



# CYBERSECURITY UPDATE: SHARPENING THE FOCUS ON SECURITY

July 19, 2023

# Today's speakers



**Ken Stasiak**

Principle, RSM US LLP

Cleveland, OH

[Ken.Stasiak@rsmus.com](mailto:Ken.Stasiak@rsmus.com)

(216) 927 8213



**Charles Barley**

Principal, RSM US LLP

McLean, VA

[Charles.Barley@rsmus.com](mailto:Charles.Barley@rsmus.com)

(703) 336 6440



**Anthony Catalano**

Principal, RSM US LLP

Cleveland, OH

[Anthony.Catalano@rsmus.com](mailto:Anthony.Catalano@rsmus.com)

(216) 927 8223



**Daniel Gabriel**

Principal, RSM US LLP

Charlotte, NC

[Daniel.Gabriel@rsmus.com](mailto:Daniel.Gabriel@rsmus.com)

(980) 256 7541



# WELCOME & OVERVIEW

Ken Stasiak

## 2023 MMBI cybersecurity special report

Six years of research

Over 400 middle market executives

Report details:

- Common cybersecurity and data privacy challenges
- Frequency of cyberattacks
- Best practices for implementing security controls and strategies



## Key trends in the cybersecurity landscape

**Breaches are slightly down, but significant cybersecurity concerns persist:** 20% of middle market executives claimed their company experienced a data breach last year.

**However, executives are still worried:** 68% anticipate that unauthorized users will attempt to access data or systems this year.

**Technology is changing:** 50% of organizations have moved to the cloud in the past year due to security concerns, up from 36% last year.

**So is cyber liability coverage:** 68% of companies carry a cyber insurance policy, and 70% say premium costs have increased.

63%

of executives feel they are at risk  
for a ransomware attack in 2023.

RSM US MIDDLE MARKET BUSINESS INDEX  
**CYBERSECURITY**  
SPECIAL REPORT

  
**RSM**

## Topics of discussion

**Business perspective:** As the business environment evolves, the middle market leans into taking a more proactive stance on security.

**Business takeover threats:** With the potential for a business takeover attack to be launched by anybody, companies need to employ various strategies discourage them.

**Regulation and data protection impacts:** 10 components of a privacy function that are the key to operating a successful and holistic privacy program.



# BUSINESS PERSPECTIVE

Anthony Catalano

# Framing it for the business

## Overview

Cyber security is inherently a RISK MANAGEMENT activity – it does not MAKE money for an organization...

- But it can help keep them from losing money!
- In some cases, can provide competitive advantage, reduce compliance costs, or optimize internal technology.

## State of the State

Though cyber threats continue to evolve throughout the years, a sustainable cyber program is the most critical element for any organization. The landscape remains fluid from both the business and threat perspective.

- Groupthink and Confirmation bias are rampant in cyber security. Organizations must implement metrics to measure the **success or failures** of cyber programs on a consistent basis and make changes quickly.

## Minimum Security Baselines are critical to a business

Ensure the cyber program is aligned with the cyber insurance policy. Then identify residual risk.

The development of processes to identify and reduce undesired risks relative to the business need is a component a successful cyber program.



# BUSINESS TAKEOVER THREATS

Daniel Gabriel

## Business takeover threats

Business takeover threats are among the most persistent and pervasive cybersecurity attacks on middle market companies.

The attacks can be straightforward, taking the form of social engineering and employee manipulation, but their low-tech nature means they can be hard to detect.

Similar to ransomware, business takeover threats require very little effort or technical skill to launch but can be very harmful to a potential victim.

**76%**

of executives feel they are at risk of an attack by manipulating employees in the coming year.

CV0





# REGULATION AND DATA PROTECTION IMPACTS

Charles Barley Jr.



# RSM top 10 considerations for an effective privacy program

Keeping pace with privacy and personal data protection requirements, regardless of the jurisdiction and industry sector, can be distilled to the following 10 components of a privacy function that are the key to operating a successful and holistic privacy program.

	<b>Governance and Accountability</b>	The organization is responsible for complying with privacy requirements and must be able to demonstrate compliance if the supervisory or regulatory authority requests evidence of administrative, physical, and technical requirements, as well as organizational measures to meet the compliance obligations for governance and accountability.		<b>Privacy by Design</b>	The organization is required to put in place appropriate administrative, physical, and technical requirements, as well as organizational measures to implement the personal data protection principles effectively and safeguard individual privacy rights. PbD essentially means that privacy is considered from the start of innovation and throughout the product or service development life cycle.
	<b>Policies and Procedures</b>	Personal data protection laws and regulations specifically require the organization to put in place personal data protection policies and procedures, where proportionate. These personal data protection policies and procedures ensure that the organization is taking steps to comply with compliance obligations for privacy requirements.		<b>Incident Response</b>	The organization must be prepared to address a privacy incident involving personal data. Privacy incident may be defined differently by stakeholders and in accordance with an organization's risk tolerance. Examples typically include inadvertent and impermissible uses and disclosures of personal data, supervisory or regulatory authority inquiries and investigations, complaints from individuals and/or private right of action as permitted by certain jurisdictions.
	<b>Notice and Communication</b>	The organization must inform individuals immediately when their personal data is collected and what their personal data is being used for along with other disclosures representative of the personal data life cycle.		<b>Breach Management</b>	Breach detection, investigation and internal reporting policies and procedures must be in place. The organization must be prepared to report certain personal data breaches to the relevant supervisory or regulatory authorities. Individuals should be notified immediately if the personal data breach has a high risk of adversely affecting individuals' rights and freedoms. Breach notification must be done within a specified period.
	<b>Personal Data Life Cycle Management</b>	The organization is responsible for providing evidence of a sustainable personal data governance program, including maintaining multi-jurisdictional records of processing activities (ROPA) registries for the purposes of documenting operational practices across the entire personal data life cycle (e.g., collection and acquisition, storage, use, share, transfer, retention, and disposal and destruction).		<b>Third Party Risk Management</b>	The organization must hold third parties accountable for being compliant with privacy requirements. Third parties should also have procedures in place to notify the organization if there is a privacy incident and/or breach of personal data.
	<b>Privacy Rights Management</b>	The organization is responsible for managing individual privacy rights and following through with requests within a specified period.		<b>Training and Awareness</b>	The organization must train employees on the importance of privacy and safeguarding personal data in the workplace and conduct such training immediately upon starting employment and at least once annually. Role-based training should also be conducted to further educate those with necessary access to personal data on a daily basis.

THANK YOU FOR  
YOUR TIME AND  
ATTENTION

**RSM US LLP**

+1 800 274 3978

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/aboutus](https://rsmus.com/aboutus) for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

© 2022 RSM US LLP. All Rights Reserved.

