CYBERSECURITY
2020 SPECIAL REPORT

July 14th, 2020
Agenda

• Background/ Pre-COVID-19
• Executive Summary
• Information and Data Security
• Cyber Insurance
• Ransomware Attacks
• Business Takeover Threats
• Privacy and Compliance Protections
• Migration to the Cloud
• Complementary Efficiency Assessment
Presenters

Daimon Geopfert
Principal
National Leader for Security, Privacy and Risk Consulting
Former DoD, AFOSI-CCI, AIA
GCIH, GREM, CEH, CISSP, CISA, CISM

Ken Stasiak
Principal
Growth and Marketing Leader for Risk Consulting
EMBA Northwestern University
Kellogg School of Management
CISSP, CISA, CGEIT, CISM
M Grill 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.

1. **Smaller** middle market companies: ($10m - $50m) in revenue.
2. **Larger** middle market companies: ($50m - $1b) in revenue.
Pre-COVID-19

• This year’s MMBI cybersecurity special report survey was conducted prior to the COVID-19 pandemic.

• The special report does address COVID-19 and potential impacts to cybersecurity during the pandemic.
Change in presentation format

- RSM is conducting a Webcast launch (today) to review the narrative behind the report at a high level.

- Breakout videos will provide more insight to various MMBI special report topics:
  1. Top 5 things to make sure your cyber liability policy covers
  2. Top 3 most prevalent attacks: Incident Response Team
  3. Tips on how to be an effective CISO / Director of Security
  4. Top 3 phishing attacks to watch out for
  5. General overview and top 3 trends in privacy
  6. Risks to using the cloud
  7. What are a few key takeaways for Canadian businesses?

- This year, we will highlight the differences between smaller middle market companies and larger middle market companies.

- Similar to last year, RSM will be offering a complementary assessment focused on determining the efficiency of your cybersecurity program.
  - Sign up information at the end of this presentation
EXECUTIVE SUMMARY

“Cybersecurity is as much an enterprise issue as it is a technical issue; senior company leaders need to work closely with their information security teams to understand the threats applied to their networks, the risks posed by malicious actors, and the risks of inaction. Advanced persistent threats require advanced and persistent countermeasures, both sophisticated and simple. In addition, cyber insurance will become an increasingly important tool in managing cyber risk, but it must be used in conjunction with—and not in lieu of—mature cybersecurity practices.”

—Christopher D. Roberti, Senior Vice President for Cyber, Intelligence and Supply Chain Security Policy, U.S. Chamber of Commerce
The Cybersecurity Threat to the Middle Market

- 18% of middle market C-suite executives said their companies experienced a data breach in the last year, up from 15% in 2019.
- COVID-19 has increased the complexity of securing organizations, and changes in business processes.
- Rise in middle market companies that carry cyber insurance.
- NetDiligence® Cyber Claim Study found that 96% of cyber insurance claims came from small to medium size business.
Cyber Threat Continued

• The continued shift:
  Protecting
  Data
  Should we even have the data?

• The 2019 NetDiligence Cyber Claims Study, sponsored by RSM, showed social engineering accounted for the highest amount of losses among middle market companies.

• 95% of middle market executives are confident in their current security posture, up 2% from last year’s report:
  1. Increase cyber insurance
  2. Increase in awareness training
  3. Increase in dedicated cybersecurity resources

Overtaking ransomware, which was the leading cause in last year’s report.
MIDDLE MARKET INSIGHT

“Navigating cybersecurity risk begins with awareness and preparedness, which is what we are focusing on from the outset with our clients.”

—Financial technology executive, RSM US MMBI Q1 survey
Information and Data Security

• 29% of larger companies suffered a data breach, compared to only 10% of smaller businesses.

• Over the past six years, data breaches have consistently risen.
  - 55% of respondents say it is likely that an attempt to access their data will be made in 2020.

• 71% indicated that they have a dedicated function focused on cybersecurity.
Three areas that increased from 2019 were:
- Purchased new or upgraded hardware
- Engaged data security consultants
- Added data security staff

16 Point drop from 2019
Data Security: RSM Lessons Learned

• Dedicated resources focused on cybersecurity is a key component to building and managing an effective cybersecurity program.
  - Unicorns, don’t exist (at least that I know of), neither do cybersecurity professionals that understand and have performed everything needed.
  - Augmenting current dedicated resources can be an effective way to increase your overall program without adding headcount.
  - The skill gap in cybersecurity is growing, with the ability for dedicated resources to effectively manage and communicate cybersecurity issues to leadership.
CYBER INSURANCE

“Our top business problem is security. You can never truly be absolutely secured in this day and age.”

– Technology executive, RSM US MMBI Q1 survey
Cyber Insurance

- 62% of organizations carry a cyber insurance policy, up from 57% last year.
- 34% of smaller middle market companies are familiar with their coverage.
- While more companies have cyber insurance policies, there was a significant drop in overall coverage or exposure areas.
Cyber Insurance Coverage

• Denial of Service coverage had the largest drop from last year's report by 16 points.

• Extortion (ransomware attacks) was the only policy coverage to increase from 2019, by only 3 points.
  - 2019 report highlight ransomware attacks

Risks or exposures the cyber insurance policy covers

<table>
<thead>
<tr>
<th></th>
<th>Q1'19 TOTAL n=100</th>
<th>Q1'20 TOTAL n=120</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data destruction</td>
<td>83</td>
<td>74</td>
</tr>
<tr>
<td>Business interruption</td>
<td>77</td>
<td>67</td>
</tr>
<tr>
<td>Hacking</td>
<td>78</td>
<td>65</td>
</tr>
<tr>
<td>Extortion (including ransomware attacks)</td>
<td>62</td>
<td>65</td>
</tr>
<tr>
<td>Theft</td>
<td>71</td>
<td>56</td>
</tr>
<tr>
<td>Post-incident investigative expenses</td>
<td>57</td>
<td>52</td>
</tr>
<tr>
<td>Failure to safeguard data</td>
<td>59</td>
<td>51</td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td>61</td>
<td>45</td>
</tr>
<tr>
<td>Post-incident public relations expenses</td>
<td>47</td>
<td>44</td>
</tr>
<tr>
<td>Defamation</td>
<td>38</td>
<td>31</td>
</tr>
<tr>
<td>None of the above</td>
<td>0</td>
<td>&lt;0.5</td>
</tr>
</tbody>
</table>

Source: RSM US Middle Market Business Index survey, Q1 2020

Have to take these results with a (*) since only 34% of the respondents were familiar with their coverage 😊
Cyber Liability Insurance: RSM Lessons Learned

• Typically the CFO fills out the questionnaire
  - Similar to life insurance, how you answer the questions dictates your premium

• Not knowing what is covered in the policy
  - Cloud providers, ransomware, employee theft

• Top questions that people say “yes” to but, often don’t have/do:
  - Compliance: Payment Card Industry (PCI)
  - Testing: Testing the Incident Response Plan, Penetration Testing
  - Program: Incident Response Plan
  - Case study: CFO responds “yes” to being PCI compliant
RANSOMWARE

“Someone tried to breach our system, but we caught it early when a red flag was raised, and we were able to stop it before they could succeed.”

—Retail executive, RSM US MMBI Q1 survey
Ransomware

• **23%** of companies experienced a ransomware attack within the past twelve months.

• **49%** of respondents are likely targets for a ransomware attack.

• With stay at home orders and a remote workforce, attacks on home devices/network may increase.

• Culture of the workforce is most impacted by remote workforce and employees’ trust.

Larger companies reported ransomware attacks at 32%

Larger companies see themselves as more of a target at 56%
Ransomware Continued

- Ransomware employs two different tactics:
  1. Repetitively sending out fraudulent emails from fake or compromised accounts with no discernible pattern.
  2. More sophisticated campaign targeting vulnerable networks or systems.

- In conjunction with the 2019 MMBI cybersecurity special report, RSM conducted over 50 complementary ransomware assessments. The following areas/controls were the most widely missed:
  - Segmentation (83%)
  - Restricting and disabling end user’s local admin privileges (75%)
  - Two-factor authentication for email (50%)
• Controller who typically works in the office got phished, resulting in her computer being compromised—including all of the payroll, benefits and customer information stored on it.
“As more organizations implement awareness programs, we see a shift in the market from generalized phishing campaigns to specifically crafted phishes in order to keep pace with emerging threats. This correlates with the decrease in employees’ ability not to act on suspicious emails—down from last year’s report.”

Ken Stasiak, Principal, RSM US LLP
Social Engineering

• Most popular type of attack.
• COVID-19 exacerbated this form of attack.
• 49% of executives indicated outside party attempted to manipulate an employee.
• 28% of these attackers were successful in manipulating an employee.
  - 11% increase from 2019
• 90% (that experienced unsuccessful attacks) listed employees not acting as the number one deterrent of these attacks.
  - 7% drop from last year’s survey

Smaller companies reported more attacks at 54%

Larger companies reported 48% of these attacks were successful
Social Engineering

• Awareness training companies provide has increased by 3% to nearly 82%.
  - With increased training, and a decrease in employees’ effectiveness in identifying phishing emails, is this working?

• Tailored awareness programs have a higher retention rate for employees than canned or generic templates.
Business Takeover: RSM Lessons Learned

• Social engineering attacks with ACH / wire transfers are common
  - Segregation of duties (accounting best practices)
  - Two-Factor authentication on bank accounts
  - Duel authorization on wire transfers

CEO sends an e-mail requesting $500k to be wired

+ No verification or duel authorization

Big accounting problems

• Case study: $250m business wires over $500k to Hong Kong
PRIVACY PROTECTIONS COMPLIANCE

"MIDDLE MARKET INSIGHT

"Federal and state regulators continue to pepper financial institutions with new regulations, tools and guidance. Many institutions are struggling to keep up with even the basic tenets of a cybersecurity risk management policy or program."

—Financial technology executive, RSM US MMBI Q1 survey"
Privacy and Compliance

• Marriott is currently under review for violating General Data Privacy Regulation (GDPR) for a 2018 breach, with a reported $123 million fine.

• Nevada Privacy Law went into effect Oct. 1, 2019.

• California Consumer Privacy Act (CCPA) became law on January 2020.
  • Massachusetts and Texas to follow, likely this year.

• 39% of respondents are familiar with GDPR
Privacy and Compliance

• Of those familiar with GDPR 83% believed their organizations will likely have to comply to some type of privacy legislation during the next two years.

• Almost all respondents are preparing for emerging privacy legislation or regulations.

• U.S. continues to lag behind other countries when it comes to data privacy.

Larger companies are making privacy a critical priority at 36%
MIGRATION TO THE CLOUD

“Cloud solutions can often simplify security configuration, monitoring and even compliance, but like any technology, companies need to understand how to deploy these solutions in a secure manner.” – Daimon Geopfert, Principal, RSM US LLP
Migration to the cloud: by the numbers

- **42%** of respondents moved data to the cloud as a result of security concerns in the last 12 months.
- **90%** stated moving to the cloud was more secure.
  - 4% drop from 2019
- **27%** that moved data to the cloud based on security concerns indicated that the solution is less expensive.
  - 3% decrease from 2019
- **29%** of respondents are pursuing blockchain technology to enhance their security and privacy efforts.
  - 7% increase from 2019
Complimentary Cybersecurity Efficiency Assessment

To help organizations quantify the efficiency of their security program, RSM is offering a complimentary 45-minute consultation to discuss your current security tools, policies and programs. During this consultation, we will cover:

1. The composition of your security program
2. The structure of your security team
3. How your business uses security tools and technologies
4. The operation of your security program

After the consultation, you will receive a quantified security efficiency score and personalized recommendations to improve your security program's effectiveness.
QUESTIONS
AND ANSWERS?