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 Daimon Geopfert

• Principal - Security, Privacy and Risk Consulting
• National Leader for SPRC
• Located in Detroit, MI
• Former DoD, AFOSI-CCI, AIA
• GCIH, GREM, CEH, CISSP, CISA, CISM
About Ken Stasiak

• Principal- Security, Privacy and Risk
• Located in Cleveland, Ohio
• EMBA Northwestern University Kellogg School of Management
• CISSP, CISA, CGEIT, CISA
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.
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.
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.

Conduct a complimentary ransomware risk assessment {stay tuned at end of WebEx to see how}
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.
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
Information filtering

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

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

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.

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

Despite the increasing threats and attack vectors middle market confidence level in safeguarding their data @ 93% overall confidence level.
INFORMATION AND DATA SECURITY
Information and data security: by the numbers

Companies experiencing data breaches in last 12 months

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1 '15</td>
<td>9%</td>
<td>91%</td>
<td>3%</td>
</tr>
<tr>
<td>Q1 '16</td>
<td>11%</td>
<td>87%</td>
<td>2%</td>
</tr>
<tr>
<td>Q1 '18</td>
<td>8%</td>
<td>92%</td>
<td>5%</td>
</tr>
<tr>
<td>Q1 '19</td>
<td>19%</td>
<td>26%</td>
<td>18%</td>
</tr>
</tbody>
</table>

Likelihood unauthorized users will attempt to access data/systems

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Very unlikely</th>
<th>Somewhat unlikely</th>
<th>Somewhat likely</th>
<th>Very likely</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1 '15</td>
<td>18%</td>
<td>50%</td>
<td>22%</td>
<td>10%</td>
</tr>
<tr>
<td>Q1 '16</td>
<td>28%</td>
<td>33%</td>
<td>29%</td>
<td>10%</td>
</tr>
<tr>
<td>Q1 '18</td>
<td>18%</td>
<td>35%</td>
<td>31%</td>
<td>16%</td>
</tr>
<tr>
<td>Q1 '19</td>
<td>19%</td>
<td>26%</td>
<td>37%</td>
<td>18%</td>
</tr>
</tbody>
</table>
Information and data security: by the numbers

Percentage of claims by cause of loss (N=298)

- Ransomware: 31%
- Hacker: 19%
- Malware/virus: 11%
- Email compromise: 11%
- Phishing: 11%
- Rogue employee: 10%
- Legal action: 4%
- Staff mistake: 3%
- Lost or stolen laptop/device: 2%
- Programming error: 2%
- All other causes: 5%

Source: 2018 NetDiligence Cyber Claims Report

Percentage of claims by sector (N=591)

- Professional services: 23%
- Manufacturing: 15%
- Technology: 10%
- Financial services: 9%
- Retail: 7%
- Public entity: 6%
- Nonprofit: 4%
- All other sectors: 2%

Source: 2018 NetDiligence Cyber Claims Report
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

- Data destruction
- Hacking
- Business interruption
- Theft
- Extortion (including ransomware)
- Denial of service attacks
- Failure to safeguard data
- Post-incident investigative expenses
- Post-incident public relations expenses
- Defamation

Familiarity with what organization’s cyber insurance policy covers

- Not familiar
- Somewhat familiar
- Familiar
- Very familiar

Organization carries a cyber-insurance policy

- Yes
- No
- Don’t know

Q1 2018 (N=412)
- Yes: 38%
- No: 52%
- Don’t know: 10%

Q1 2019 (N=404)
- Yes: 33%
- No: 57%
- Don’t know: 10%
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 unsure about the specifics of their 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).
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.
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 and D&O.

✔ 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.
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

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

- Q1 2018 (N=412): 49% Yes, 43% No, 8% Don't know
- Q1 2019 (N=404): 53% Yes, 42% No, 5% Don't know
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 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.
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: 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.
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.
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.

- Change in the regulatory climate: 48.9%
- Economic slowdown: 48.3%
- Cybersecurity threats: 41.8%
- Business model disruptions: 39.8%
- Geopolitical volatility: 39.0%

NACD 2018-2019 Public Company Governance Survey
Overall recommendations
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.
Complimentary ransomware risk assessment


• Enter code: NotME

• Over the phone consultation focused on NIST CSF based on controls that are most prevalent to Ransomware.
  - Report with observations and recommendations

![](chart.png)

- Identify (ID)
- Prevent (PR)
- Detect (DE)
- Respond (RS)
- Recover (RE)

Comparision Chart

Your Results  Industry Average
QUESTIONS AND ANSWERS?
Contact us for questions, concerns, or inquiries

Ken Stasiak
Principal - Security, Privacy and Risk
Email: Ken.Stasiak@rsmus.com
Phone: 216 927 8213

Daimon Geopfert
Principal - Security, Privacy and Risk
Email: Daimon.Geopfert@rsmus.com
Phone: 313 335 3888