WEINLANDER FITZHUGH
Certified Public Accountants & Advisors

Insights and Resources

As a member of the RSM US Alliance, we would like to share the following with you:

Cybercrime risk: Top middle market vulnerabilities

LOCALLY OWNED. NATIONALLY AFFILIATED. GLOBALLY CONNECTED.

An independently owned member
RSM US Alliance

RSM

Weinlander Fitzhugh is a proud member of the RSM US Alliance, a premier affiliation of independent accounting and consulting firms in the United States. RSM US Alliance provides our firm with access to resources of RSM US LLP, the leading provider of audit, tax and consulting services focused on the middle market. RSM US LLP is a licensed CPA firm and the U.S. member of RSM International, a global network of independent audit, tax and consulting firms with more than 43,000 people in over 120 countries.

Our membership in RSM US Alliance has elevated our capabilities in the marketplace, helping to differentiate our firm from the competition while allowing us to maintain our independence and entrepreneurial culture. We have access to a valuable peer network of like-sized firms as well as a broad range of tools, expertise and technical resources.

Bay City Office
1600 Center Ave.
Bay City, MI 48708
(989) 893-5577

Clare Office
601 Beech St.
Clare, MI 48617
(989) 386-3481

Gladwin Office
1312 W. Cedar Ave.
Gladwin, MI 48624
(989) 426-8482

West Branch Office
108 N. Third St.
West Branch, MI 48661
(989) 345-3404

CYBERCRIME RISK

TOP MIDDLE MARKET VULNERABILITIES

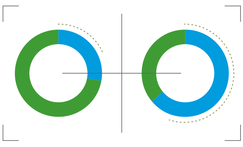
A recent study reveals that cybercriminals continued targeting middle market companies during the global pandemic, leading to the highest level of attacks since RSM began tracking data in 2015. Here's a closer look at the threat landscape from RSM's 2021 Middle Market Business Index Cybersecurity Report.

The middle market is under attack

28%

of middle market companies experienced a data breach in 2020.

Up from 18% in 2019



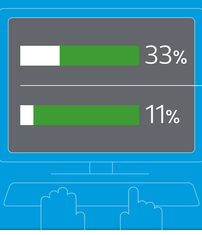
64%

anticipate that unauthorized users will attempt to access data or systems in 2021.

Up from 55% in both 2019 and 2020

Ransomware is on the rise

When a hacker seizes systems in demand for payment, your entire organization can grind to a halt.



33% of companies reported a ransomware attack in 2020.

11% experienced more than one attack in 2020, a common tactic used by hackers to re-target vulnerable systems.

Social engineering attacks persist

Social engineering, or account takeover, refers to obtaining a legitimate user's credentials, typically through misrepresentation, to gain entry into an organization's systems.

51%

of companies suffered a social engineering attack.

Up 2% from 2019

70%

say they're at risk of an attack through manipulation of employees in the next 12 months.

Up 7% from 2019

Heavy investments

Middle market companies are investing in cybersecurity protections...

71% have a dedicated function focused on data security and privacy.

65% carry a cyberinsurance policy.

33% are adding data security staff.

Lower coverage

...but they're neglecting basic strategies, resulting in potential overconfidence.

Fewer companies (60%) updated security protocols this year.

Down from 71% in 2020

Just 46% purchased or upgraded software.

Consider outsourcing

Instead of handling complex data security in-house, middle market companies should consider outsourcing this critical function to a trusted and experienced third party. This approach lets you:

1. Fill critical skills gaps
2. Leverage experience
3. Achieve around-the-clock service
4. Scale data infrastructure without disruption
5. Enable agility by allowing internal teams to focus more on strategic IT initiatives

Discover more ways to manage vulnerabilities with "5 ways managed service providers can strengthen risk management."

READ ARTICLE

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

lg-int-mc-all-0521