years of design and leadership experience. His experience includes developing and implementing value added human resources and compensation programs, HR technology solutions and diversity and inclusion strategies, resulting in improved workforce effectiveness and operational excellence.

Qualifications

- Certified Compensation Professional (CCP): WorldatWork
- Certified Professional in Human Resources (PHR): Human Resource Certification Institute
- Certified Change Management Practitioner: Prosci Change Management Institute

RSM US MIDDLE MARKET BUSINESS INDEX CYBERSECURITY

SPECIAL REPORT



Q1 2019

Agenda

- Top 8 Key Takeaways
- Middle market awareness
- Growing confidence conflicts with rising cyber concerns
- Information data security
- Cyber insurance
- Ransomware attacks
- Business account takeover threats
- Privacy protections compliance
- Migration to the cloud
- NACD roundtable discussions

About Chris Hannifin

- Manager - Security, Privacy and Risk Consulting
- San Antonio Leader for SPRC
- Located in San Antonio, TX
- Current USAFR Cyber Threat Intelligence Officer (19 years)
- MBA, GSEC, CISSP



MMBI Cybersecurity Special Report

- RSM US LLP (RSM) and the U.S. Chamber of Commerce have joined forces to present the RSM US Middle Market Business Index (MMBI)—a first-of-its-kind middle market economic index developed by RSM in collaboration with Moody's Analytics.
- Data for the MMBI is gathered through quarterly surveys of the RSM US Middle Market Leadership Council, a panel of 700 middle market executives managed by the Harris Poll.
- Smaller middle market companies (\$10 million - \$50 million) in revenue.
- Larger middle market companies (\$50 million - \$1 billion) in revenue.

In Collaboration With:



U.S. CHAMBER OF COMMERCE

MOODY'S
ANALYTICS

the harris poll®

NetDiligence®

8 key takeaways from this year's report

1. Only 40% of executives report familiarity with GDPR or other privacy regulations.
 - Smaller organizations are not as familiar with GDPR (27%).
 - Larger organizations are more familiar with GDPR (56%).
 - California Consumer Protection Act is scheduled to take effect in 2020.
 - First complaint filed against Google, led to a \$57 million fine. The penalty was assessed based on how Google handled it's data {not a breach of data}.
2. The Shift: from protecting data, to “should we even have the data.”

8 key takeaways from this year's report

3. **93%** of middle market executives claim that they are confident in their organization's measures to safeguard sensitive customer data or their own environments for the second consecutive year.
4. Testing the security program can determine the overall effectiveness, reduce overconfidence bias.
 - Of those infected with ransomware **50%** indicated missing or ineffective security and operational controls.
 - **79%** of middle market companies provide security awareness training. Opportunity to discuss testing their program with social engineering, phishing attack coupled with vishing.



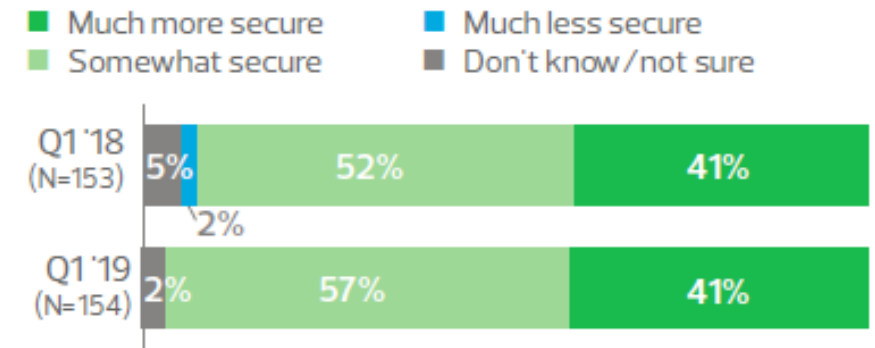
©2013 Behavior Gap

Overconfidence effect

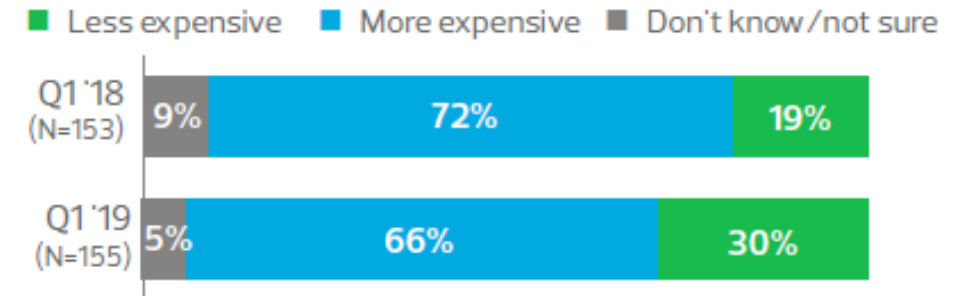
8 key takeaways from this year's report

5. 30% of smaller middle market companies are familiar with their cyber liability insurance coverage, a drop of 21% from last year.
6. 38% of respondents moved data to the cloud as a result of security concerns in the last 12 months.
 - Transferring the (data) risk to third party service providers unfortunately does not reduce reputational risk.

Actual impact of moving data to the cloud due to security concerns



Cost impact of maintaining data in the cloud due to security concerns



8 key takeaways from this year's report

7. 38% of larger middle market companies are evaluating blockchain technology to ensure security or privacy of data.
8. Cost savings can lead to less security (budgetary constraints)
 - Logging and monitoring solutions can be expensive given the amount of data being stored. Some companies have chosen to only store 30 days of logs, however time to identify an incident is on average over 180 days.
 - This is a good example of having a solid control/framework in place, but the effectiveness is only good for 17% of the time.

THE MIDDLE MARKET REALIZES THE

CYBER THREAT

BUT UNCERTAINTY REMAINS

Cyber threat: by the numbers

- 15% of middle market C-suite executives said their companies experienced a data breach in the last year, up from 13% in 2018 and a significant jump from 5% just four years ago.
- Ransomware has altered the term “data breach,” which historically was related to stolen data. Ransomware doesn’t care about the data; it’s about immobilizing a company’s operations.
- Over half of middle market executives surveyed indicated it is likely that unauthorized users will attempt to access their organization’s data or systems in 2019.
- More than half of midsize companies report carrying cyber insurance. However, only 43% of executives claim familiarity with policy details.
- Only 40% of executives report familiarity with GDPR or other privacy regulations.

Cyber threat: in summary

- The Shift—from protecting data, to “should we even have the data?”
 - The European Union’s General Data Privacy Regulation (GDPR)
 - California Consumer Protection Act (CCPA)
 - Congressional hearings around regulation at the federal level
- The 2018 NetDiligence Cyber Claims Study, sponsored by RSM, showed ransomware has become the most common form of cyber incident.
- Evolution of hacking used to steal data, now the focus is on extracting payment directly from the victim.

While major cyber incidents and data breaches at large corporations continue to capture global headlines, middle market companies are starting to recognize that they are often the prime target for cybercriminals.

Polling question

Has your organization been a victim of ransomware within the last 18 months?

Growing confidence
CONFLICTS
with rising cyber concerns



Growing confidence amid rising cyber concerns

- For the second year in a row, RSM's survey found that **93%** of middle market executives claim that they are confident in their organization's measures to safeguard sensitive customer data or their own.
- While the number of reported breaches has tripled over the last five years, the level of confidence expressed by executives has actually grown by **18%**.
- Increased spending on information security is one potential reason for a high level of confidence. A research study from Gartner projected that worldwide spending on information security products and services would grow **12.4%** in 2018 and an additional **8.7%** in 2019.



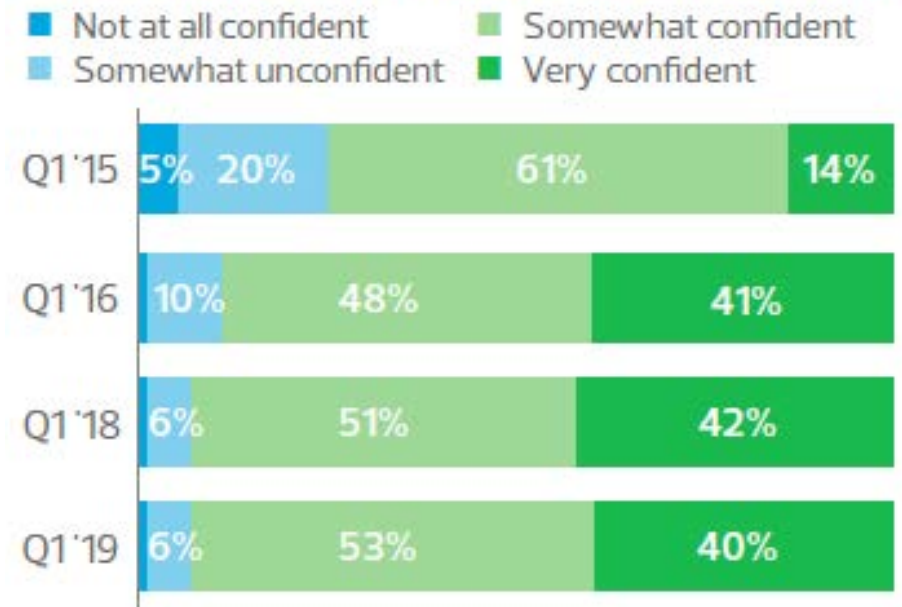
© 2013 Behavior Gap

overconfidence effect

Side step overconfidence

- Gartner estimates that nearly 50 percent of U.S. organizations will adopt the NIST Cybersecurity Framework (CSF) by 2020.
- Testing the effectiveness of the security program helps reduce overconfidence bias.
- Areas that may reduce the effectiveness of testing:
 - Limiting scope of the testing
 - Information filtering or over-summarizing the findings
 - Restrictions on the testing methodology or testing procedures

Confidence in current measures to safeguard data



Information filtering

Despite the increasing threats and attack vectors middle market confidence level in safeguarding their data at 93% overall confidence level.

Ace, here is the latest penetration test report, not too bad, we are addressing most of these already.

Hey Joe, here is the latest penetration test report, Ken and I think we can mitigate most of the major vulnerabilities!

Report





CIO



Director of IT

Report






Cybersecurity



Board of Directors

Report



Hmm, I wonder if we are getting all the information?

Hey Bob, here is the latest penetration test report, we have some major vulnerabilities, same ones we identified last time.

Bob, are you guys doing another penetration test this year? I was hoping to see the results from the last one we performed.



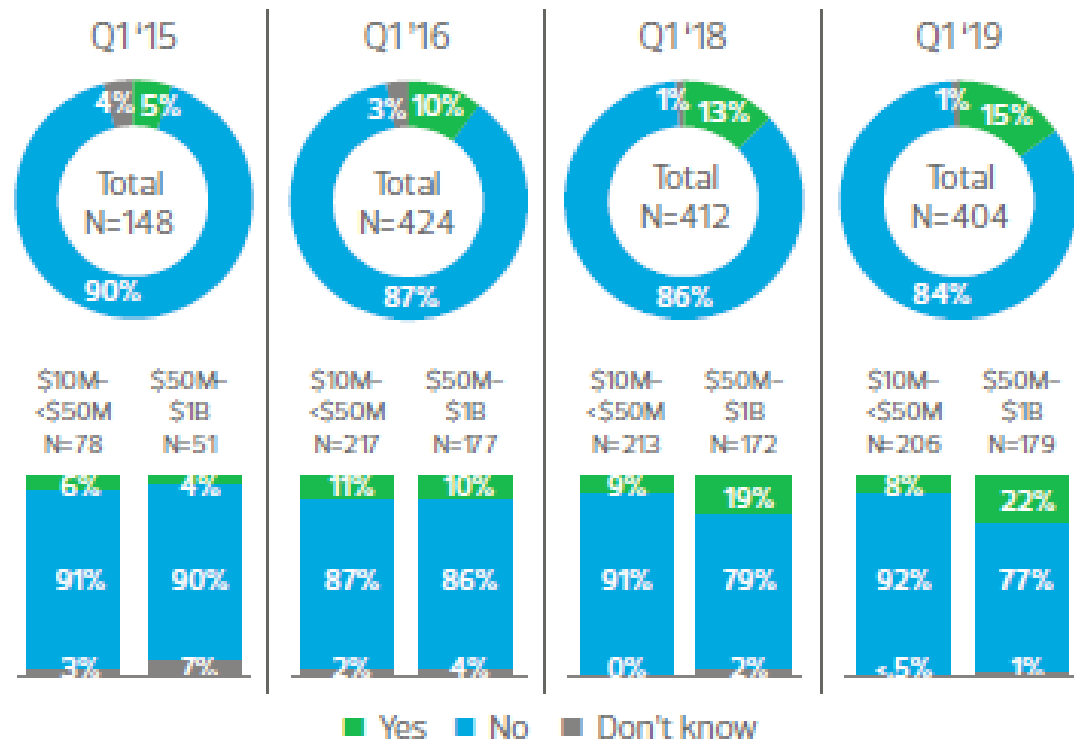
Internal Audit



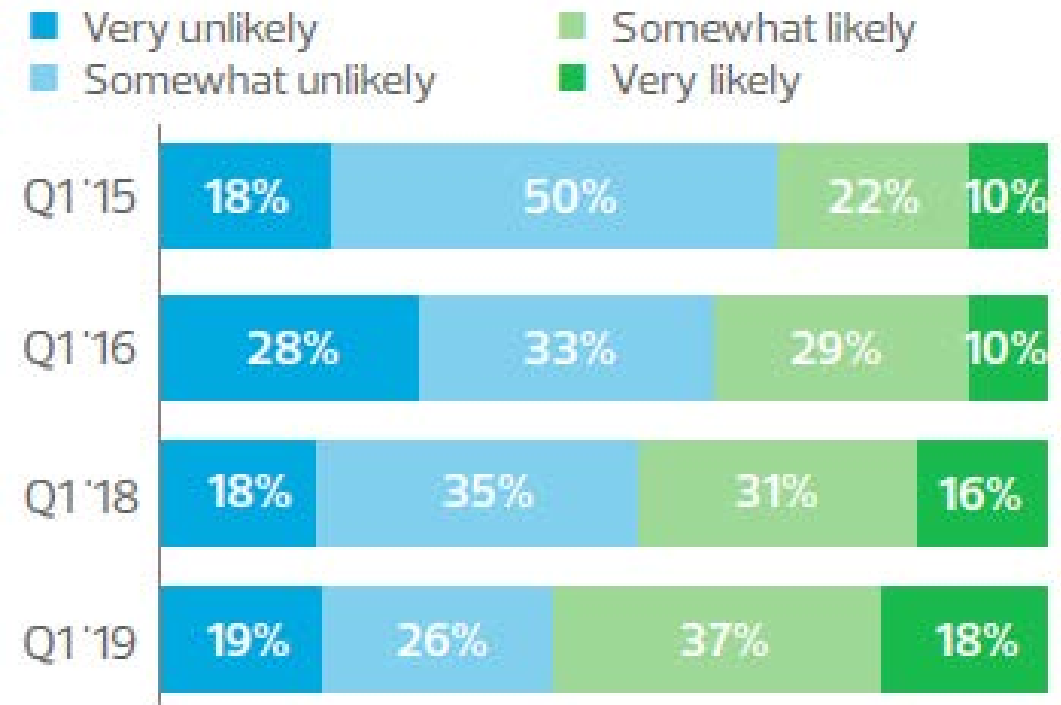
INFORMATION AND **DATA SECURITY**

Information and data security: by the numbers

Companies experiencing data breaches in last 12 months

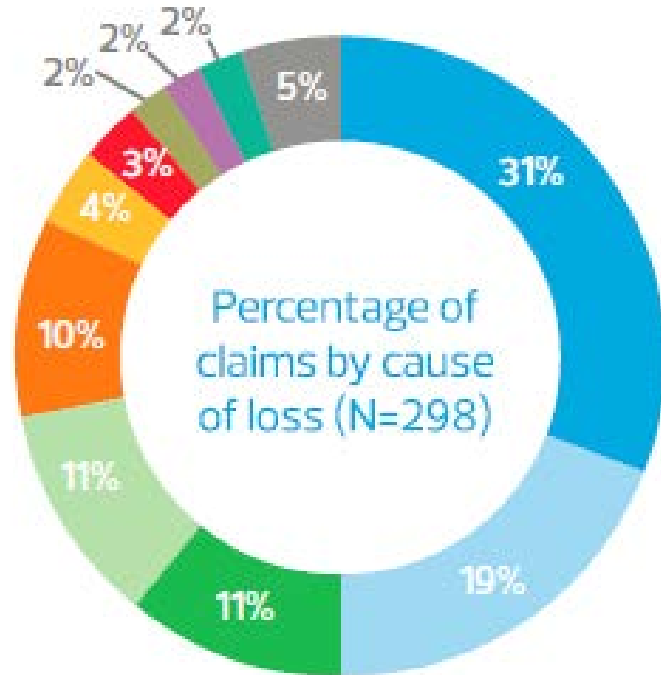


Likelihood unauthorized users will attempt to access data/ systems



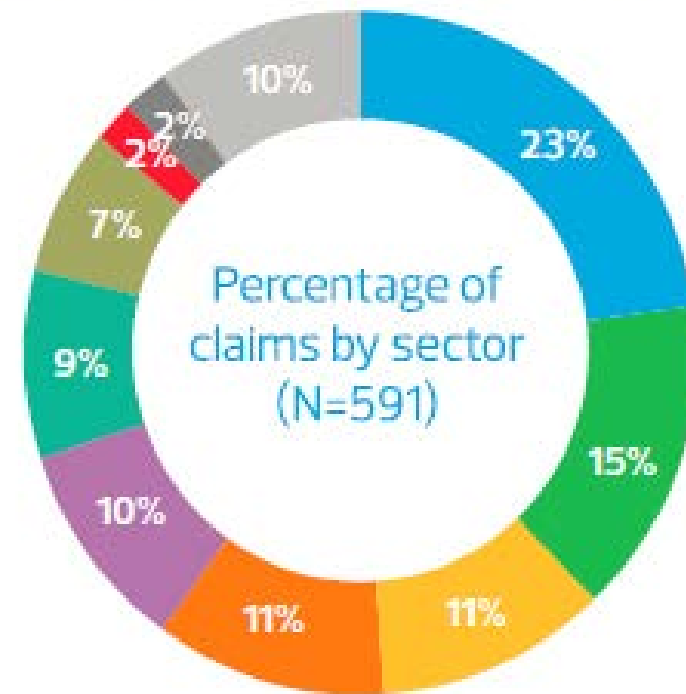
Information and data security: by the numbers

- Ransomware
- Hacker
- Malware/virus
- Email compromise
- Phishing
- Rogue employee
- Legal action
- Staff mistake
- Lost or stolen laptop/device
- Programming error
- All other causes



Source: 2018 NetDiligence Cyber Claims Report

- Professional services
- Health care
- Financial services
- Retail
- Education
- Manufacturing
- Public entity
- Technology
- Nonprofit
- All other sectors



Source: 2018 NetDiligence Cyber Claims Report

Information and data security: in summary

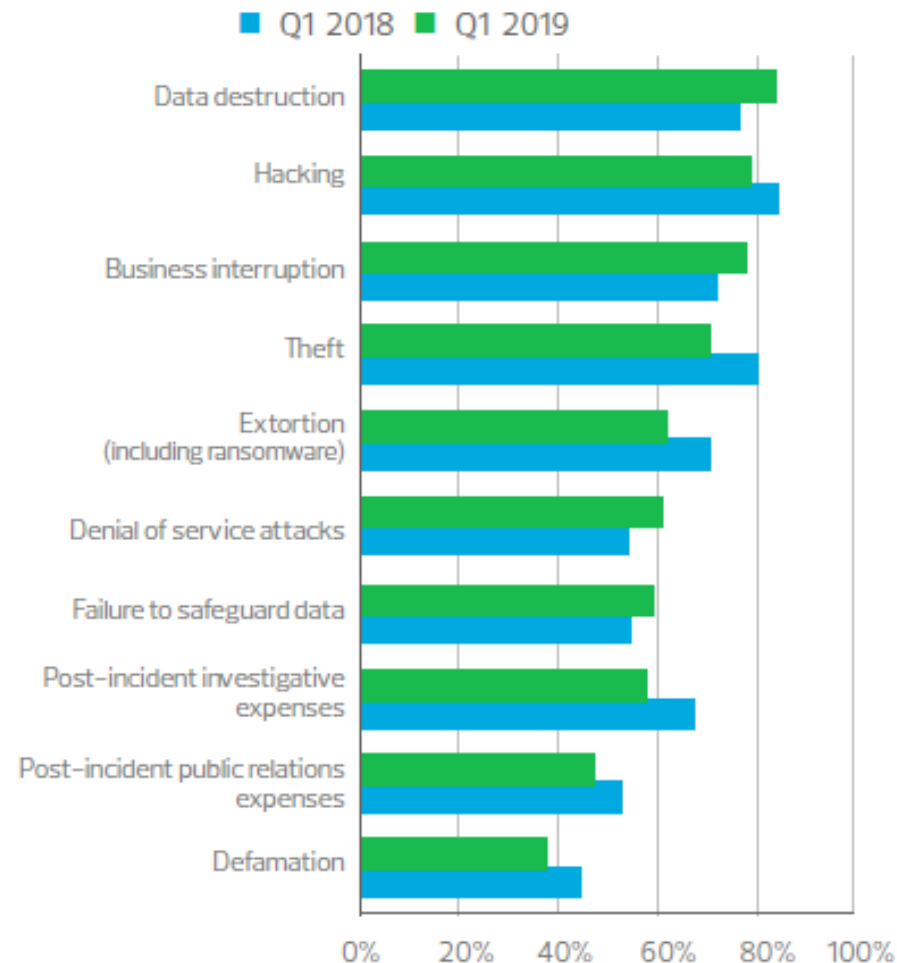
- The NetDiligence 2018 Cyber Claims Study found that
 - 61% of cyber claims were from companies with less than \$50 million in revenue.
 - 21% from companies with revenue of \$50 million to \$300 million in revenue.
 - All told, companies with revenue under \$2 billion accounted for 88% of claims in 2018.
- 55% of middle market executives indicated an attempt to illegally access their data. 23% increase from the survey five years ago.
- According to NetDiligence research the average breach cost submitted for cybersecurity claims in 2017 was \$604,000.
- Average mean time to *identify* a data breach was 190.7 days (over six months)
- Average mean time to *contain* a data breach was 66.2 days (over two months)
- Professional services firms top the list for claims submitted.

CYBER INSURANCE

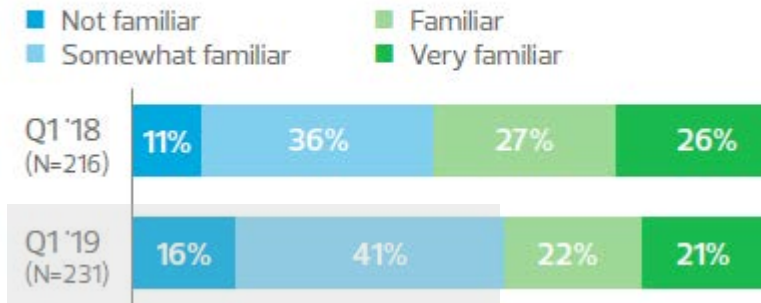


Cyber insurance: by the numbers

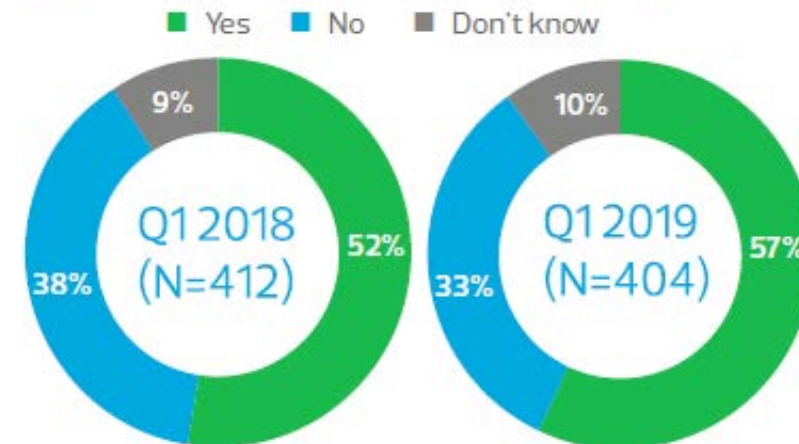
Risks or exposures the cyber insurance policy covers



Familiarity with what organization's cyber insurance policy covers



Organization carries a cyber-insurance policy



Cyber insurance: in summary

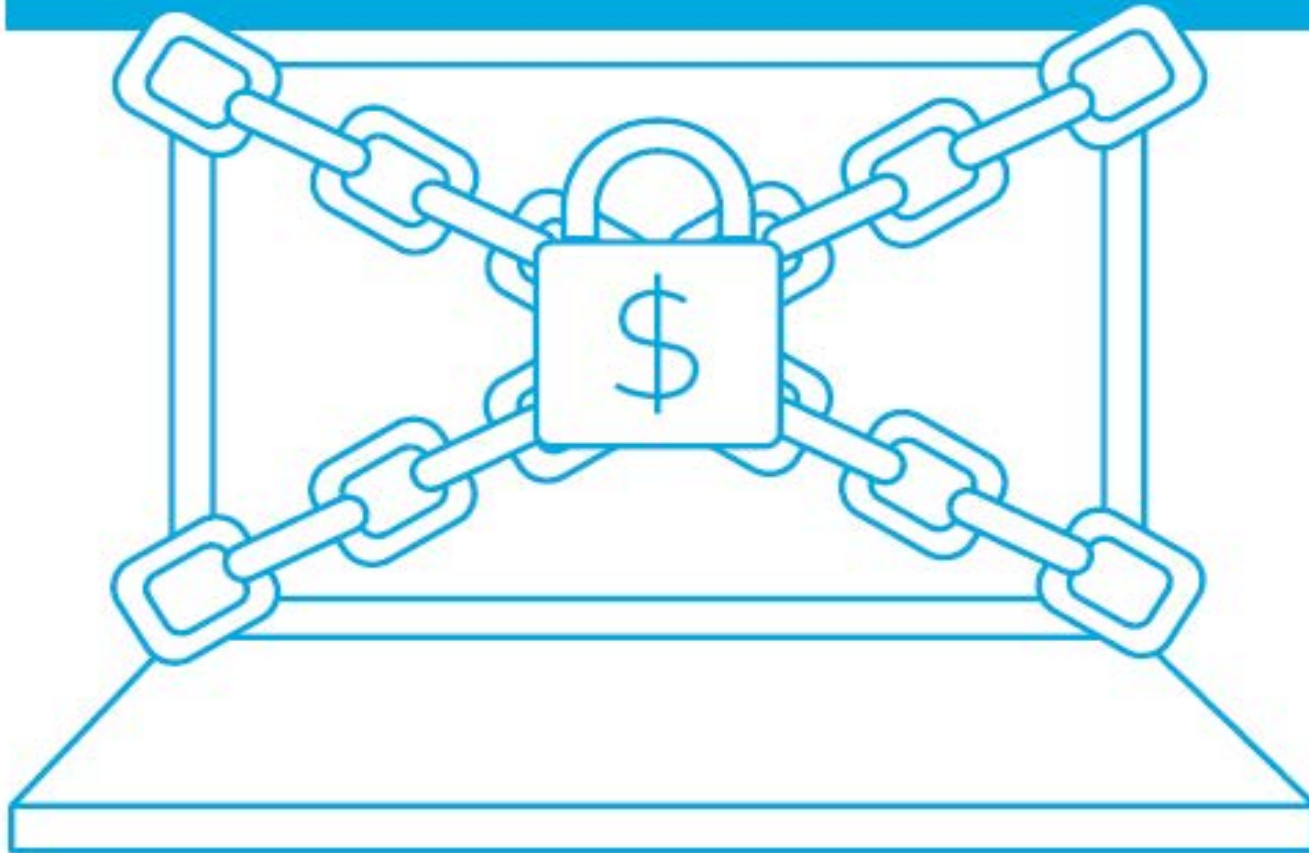
- 57% utilize a cyber insurance policy to protect their company against internet-based risks, up from 52% last year.
- Larger middle market companies are 10% more likely to invest in insurance policies than smaller organizations.
- 30% of smaller middle market companies are familiar with their coverage, a drop of 21% from last year.
- 10% of all mid market businesses do not know if they carry a policy
- Things to consider:
 - An alarming number of decision makers are ignorant of coverage.
 - During an incident, you don't want to waste time trying to figure out if/how you're covered.
 - Does your insurance require you to do things you're not doing? (e.g. penetration tests, IR testing, risk assessment)
 - Ensure your policies cover your cloud providers, as well as different types of attacks (ransomware).

Polling question

Does your organization have a cyber liability policy?

RANSOMWARE

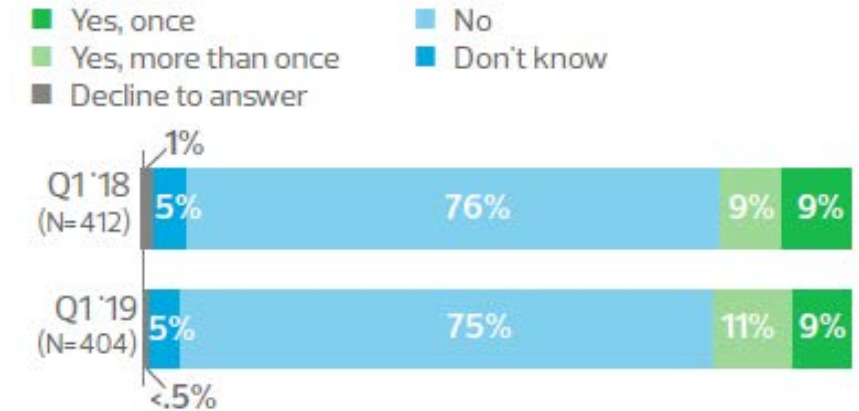
ATTACKS



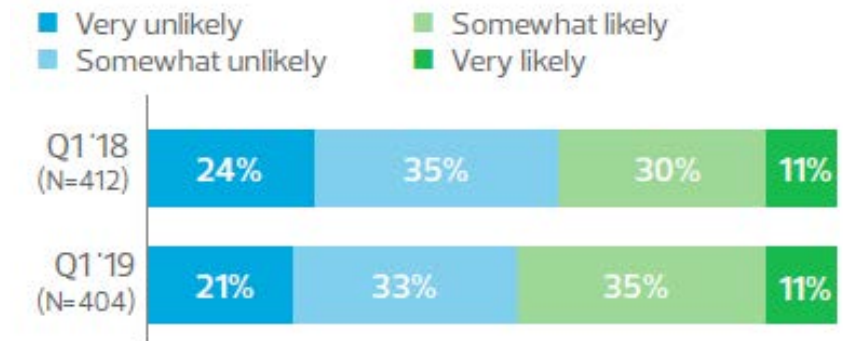
Ransomware: by the numbers

- 20% of companies experienced a ransomware attack within the past twelve months.
- Of those infected with ransomware 50% indicated missing or ineffective security and operational controls.
- Ransomware is the leading cause of cyber insurance claims, but only about 60% of policies cover it.

Experienced a ransomware attack or demand during the last 12 months



Likelihood organization is at risk of ransomware attack in next 12 months



Ransomware: in summary

- Ransomware is about the operations of the company, and holding it hostage. While the data can be important the on-going operations of a company is often more valuable to the attacker.



Quick check: When was the last time you conducted an IR table top exercise?
Would you pay the ransom?

- Containment of a ransomware attack can reduce the overall exposure to an organization. Ensure company assets are restricted to reduce the chances of ransomware spreading.

Polling question

Would you (organization) pay a ransom?



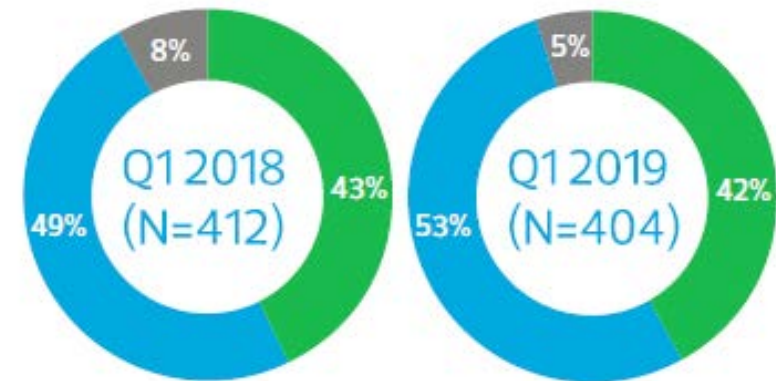
BUSINESS TAKEOVER THREATS

Social engineering: by the numbers

- 42% of executives indicated outside party attempted to manipulate an employee
- 83% of attackers were unsuccessful when employee did not act.
 - 58% secondary controls prevented completion of the attack.
 - 43% had system controls that prevented the attack reaching employees.
- 79% of middle market companies provide *some* security awareness training.

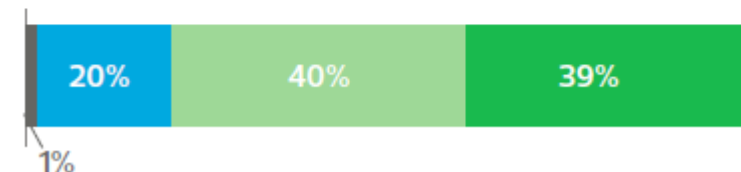
Outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives

■ Yes ■ No ■ Don't know



Organization provides training on how to detect, identify and prevent attempts of unauthorized access

■ Yes, formal training provided to all employees
■ Yes, formal training provided to some/most employees
■ No, formal training not provided to employees
■ Not sure



Social engineering: in summary

- Phishing attacks coupled with vishing (over the phone) are becoming more popular, and the results can be devastating.
- Conducting regular phishing campaigns can be a great way to ensure the effectiveness of your awareness program.
- Tailored awareness programs have a higher retention rate for employees than canned or generic templates.

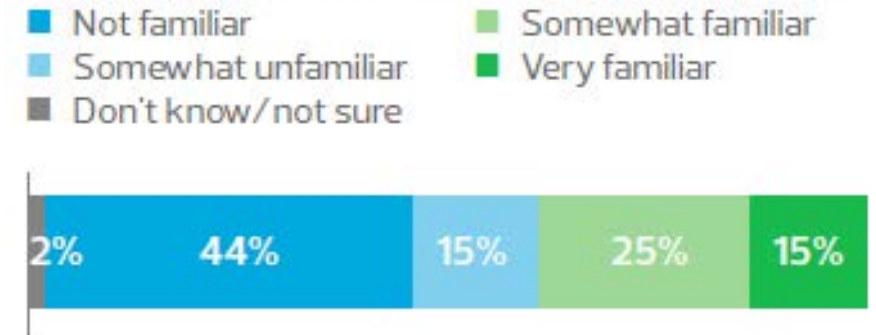


PRIVACY PROTECTIONS COMPLIANCE

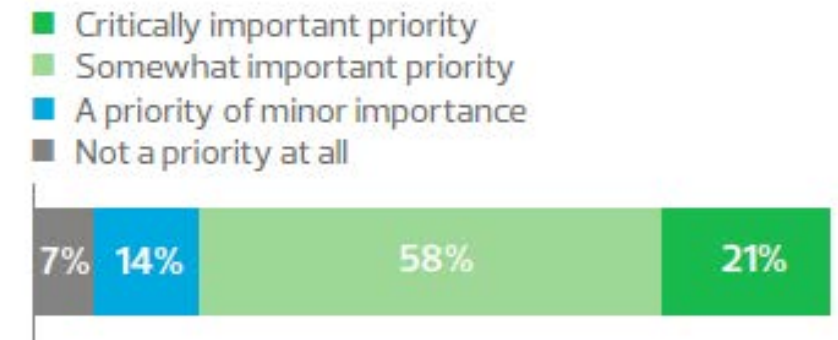
Privacy and compliance: by the numbers

- 40% of middle market organizations indicated that they were familiar with GDPR.
- 79% of companies believe privacy legislation or regulation is a priority.
- First complaint filed against Google, led to a \$57 million fine. The penalty was assessed based on how Google handled its data.

Familiarity with requirements of the GDPR (N=404)



How much of a priority is preparing for emerging privacy legislation or regulation (N=159)



Privacy and compliance: in summary

- Consumers are filing complaints at a rate of 400 per day.
- Privacy is effecting the downstream liability via third party service providers. Size in privacy isn't always a leading indicator—collecting data is.
 - Smaller organization are not as familiar with GDPR (27%)
 - Larger organizations are more familiar with GDPR (56%)
- California Consumer Protection Act is scheduled to take effect in 2020, while Massachusetts and Texas already have certain data privacy protections in place. In addition, Congress has held preliminary hearings over similar legislation at the federal level.

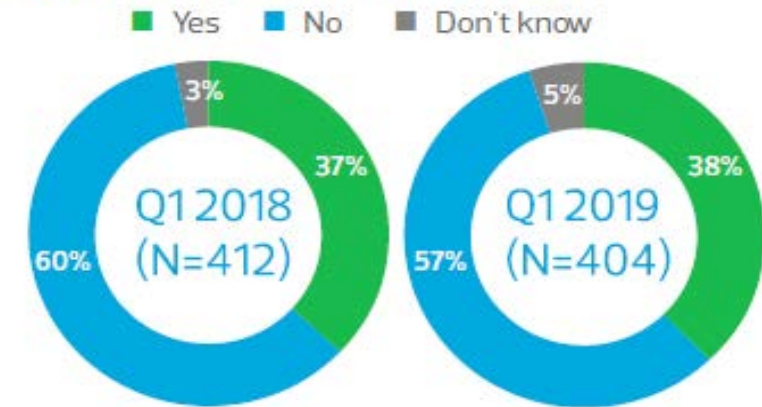
MIGRATION TO THE CLOUD



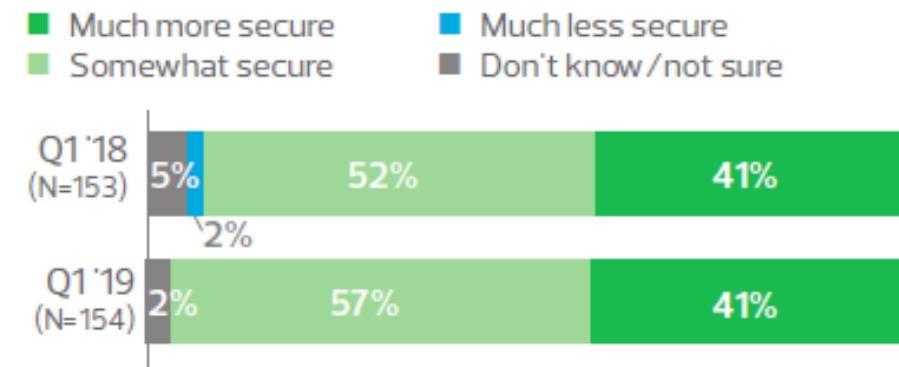
Migration to the cloud: by the numbers

- 38% of respondents moved data to the cloud as a result of security concerns in the last 12 months.
- 66% stated moving to the cloud was more expensive due to security concerns.
- 38% of larger middle market companies are evaluating blockchain to ensure security or privacy of data.

Organization moved or migrated data to the cloud for security concerns during the past year



Actual impact of moving data to the cloud due to security concerns



Migration to the cloud: in summary

- Transferring the risk of cybersecurity to the cloud can be expensive and have hidden risks.
 - Reputational risks are still an ongoing concern.
- Ensure that your cyber insurance covers a breach at a cloud provider.

Polling question

Do you feel that having your data in the cloud is safer?



Security mavericks to middle
market directors:

BECOME A **HARDER TARGET**

The National Association of Corporate Directors, which has a partnership with RSM, recently held a roundtable to discuss cybersecurity risks and challenges.

NACD roundtable discussion points

- Third Party Service Providers
 - Ensure contractual agreements are in place to protect the organization from cyber risks.
- When a breach does occur, working with third party services providers (including cloud providers) can cause a series of unforeseen issues.
 - Include service providers in your annual incident response tabletop exercise.
- Verify that segmentation is in place and is effective at third party service providers.
 - Cost for cloud solutions is decreasing, and the competition is increasing, which may lead to less security controls.
- Boards need to determine their risk appetite and document their security processes.
 - Business process risk assessments can be a great avenue to document the processes that store, process, transmit or access sensitive information.

NACD roundtable discussion points

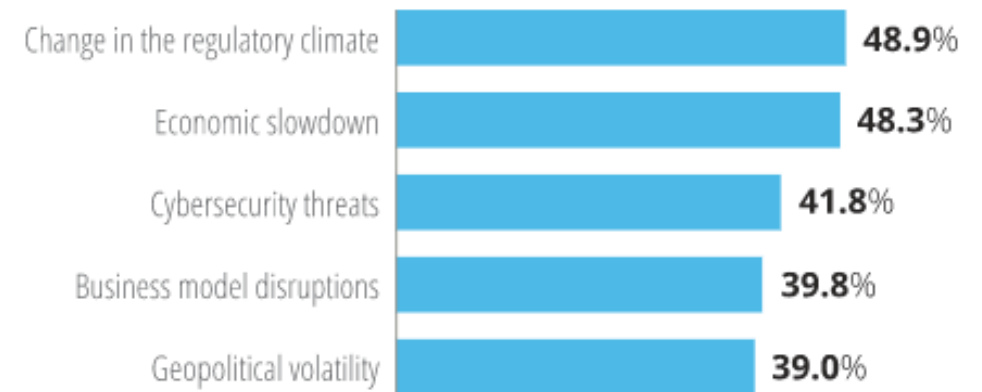
- Cost savings can lead to less security
 - Logging and monitoring solutions can be expensive given the amount of data being stored. Some companies have chosen to only store 30 days of logs, but the average time to identify an incident is over 6 months.
 - This is a good example of having a solid control/framework in place, but the effectiveness is only good for 17% of the time.
- SWOT analysis
 - Smaller organizations have less surface area for attack and fewer people to train in security.
 - The opportunity for smaller organizations to have just enough security so attackers move onto softer targets.

Board involvement

- Increase risk visibility and transparency by articulating cyber risk and allowing the business to make decisions on how to handle cyber risk.
 - Cyber risk based decisions
 - Accept
 - Mitigate
 - Transfer
 - Hold
 - Ignore

What five trends do you foresee having the greatest effect on your company over the next 12 months?

Five trends could be selected by respondents from a list of 14. Bars represent the percentage of respondents selecting a trend. Only the top five trends are shown below.

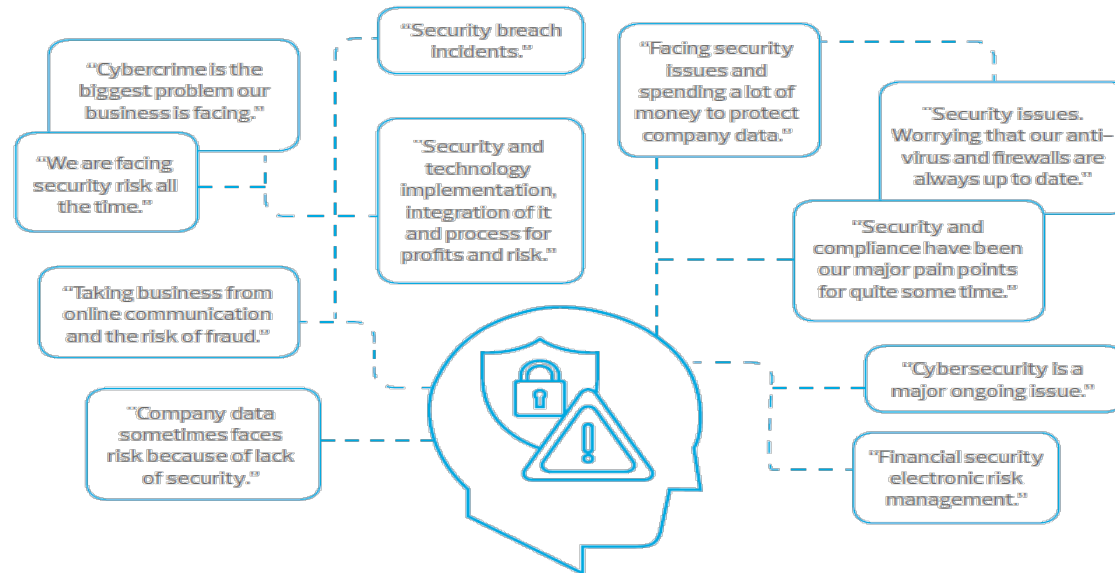


NACD 2018-2019 Public Company Governance Survey

Overall recommendations

Top of mind cybersecurity concerns in the middle market

We asked about cybersecurity in the first quarter 2019 MMBI questions section. It appears that cyber-related themes were among the leading issues for many of the business owners polled. Here is a sampling of cyber-focused responses when executives were asked to describe "a top business concern" for their companies.



Cybersecurity key considerations

- Third-party vendor management
 - Ensure data that is processed, transmitted, stored and accessed is properly secured.
- Identity and access management (IAM)
 - Implement solution to provide users transparency to applications/systems while increasing security controls.
- Vulnerability management program (VMP)
 - Implement a vulnerability program that identifies assets, and can prioritize vulnerabilities based on impact to the business.
- Culture of awareness
 - Ensure that the organization has a culture of security awareness. Empower end-users to understand their part in cybersecurity and the threats that can leverage their lack of awareness.
- Benchmarking
 - Conduct a risk assessment that aligns to the industry. Develop a risk registry that captures the highest risk items.

Cybersecurity key considerations

- Compliance
 - Ensure that the organization understands the data and the business processes that use that data. Leverage business process risk assessments to quantify the risk associated with storing, processing, transmitting or access the regulatory data.
- Incident response plan/testing
 - Whether listed in the cyber insurance policy or required for regulatory compliance, testing the incident response is critical to ensure that the organization can response appropriately to an incident.
- Cyber liability insurance
 - Ensure your cyber liability insurance is correlated back to the risk assessment findings.
- Cybersecurity steering committee
 - The most effective way to reduce information filtering and increase cyber risk visibility is to implement a cybersecurity steering committee.

Contact us for questions, concerns, or inquiries



Chris Hannifin

Manager - Security, Privacy and Risk

Email: Chris.Hannifin@rsmus.com

Phone: 865 661 9779



Tauseef Ghazi

Principal - Security, Privacy and Risk

Email: Tauseef.Ghazi@rsmus.com

Phone: 832 878 9211



QUESTIONS AND ANSWERS?

TOTAL REWARDS TRENDS & RELATED COMPLIANCE UPDATES

July 24, 2019

THE POWER
OF BEING
UNDERSTOOD

Agenda

- Middle Market Labor and Compensation Strategy Trends
- Competing Forces Affecting Total Rewards
- Key Market Trends in Total Rewards
- Legal Updates: Employment Laws Impacting Total Rewards
- Recommendations
- Additional Research and Data Resources

Introduction

Rob McGee, PHR, CCP
Manager, Management Consulting: People & Organization
Austin, Texas
robert.mcgee@rsmus.com

Areas of Specialty Include:

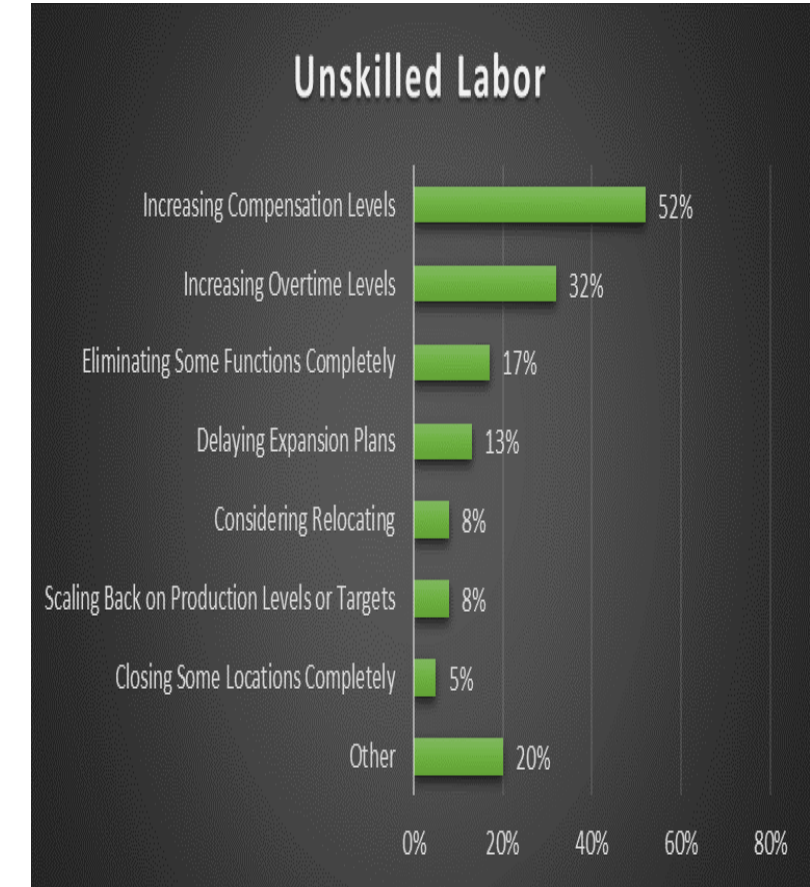
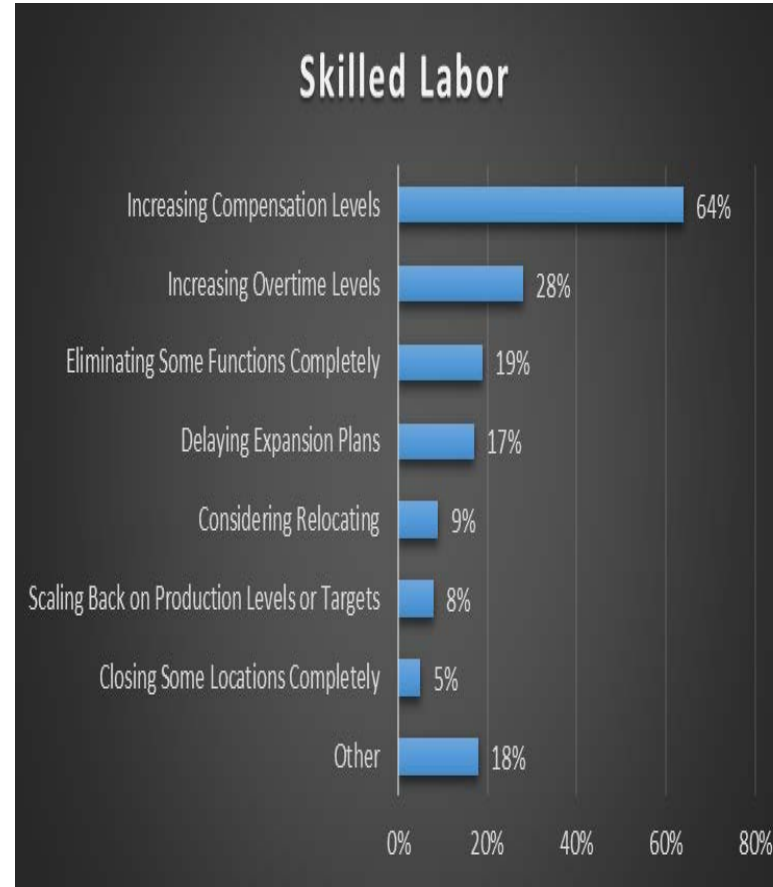
- Compensation infrastructure design
- Variable pay plan design
- Job development, evaluation and market pricing
- Compensation administration and employee pay assessments
- HRIS and HCM selection and implementation
- HR operational assessments and process design
- HR compliance assessments
- Diversity & Inclusion analysis and strategy development



How is the Middle Market Responding to Labor Shortages?

RSM U.S. Middle Market Leadership Council (MMLC) Survey Results:

- The #1 staffing challenge across all industries is lack of available qualified workers
- 72% of companies are struggling (to some extent) to find skilled labor, while 42% are experiencing the same level of difficulty with unskilled labor
- Job vacancy durations have surpassed pre-recession levels; employers are intensifying their recruiting efforts to fill vacancies
- Voluntary turnover has recovered back to pre-recession levels as employees gain confidence in leaving their current jobs for opportunities with new employers



What's Driving Middle Market Employer Pay Strategies?

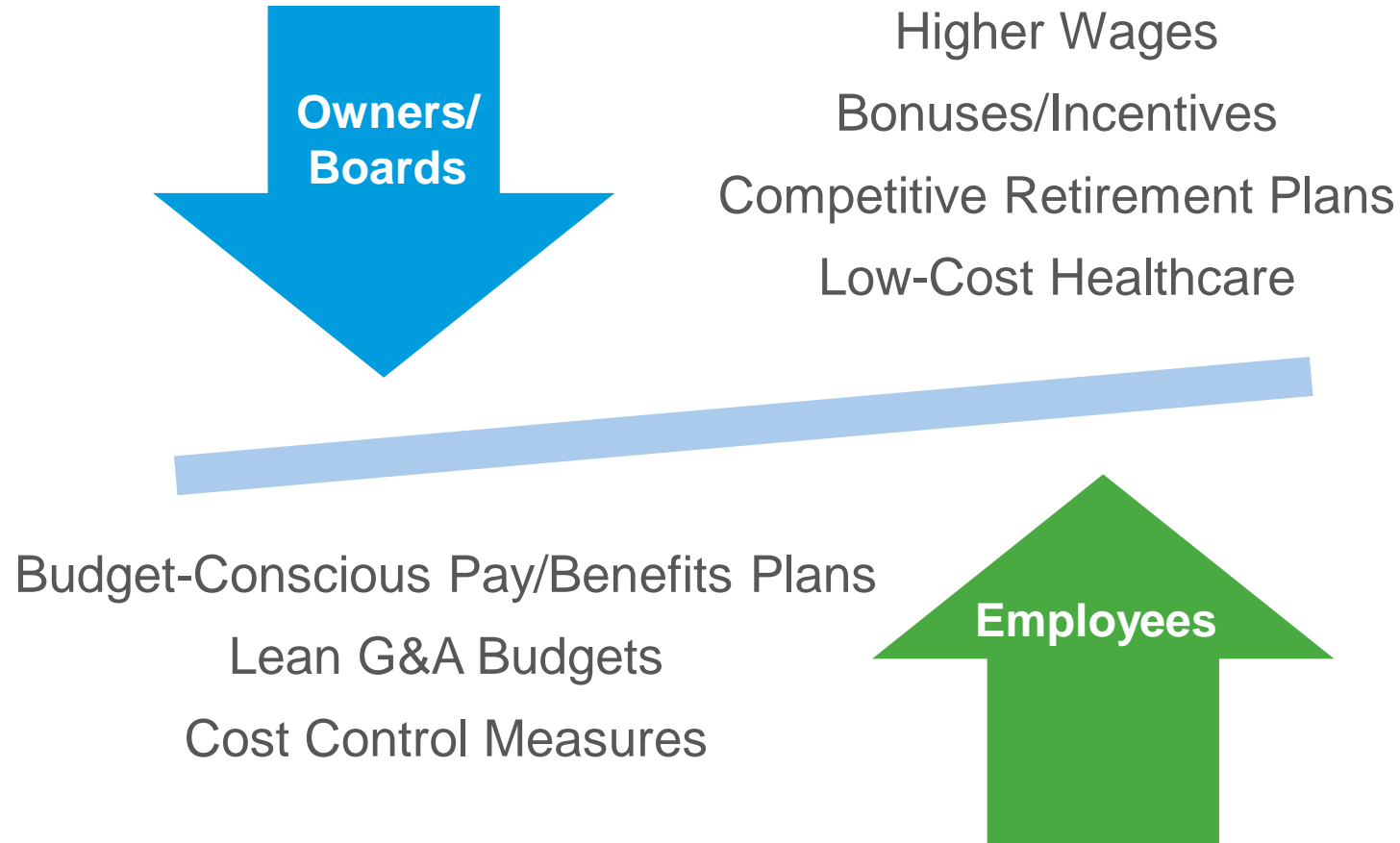
Top driver of the organization's compensation management strategy:

	< 500 Employees	501 - 999 Employees	1,000+ Employees
Retain Talent	57%	56%	56%
Recruit Talent	48%	61%	62%
Be an Employer of Choice	28%	31%	30%

Key Performance Indicators used to measure the success of the organization's compensation management strategy:

	< 500 Employees	501 - 999 Employees	1,000+ Employees
Employee Retention	63%	66%	60%
External Salary Benchmarking	54%	61%	60%
Employee Engagement	42%	43%	45%

Competing Forces Affecting Total Rewards



Key Market Trends in Total Rewards

Low Unemployment Fuels Talent Wars



Unemployment has hovered below 4% and is expected to drop as low as 3.3% by EOY 2019. Forces higher wages amid a tightening labor pool of qualified workers for hire.

Merit Increase Budgets Climb



2019 average merit budget forecast is 3.2%, demonstrating a continued year-over-year increase trend since 2015; however, wage growth for “hot jobs” will outpace this rate.

Tax Reform and your Competitive Edge



Employers are considering cash freed up by corporate tax rate cuts as an opportunity to boost compensation and benefits programs, among other options, to attract and retain key talent.

Cash is not King



60% of employees are likely to accept a lower salary in exchange for better benefits and work-life balance conditions.

Key Market Trends in Total Rewards (continued)

Fair Pay Drives Engagement



On average, companies who make pay equity a priority will yield 13% higher employee engagement, and are 19% more likely to exceed industry-average levels of productivity.

The “Gig” Economy is Booming



In 2017, 35% of the U.S. workforce (55 million people) were “gig workers”, 43% anticipated by 2020; gig jobs are replacing traditional employee pay growth tactics.

Annual Performance Reviews Lose Momentum Differentiated Pay Strategies on the Rise

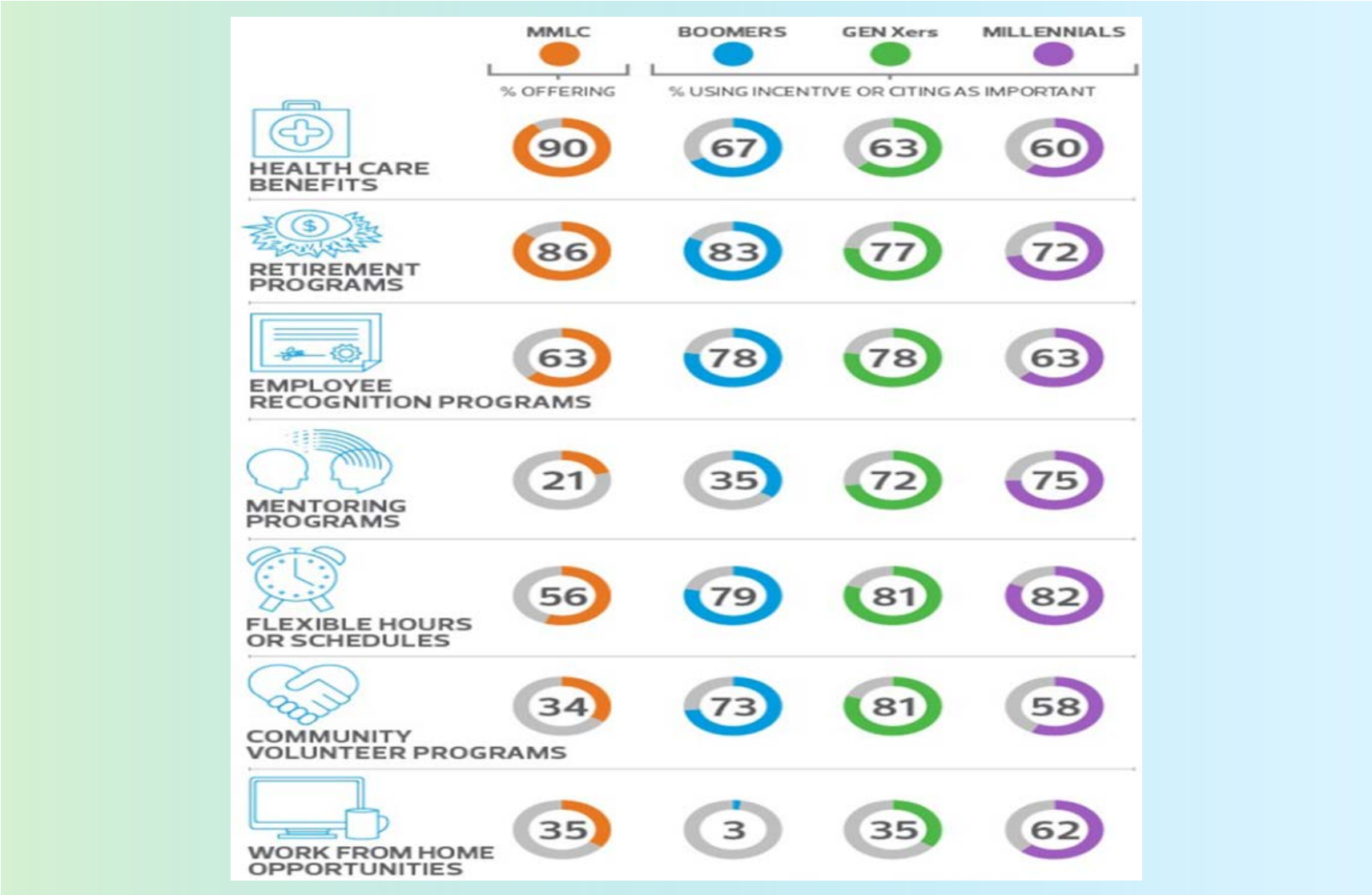


Long deemed marginally effective, annual performance reviews and ratings are gradually morphing into rating-less monthly performance and coaching discussions and pay increase decisions being tied to employee impact and market compensation data benchmarks.



Industry-specific niche skills or universal hot skills in technology and data & analytics are in high demand and short supply, driving innovation in pay strategies to attract and retain employees possessing them.

Utilization of Total Rewards Programs by Generation



Employment Law Updates Impacting Total Rewards



Legal Update: Fair Labor Standards Act (FLSA)

Proposed Changes

Exempt Employees:

- Proposed rule would increase minimum salary threshold from \$455 per week (\$23,660 annually) to \$679 per week (\$35,308 annually)
 - This is lower than the 2016 proposed rule of \$913 (\$47,476 annually)

Highly Compensated Employees:

- Total annual compensation requirement for this classification would increase from \$100,000 to \$147,414 per year
 - Primarily impacts annual 401(k) non-discrimination testing required by the IRS

Methodology:

- Minimum Salary Threshold: Aligned to the 20th percentile of earnings of full-time salaried workers in the lowest-wage census region (South), and in the retail sector
- Highly Compensation Employees: Aligned to the 90th percentile of full-time salaried workers nationally
- Thresholds were also informed by over 200,000 comments received by the DOL during the Public Comment process following the 2016 proposals

Legal Update: Fair Labor Standards Act (FLSA)

Implementation Considerations

Implementation, if enacted:

- Any employee earning less than the new salary threshold must be classified as non-exempt and receive overtime pay according to state/federal regulations
- Anticipated to take effect starting January 2020
- Would be subject to review and possible salary threshold increases every 4 years

Bridging the Gap:

- The final regulations will allow employers to use non-discretionary bonuses and incentive payments (including commissions) to satisfy up to 10 % of the new standard salary level
- To qualify, non-discretionary bonuses and/or incentive payments must be paid within one pay period after the end of each 52-week period
 - Employer must still pay at least \$611.10 per week for exempt employees paid via this eligibility option

Legal Update: EEO-1 Pay Data Reporting Requirements

- “Component 1” Data Submissions:

- Data Fields: Job category, race, ethnicity and sex
- This is the original required EEO-1 component form
- Required for employers with 100 or more employees
 - Federal contract employers with 50 or more employees and/or \$50,000+ in federal contract revenue
 - Submissions were due by May 31, 2019 (reporting data from 2018)

- “Component 2” Data Submissions:

- **New requirement**
- Data Fields: Employers must now submit hours worked and employee pay data from their W-2 forms by job category, race, ethnicity and sex for **2017 and 2018**
- Only applies to employers (and federal contract employers) with 100+ employees
 - Submissions are due by September 30, 2019
 - Filing system is now available

Legal Update: San Antonio Paid Sick Leave Ordinance

DELAYED

Ordinance Summary:

- Affects employers with six or more employees
 - Five or less employees goes into effect August 1, 2021
- Grants all employees one hour of earned paid sick leave for every thirty (30) hours worked for San Antonio employers
 - Annual Accrual Caps: 64 hours for middle/large employers; 48 for small employers
- Starts immediately upon employment, or the effective date of this ordinance; may restrict use for new-hires up to 60 days
- Unused hours roll over into subsequent years
- Even if paid out at time of separation, employer must reinstate the balance that existed at the time of separation if the employee is rehired within six months (likely to change)

Implementation:

- Originally scheduled to go into effect on August 1, 2019
- Businesses and Business Associations filed a suit to stop its implementation
 - Texas Attorney General Paxton intervened on July 19, 2019
 - City of San Antonio agrees to delay the ordinance until December 1, 2019
 - First hearing is scheduled for July 24, 2019

Legal Update: Federal Minimum Wage Increase Proposal

- July 18, 2019: 201 U.S. House of Representatives members approved a bill that would gradually raise minimum wage to \$15.00 per hour by 2025
 - Though passed by the House of Representatives, it will likely not be considered by the Senate

Recommendations

- Engage your HR leadership team in an assessment of your current total rewards programs
- Use data-driven insights and employee feedback to shape your pay and benefit programs
 - Alignment to industry market data benchmarks
 - Employee value and utilization of each reward component
- Discuss differentiated reward strategy options to position your organization as an employer of choice
- Consider implementing buzzworthy benefit programs
 - Paid maternity/paternity leave
 - Zero-balance PTO program
 - Student loan repayment assistance program for hired interns
 - Casual dress code for all employees
- Keep an eye on employment law updates and changes
 - Preparation could require a significant amount of work for your HR, Finance and Legal functions
 - Failure to comply by required deadlines could come with costly penalties
- Plan for the future; workforce conditions will definitely change

Additional Resources

RSM Resource Center: [Labor & Workforce Trends](#)

RSM Resource Center: [Employee Benefits Insights](#)



QUESTIONS AND ANSWERS

Real Economy and Middle Market Business Index

Real Economy

Identifying the exact month or months when a business cycle starts and ends is part science and part art. While our estimation is that we have a near miss on a recession this year, the probability of an end to the current business cycle is rising due to trade policy and tight monetary policy. The bond market is clearly signaling that absent a cessation of trade hostilities or a shift in monetary policy, we are now late in the business cycle.

In this issue of *The Real Economy*, we explore what [the bond market and other indicators](#) are saying about future economic growth for the middle market. In addition, we look at what's under the hood in the [recent jobs report](#). In our Industry Spotlight, we examine [hospital revenue bond activity](#).

[Download the full report.](#)



Middle Market Business Index

[Download the Second Quarter Report here.](#)

Workforce Generations Defined

1900 - 1945

Traditionalists

- Identified by the importance they place on duty and loyalty; Value is placed higher on job stability than earnings
- Inclined to follow rules, but their experience encourages them to sometimes overestimate their abilities; Expect their experience to be respected
- Embrace self-reliance and pragmatism; Less likely to report issues to management; Strong team players
- May struggle with technology, but are the most engaged generation and want opportunities to develop and learn.

1946 - 1964

Baby Boomers

- Often ties the evaluation of their self-worth to their careers; Seen by others as “workaholics” who are driven by material acquisitions, titles and personal success
- Value is placed on growth opportunities and financial security
- Typically have an optimistic outlook and embrace the latest technology, though direct person-to-person communications is still their preference
- Team-oriented, and often demonstrate strong leadership capabilities

1965 - 1980

Generation X’ers

- Known as the “latchkey kids”; Learned at an early age to be independent due to typically having two working parents
- Independent and self-directed in the workplace; Adaptable and focused on results
- Value is placed on recognition and pay levels that are commensurate with their level of performance
- Technology literate and not deterred from having to learn new technologies to perform their job

1981 - 2000

Millennials

- The first generation to grow up using the internet and information technology from a very young age; Often seen as technology experts
- Typically confident (and sometimes over-confident) due to highly involved and affirming parents; Seek regular feedback and opportunities for learning and professional advancement
- Childhood was often over-scheduled, resulting in them being very comfortable with multi-tasking and frequent change
- Idealistic; Value work/life balance over pay, and expect corporate social responsibility and robust diversity and inclusion initiatives from their employer

2001 - Present

Nexters

- Generally, similar in values to Millennials but demonstrate a few key differences
- Possess a stronger desire to work a variety of jobs, even within a singular employer, versus a routine job
- Immersed in technology, but prefer face-to-face communications and enjoy working in small, structured teams
- Likely to embrace “gig jobs” as a pay growth strategy over traditional methodologies



RSM US LLP
San Antonio, Texas
+1 800 274 3978
www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/about-us for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood®* is a registered trademark of RSM US LLP.

© 2018 RSM US LLP. All Rights Reserved.