RSM

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
(216) 927 8213

Charles Barley
Principal, RSM US LLP
McLean, VA
Charles.Barley@rsmus.com
(703) 336 6440

Anthony Catalano
Principal, RSM US LLP
Cleveland, OH
Anthony.Catalano@rsmus.com
(216) 927 8223

Daniel Gabriel
Principal, RSM US LLP
Charlotte, NC
Daniel.Gabriel@rsmus.com
(980) 256 7541

RSM

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

RSM

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.

RSM

RSM

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.

GD0

RSM

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

RSM

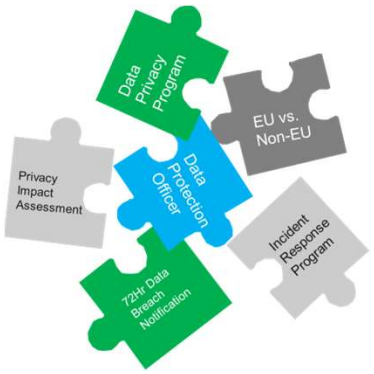
REGULATION AND DATA PROTECTION IMPACTS

Charles Barley Jr.

What should I think about data protection?

Key considerations:

- Data protection is a business issue
- Data protection is enabled by cybersecurity to protect the critical information and information assets
- Data protection is more than a legal compliance activity
- State & Local privacy laws are on the rise (10 states as of today)



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.

THANK YOU FOR YOUR TIME AND ATTENTION

RSM

RSM US LLP

+1 800 274 3978
rsmus.com

RSM