THE STATE OF CYBERSECURITY IN CENTRAL VIRGINIA

OCTOBER 2018

brought to you by

THE CHAMBER
Charlottesville Regional Chamber of Commerce

advanced network systems

ABOUT THIS SURVEY

The Charlottesville Regional Chamber of Commerce is pleased to present the results of our second annual benchmark study, *The State of Cybersecurity in Central Virginia 2018,* co-sponsored by Advanced Network Systems, Inc.

This report provides insights into: (a) the perceptions of regional business owners, executives and other professionals, regarding the state of cybersecurity threats in general and, (b) how their organizations are prepared to combat the growing number and variety of attacks. Survey respondents came from both the Chamber membership community and the regional community at large. This year's information was compiled from survey responses of 110 participants, from organizations with employee headcounts from less than 50 to over 1,000.

Industry analysts are unanimous in their assessments that, when it comes to the volume, prevalence and sophistication of cyberthreats, we are moving into an ever-more dangerous year to come. We know that cyberthreats, and their negative impact on organizations, are a global issue; *but they are also a local issue*. Regardless of industry sector, geographic location, or size, all organizations must increase their cybersecurity focus to protect their data, operations, and reputation.

As you read this report, you'll get a glimpse into how the Greater Charlottesville business community is dealing with the issue of cybersecurity—how many organizations report having experienced some form of cyber incident, how they view their level of risk, and what steps they are taking to protect themselves from known and unknown threats.

EXECUTIVE SUMMARY

Among respondents, 53% reported being the victim of one or more attacks within the past five years. This figure is down slightly from last year's reporting of 57% and remains generally in line with statistics reported for small and medium-sized organizations overall.[1] Of note is the number of "Don't Know" responses to this question which rose from 7% in 2017, to 18% in the current year.

Once again, 2018 respondent's perceptions of the dangers and risks cyberattacks pose in general, appear to be incongruent with what they believe actually applies to their own organizations. In terms of turning cybersecurity threat awareness into action, responses continue to suggest a disconnect between what respondents know is "possible," and what they think is "probable" within their own operating environments.

An example of this is that 79% of respondents reported that they believe cybercrime will be a bigger threat to organizations overall in the coming year (up from 72% in 2017). Yet, at the same time, 81% of respondents believe cybercrime is only a moderate or low risk to their organization (on par with 82% in 2017). The disconnect is further emphasized when we see that 64% of respondents reported that their security budget won't increase in the coming year while, at the same time, only 36% reported feeling either very confident or extremely confident about being able to defend against an attack.

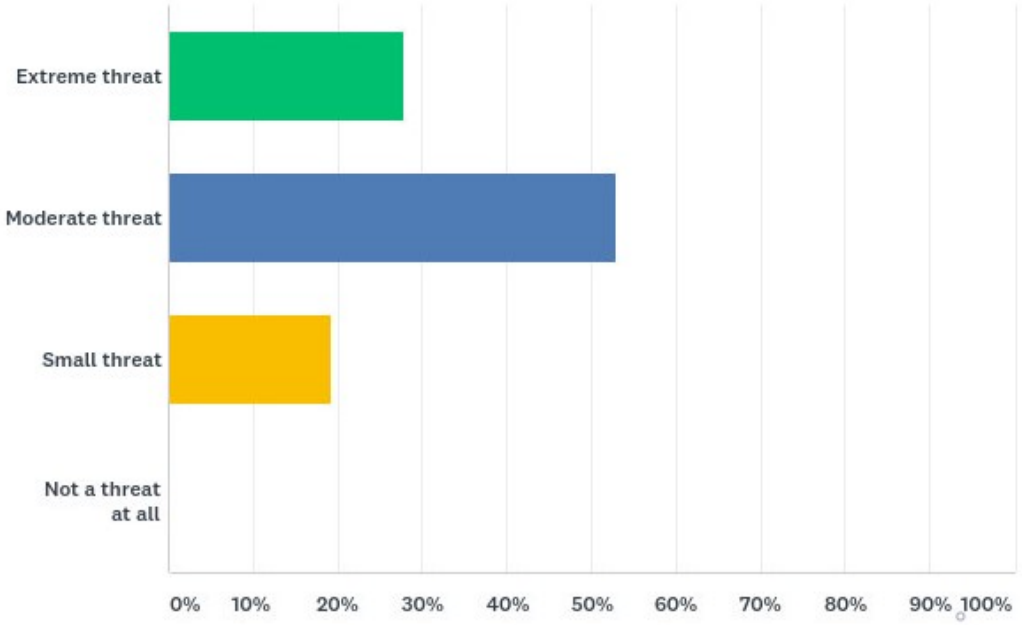
In terms of the predicted business disruption caused by a cyberattack, 40% of respondents felt it would take more than a day to recover from a cyberattack (down from 44% in 2017), with an additional 23% unsure about how long a recovery would take (up from 14% in 2017). Overall, the responses to this question may be overly optimistic given that Intermedia's latest ransomware report found that almost two-thirds of organizations could not access their data for at least two days following an attack, and 32% lost access for five days or more.[2]

When responding to the question of what the biggest obstacles are to improving cybersecurity defenses, 39% of participants responded: uncertainty over the right solution (up 27%), 31% said lack of budget (up 10%), and 30% responded a lack of understanding of exposure and risks (up 16%).

Two new questions posed this year revealed that only 33% of respondents reported having a cyber liability insurance policy. Also, of note, is that 81% of participants responded that they would like to see The Chamber do more to inform, educate and otherwise support their cybersecurity efforts.

1 Verizon 2018 Data Breach Investigation Report
2 https://www.intermedia.net/report/ransomware

How significant a threat do you believe cybercrime is to your organization?

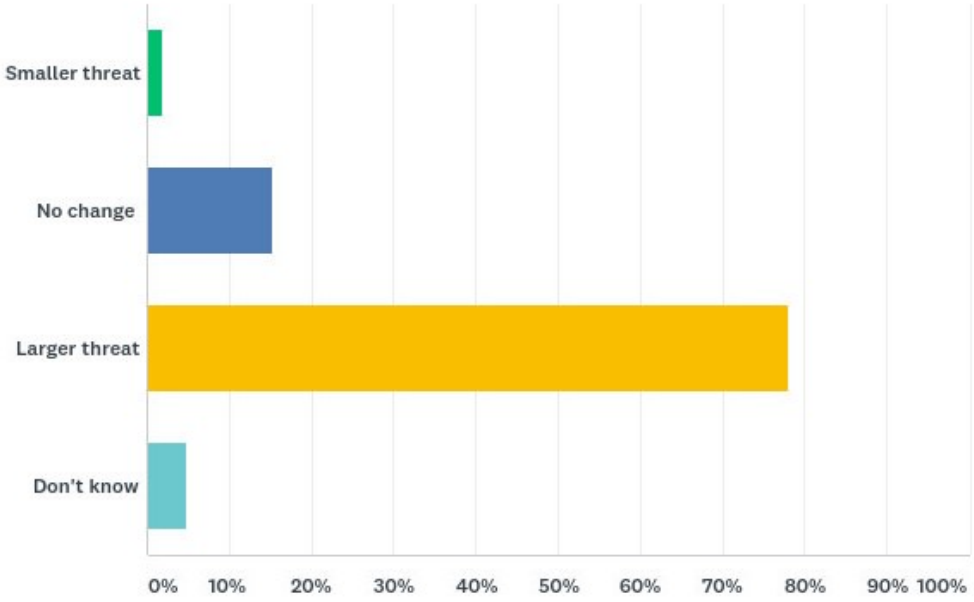


81%

Up 1% from 2017

responded that they believe cybercrime is only a moderate or small threat to their organization

In the next 12 months, do you think cybercrime will be a larger or smaller threat to organizations?



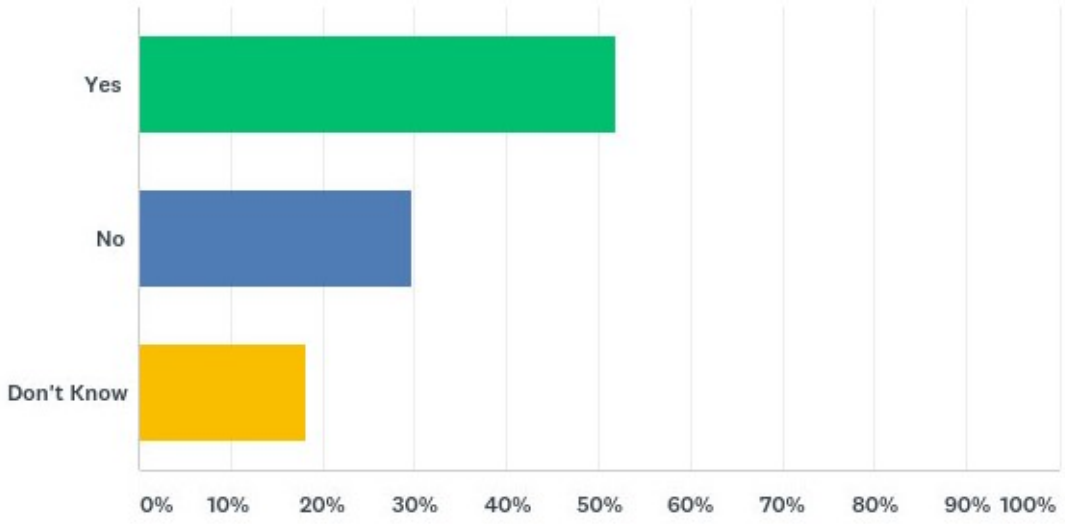
79%

of respondents think cybercrime will be a bigger threat in the coming year

Up 7% from 2017

Has your organization experienced one or more cyberattacks in the past 5 years?

This includes having one or more of your systems infected with viruses, spyware, ransomware or any other type of malicious software OR the hack (break-in) of a computer system, stored data or web site.



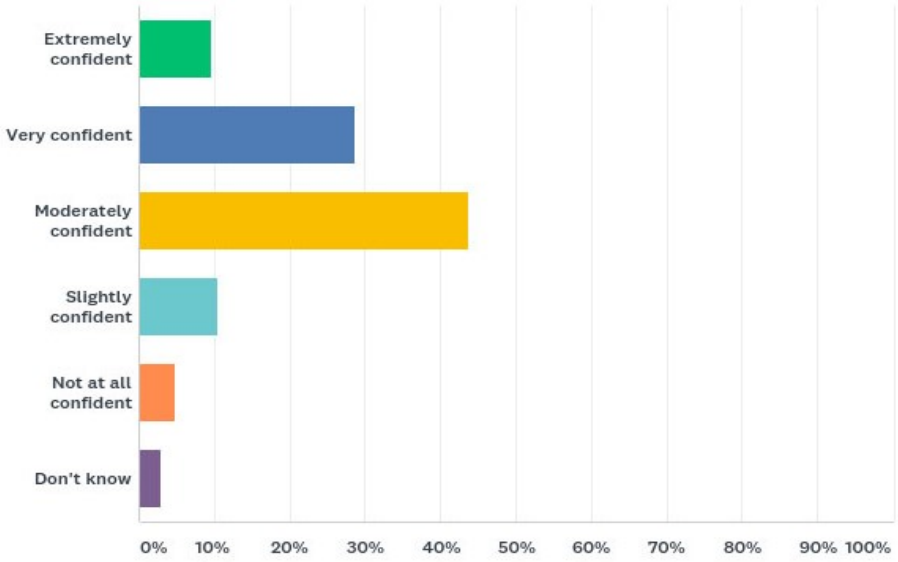
53%

of respondents reported at least one cyber-related attack in the past five years

Down 4% from 2017

"Don't Know" response rose from 7% to 18%

How confident are you that your organization's defenses are capable of detecting and blocking a computer hack or malicious software before it affects critical systems and files?

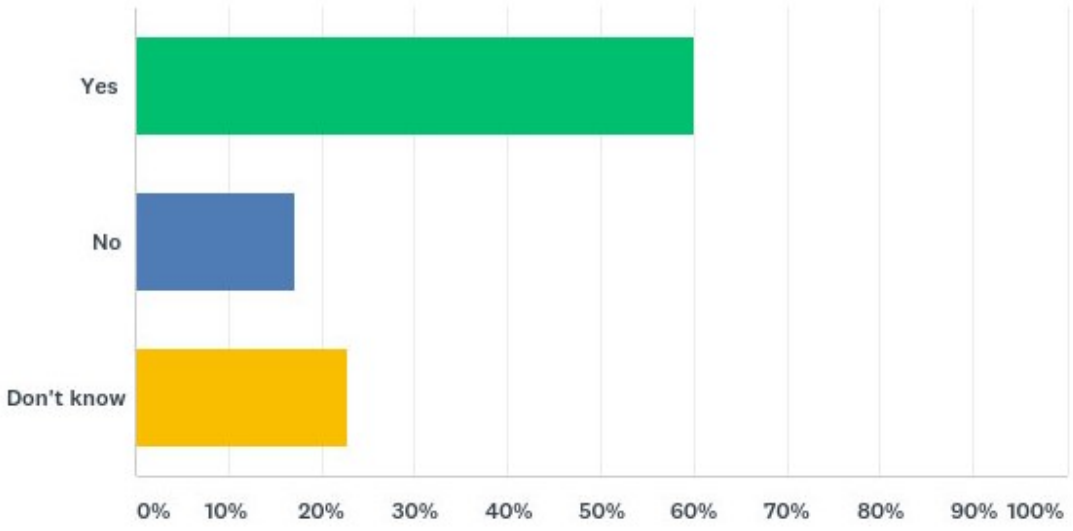


38%

of respondents reported feeling highly confident about the ability to defend against an attack

Up 3% from 2017

Does your organization have a response plan in place to detect, contain and recover from a cyberattack?



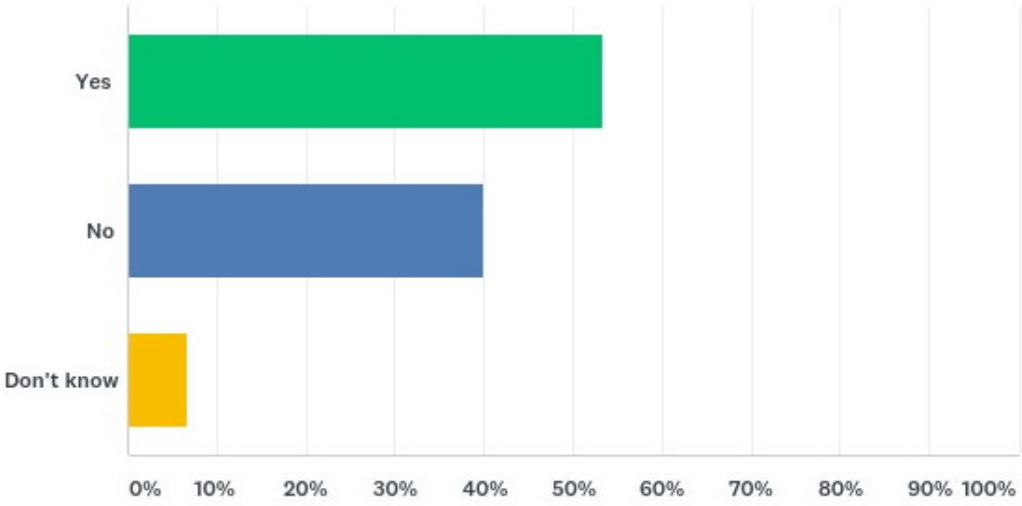
40%

responded they either don't have a cyber incident response plan, or don't know if they have one

Up 6% from 2017

"Don't Know" response rose from 7% to 22%

Does your organization have a training program in place to educate employees and raise awareness for defense against cyberattacks that come in through their workstations, laptops and mobile devices?

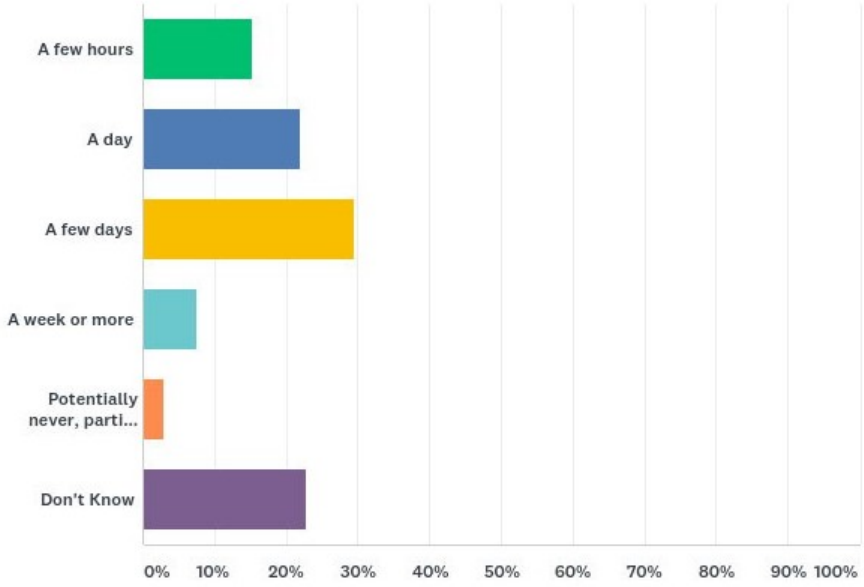


47%

Down 1% from 2017

of respondents say employees are not trained to defend against cyberattacks

How quickly do you think your organization would be able to recover if hit by a cyberattack?



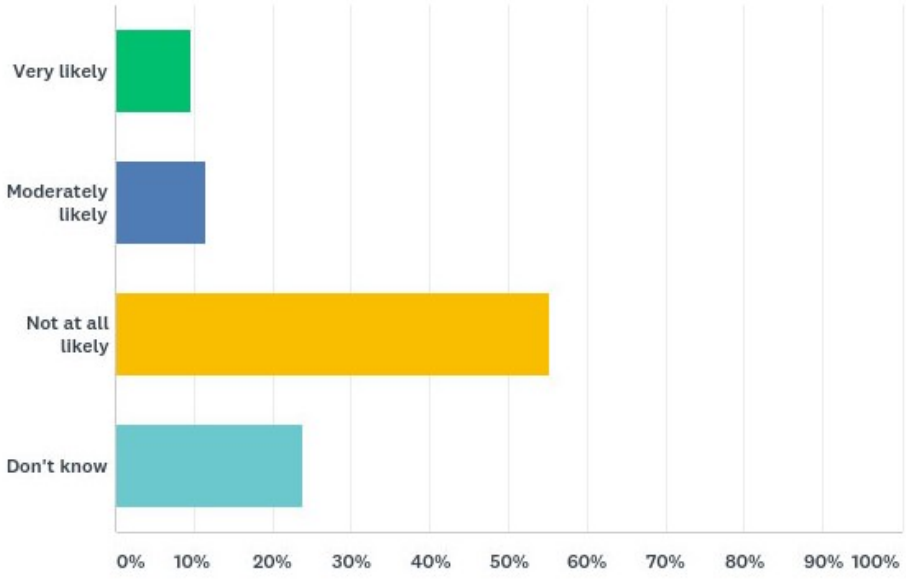
40%

of respondents predict
it would take more than a day
to recover from an attack

Down 4%
from 2017

How likely is your organization to pay for recovering data affected from a ransomware attack?

Ransomware is a type of cyberattack where malicious software enters a computer system and effectively blocks access to computer information (holds it hostage) until a "ransom" fee is paid.

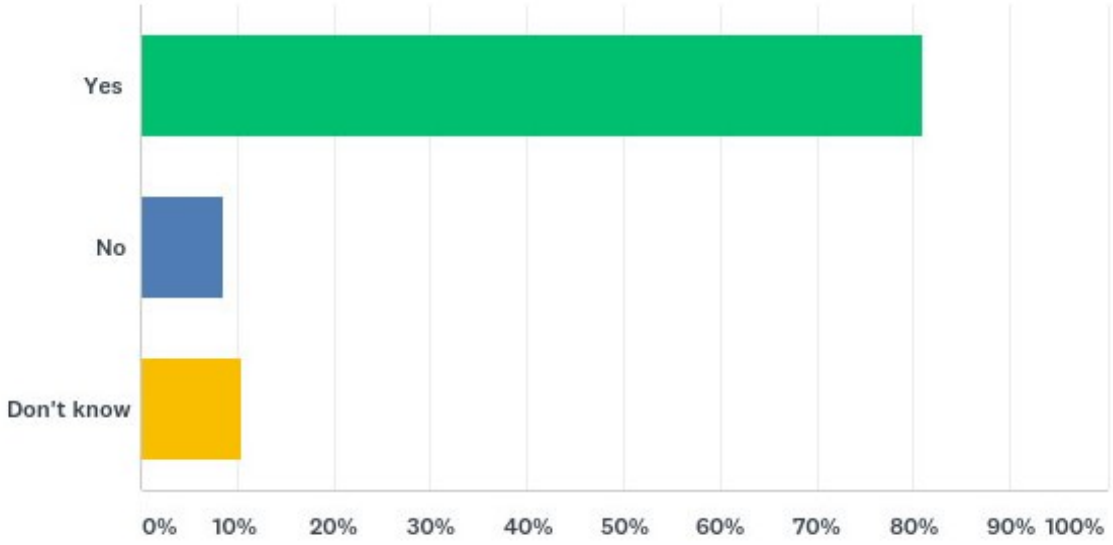


56%

responded that they would not pay ransom to recover their data

Down 4% from 2017

Does your organization have a data backup and recovery strategy that is tested on a regular basis?

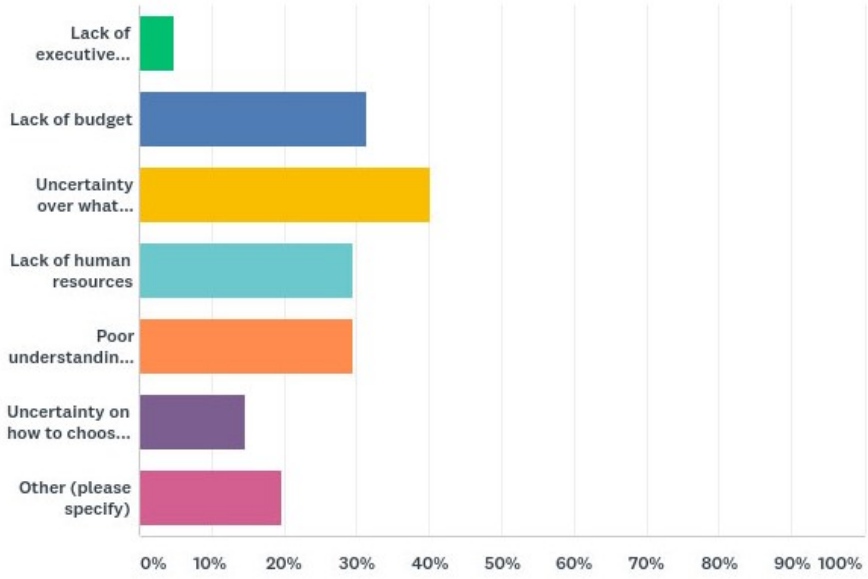


81%

of respondents have a backup and recovery strategy in place

Down 1% from 2017

What do you think is your organization's biggest obstacle to improving its cybersecurity defenses?



39%

responded uncertainty over the right solution

Up 27% from 2017

31%

responded lack of budget

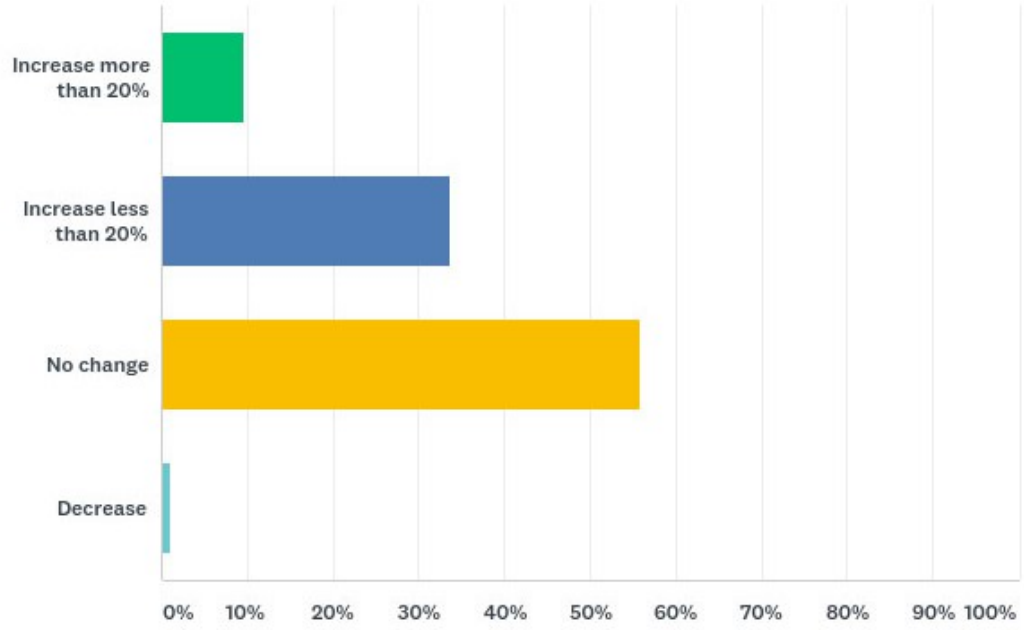
Up 10% from 2017

30%

responded lack of understanding of risks

Up 16% from 2017

How do you expect your organization's budget for cybersecurity to change in the next 12 months?

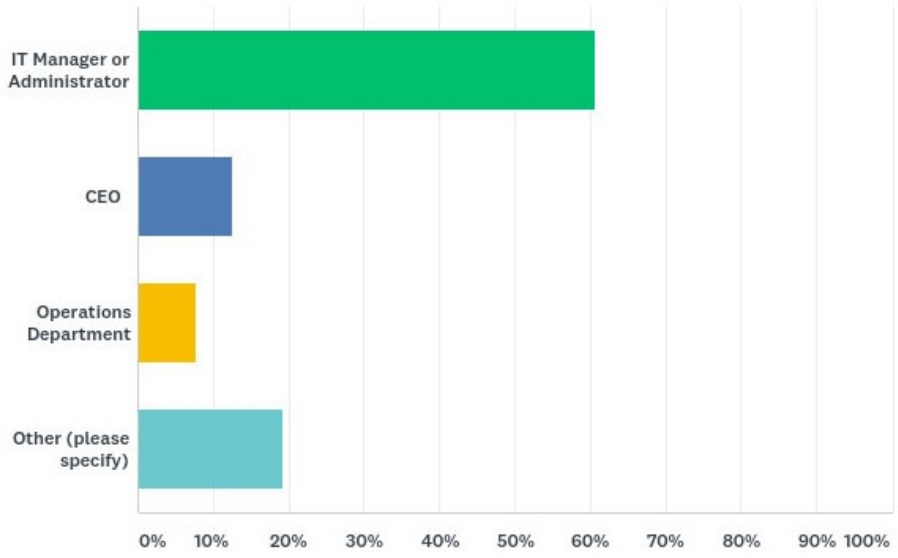


44%

responded that their security budget will increase in the next year

Up 11% from 2017

Who in your organization is responsible for protecting against cyberattacks?

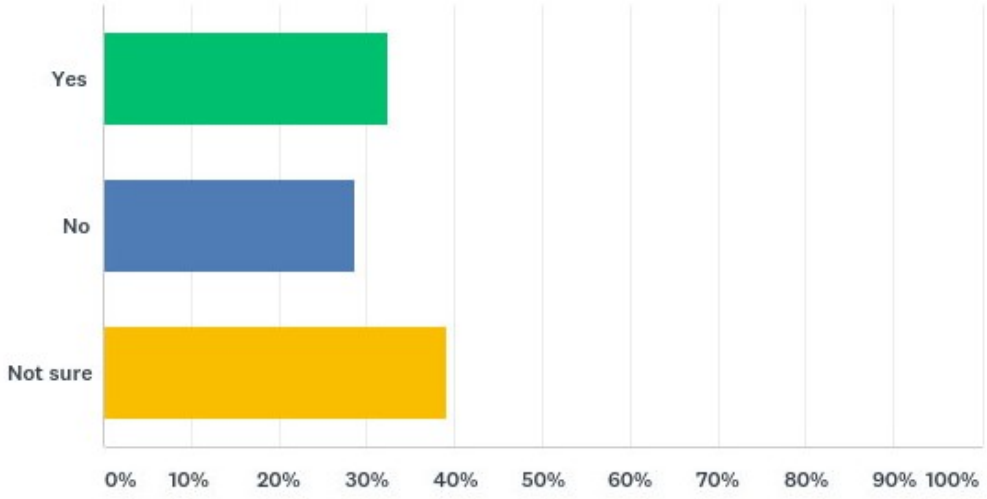


39%

responded that someone other than an IT Manager or IT Administrator is responsible for cybersecurity

Down 13% from 2017

Does your organization have a cyber liability insurance policy?

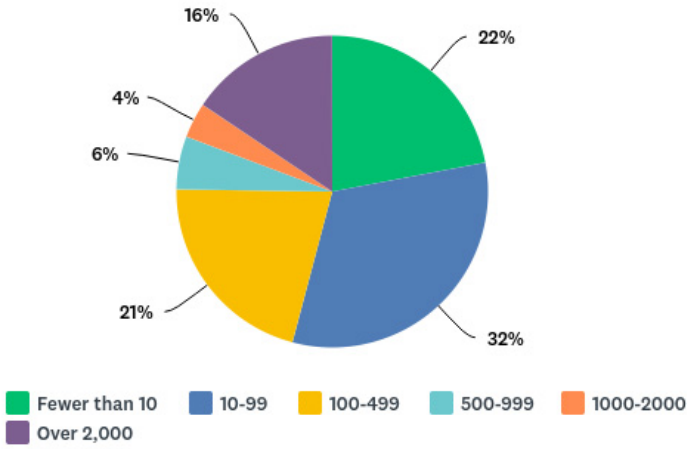


33%

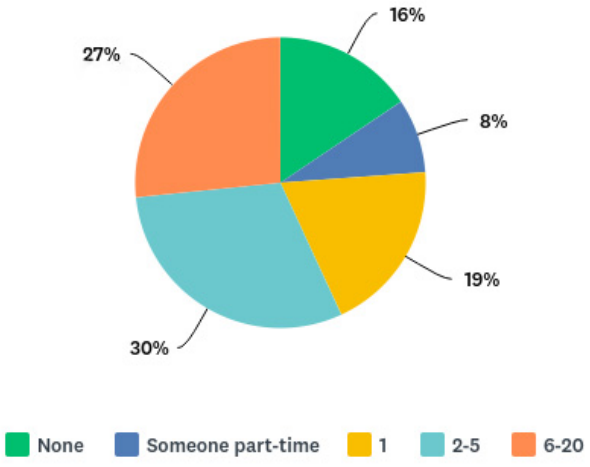
responded that they had
a cyber liability insurance policy

Respondent's Organizational Profile

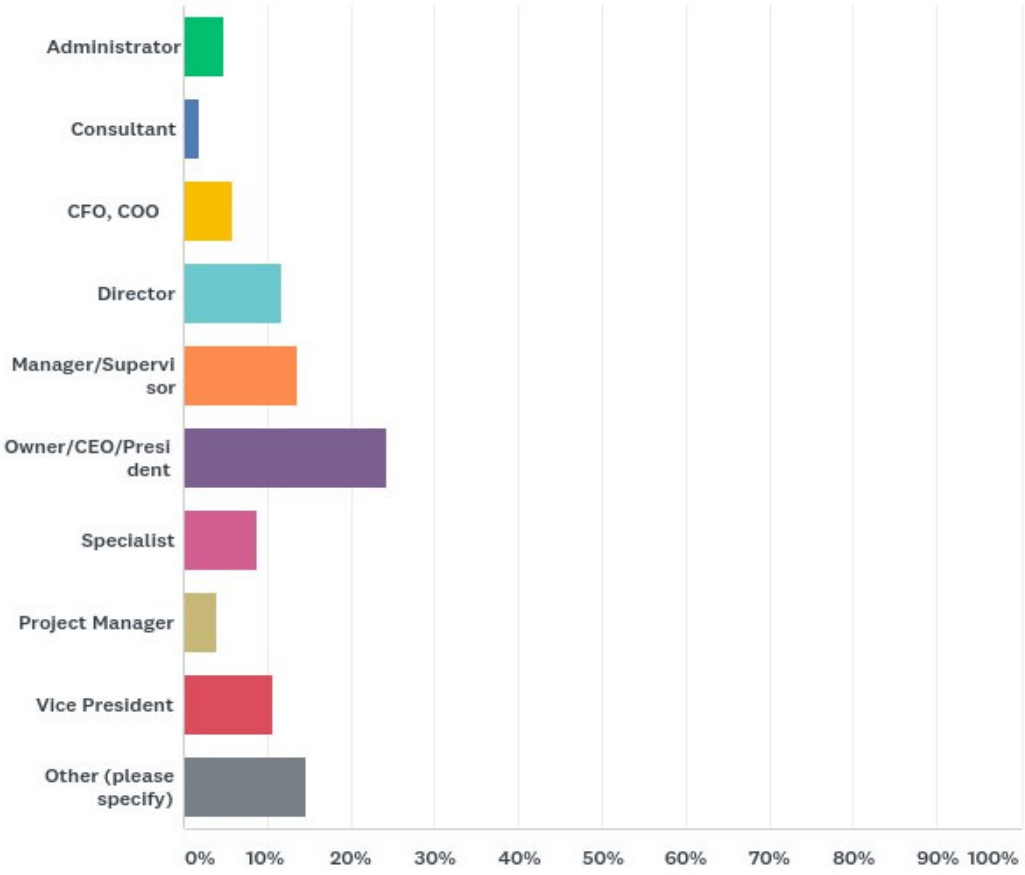
Number of Employees



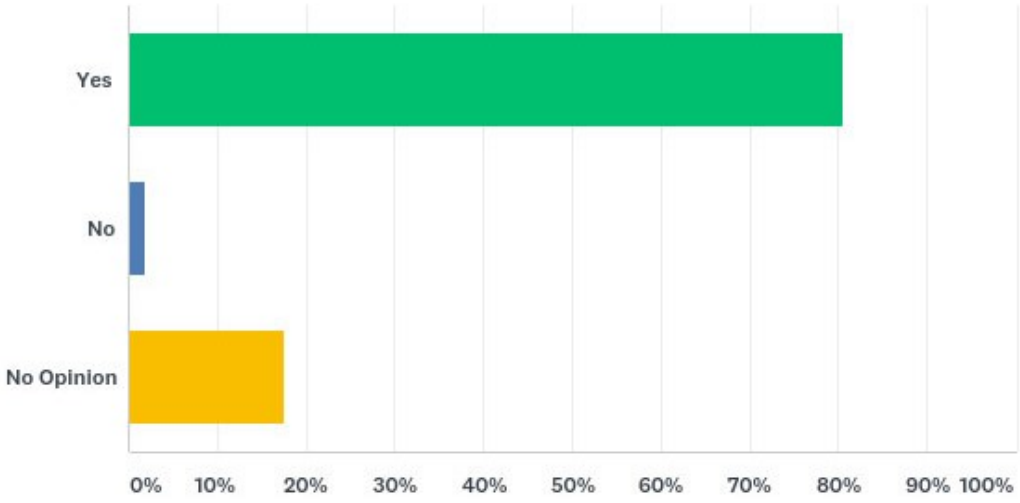
Number of IT Staff



Respondent's Professional Profile



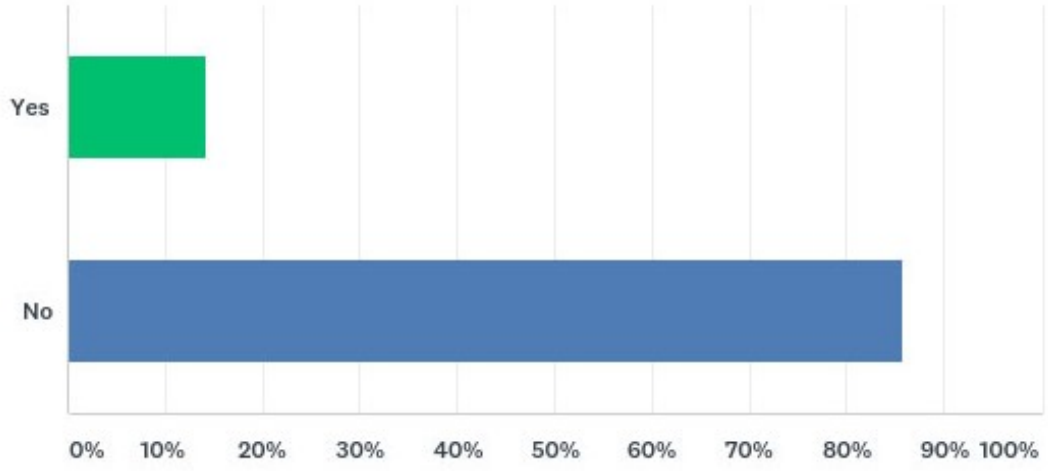
Would you like to see The Chamber do more to inform, educate and otherwise support the cybersecurity efforts of regional organizations?



81%

responded that they would like additional information and support from The Chamber

Did you participate in this cybersecurity survey last year?



85%

responded that they had not participated in the 2017 survey

The Chamber would like to recognize the following organizations for their support of this project:

advanced network systems

University of Virginia

Extreme®
Connect Beyond the Network