



## Department of Commerce

Division of Securities  
77 South High Street, 22nd Floor  
Columbus, Ohio 43215-6131  
Telephone (614) 644-7381

# Cybersecurity Practices of Ohio Investment Advisers; A Summary of Survey Responses

October 2014

## A Pilot Survey to Compile Cybersecurity Information

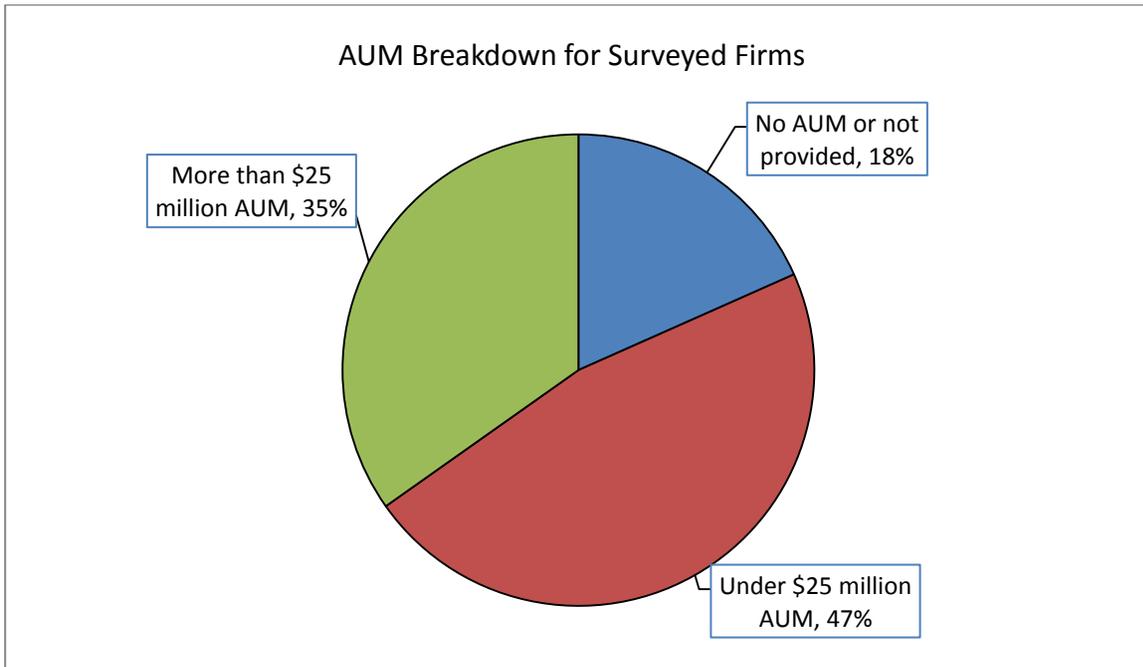
In July 2014, the Ohio Division of Securities participated in the North American Securities Administrators Association's ("NASAA") pilot cybersecurity project. For this project, NASAA worked with state securities regulators to utilize a template survey sent to state-licensed investment advisers in order to elicit information about the technology and data practices of that registrant population. A compilation of results of NASAA's survey can be found at: [www.nasaa.org/industry-resources/investment-advisers/nasaa-cybersecurity-report/](http://www.nasaa.org/industry-resources/investment-advisers/nasaa-cybersecurity-report/).

For its effort, the Ohio Division of Securities surveyed over 500 Ohio-domiciled, state-licensed investment advisers. This report summarizes the 266 responses received. The Division thanks our investment adviser community for dedicating their time and insight to provide thorough, thoughtful, and timely responses. The Division also thanks NASAA for its support in conducting and compiling this important survey.

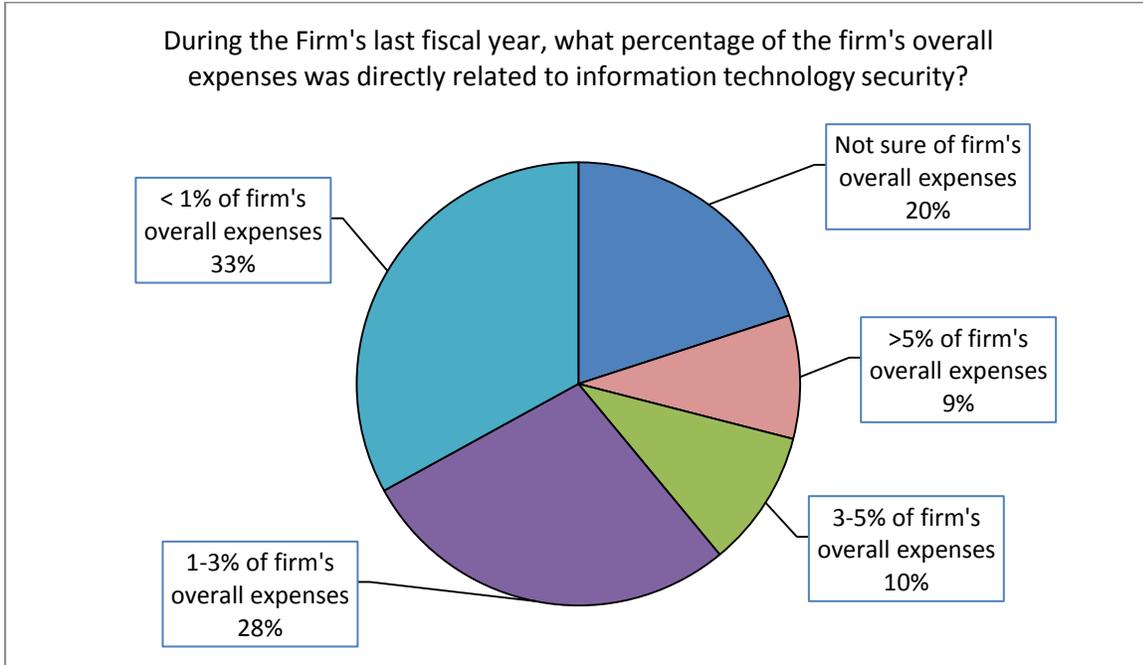
### Ohio Pilot Project Survey Results:

- Only 3% of responding firms indicated they had experienced a cybersecurity incident and even fewer, less than 1%, indicated they had experienced theft, loss, unauthorized exposure, or unauthorized use of, or access to, confidential information.
- The majority of responding firms (87%) use computers, tablets, smartphones, or other electronic devices to access client information.
- 88.9% of responding firms use e-mail to contact clients. Only 54% of those firms, however, use secure e-mail.
- Of those that use e-mail to contact clients, 45% of responding firms have procedures in place to authenticate instructions received from their clients electronically.
- 62% of responding firms report undergoing a cybersecurity risk assessment. The frequency of these assessments varied widely.
- Less than half of responding firms (40%) report having policies and procedures or training in place related to cybersecurity. Similarly, 44% of responding firms report having policies and procedures or training related to the disposal of electronic data storage devices. Only one third of reporting firms (32%) have policies, procedures, or training programs designed to detect unauthorized activity on their networks or devices.

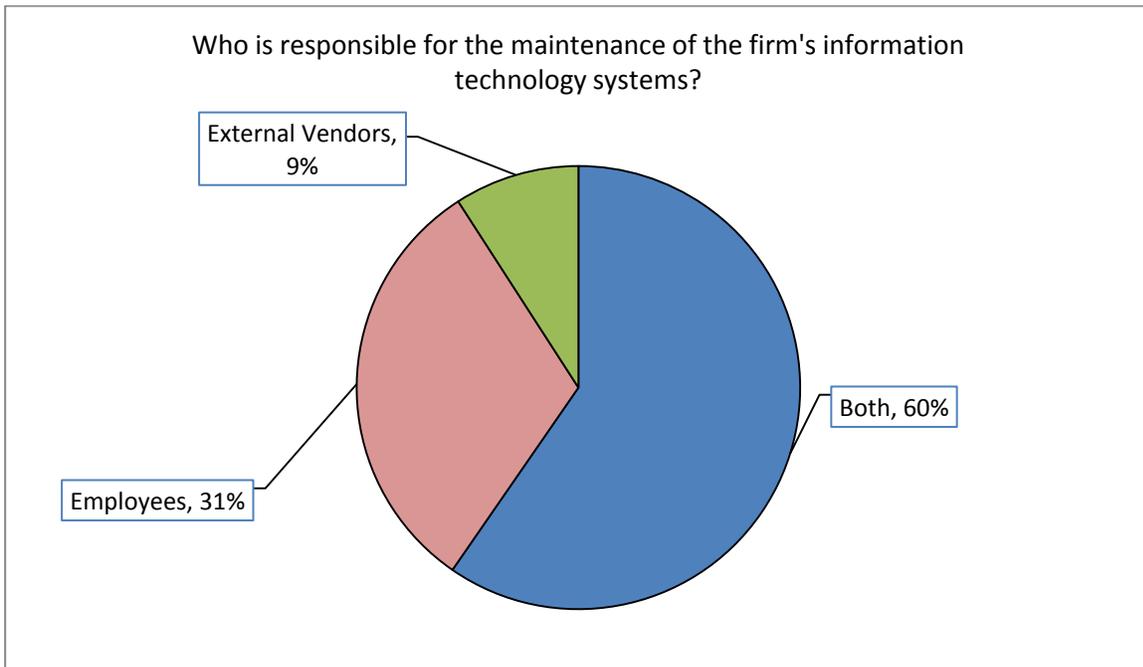
## Survey Results



## Expenses Directly Related to Information Technology Security

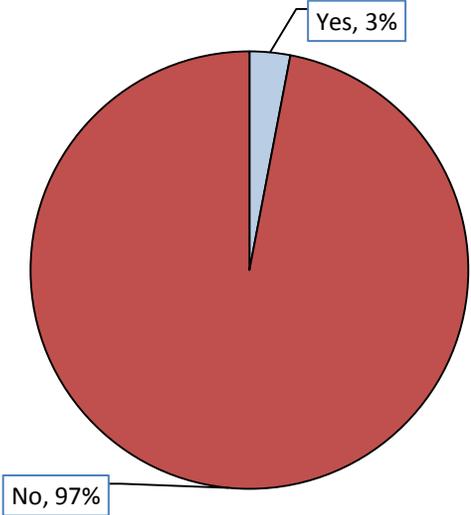


## Maintenance of the Firm's Information Technology Systems



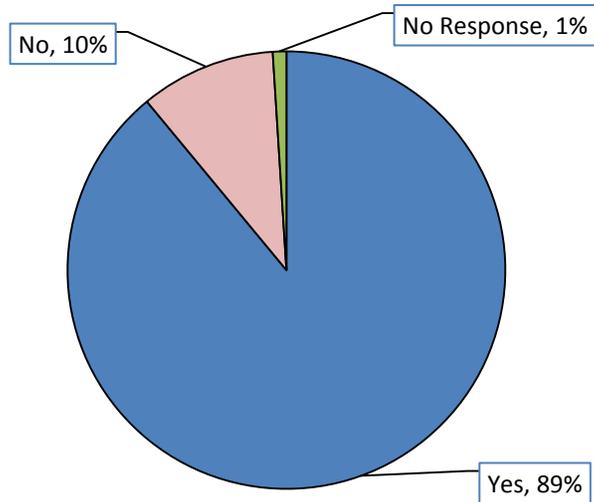
# Rate of Cybersecurity Incidents

Has the firm experienced a cybersecurity incident during its registration in the jurisdiction in which it is registered?

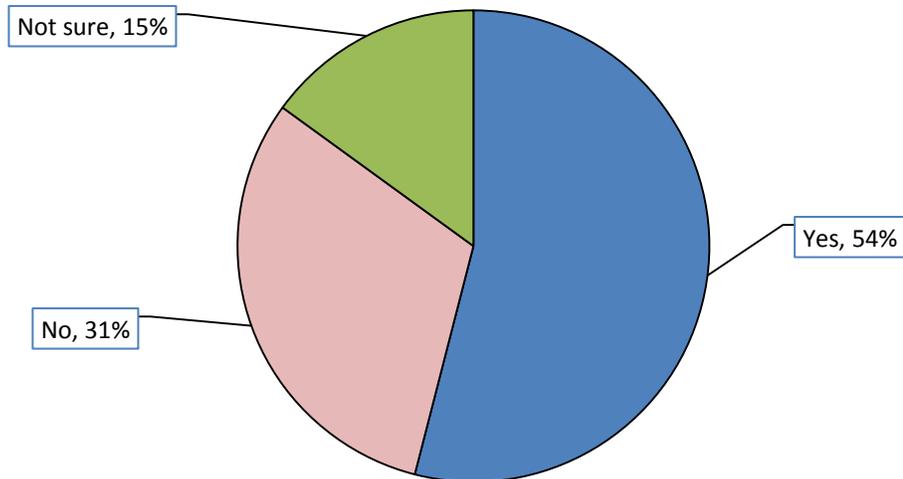


## Client Contact via Email & Use of Secure E-mail

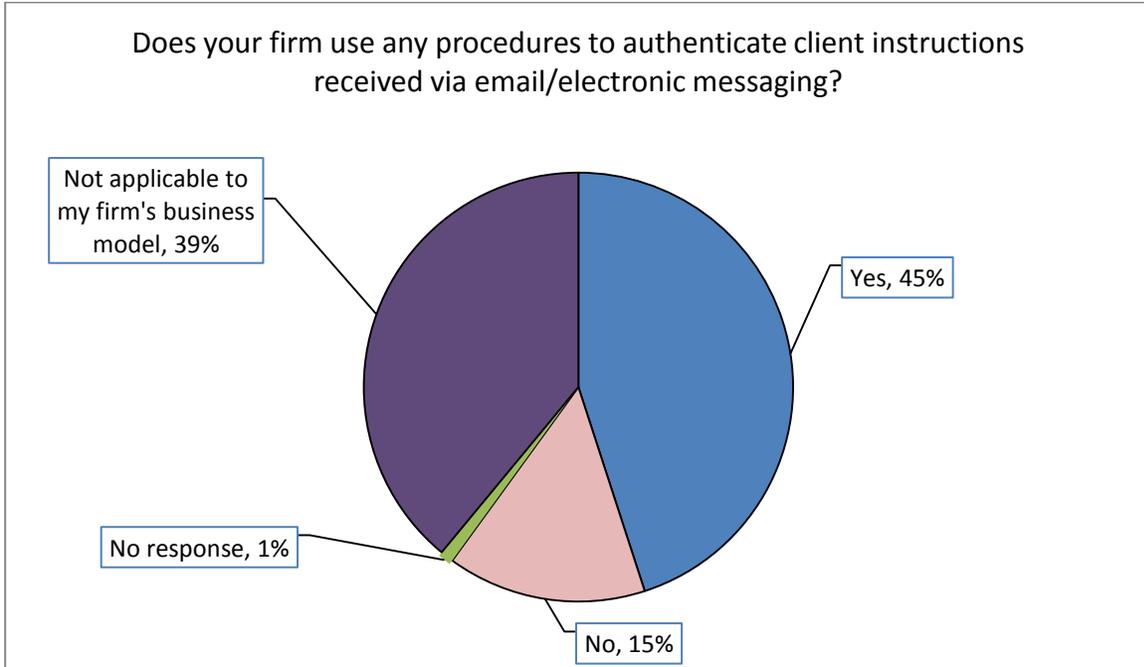
Does your firm contact clients via e-mail or other electronic messaging?



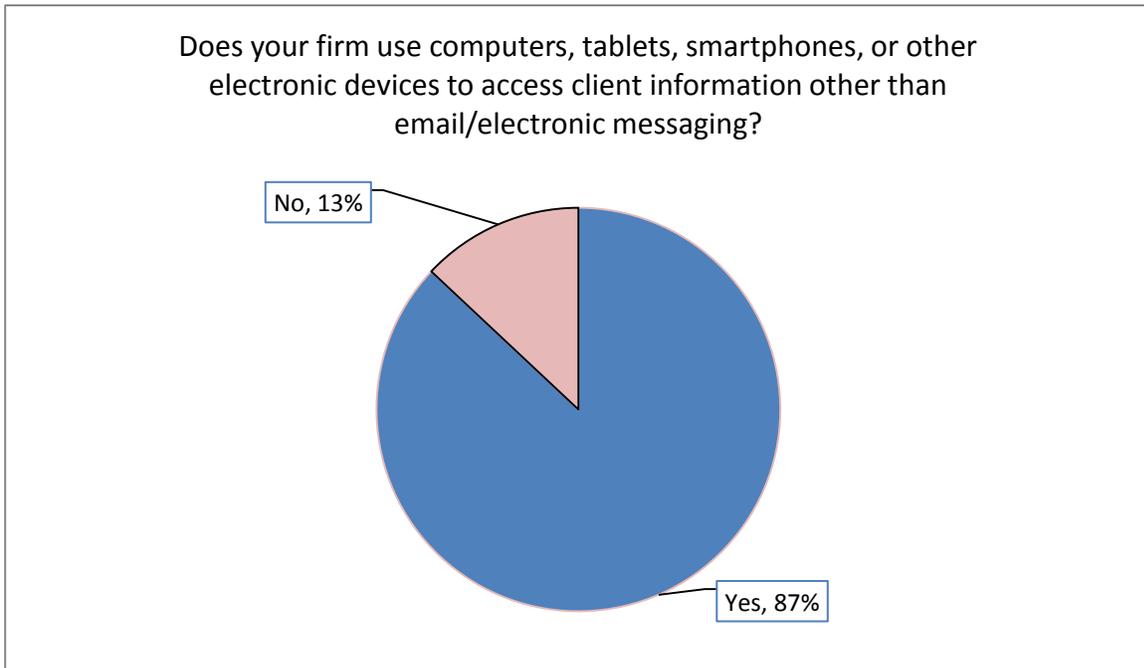
If yes, does your firm use secure email?



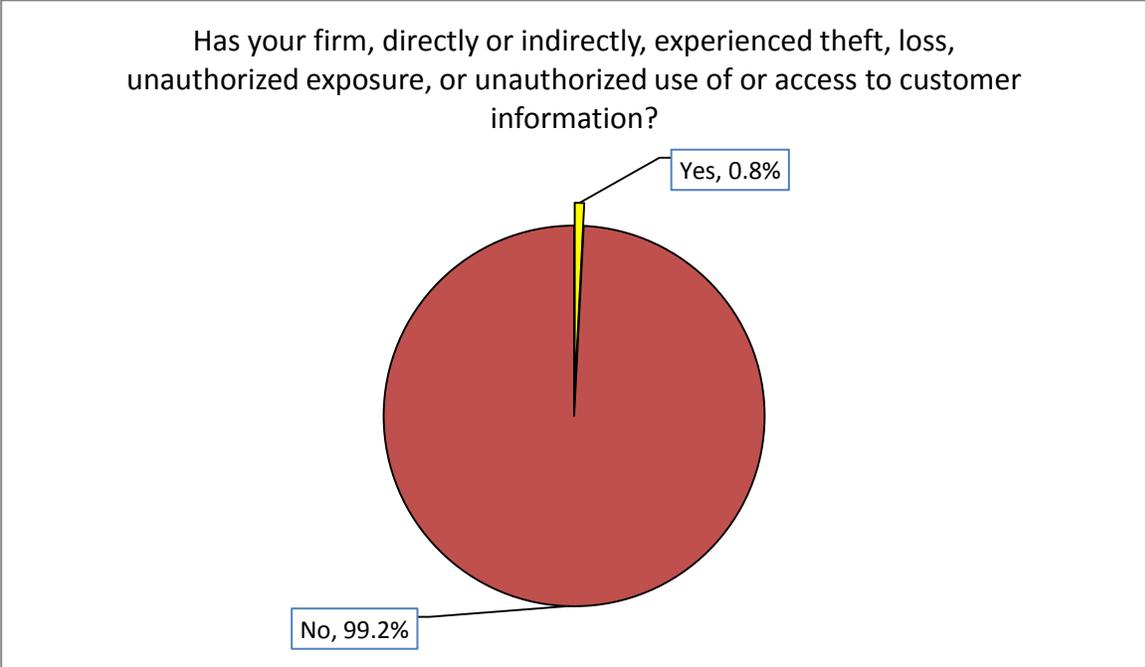
## Authentication of Client Instructions Received Electronically



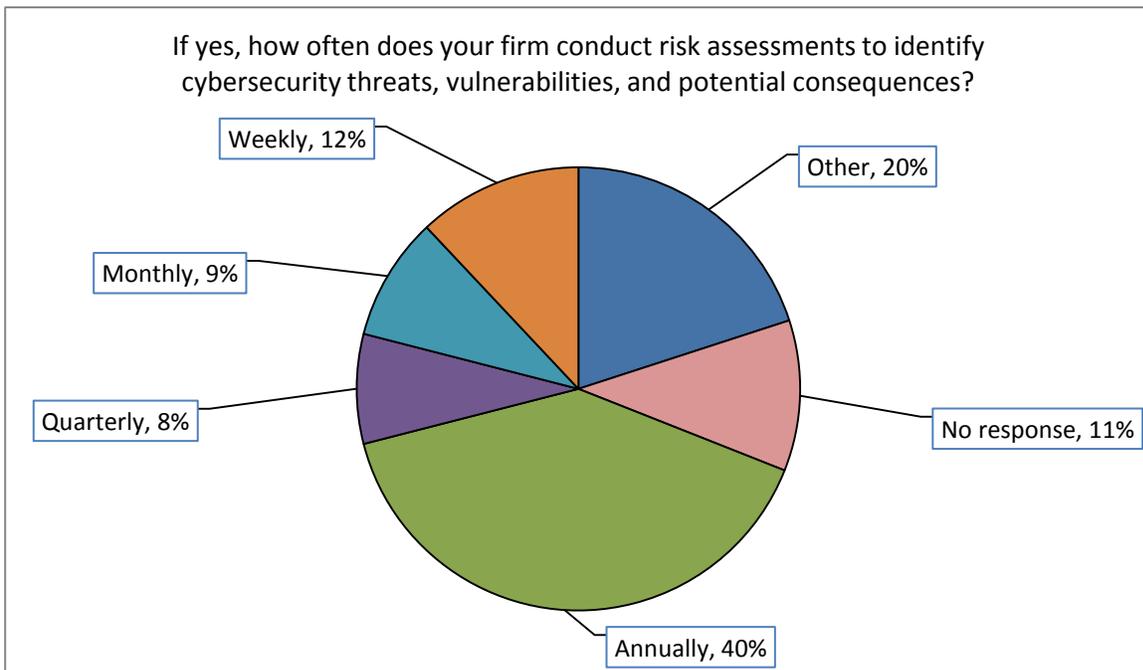
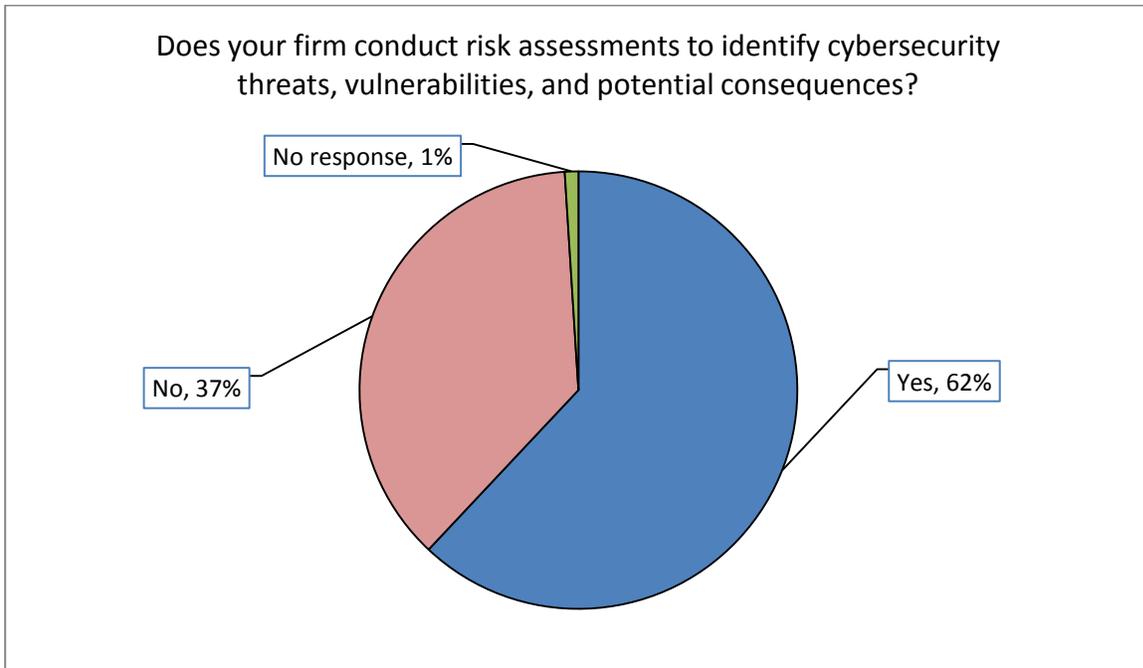
## Devices Used to Access Client Information



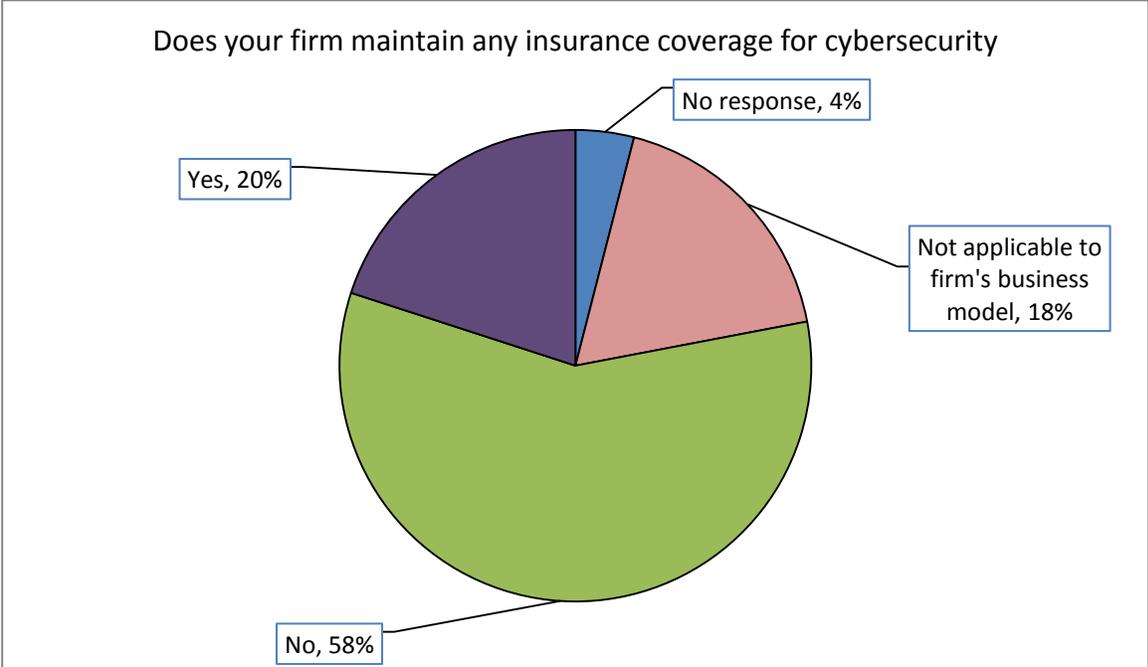
## Unauthorized Use or Access to Customer Information



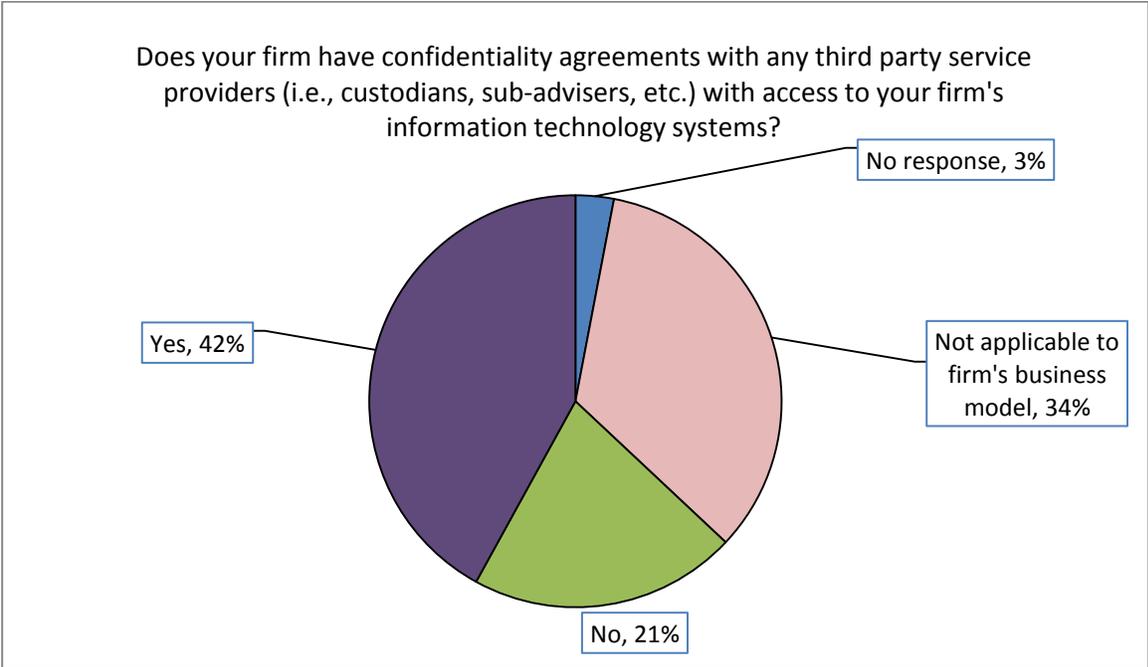
## Risk Assessments Related to Cybersecurity & Frequency Risk Assessments



### Insurance Coverage for Cybersecurity

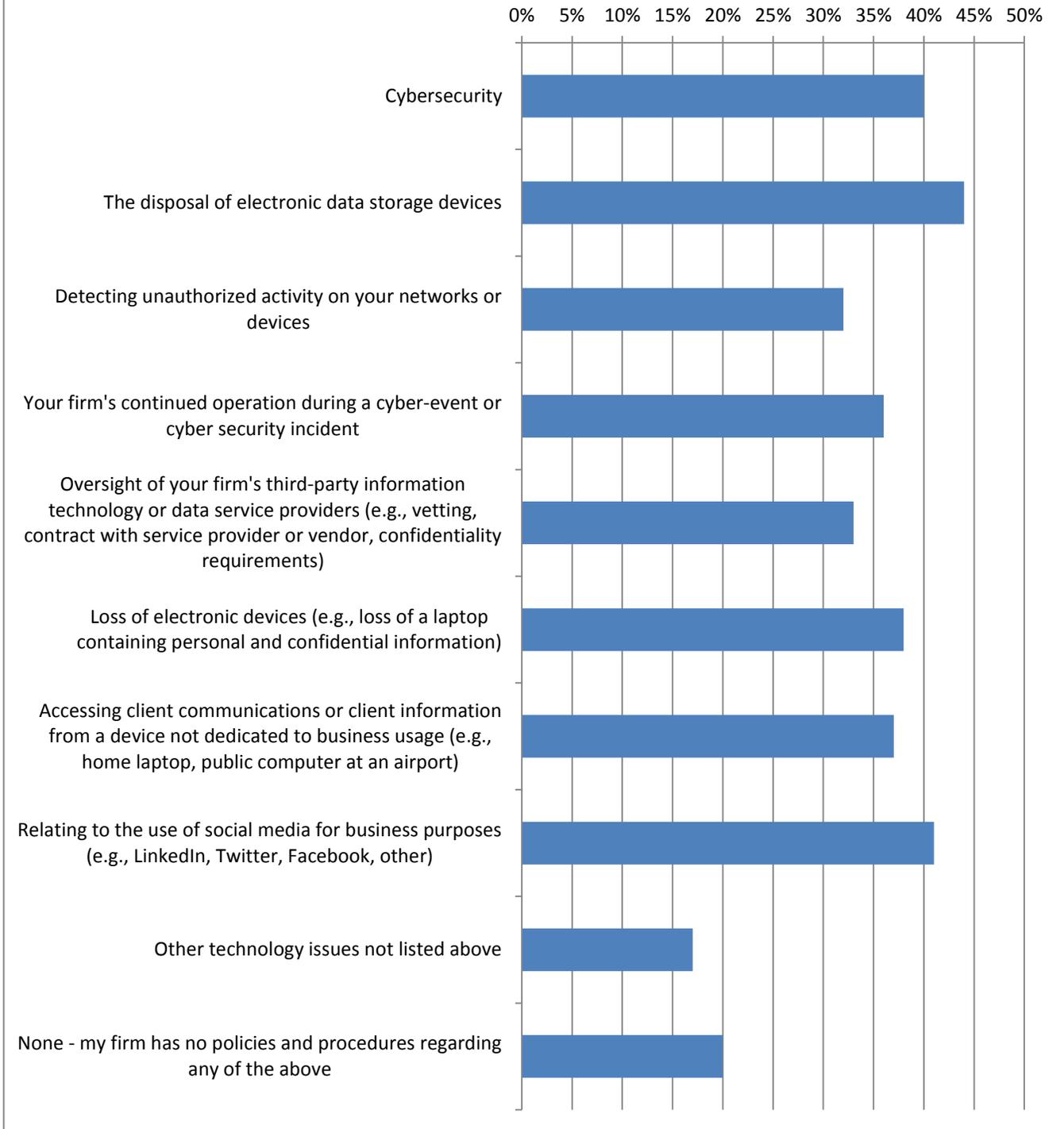


### Confidentiality Agreements with Third Party Service Providers with Access to Firm IT Systems



## Policies, Procedures, and Training Programs

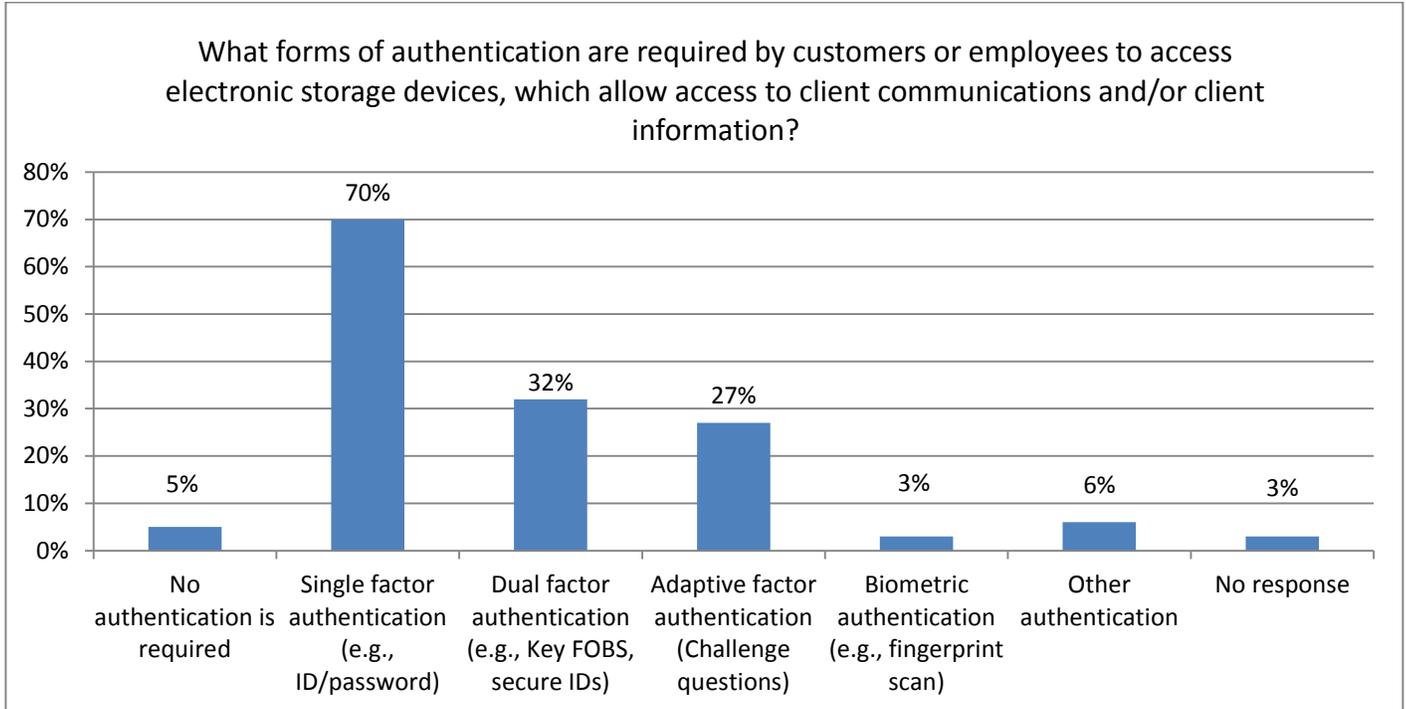
Does your firm have policies and procedures or training programs in place regarding any of the following?



1

<sup>1</sup> Note: this question required that respondents check all categories that applied.

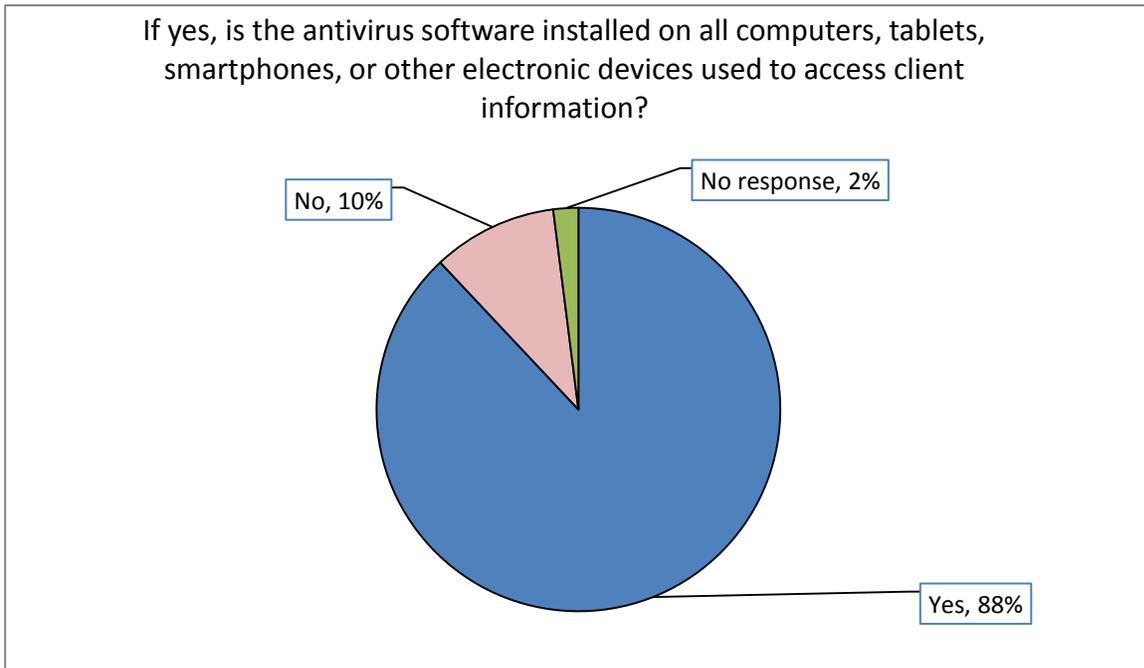
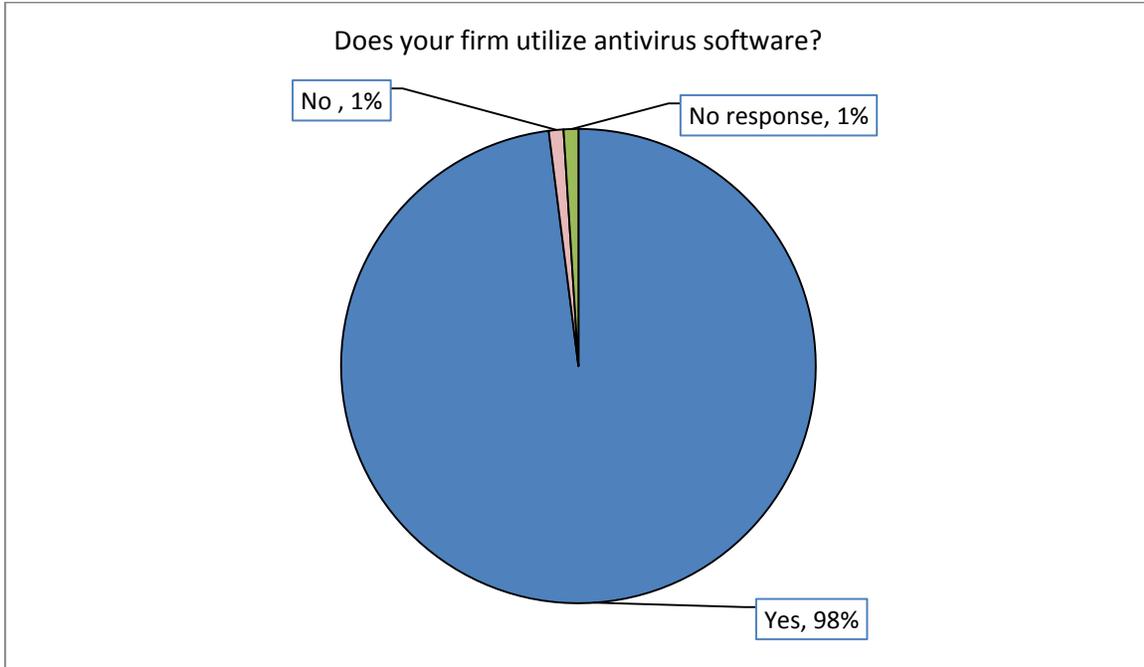
## Authentication Practices



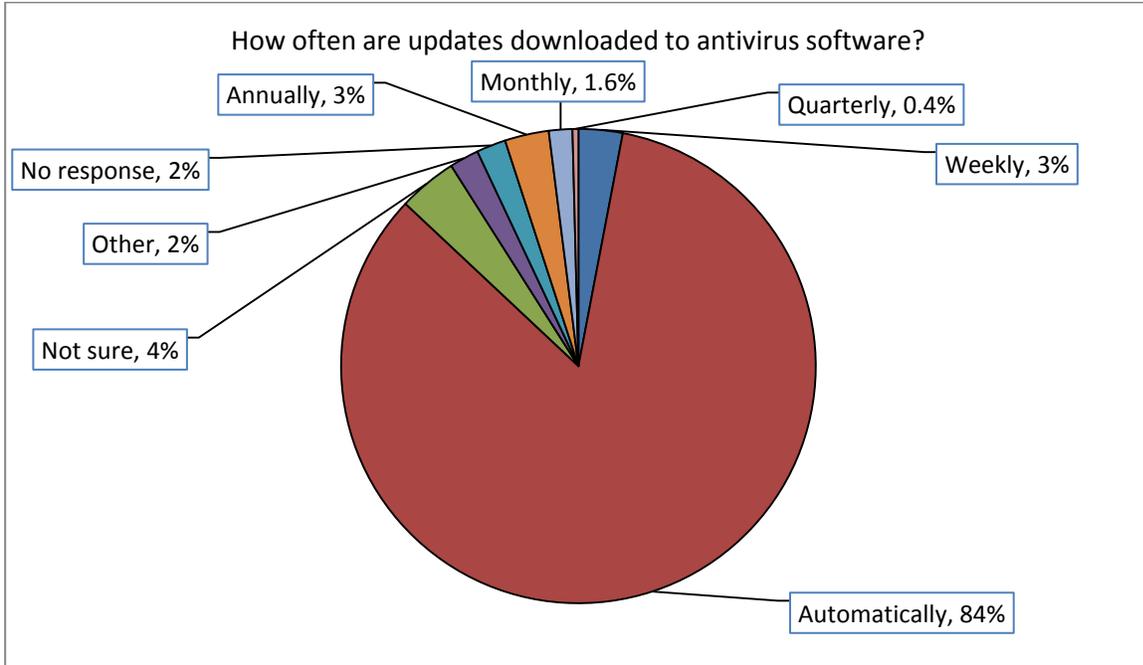
<sup>2</sup>

<sup>2</sup> Note: this question required that respondents check all categories that applied.

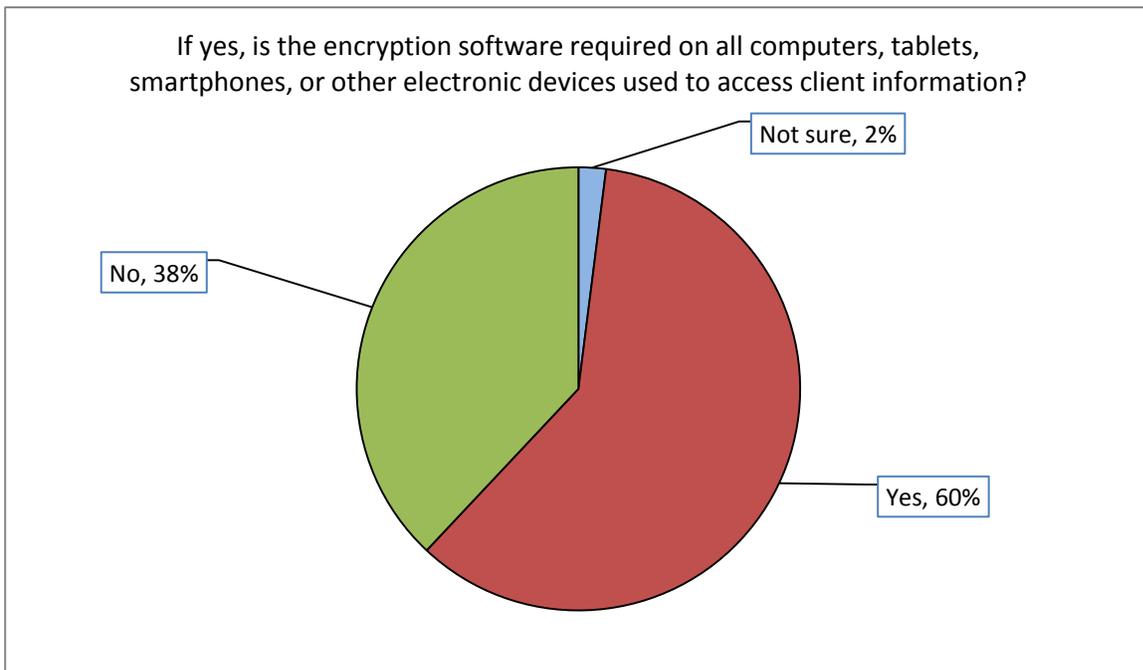
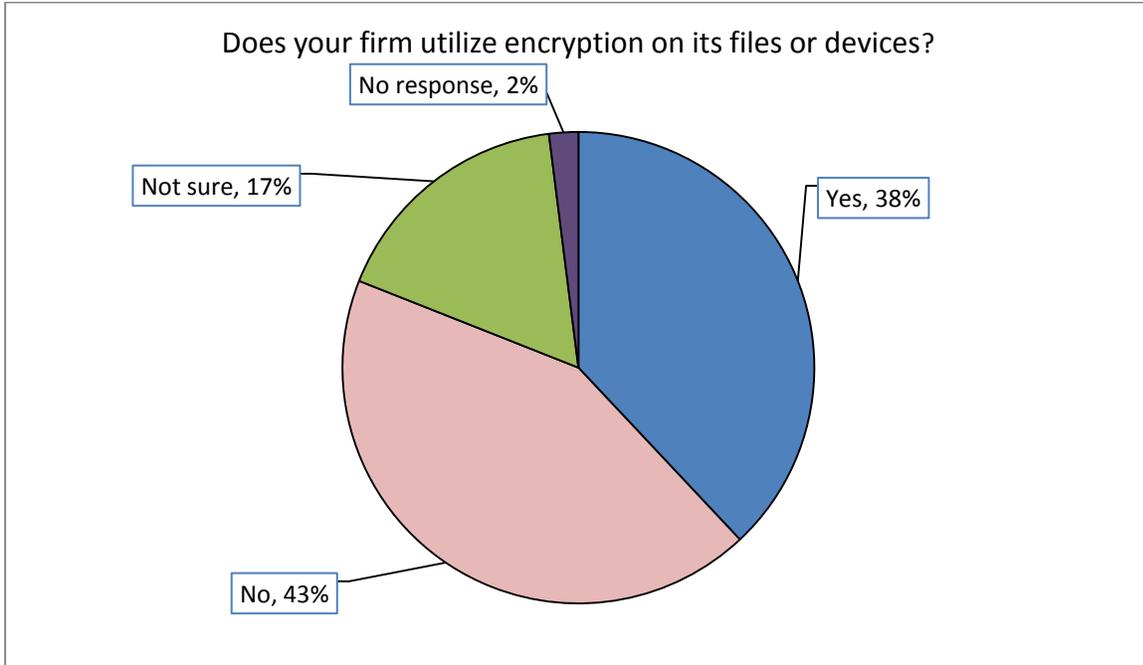
## Use of Antivirus Software



## Frequency of Antivirus Updates

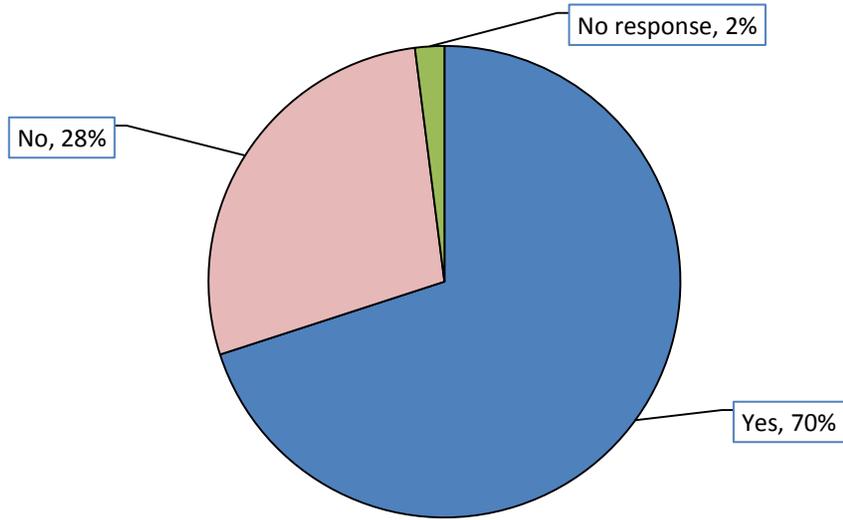


## Use of Encryption

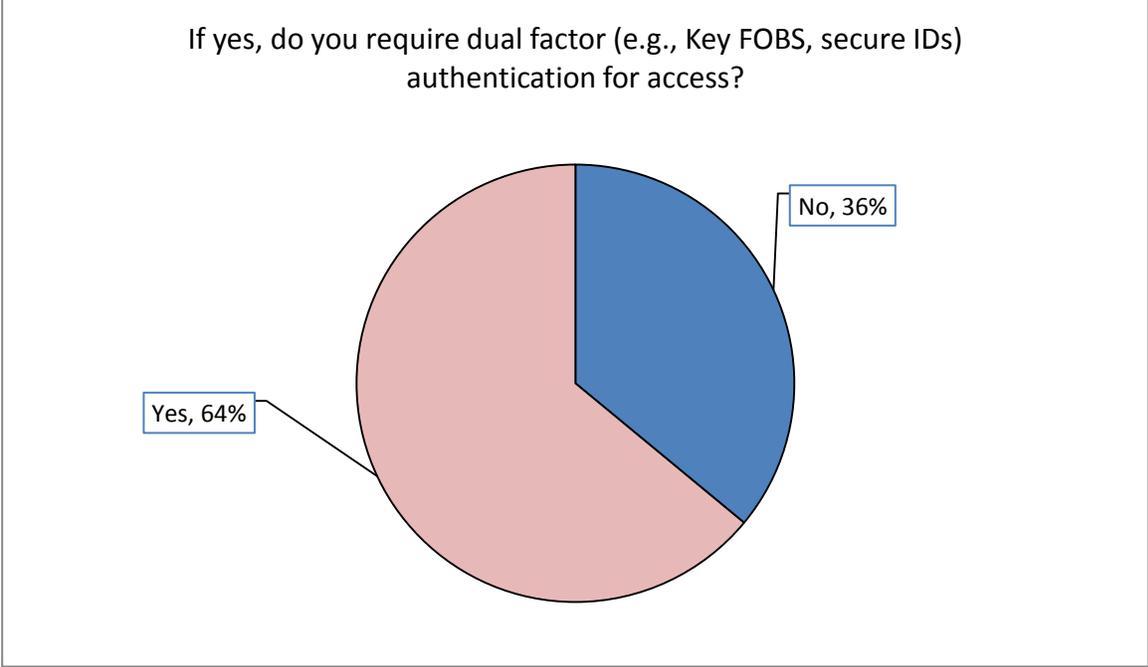
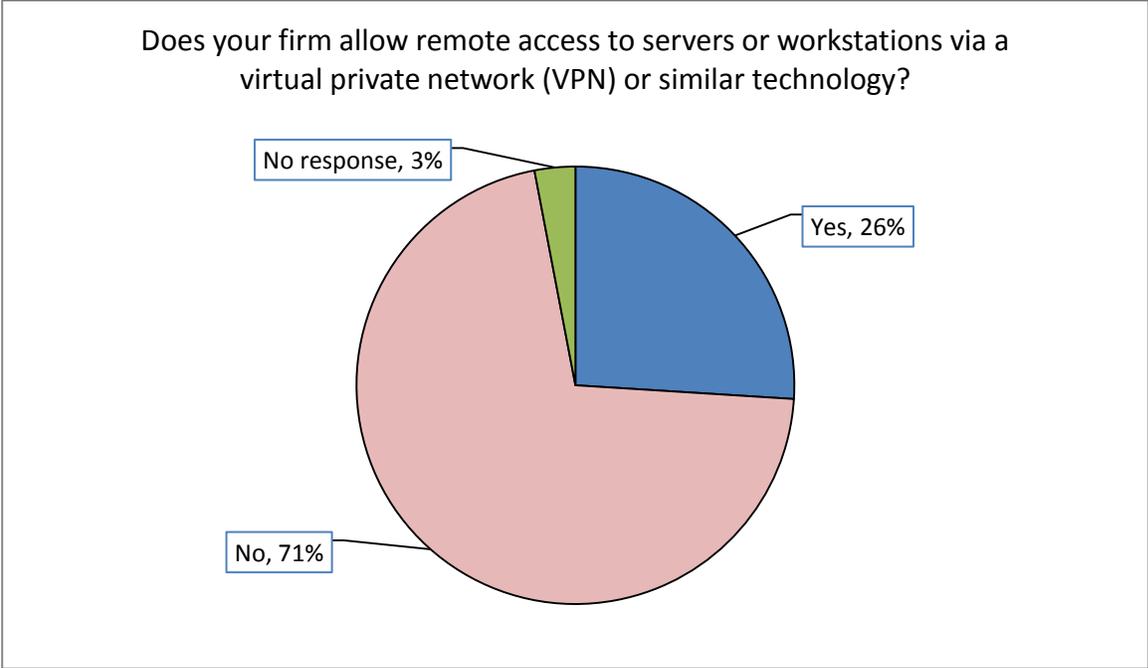


## Use of Online or Remote Backup of Electronic Files

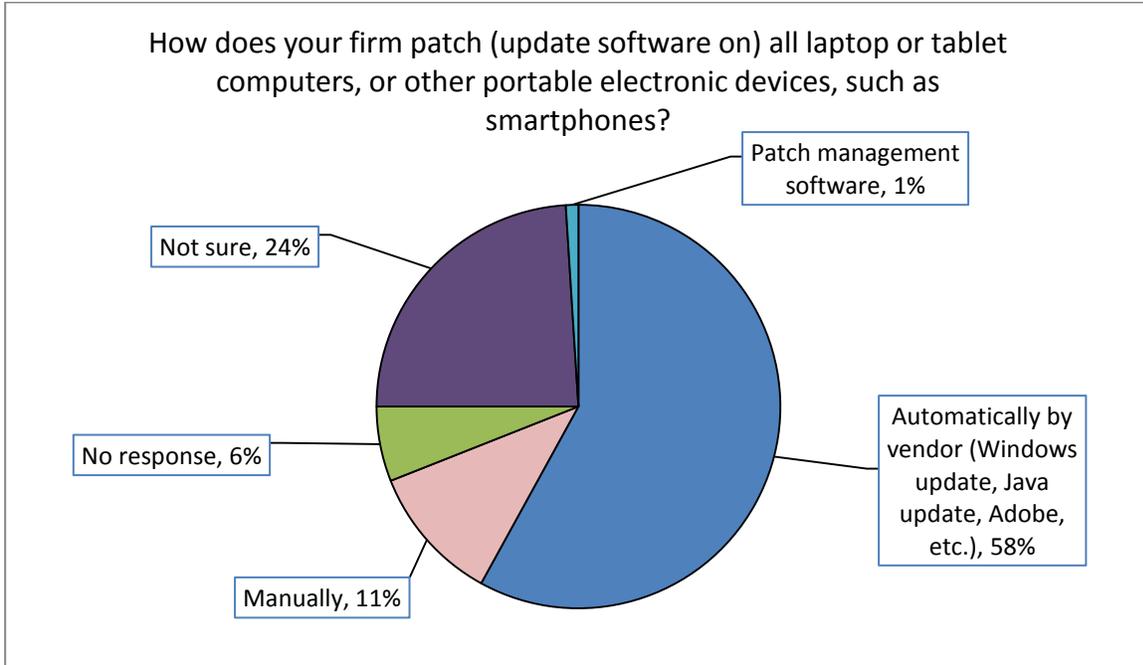
Does your firm utilize online or remote backup of electronic files?



# Use of Remote Access to Servers or Workstations via VPN or Similar Technology & Dual Factor Authentication

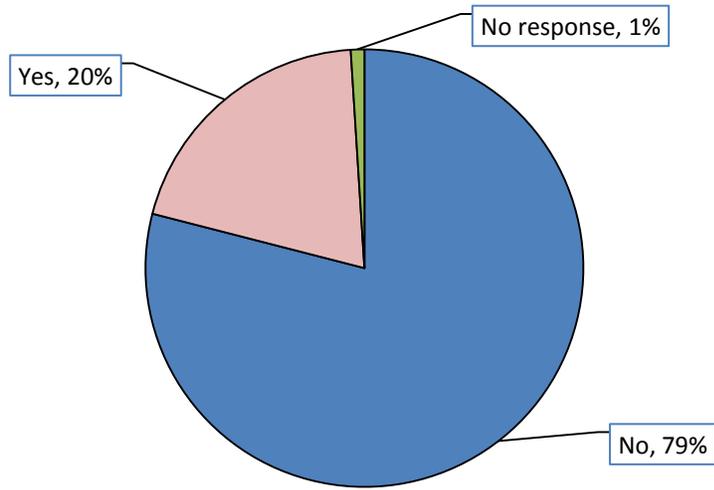


## Patch Updates/Software Updates

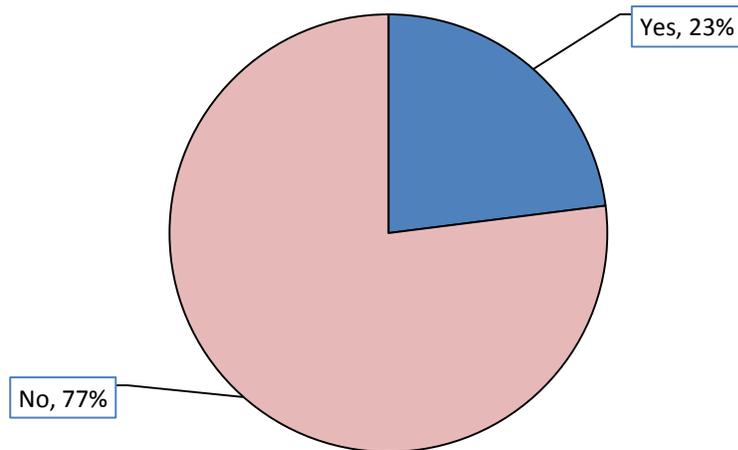


## Use of Free Cloud Services

Does your firm use free Cloud services such as iCloud, Dropbox, or Google Drive, to store personal and confidential client information?

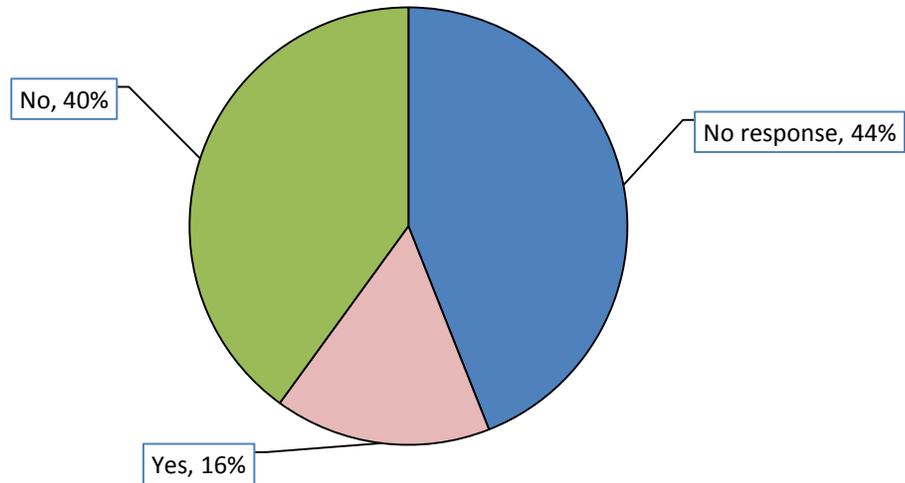


If yes, is there a policy that stipulates how these services are to be used?



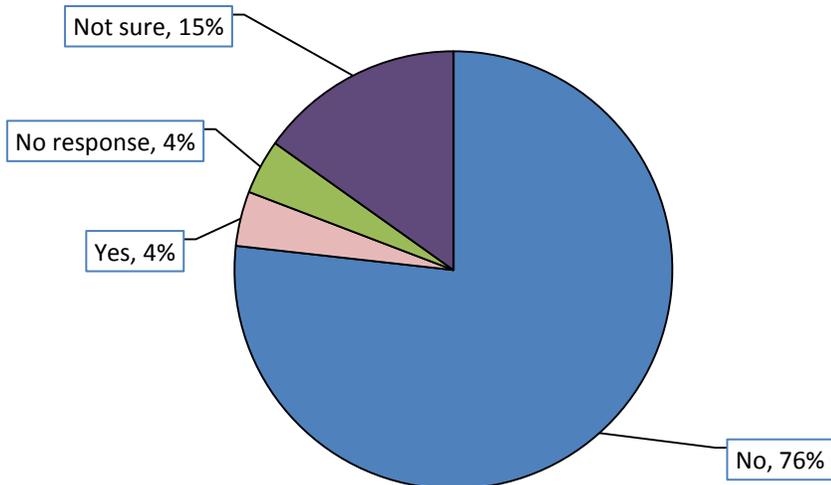
## Use of Software as a Service (SAAS) Vendors

If your firm uses Software As A Service (SAAS) vendors for application development, do you vet the vendor for security issues?

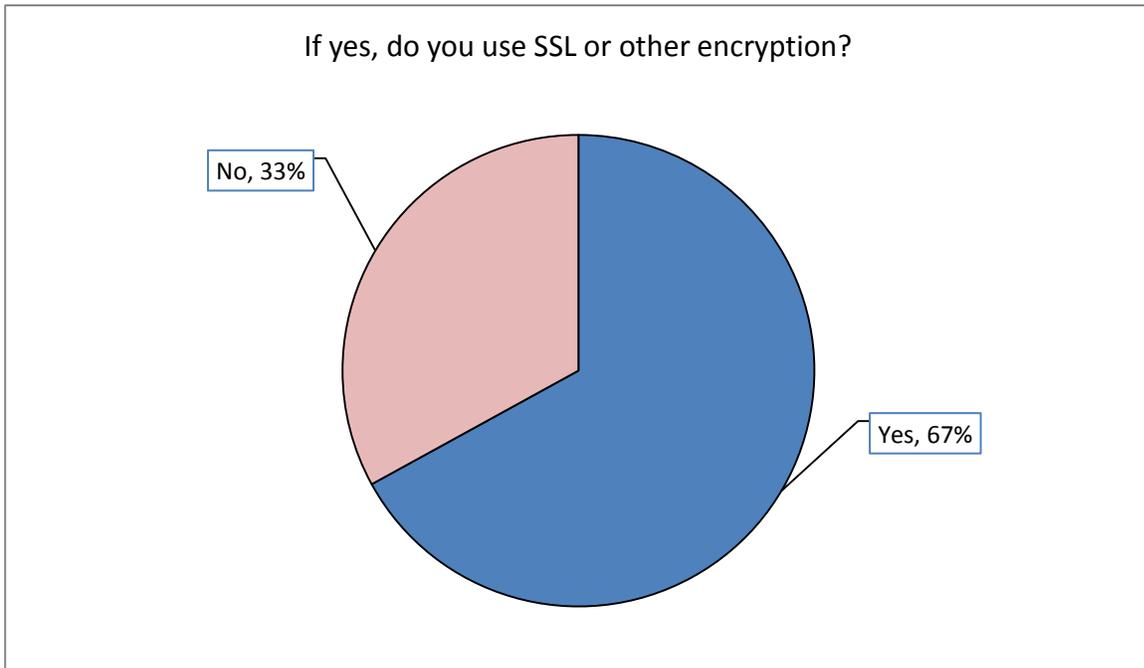
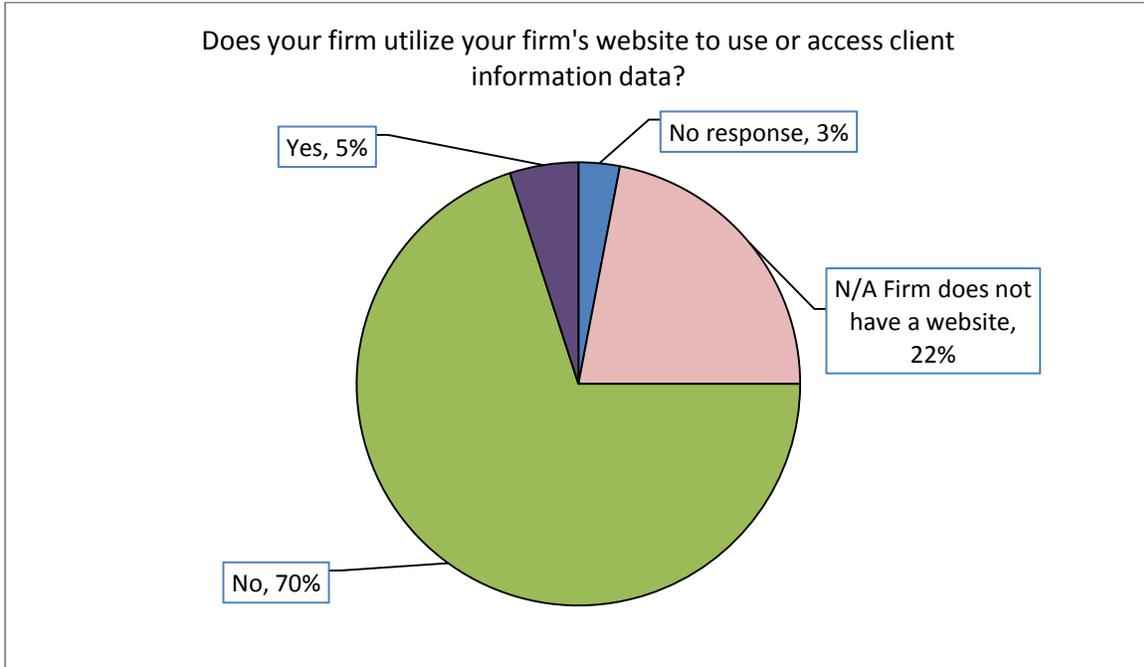


## Use of Mobile Device Management (MDM) Tools

Does your firm utilize a Mobile Device Management (MDM) tool (e.g., Airwatch, MobileIron, Citrix/XenMobile)?



## Use of Firm Websites to Access Client Data



## Use of Client Portals on Firm Websites

