ALLIANT
CYBERSECURITY
An alliantgroup Company

SMALL BUSINESSES, THE FLIGHT TO REMOTE WORKING & CYBERSECURITY REPORT

Alliant Cybersecurity's Report On
Executive Cybersecurity Sentiments

RIZWAN VIRANI

CYBERSECURITY PRESIDENT,
ALLIANT CYBERSECURITY

Never before have we seen such a dramatic shift in the flow of data and sensitive information for businesses. As the world has been shocked into isolation due to the coronavirus pandemic, businesses of all sizes are forced to upend work as they know it in order to comply with social distancing mandates – which some estimates say could last until 2021/2022. With so many businesses rapidly switching to remote work for the foreseeable future, we are facing unprecedented vulnerabilities, especially for small to medium-sized businesses lacking telecommuting experience.

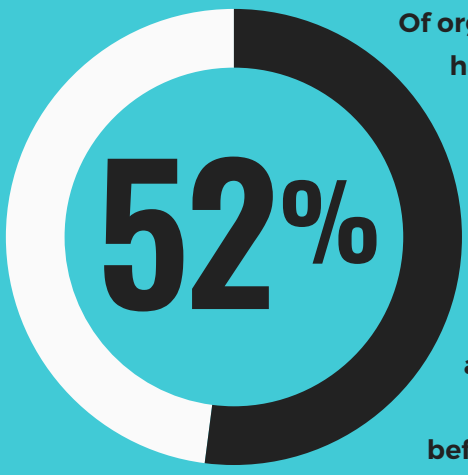
Remote work presents new considerations for everything cybersecurity. While large corporations have entire departments dedicated to these systems, SMBs are often lacking the knowledge and ability to have similarly robust protections in place. As such, we wanted to analyze just how vulnerable these businesses are and whether or not senior decision makers in charge are ready to address new cybersecurity considerations. This report found respondents feel confident in their efforts to mitigate cyberattacks, but upon further investigation this sentiment is ultimately unfounded.

These senior decision makers are vastly underestimating the opportunities for hackers to capitalize on the increased spread of information via cyber channels. Vulnerabilities are prevalent through a plethora of work channels, take the popular videoconferencing platform, Zoom which came under fire for poor data privacy and user security practices at the beginning of this remote work wave. Since then major institutions such as the New York City school district, Google and even SpaceX have all banned the platform due to concerns.

Those responsible for the well-being of businesses across the country need to take a step back and reassess their own internal capabilities to protect sensitive information. At the end of the day these findings clearly showcase the need for businesses to take the offensive, and not remain complacent in what may be a defining moment for cybersecurity resiliency over the next twelve months.

THE MAD DASH TO AN UNKNOWN WORLD OF TELECOMMUTING

As cities across the U.S. have gone into lockdown due to the coronavirus pandemic, we've seen an unprecedented flight to remote working in industries that have either little or no experience with this workflow.

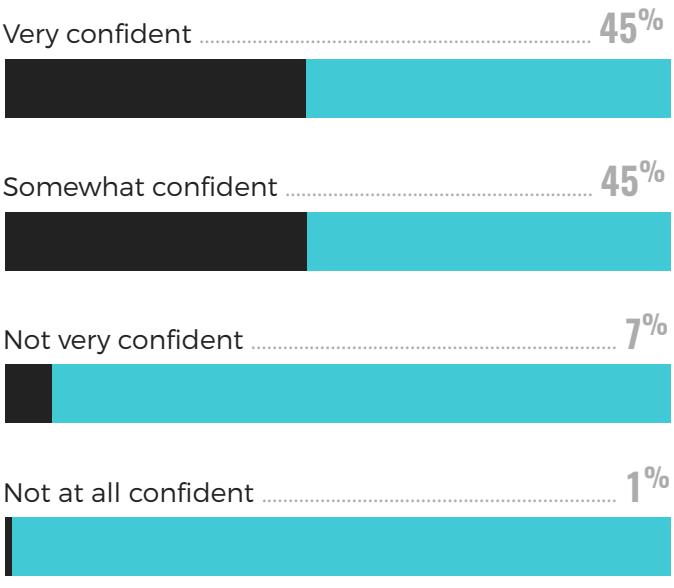


Of organizations that have transitioned operations to virtual/remote working since the outbreak began DID NOT allow for regular remote working before coronavirus.

Even with their lack of prior experience, respondents have high levels of confidence that their organization is working to mitigate potential cybersecurity threats and attacks.

Begging the question, is this confidence unfounded or backed by plans and initiatives?

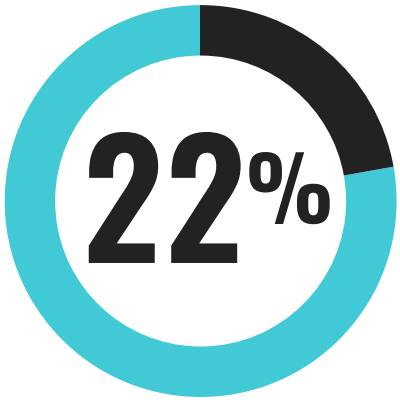
EXECUTIVE CONFIDENCE IN MITIGATING CYBERSECURITY THREATS



[Base: All Senior Decision Makers in SMBs who have transitioned to remote working since COVID-19 outbreak]

BRINGING REMOTE WORK BACK TO REALITY

While respondents feel confident in their cybersecurity competency, upon further scrutiny many are missing the necessary actions to protect their business.



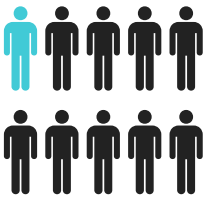
In fact, more than 1 in 5 (22%) senior decision makers agree that their organization transitioned to remote working WITHOUT a clear policy to mitigate or prevent cybersecurity threats/attacks.

Even further, respondents agree that their organization is:

At an increased risk for a cyberattack 17%

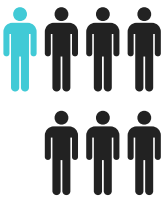
Would not know how to respond to a cyberattack 12%

Was not prepared to work from home securely 13%



Many senior decision makers simply haven't come to the reality with their cybersecurity capabilities.

Just 10% agree they're scared it's only a matter of time until their organization experiences a cyberattack, but **almost 1 in 7 (13%) agree their organization has already experienced at least one cyberattack they are aware of.**



[Base: All Senior Decision Makers in SMBs who have transitioned to remote working since COVID-19 outbreak]

THE FUTURE OF SECURE REMOTE WORK

Social distancing measures could stay in place until 2021/22 meaning cyber-working will continue to be the method businesses must consider how to combat threats immediately.

Respondents agree that their organization needs to:

Invest more in cybersecurity 21%

Create a response plan to a cyberattack 24%

Be better prepared to handle a scenario like this in the future 30%

Implement clear remote work policies to secure our business from cybersecuritythreats when remote working 25%

[Base: All Senior Decision Makers in SMBs who have transitioned to remote working since COVID-19 outbreak]

"Investment in cybersecurity can often feel like a daunting task for small business owners but it's not something that can be overlooked," said Virani. "Only a tenth of respondents felt they needed to hire a cybersecurity expert, which is far too low when we see companies of all sizes falling victim to hackers on a daily basis. Cybersecurity needs must be a paramount component of any business – whether it be completing cyber risk and resilience reviews, cybersecurity training and awareness programs or at a minimum, developing operational policies and procedures for data security, businesses must be taking these initiatives into consideration. alliantgroup is able to offer these services and act as a resource for those businesses not considering an internal team. We have intimate knowledge of SMBs and can act as an integral partner so business leaders can focus on running their organizations with a peace of mind that data and information is secure."

METHODOLOGY

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 507 senior decision makers at companies with 500 employees or less. Fieldwork was undertaken between 7th - 13th April 2020. The survey was carried out online. The figures have been weighted and are representative of all US SDM at companies with 500 employees or less.

ALLIANT
CYBERSECURITY
An alliantgroup Company

AlliantCybersecurity.com | 1-877-842-9237

BE AWARE. BE SECURE.