Compilation of Results of a Pilot Survey of Cybersecurity Practices of Small and Mid-Sized Investment Adviser Firms

North American Securities Administrators Association
www.nasaa.org

September 2014

About NASAA

Organized in 1919, the North American Securities Administrators Association ("NASAA") is the oldest international organization devoted to investor protection. NASAA is a voluntary association with a membership consisting of securities administrators in the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Canada and Mexico.

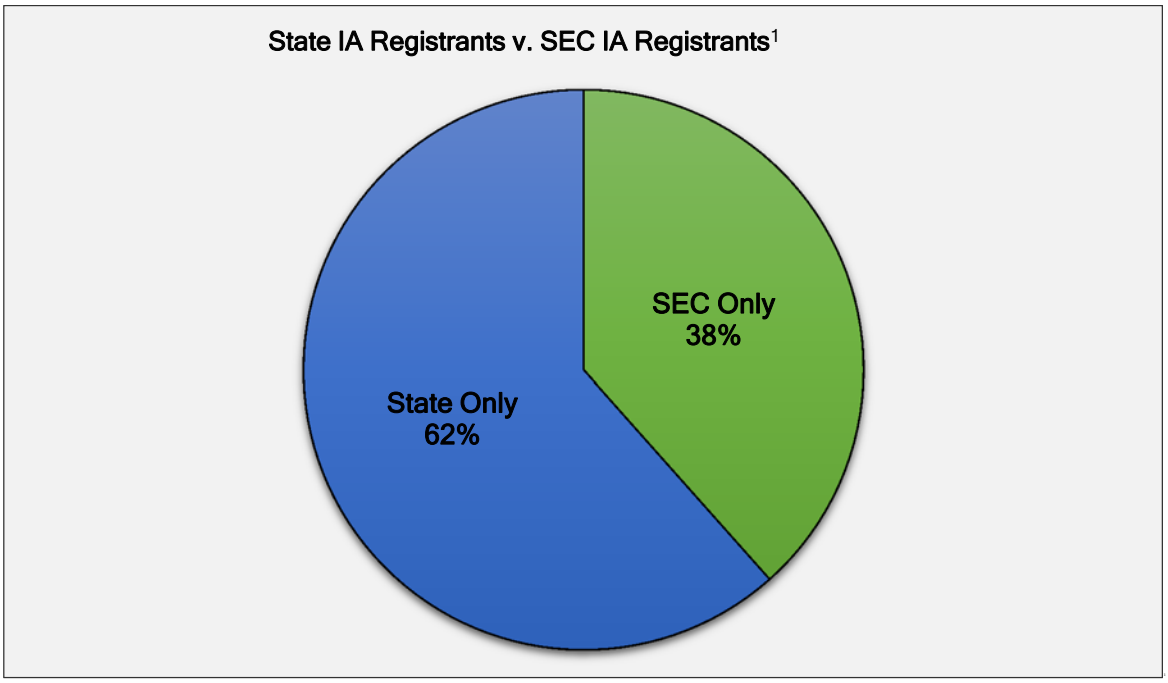
State and provincial securities regulators have been protecting investors from fraud and abusive sales practices since the passage of the first "blue sky" law in Kansas in 1911 and since 1912 in Canada when Manitoba became the first province to approve securities legislation. In the United States, state securities regulation preceded federal securities laws, including the creation of the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), formerly the NASD.

As the preeminent organization of securities regulators, NASAA is committed to protecting investors from fraud and abuse, educating investors, supporting capital formation, and helping ensure the integrity and efficiency of financial markets.

A Pilot Survey To Compile Cybersecurity Information

Introduction: Developing A Pilot Cybersecurity Project

NASAA's pilot cybersecurity project was designed to better understand the cybersecurity practices of state-registered investment advisers, which account for over half of the registered investment advisers conducting business in the United States. Through the use of a template survey, the pilot project sought to elicit information to better understand the technology and data practices of state-registered investment advisers; how these advisers communicate with clients; and what types of policies and procedures these advisers currently maintain. The pilot project also focused on specific uses of technology and websites, with a goal of understanding the safeguards used by state-registered investment advisers to protect client information; to inform state examination programs; and to identify national cybersecurity trends relevant to state-registered investment advisers.



States participating in the pilot project used the survey as part of their examinations and audit inspection programs or as a separate survey or document request tool. The survey allowed states participating in the pilot program to collect information on either an identifiable or anonymous basis. Some states sent the survey to a limited number of investment advisers registered in their states while others sent it to all of the investment advisers registered in their states. About half of the survey responses collected were collected on an anonymous basis initially, while the remainder were collected in an identifiable setting, whether through examinations or a document request. Several states also made the optional request that investment advisers submit relevant policies and

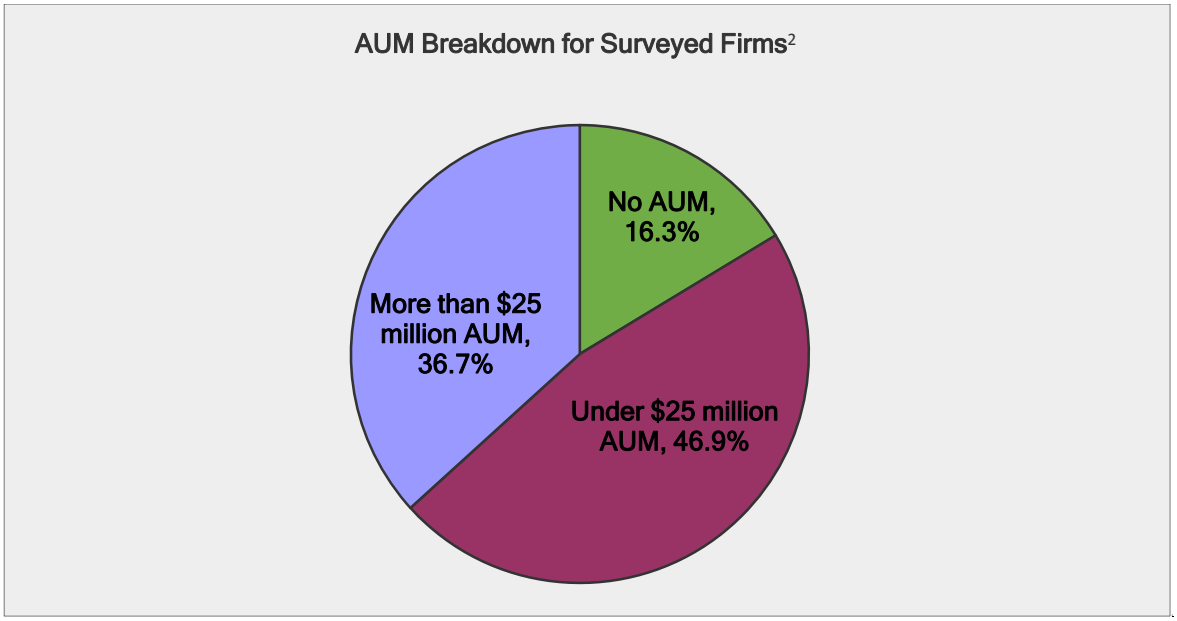
[1] About one percent of investment registrants are registered with both the SEC and the states.

procedures. Nine states reported a subset of the investment adviser firms' responses to NASAA on a non-identifiable basis.

Pilot Project Survey Results:

A Compilation of Data from 440 Registered Investment Advisers in 9 States

This subset of data includes 440 state-registered investment adviser firms of varying sizes. Forty-seven percent have assets under management of less than $25 million, thirty-seven percent manage more than $25 million, and sixteen percent do not manage assets. The firms have between 1 and 100 employees and between 1 and 39 investment adviser representatives. The firms average three employees and two investment adviser representatives.



State securities regulators are continuing to review the survey data, but note the following preliminary findings:

- Only 4.1% of firms indicated they had experienced a cybersecurity incident and even fewer, only 1.1%, indicated they had experienced theft, loss, unauthorized exposure, or unauthorized use of or access to confidential information.

- Most state-registered investment advisers (85%) use computers, tablets, smartphones, or other electronic devices to access client information.

- While 92% of firms use e-mail to contact clients, only 50% of the firms use secure e-mail. Furthermore, 56.7% of firms have procedures in place to authenticate instructions received from their clients via e-mail.

[2] All surveyed firms are state registered.

- 62% of firms report undergoing a cybersecurity risk assessment. The frequency of these assessments varied widely.

- Just under one half of firms (44.4%) report having policies and procedures or training in place related to cybersecurity. Similarly, 47.5% of firms report having policies and procedures or training related to the disposal of electronic data storage devices. A total of 76.8% of firms reported maintaining policies and procedures related to technology or cybersecurity.[3]

Beyond Pilot Survey Results: Continuing the Regulatory Conversation on Cybersecurity

As state regulators continue to review the data, NASAA is now releasing the compilation of the pilot survey results to further inform regulatory and industry conversations on cybersecurity. Additional jurisdictions are administering the template survey, which will further enrich the ongoing regulatory conversations on cybersecurity. NASAA plans to continue to work with the jurisdictions that were pilot participants as well as additional jurisdictions to further analyze how cybersecurity developments affect state-registered investment advisers. Despite the relatively low rate in cybersecurity incidents identified in the compilation of pilot results, state securities regulators are aware of the increase in cyber-attacks in the financial services industry, and the importance and associated difficulties of securely maintaining private data.[4]

As NASAA's study of cybersecurity practices of state-registered investment advisers continues, NASAA expects to begin working toward recommended practices and engage in additional conversation with industry.

For more information, please contact:

A.Valerie Mirko
Deputy General Counsel
NASAA
Email: vm@nasaa.org

Andrew Hartnett
Missouri Commissioner of Securities
& Chair of NASAA's Investment Adviser
Cybersecurity & Technology Project Group
Email: andrew.hartnett@sos.mo.gov

NASAA Legal Department
750 First Street, NE, Suite 1140
Washington, DC 20002
202 737 0900

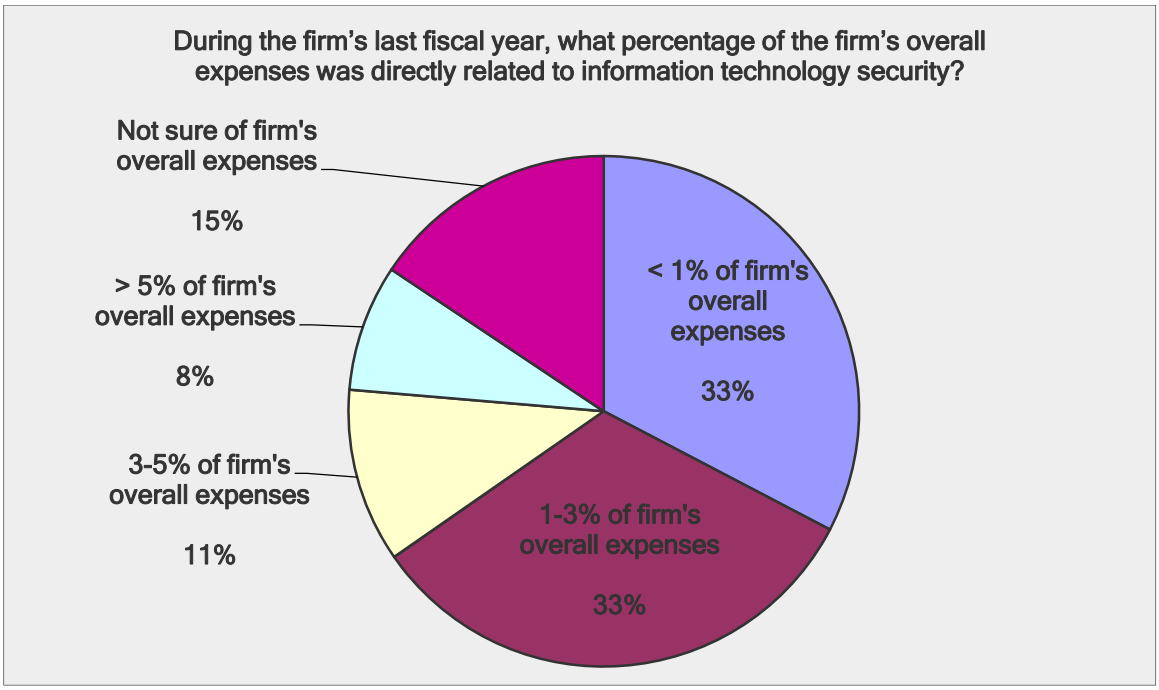
Missouri Secretary of State's Office
600 W Main St.
Jefferson City, MO 65101
573 751 4136

[3] The pilot project cybersecurity survey elicited information regarding a wide array of policies and procedures or training programs relating to technology, including cybersecurity, disposal of electronic data storage devices, use of social media, and other related topics. Please see page 13 for a full list.

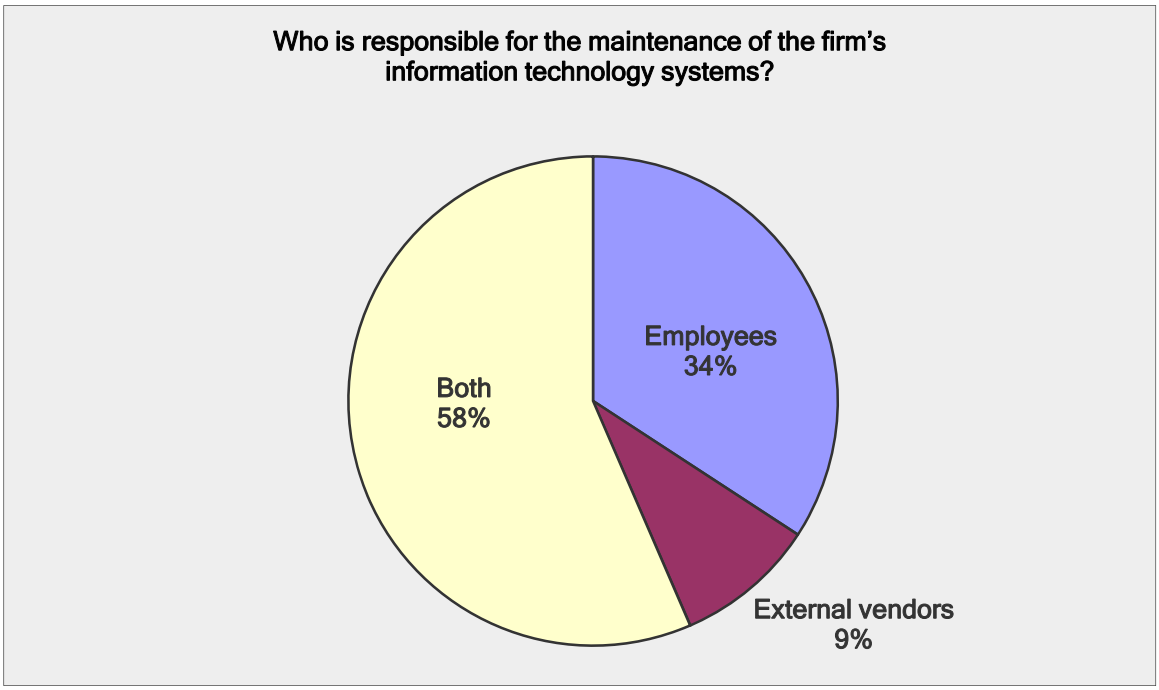
[4] *See* Jacob J. Lew, Secretary, U.S. Dept. of the Treasury, Remarks at the 2014 Delivering Alpha Conference Hosted by CNBC and Institutional Investor (July 16, 2014), available at http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx.

Preliminary Survey Results:

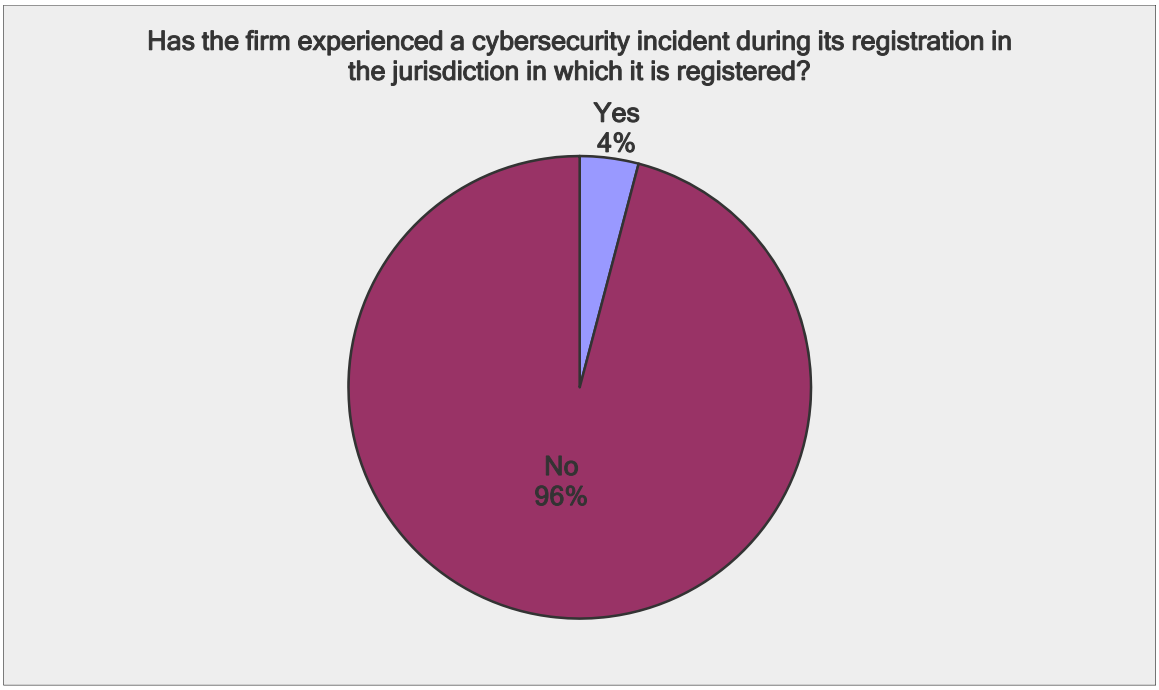
Expenses Directly Related to Information Technology Security



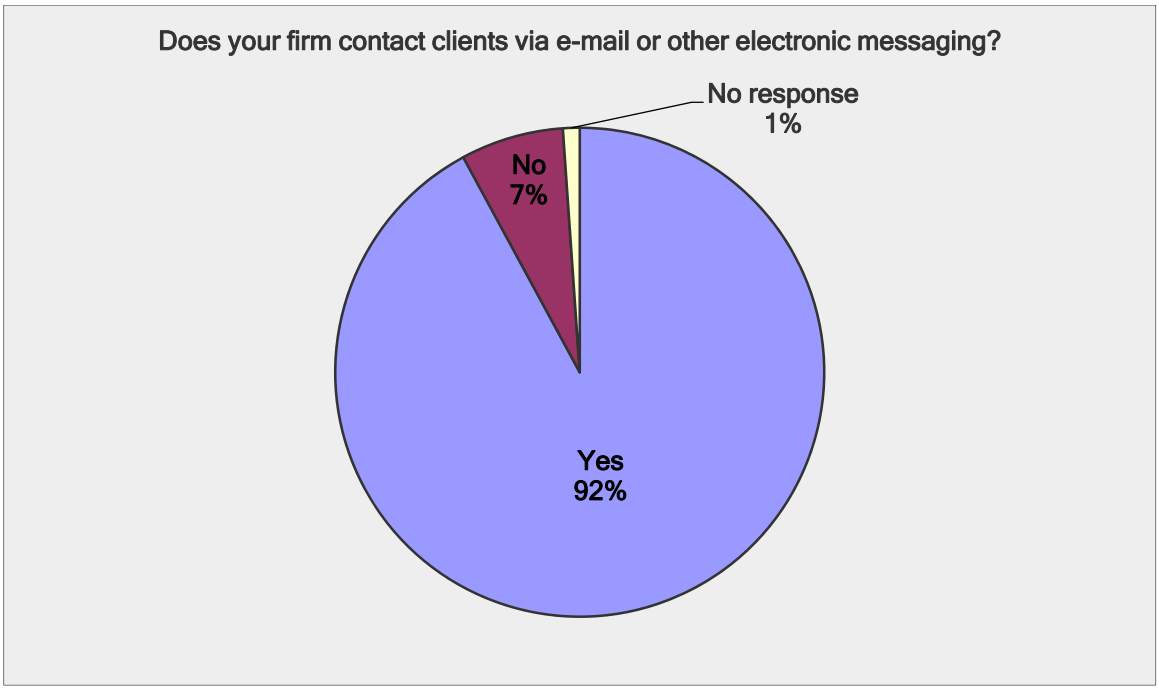
Maintenance of the Firm's Information Technology Systems

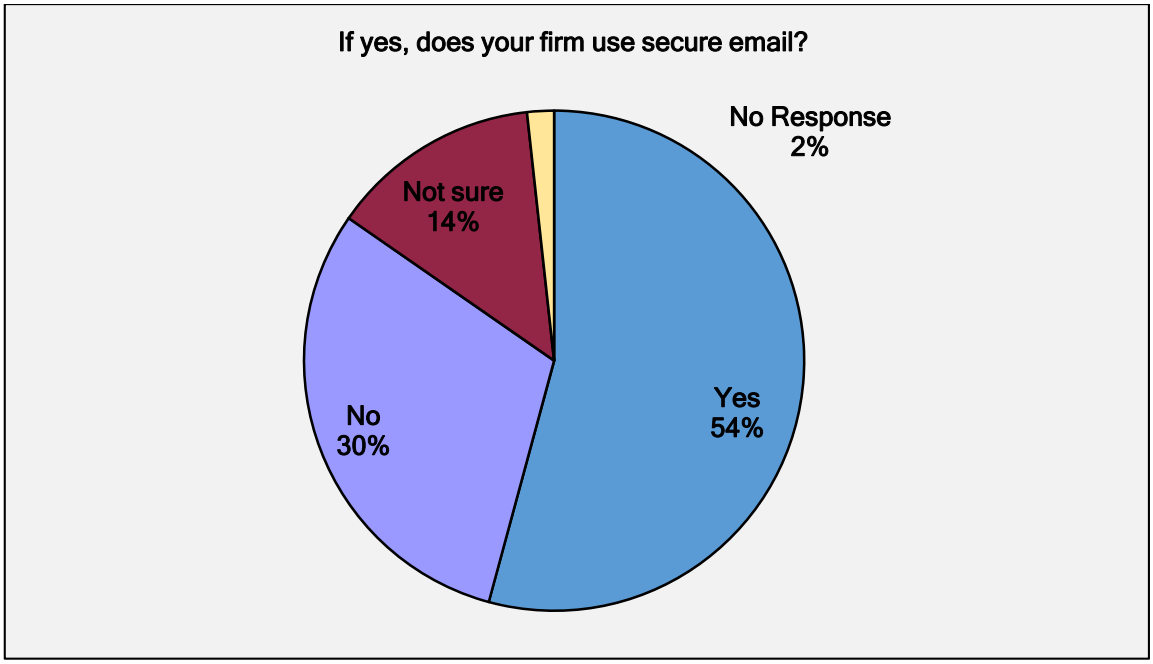


Rate of Cybersecurity Incidents

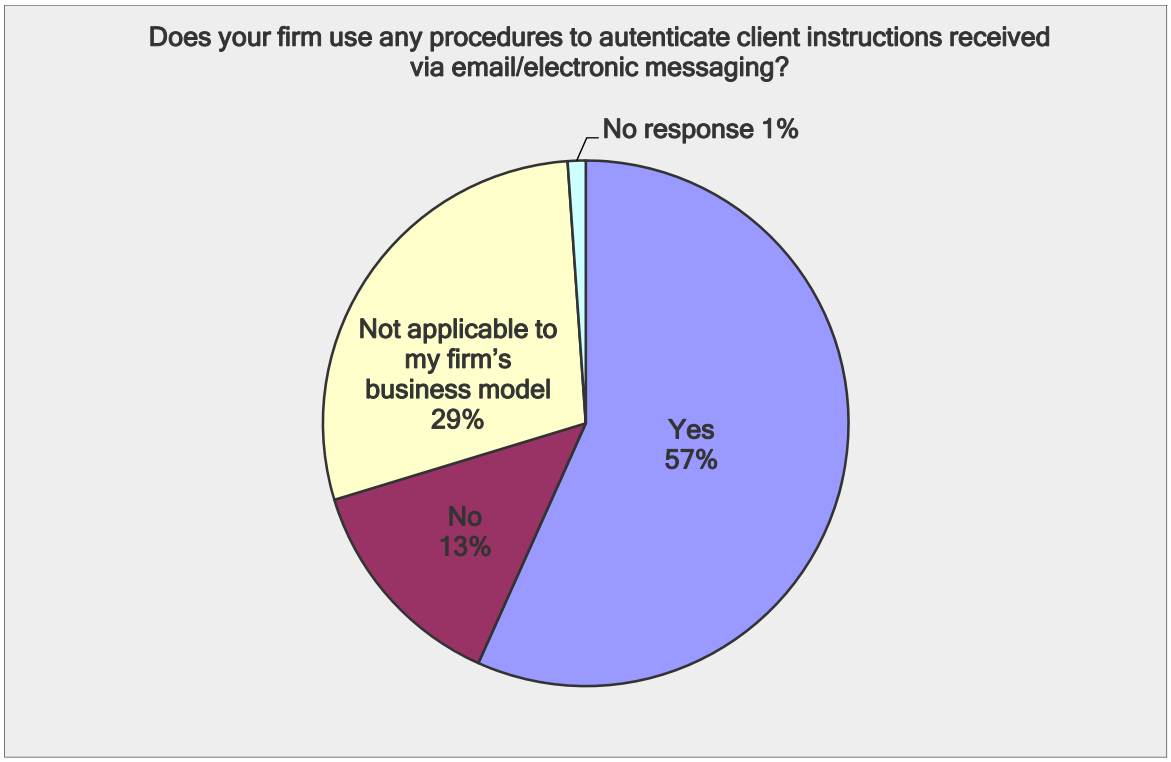


Client Contact via E-mail & Use of Secure E-mail

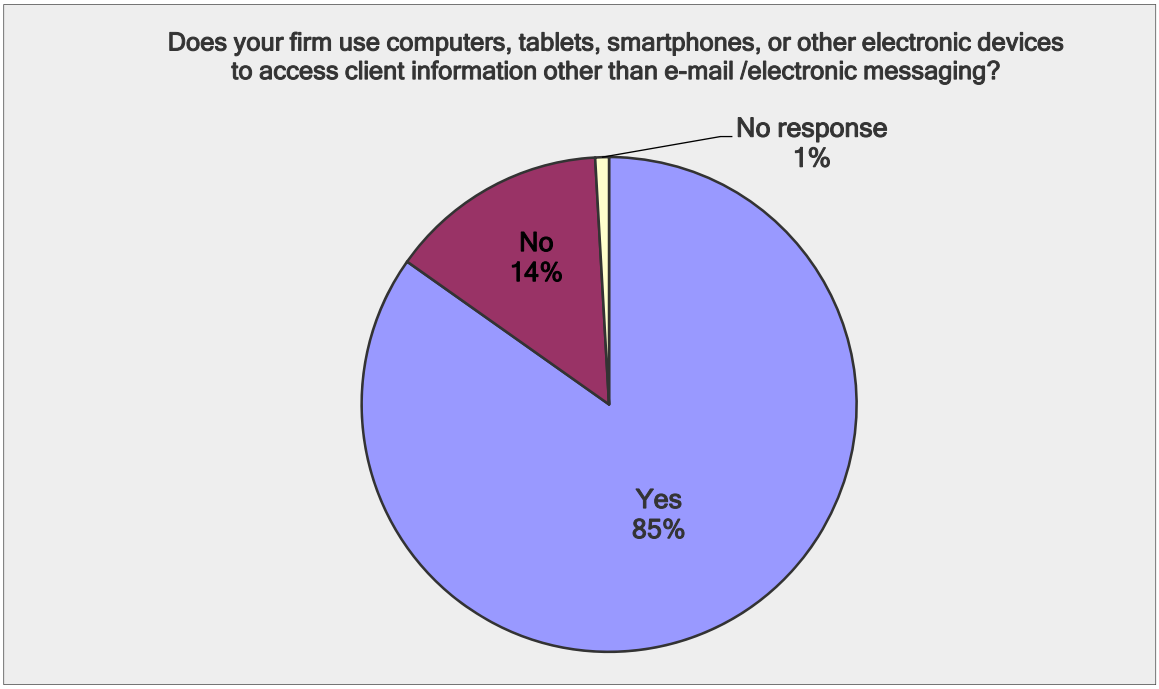




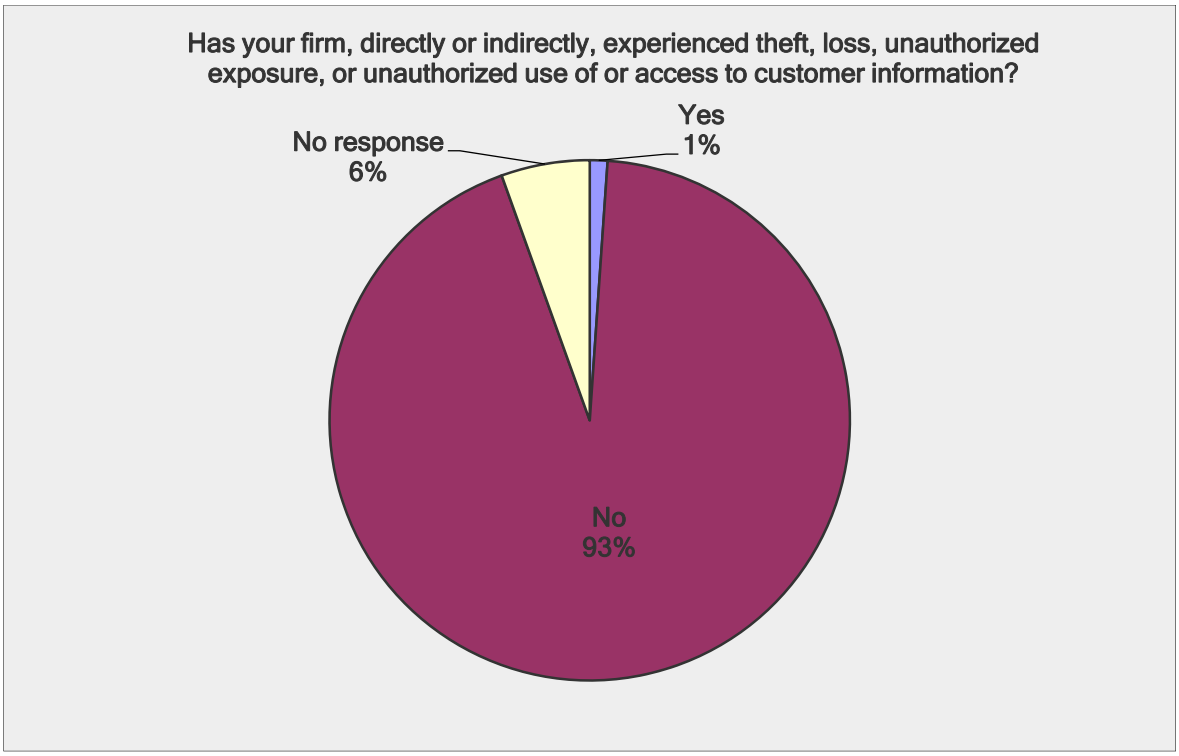
Authentication of Client Instructions Received Electronically



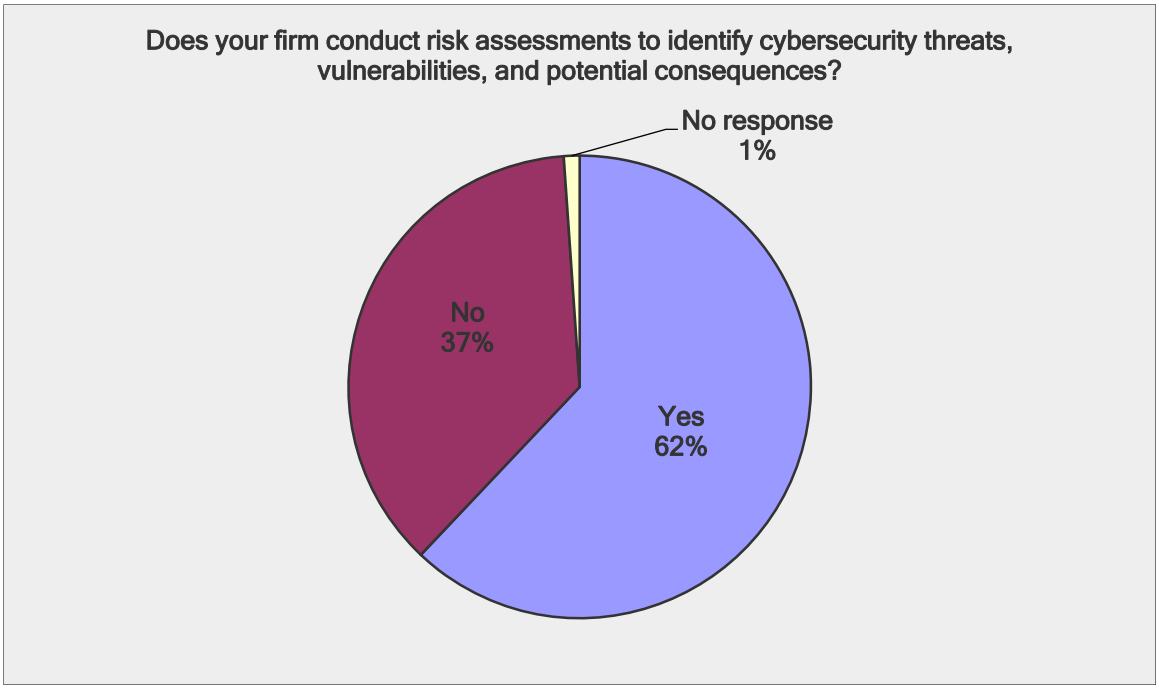
Devices Used to Access Client Information

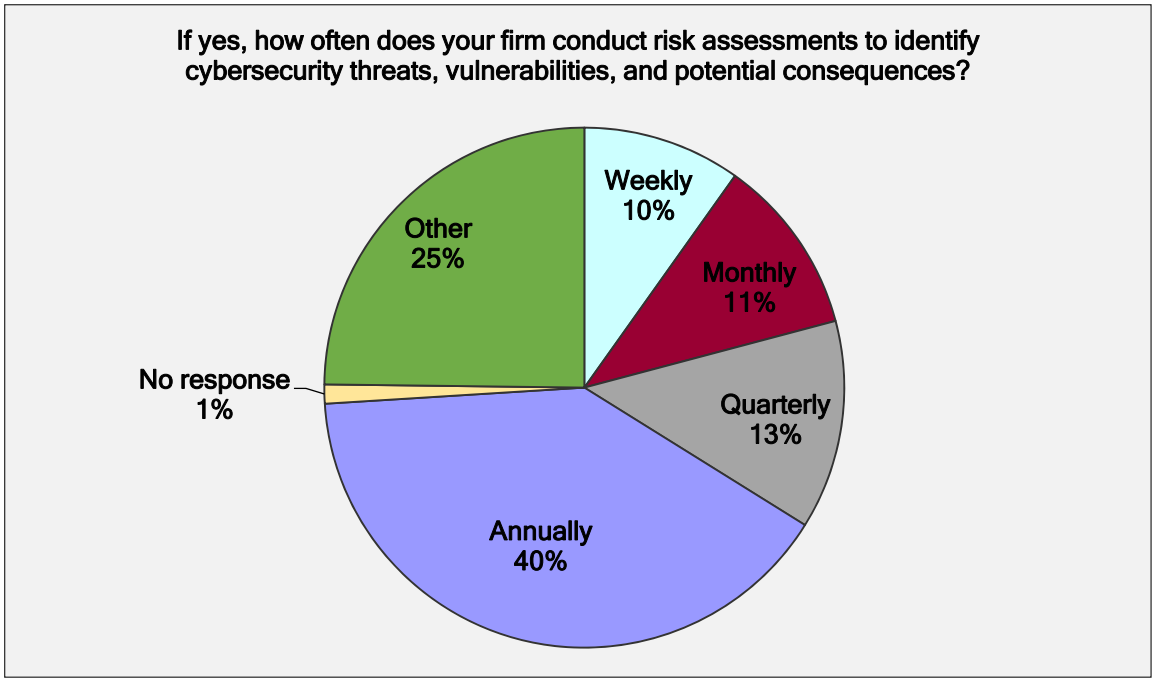


Unauthorized Use or Access to Customer Information

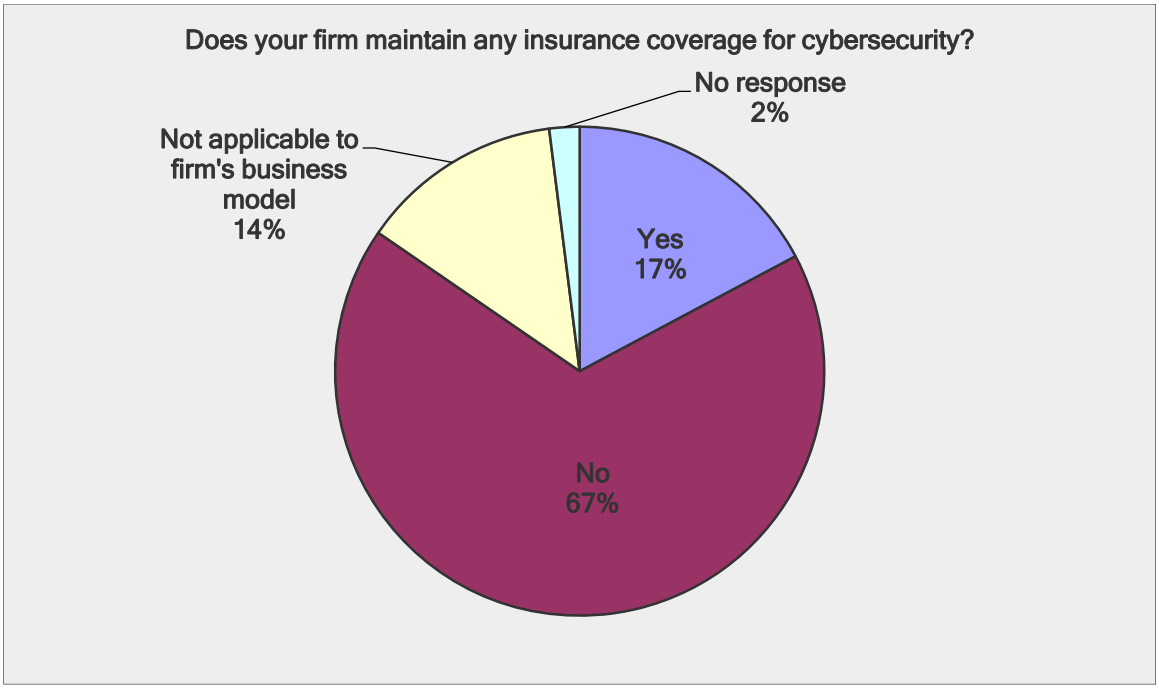


Risk Assessments Related to Cybersecurity & Frequency of Risk Assessments

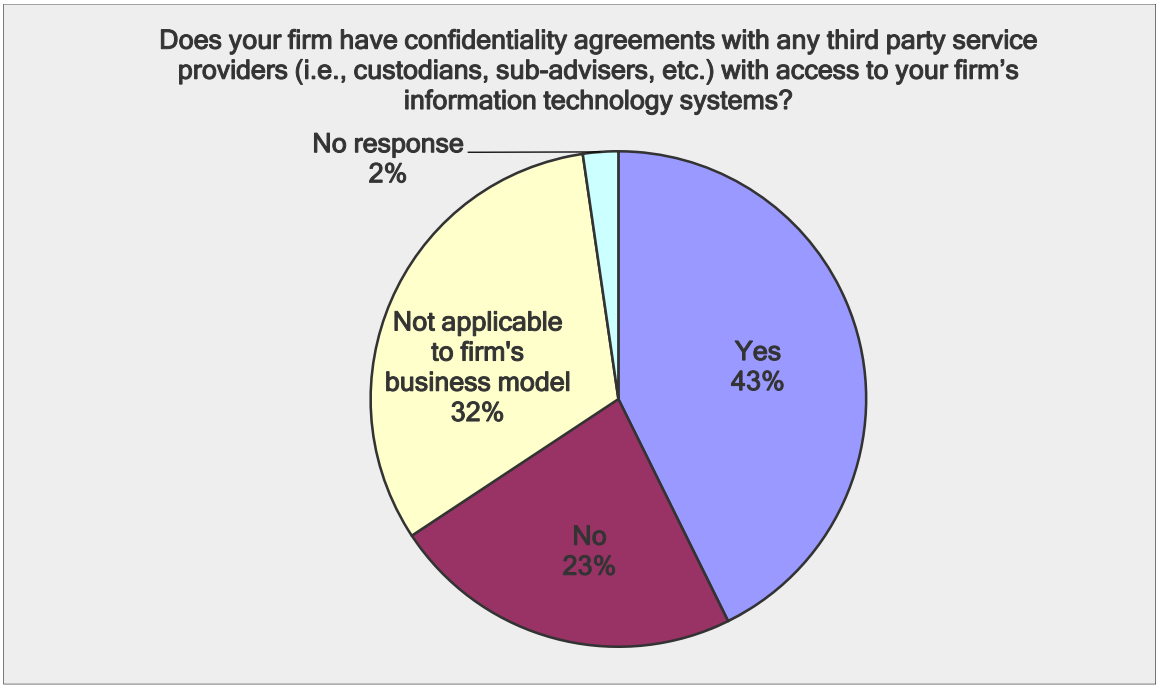




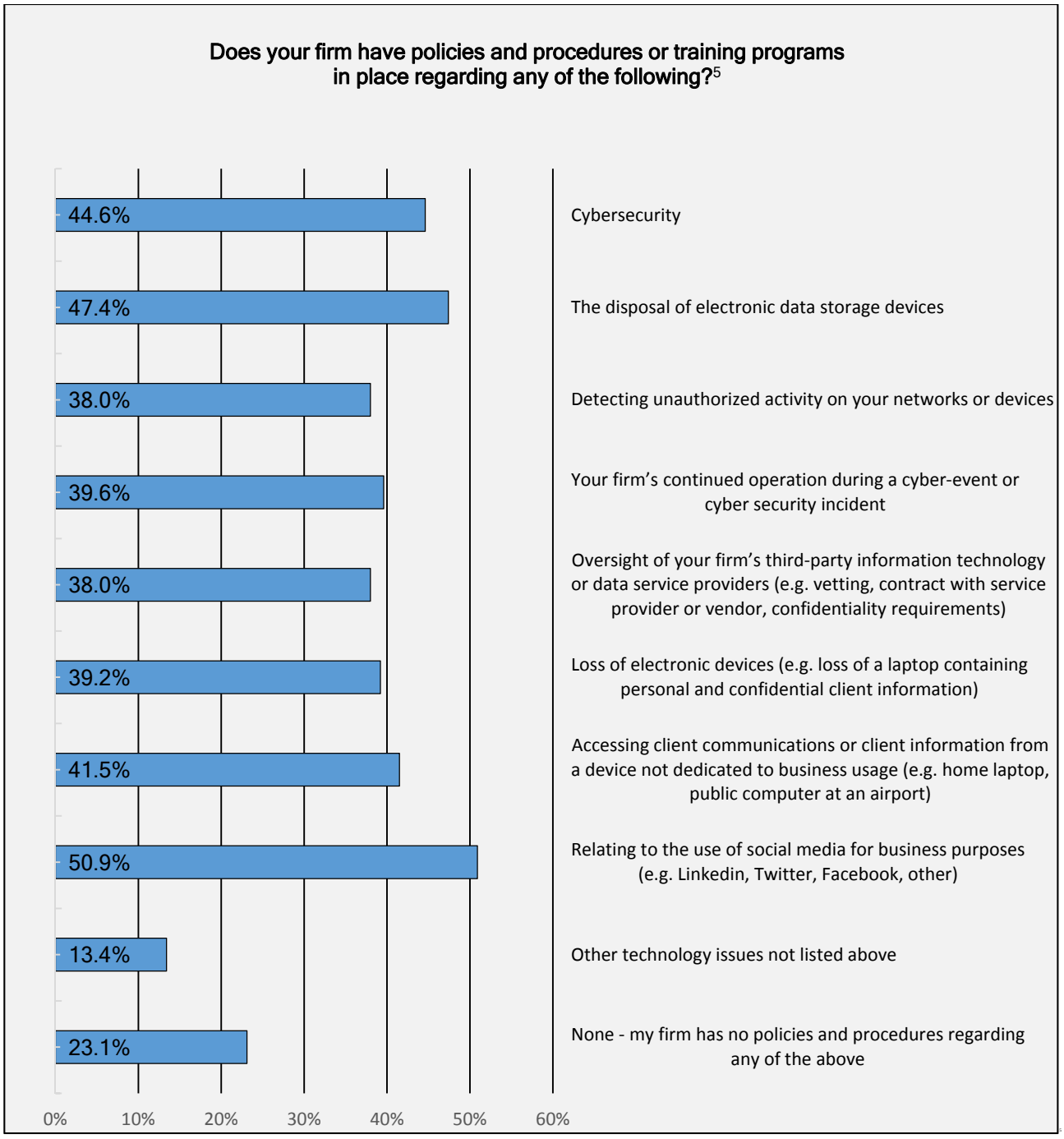
Insurance Coverage for Cybersecurity



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

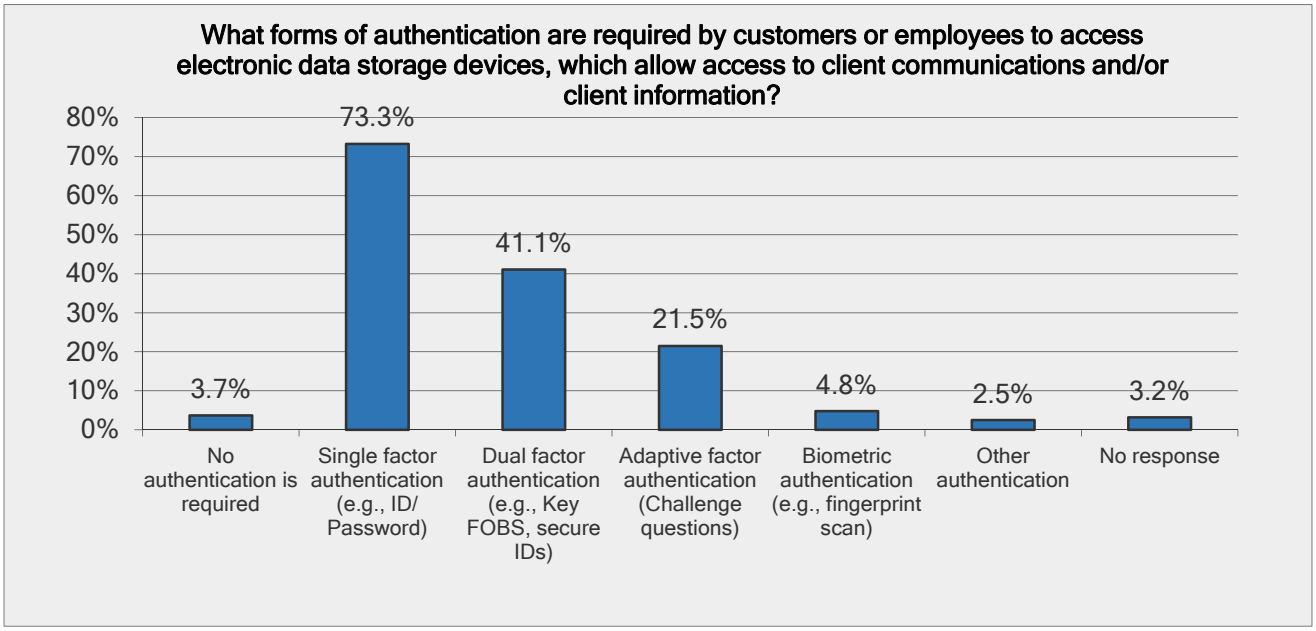


Policies, Procedures and Training Programs

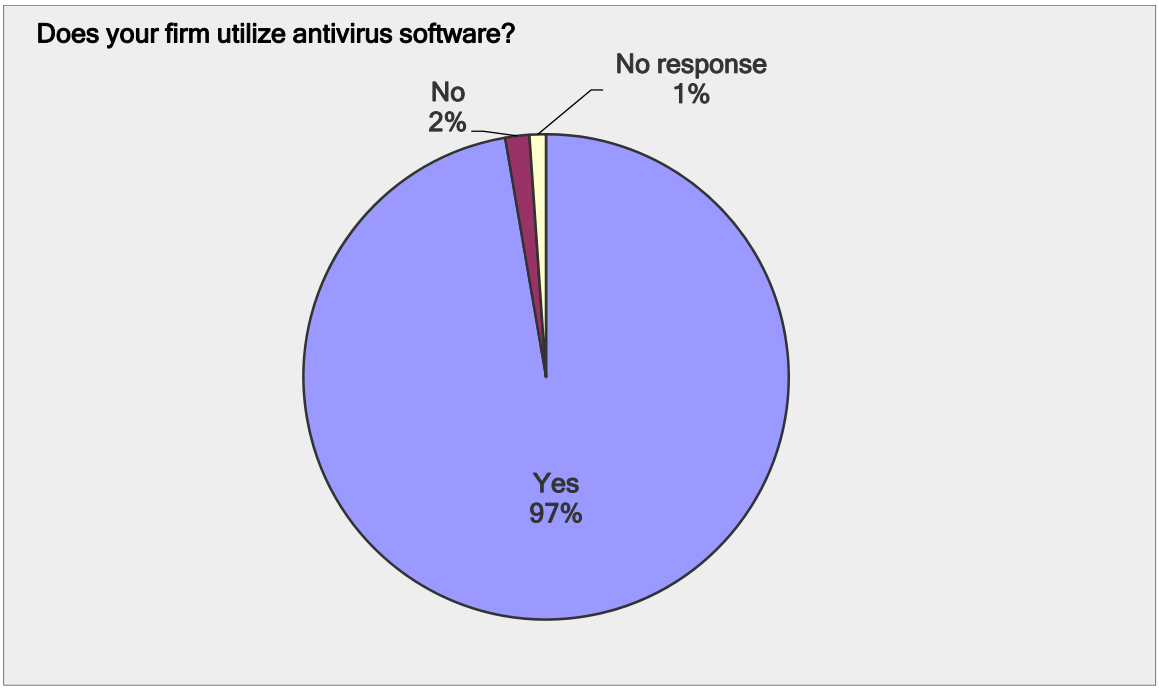


[5] This question required that respondents check all categories that applied.

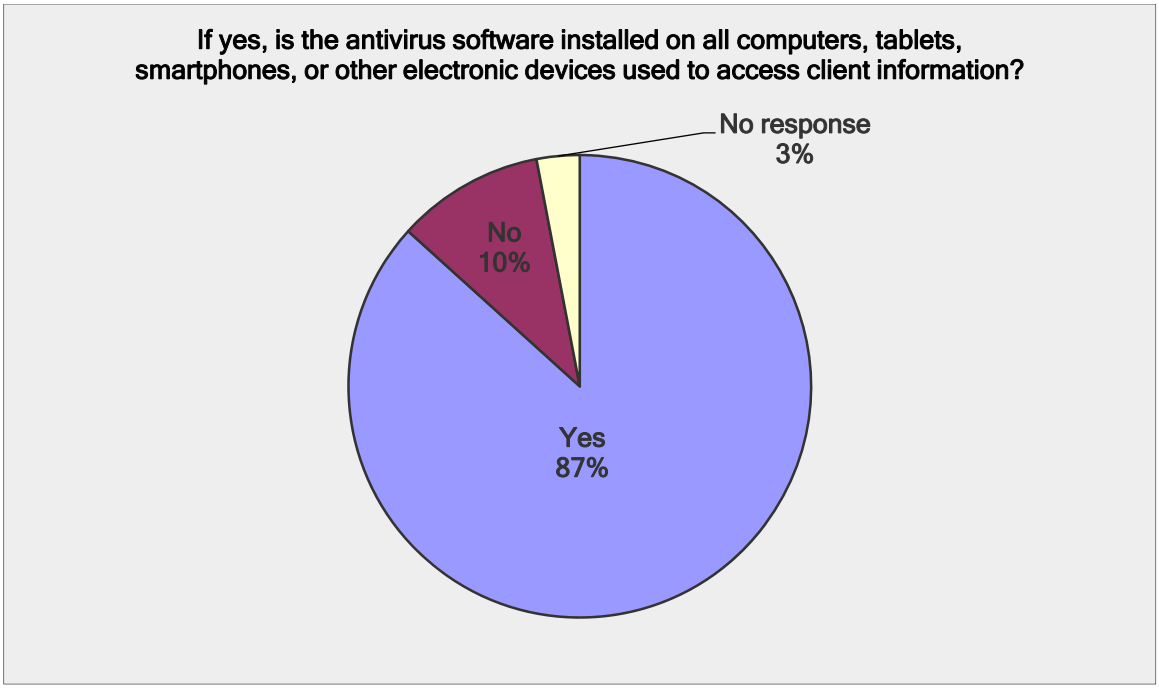
Authentication Practices



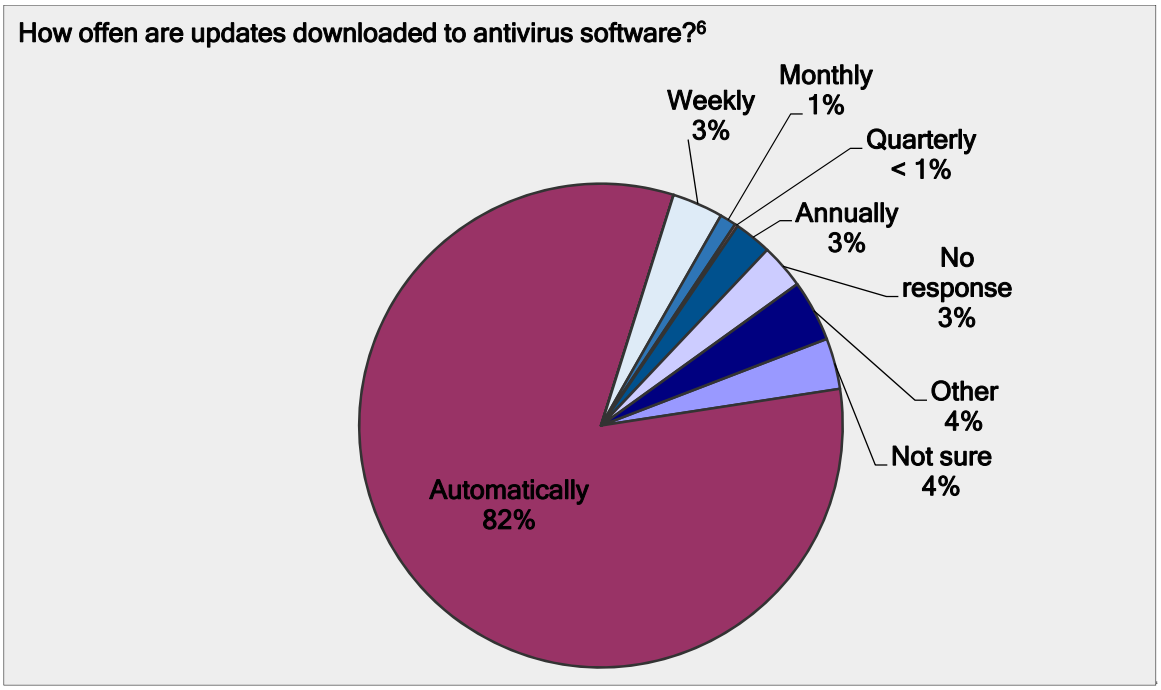
Use of Antivirus Software



Antivirus Software Installed on Electronic Devices Used to Access Client Information

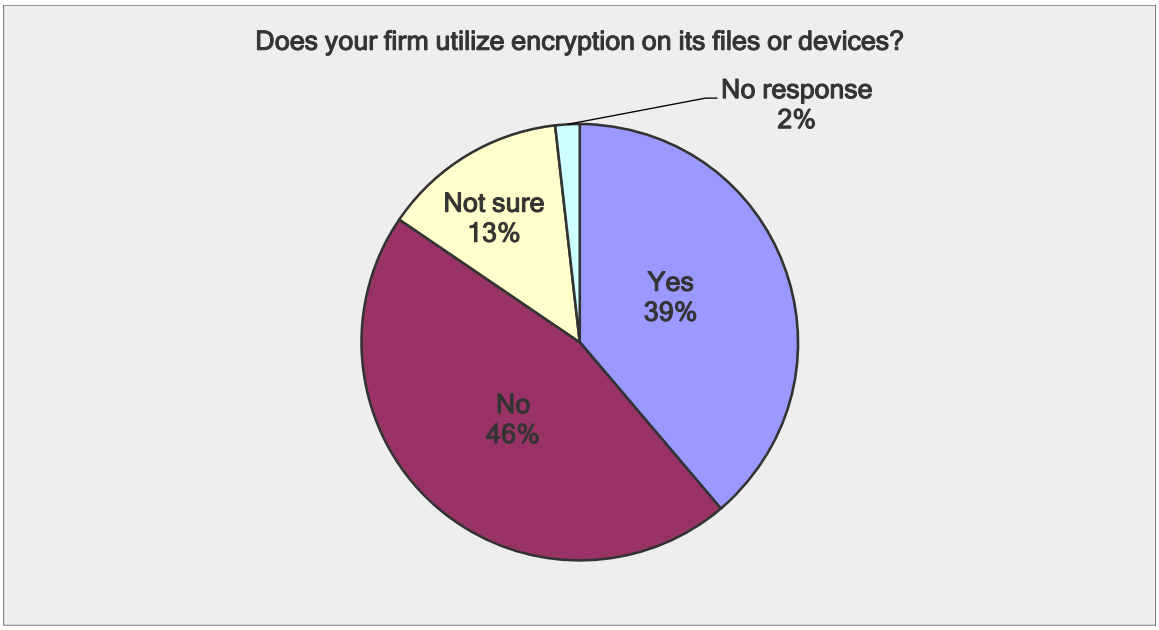


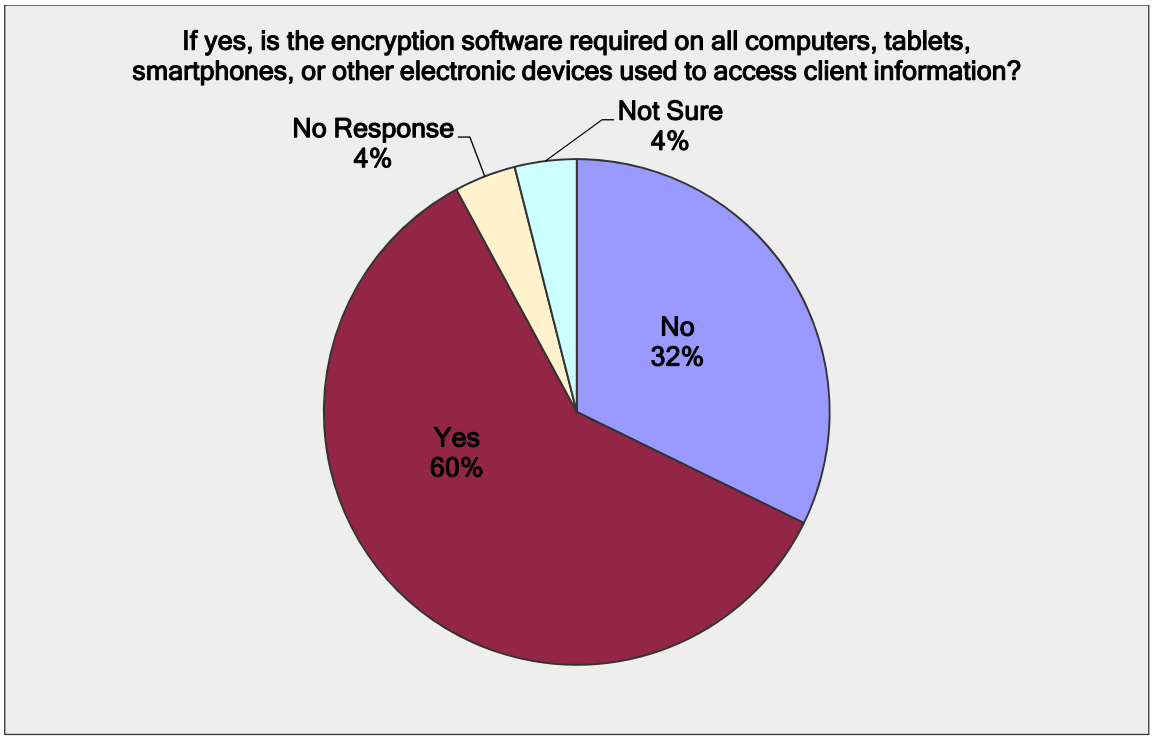
Frequency of Antivirus Updates



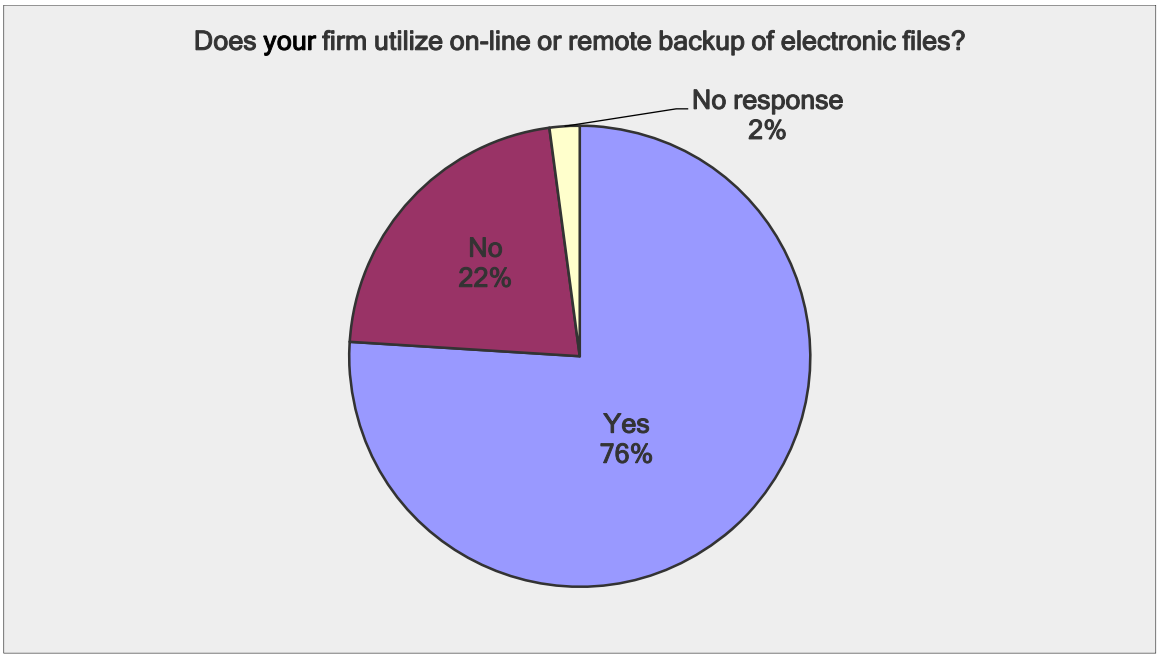
[6] All firms that reported utilizing antivirus software reported that such software is updated periodically.

Use of Encryption

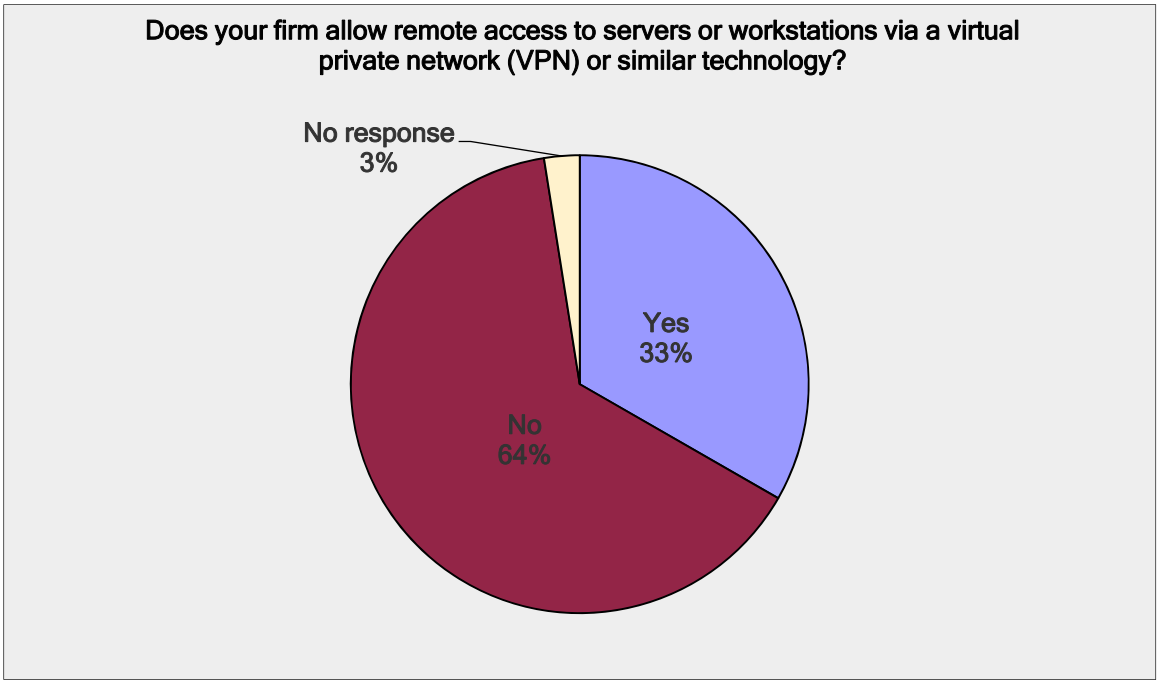


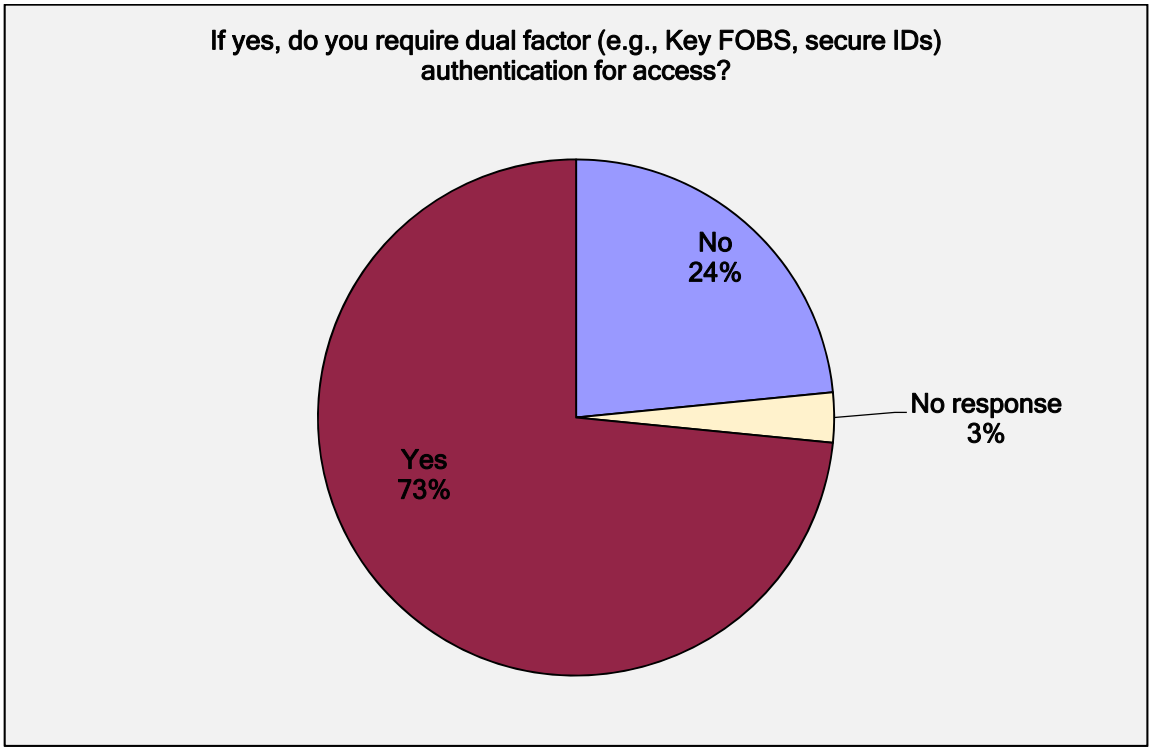


Use of On-Line or Remote Backup of Electronic Files

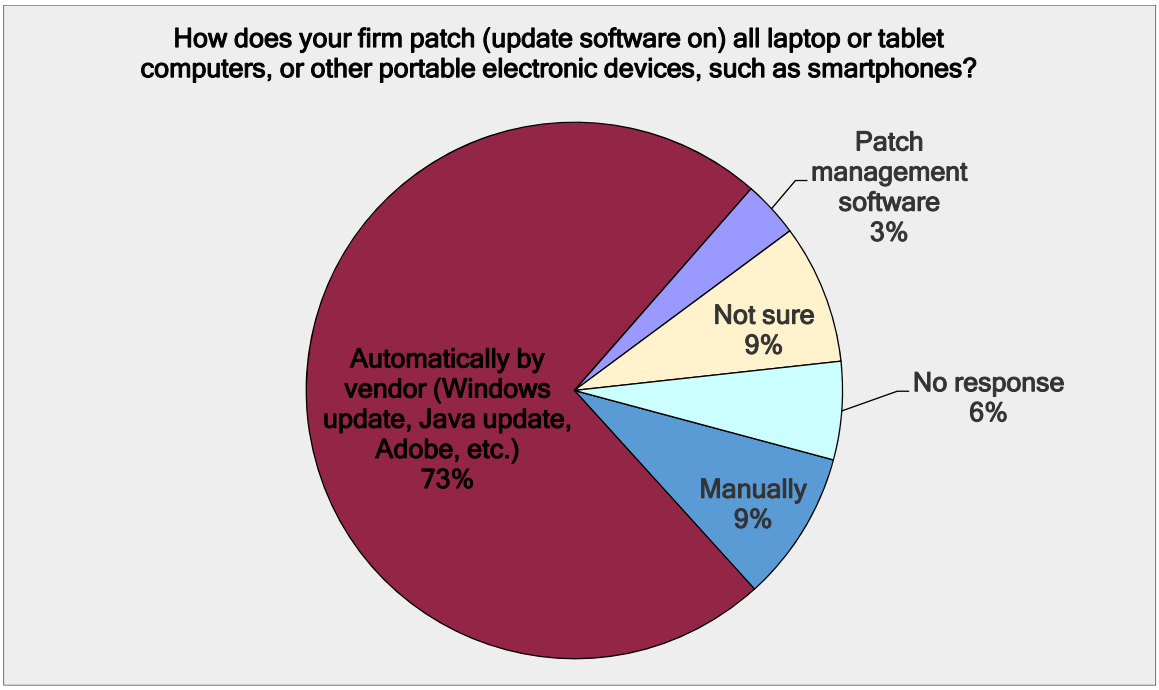


Use of Remote Access to Servers or Workstations via VPN or Similar Technology & Dual Factor Authentication

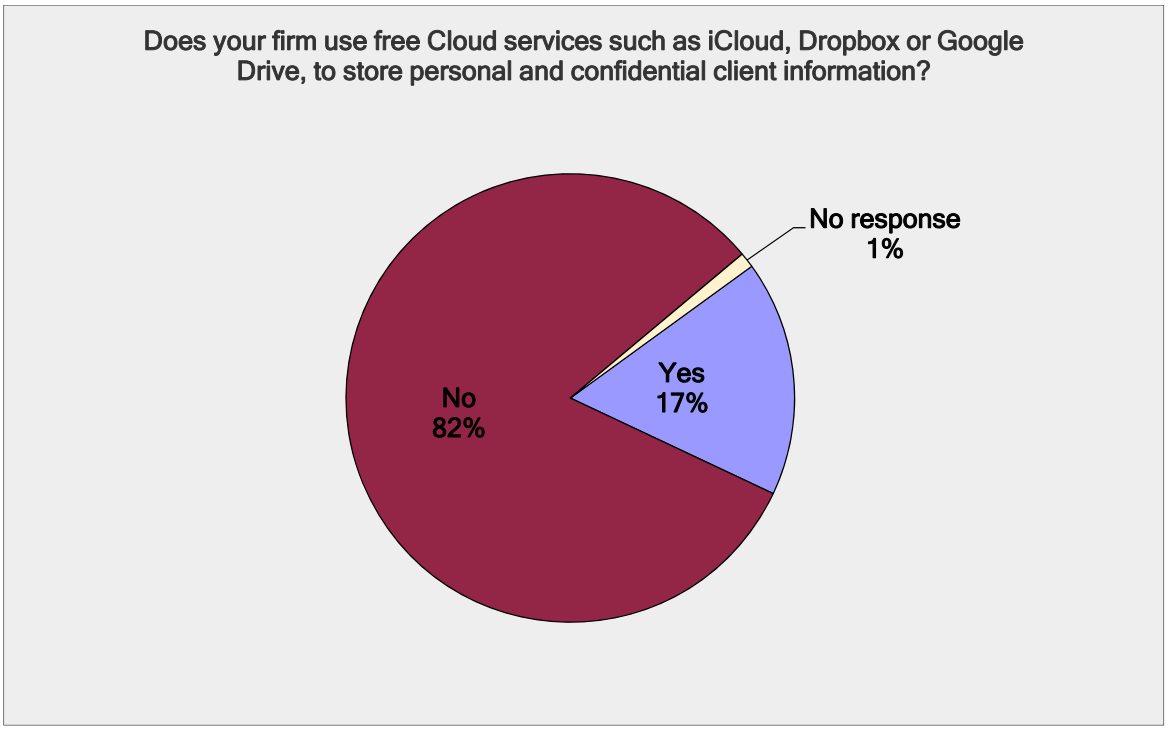


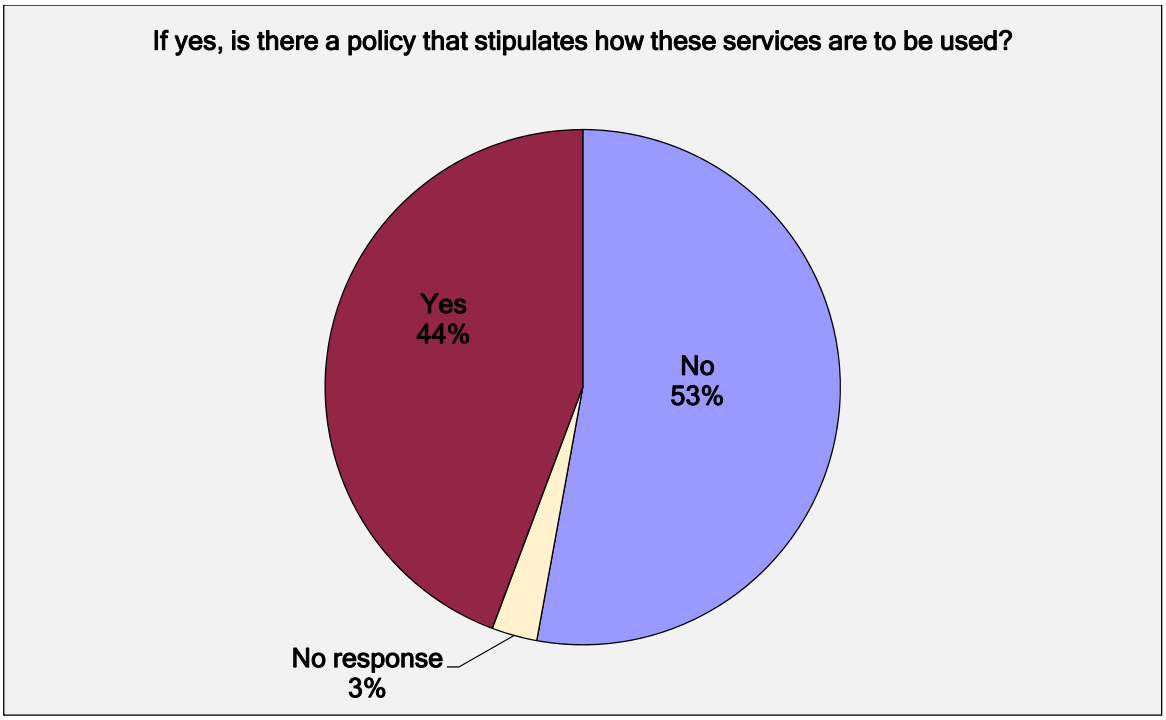


Patch Updates / Software Updates

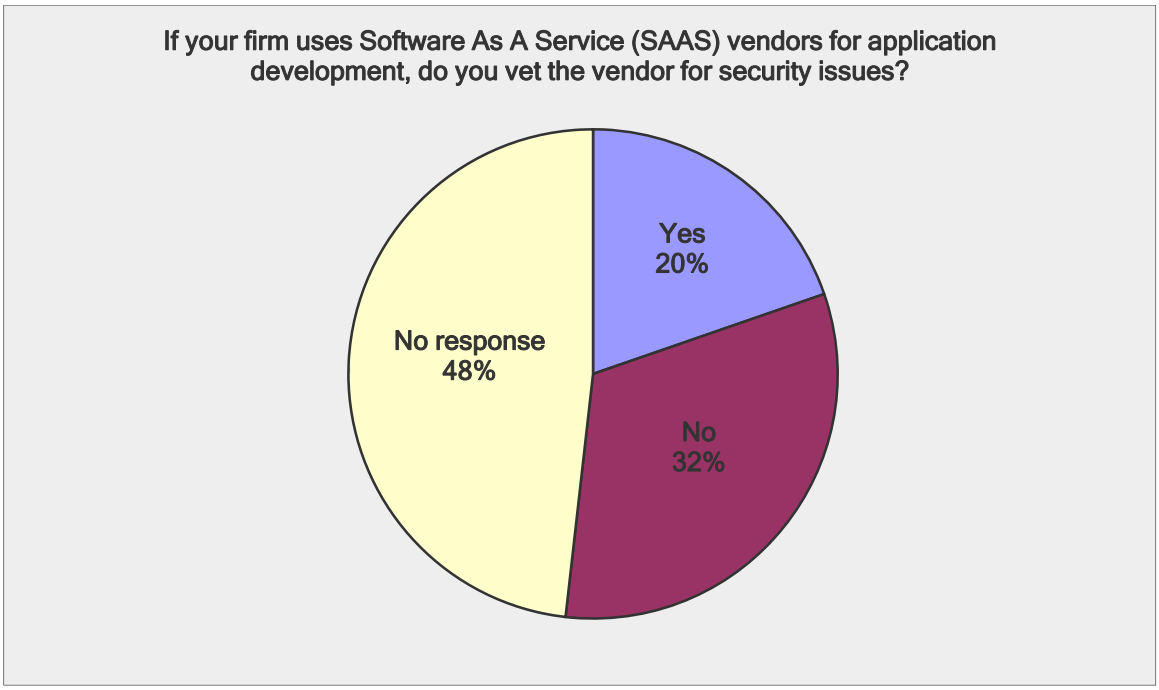


Use of Free Cloud Services

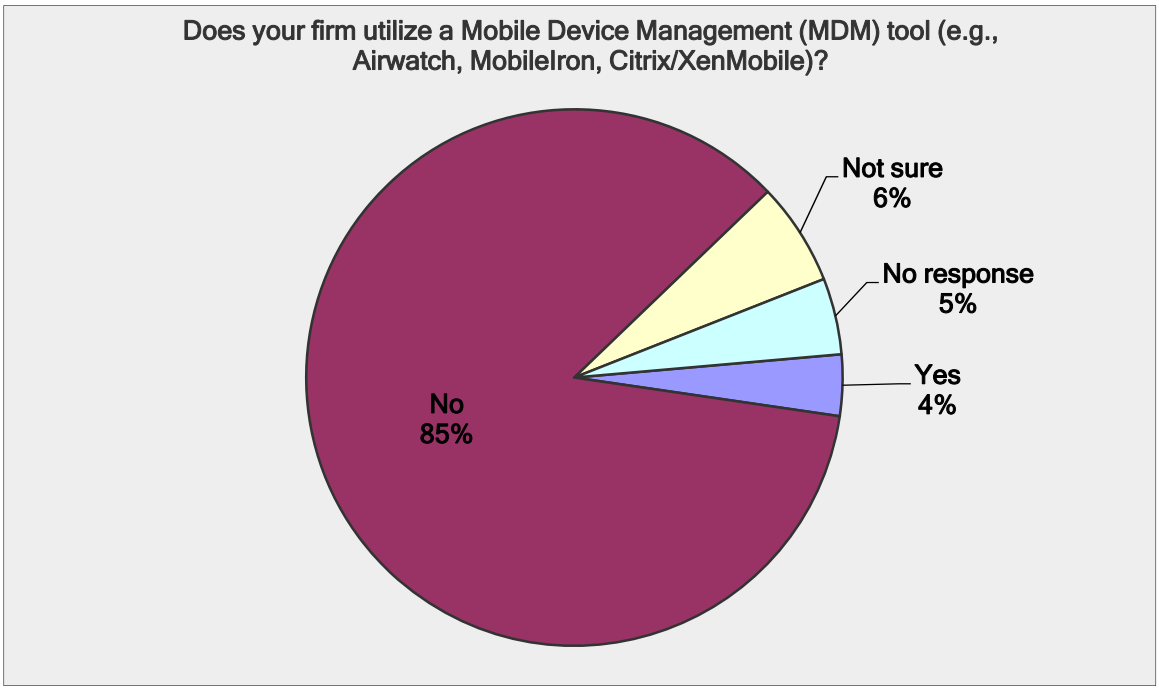




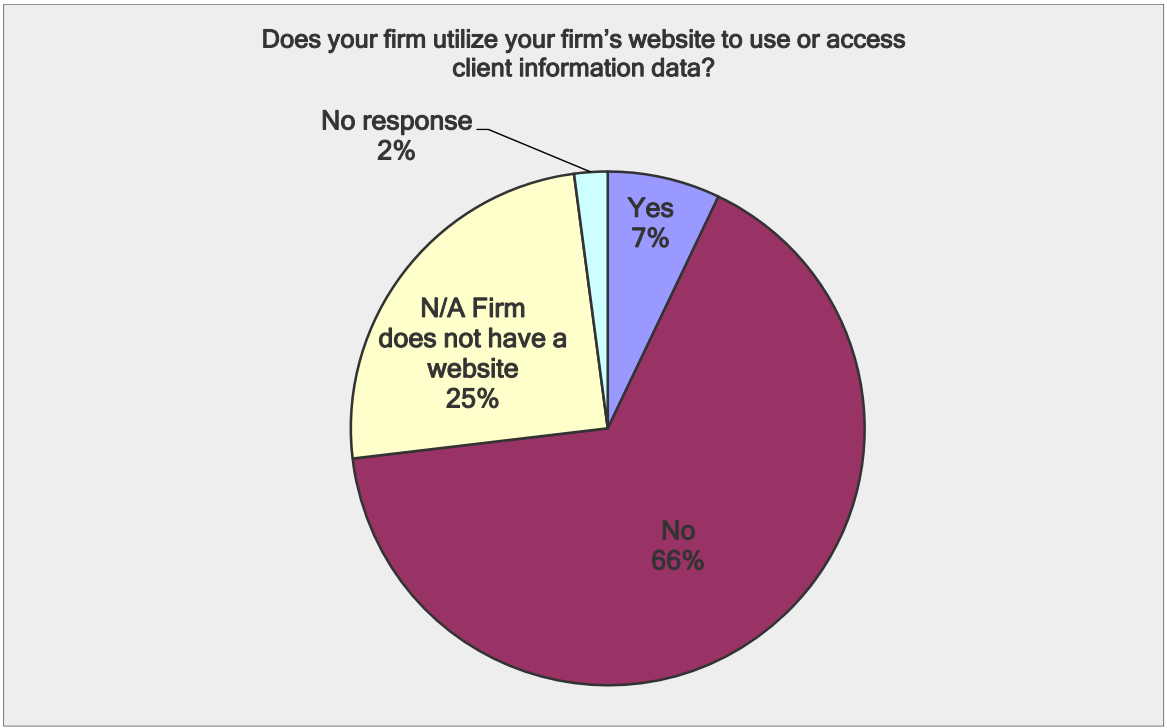
Use of Software as a Service (SAAS) Vendors

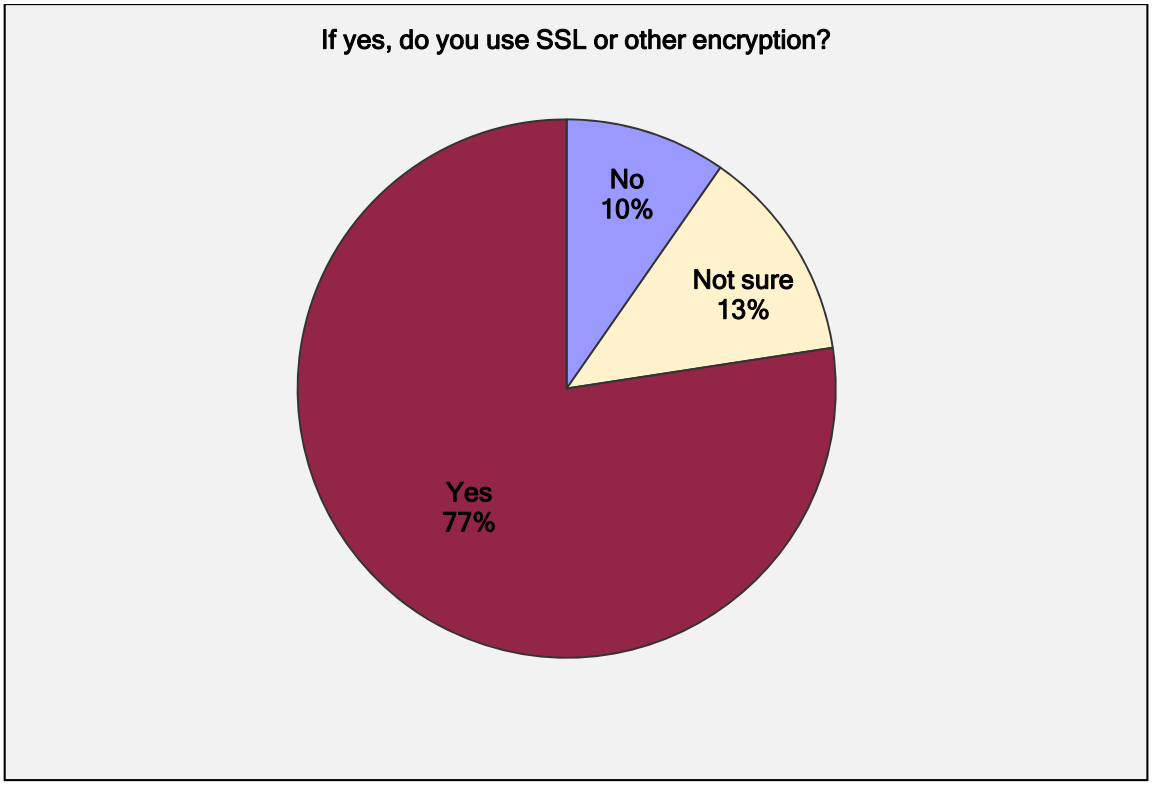


Use of Mobile Device Management (MDM) Tools

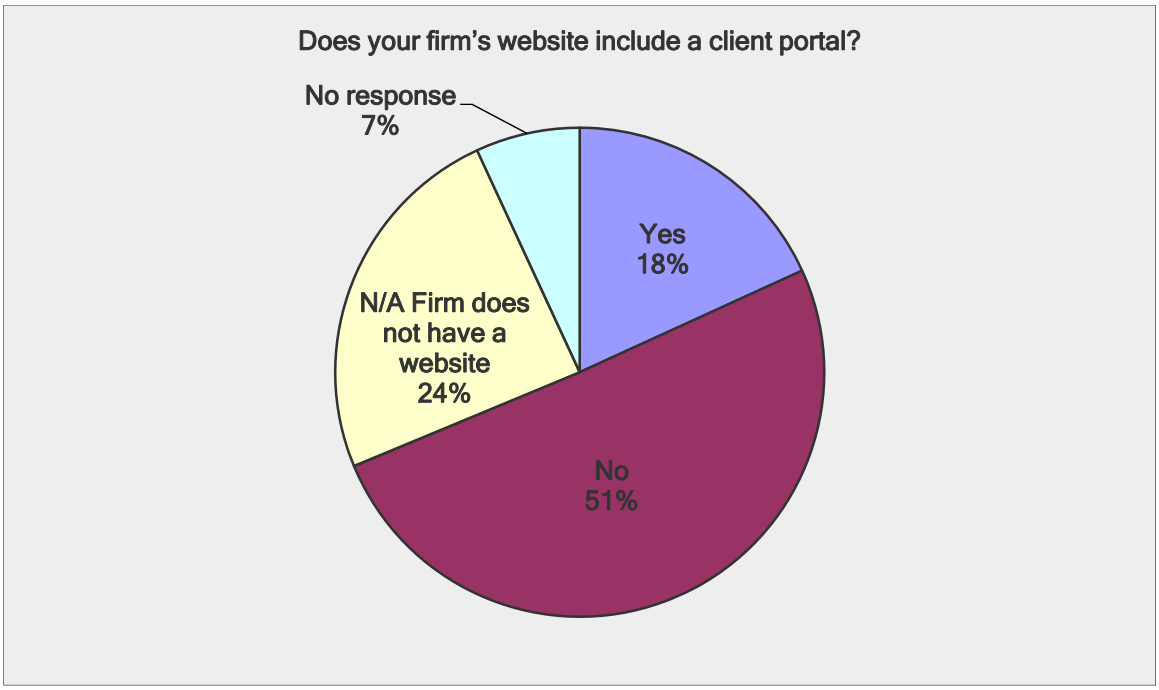


Use of Firm Websites to Access Client Data





Use of Client Portals on Firm Websites



Use of SSL or Other Encryption on Website's Client Portal