NEBRASKA
DEPARTMENT OF BANKING AND FINANCE

2018 Cybersecurity Survey of Nebraska-Registered Investment Advisers

The financial services industry is consistently ranked among the most cyber-attacked industries. Cybercriminals are interested in gaining access to valuable client information and assets. Cyberattacks can happen against large and small firms and can include denial of service attacks, malware, ransomware, phishing, and password attacks. Failure to keep client information and assets safe from cyber threats can be costly and harmful to a firm's reputation. The firm may also be required notify clients of data breaches.

The Nebraska Department of Banking and Finance, Bureau of Securities is responsible for implementing the Securities Act of Nebraska and serves as primary regulator for Nebraska-registered investment advisers. Due to the threat of cyberattacks against the financial industry and its clients, the Department collected information about firm practices to provide practical guidance for the Nebraska advisers.

In 2016, the Department issued a voluntary survey to all Nebraska-registered investment advisers to assess cybersecurity practices and risk management. The Department found that in general firms took cybersecurity threats seriously, developed policies and procedures to address cybersecurity, and made efforts to protect sensitive information. The Department also found that firms could improve cybersecurity practices, including using stronger passwords, using or layering additional encryption, and ensuring that anti-virus and anti-malware software was up to date.

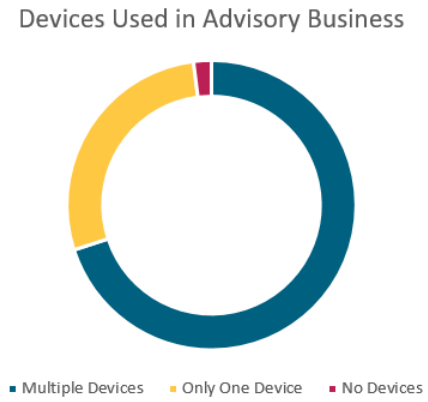
In 2018, the Department again surveyed all Nebraska-registered investment advisers to determine whether firms had improved their cybersecurity practices. The Department issued the 2018 Cybersecurity Survey to 92 Nebraska-registered investment advisers. Fifty-seven firms responded and fifty-six firms indicated that they use some type of device in their advisory business.

The Department thanks all of the investment advisers for their participation in the 2018 Cybersecurity Survey. The following information contains selected results and best practices to improve cybersecurity practices for Nebraska-registered investment advisers.

DEVICES

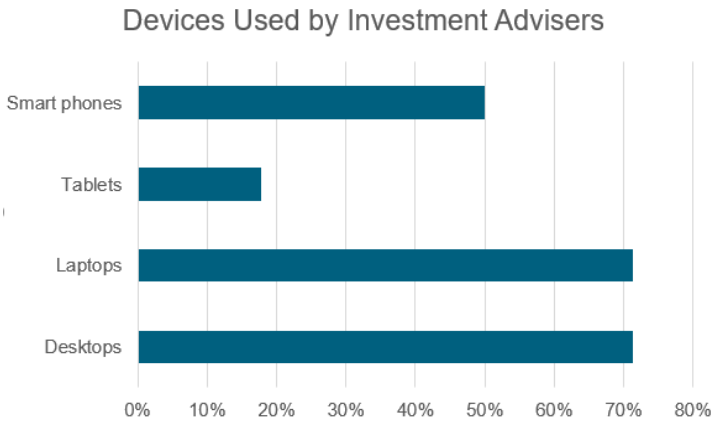
People use smartphones and tablets more and more in everyday life, including transacting business and accessing or sharing sensitive information. Nebraska advisers reported that 70% used more than one type of device, including smart phones, tablets, laptops, and desktop computers.

The most commonly used devices were laptops and desktop computers, but 50% of firms reported using smartphones to transact investment advisory business. Another 18% reported also using a tablet.



Cybersecurity Threat:

Many devices – like tablets and printers – connect to the internet and create a pathway for hackers to gain unauthorized access to your critical data. Any device, regardless of the manufacturer, is susceptible to cyberattack through unsecured internet connections or downloading malicious applications. Any Wi-Fi capable device, such as wireless printers or the Wi-Fi router itself, can be leveraged to gain access to other devices on the network.



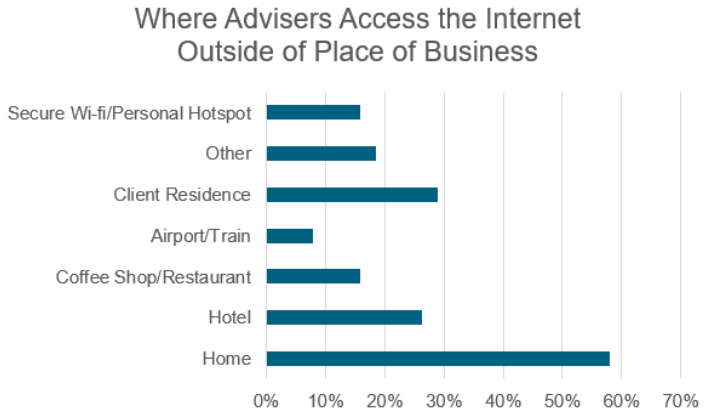
Best Practices:

- Use devices with built-in security and encryption
- Keep operating systems up-to-date
- Allow remote “wiping” of the device if lost or stolen
- Turn off Universal Plug and Play (UPnP) on your router and devices
- Use unique passwords on each device

WI-FI

Nebraska advisers are using devices outside of the office – 71% of firms reported using laptops, tablets, and smart phones to conduct advisory business away from their place of business.

Of those advisers that reported using their devices away from their office, 95% stated that they used devices to access the internet. Firms reported that use of the internet was primarily at home (58%),



client residences (29%), or otherwise using secure Wi-Fi or personal hotspots (16%). However, advisers also indicated that they accessed the internet at a variety of public spaces including hotels (26%), coffee shops and restaurants (16%), airports and train stations (8%), and other spaces (16%).

Cybersecurity Threat:

The use of public Wi-Fi, free or fee-based, can pose a security risk to your device, and potentially client data. These networks generally do not require authentication to establish a network connection and allow anyone to establish a connection. A hacker can position a malicious device between you and the connection point or pose as a legitimate public network. Instead of connecting to a legitimate hotspot, a person sends information directly to a hacker. This increases the opportunity for someone to gain access to an unsecured device. Hackers can also use unsecured Wi-Fi, like in coffee shops or airports, to distribute malware to people accessing those networks.

Using a wireless connection in your home is convenient, but also raises security concerns. Unsecured Wi-Fi can allow a hacker to intercept data, gain access to shared files, or even take over your internet connection, even from some distance from the home.

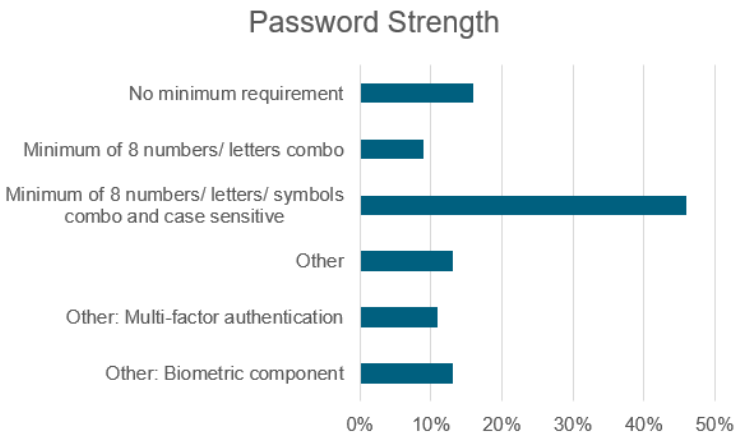
Best Practices:

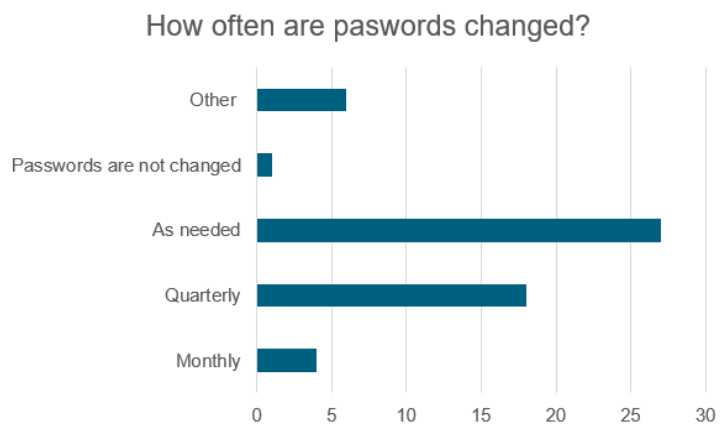
- Only use secure internet connections or personal hotspots
- Use VPN connections
- Do not share files over unsecured networks and turn off file sharing
- Turn off Wi-Fi and Bluetooth connections when not in use
- Encrypt data that is sent over the internet
- Bottom line: If you don't control it, don't use it

PASSWORDS

All Nebraska advisers reported using passwords on their devices. However, firms reported that the strength of those passwords varied among firms. New this year, 11% of firms reported that passwords required multi-factor authentication and 13% reported that access to devices required some type of biometric component such as a fingerprint or facial recognition.

Additionally, firms varied on how frequently they changed passwords. Firms reported that 48% changed passwords only "as needed" and 2% stated that they did not change passwords.





Cybersecurity Threat:

Weak and easy to guess passwords are one of the easiest ways for hackers to access your systems. Hackers have tools that can break any password if given enough time, especially if the password is short or contains common words or names. Keeping written passwords next to your computer invites anyone who has access to your office to also access your systems. Reusing passwords increases the risk that if someone gains access to one password, they now have access to any other system that uses that same password.

Best Practices:

- Keep passwords private and do not share with anyone
- Use longer passwords or passphrases that are harder to crack
- Regularly change passwords
- Use unique passwords for each system
- Use a secure password manager rather than writing them down on paper
- Use multi-factor authentication to add an extra layer of protection

[Password Fatigue]

Password fatigue occurs when you manage numerous unique and complex passwords. It can be confusing and difficult to remember each password, or to create new passwords. This causes people to use weak or reused passwords, creating a cybersecurity risk.

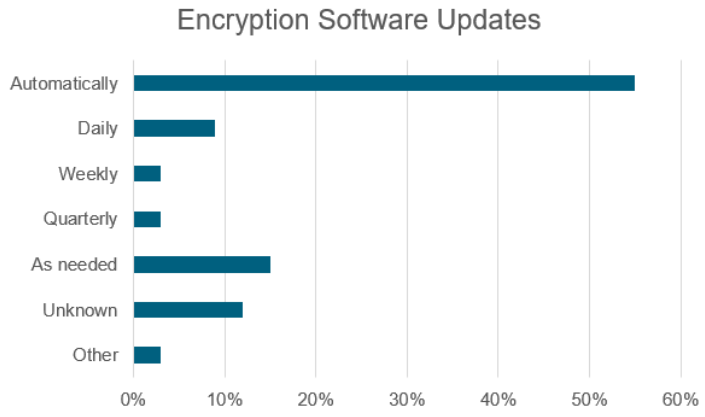
[Password Entropy]

Password entropy describes how long it takes to crack a password. Short passwords or passwords using common dictionary words can be cracked in minutes using readily available hacking tools. Longer, more complex passwords can take years to crack.

ENCYRPTION

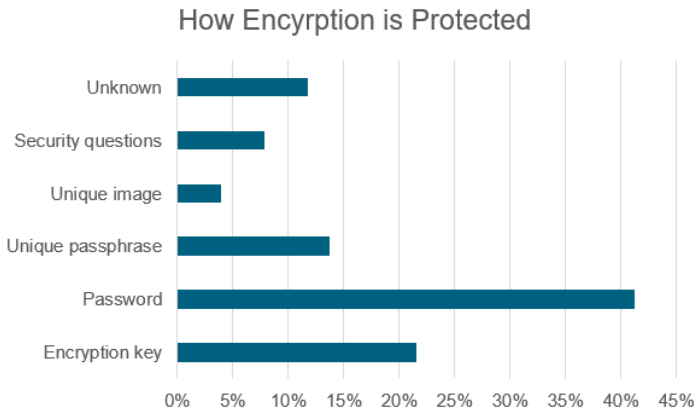
Encryption is an essential tool to protecting systems and client data. Of concern to the Department, Nebraska advisers responded that only 63% used encryption on their files or devices.

Encryption software works best when it is up-to-date. Encryption features also vary based on the age and “enterprise nature” of the device. Not all retail devices have TPM (Trusted Protection Module) chips. These TPM modules are what house the encryption keys. Most firms using encryption frequently update their software, with 67% of firms updating encryption software automatically, daily, or weekly. Firms are using a variety of methods of protect their encryption, including security questions and encryption keys.



Cybersecurity Threat:

Client and firm data, particularly in the financial industry, are subject to cyberattacks and potential data breaches. Encryption keeps data safe when sent over the internet by scrambling data so that only authorized users can read it. Encryption protects a user's identity and privacy. Encryption also provides an additional layer of security to data should someone gain access to your systems.



Best Practices:

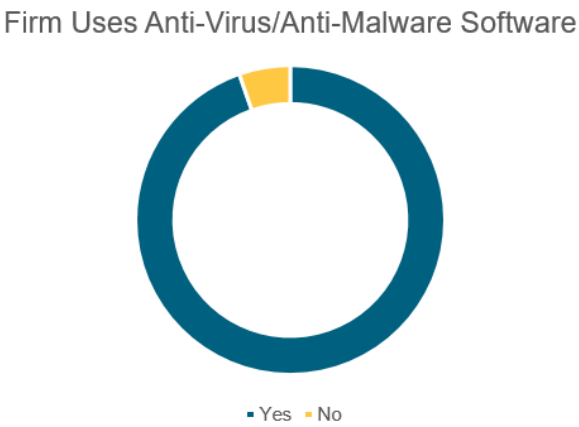
- Use encryption on all sensitive files and data
- Encrypt in layers (on files, hard drives, databases, etc.) to make it more difficult for hackers
- Store encryption keys securely
- Only visit websites with HTTPS
- Keep operating systems, software, and applications up-to-date on all devices
- Refresh devices used for business purposes at least every five years

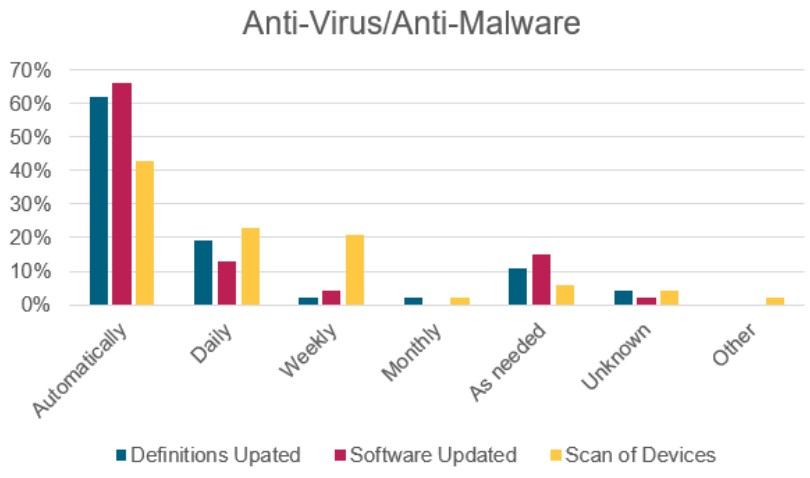
ANTI-VIRUS/ANTI-MALWARE PROTECTION

Every firm should be using anti-virus and anti-malware software to protect their systems and client data. Of concern to the Department is that 5% of Nebraska advisers reported that they did not have anti-virus or anti-malware software or were unaware if they had such software.

The most frequently cited reason for not having such software was that the firm only or primarily used devices believed to be protected by the manufacturer. It is important to note that any device, regardless of manufacturer, can be targeted by phishing schemes, viruses and malware and so firms should be taking precautions to protect client and firm data.

Nebraska advisers reported that they frequently update software and definitions to address current threats and risks – 83% of firms update definitions and software automatically, daily, or weekly. Firms reported that 87% scan their devices for viruses and malware automatically, daily, or weekly.





Cybersecurity Threat:

Viruses, worms, spyware, Trojan horses, ransomware, and other malware harm your systems by deleting files, accessing personal data, or even using your computer to attack others. These types of attacks are not just against large firms. Even small firms are targets because of the information and assets they hold and may be at a larger risk since they may lack expertise or resources to address cyber threats. Additionally, clients may be hacked in an attempt to infect firm systems to gain additional access.

Effective anti-virus and anti-malware programs can assist firms in protecting their systems. Cyber criminals are continuously creating viruses and malware to attack systems. Outdated software and definitions leave systems vulnerable to new cyberattacks. Even if you have installed anti-virus and anti-malware software, regularly scan your systems in order to identify and remove threats. Good tests of these practices include vulnerability scanning software and other third-party cybersecurity audits. Although it will not prevent every attack, anti-virus and anti-malware programs are an essential tool to help firms protect their systems and data.

[What is the Difference?]

Malware is any type of unwanted or malicious software that attacks host systems and includes adware, spyware, and ransomware.

Viruses are a type of malware, where a contagious piece of code infects a system and seeks to be shared between computers.

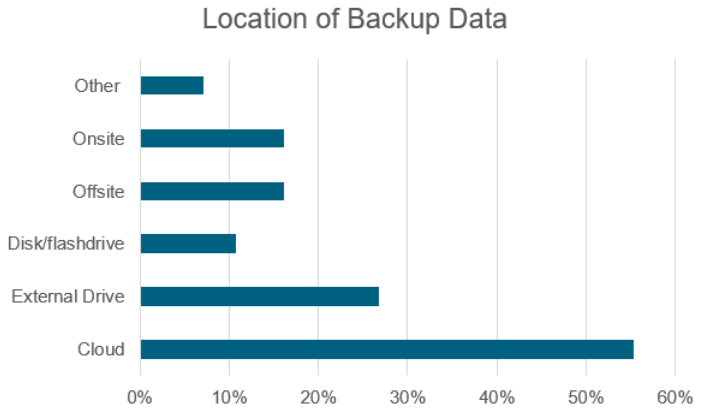
Most anti-malware software protects against viruses, and vice-versa. However, when selecting anti-virus/anti-malware protection, be sure to cover all types of threats.

Best Practices:

- Ensure that all devices, regardless of manufacturer, have strong anti-virus/anti-malware protection
- Regularly update anti-virus/anti-malware software and definitions
- Regularly scan all devices
- Be careful when clicking on links, downloading files, and downloading applications
- Update operating systems on all devices
- Use secure networks
- When in doubt, err on the side of caution
- Have systems and practices externally audited

DATA STORAGE AND BACKUP

It is important to store client data securely and to back up data to prevent the loss of data due to loss, theft, corruption, destruction, or ransomware. Nebraska advisers reported that 95% have a backup solution. How and where firms back up data is an important component to a firm's backup plan. Of the firms that reported that they backup data, 16% reported that they store the backup onsite and 17% reported that they do not encrypt the backup.



Increasingly, investment advisers are using the cloud and third party service providers to store and backup data. Of the firms that back up data, 55% use the cloud to store data and 74% use a third party services provider. Firms using a third party vendor reported that 85% have a written contract with that vendor and that 94% of those contracts include a non-disclosure or confidentiality clause.

Cybersecurity Threat:

Firms that do not back up firm or client data are at risk of interrupting business operations or potentially harming client assets if they lose or otherwise are unable to gain access to their files or systems. Encrypting backups is an important element to a cybersecurity plan. Firms should also consider keeping the backup stored in remote location. While maintaining onsite storage allows for easy access, it will also make accessing the backup difficult if something prevents you from accessing that location.

[What is the Cloud?]

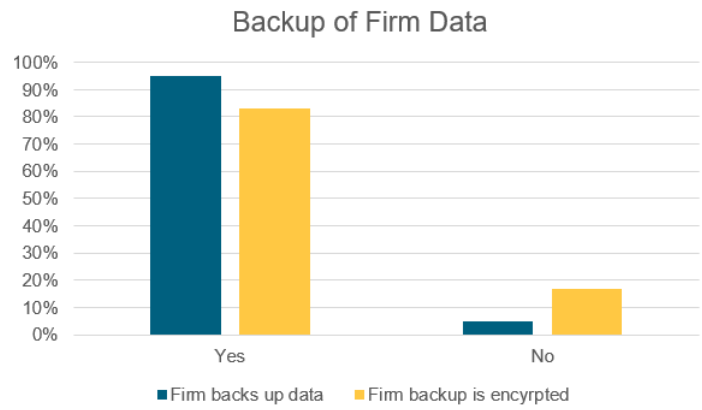
The cloud does not mean that your information and data are stored somewhere in the air. Cloud computing stores data or programs on a remote network of servers and accesses that data through the internet.

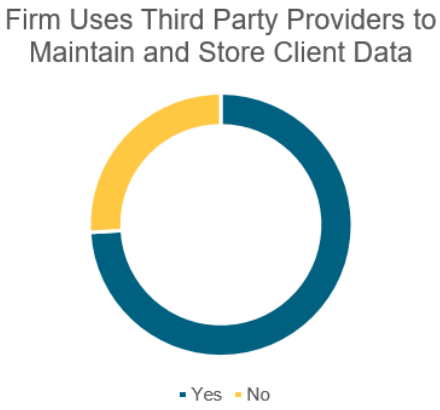
The cloud allows you to easily store and backup data without having to rely on your own hard drives or servers. It does mean that you will need to maintain an internet connection to access this information, which should be considered when developing a business continuity plan.

Depending on the terms of service, you may or may not own or control data once it is stored in the cloud.

Records maintained in the cloud or with a third party service provider must be safeguarded from possible data breaches, as hackers are increasingly looking to gain access to cloud systems. The cybersecurity and record retention practices from each vendor can vary considerably. Firms may not properly implement or use the vendor's systems, resulting in a storage solution that may not be as secure as the vendor can support.

It is the adviser's responsibility to conduct due diligence on these vendors to ensure that the vendor has sufficient cybersecurity controls to protect firm and client information and that use of the vendor are consistent with the adviser's requirements under the rules regarding record retention and confidentiality. Use of a vendor does not alleviate the adviser's responsibility to comply with securities laws.





Best Practices:

- Regularly review the services and protections provided by cloud vendors
- Read user agreements completely to understand how the vendor addresses record retention, data breaches, confidentiality, and what is your service level agreement
- Review privacy policies closely and configure privacy settings consistent with your obligations under securities laws
- Use strong passwords and multi-factor authentication
- Ensure data is encrypted both in transit and in storage
- Practice strong network security
- Take backups frequently and on a regular schedule

ADDRESSING CYBERSECURITY RISKS

In 2018, 5% of Nebraska advisers reported that in the last 24 months either the individual, the firm, or an employee had experienced theft, compromise, unauthorized access, or an attempt to steal, compromise, or gained access to firm data. With everything we know about cybersecurity and data breaches: it is a matter of when, not if, a data breach or hack will happen.

There are steps that Nebraska-registered investment advisers can do help protect their firm and their clients.

Cybersecurity Risk Assessments:

How and why your firm may be vulnerable to attack will vary from firm to firm. Conducting a cybersecurity risk assessment is an important tool to protect against threats. A cybersecurity assessment should take a thorough look at your systems, identify areas that may be vulnerable to attack, rate the severity of any impact, and rate the effectiveness of your current system. The risk assessment allows firms to allocate resources appropriately. A comprehensive assessment should be done in addition to any ongoing monitoring done by anti-virus/anti-malware programs.

The person conducting the assessment should be familiar with your systems and have sufficient knowledge about cybersecurity threats. It may be helpful for firms to use the services of an outside specialist for IT or cybersecurity matters. Nebraska advisers reported that 54% use such an outside specialist. It is important to perform your due diligence on any outside specialist.

[Risk Assessment Tools]

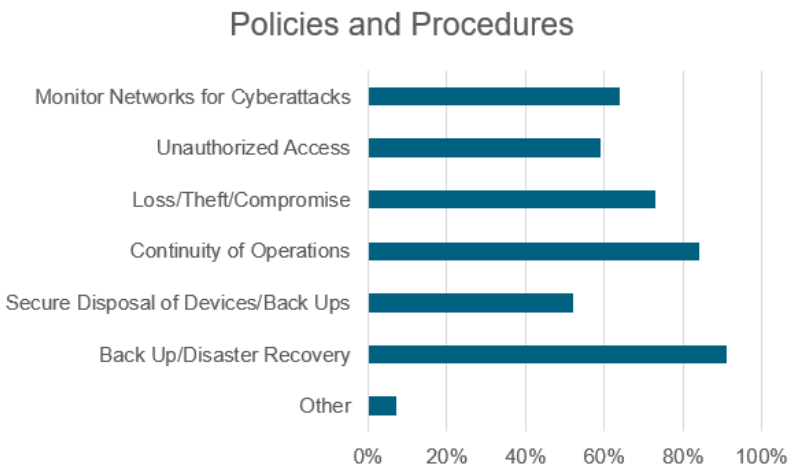
NASAA Cybersecurity Checklist for Investment Advisers
http://www.nasaa.org/industry-resources/investment-advisers/nasaa-cybersecurity-checklist/

FINRA Small Firm Cybersecurity Checklist
http://www.finra.org/industry/small-firm-cybersecurity-checklist

NIST Cybersecurity Framework
https://www.nist.gov/cyberframework

Cybersecurity Plans and Training:

The Securities Act of Nebraska does not require that investment advisers maintain policies and procedures that specifically address cybersecurity. However, it is considered a best practice to do so. Establishing strong cybersecurity policies and procedures is also consistent with Nebraska's requirement to create a business continuity plan and to maintain the confidentiality of client information.



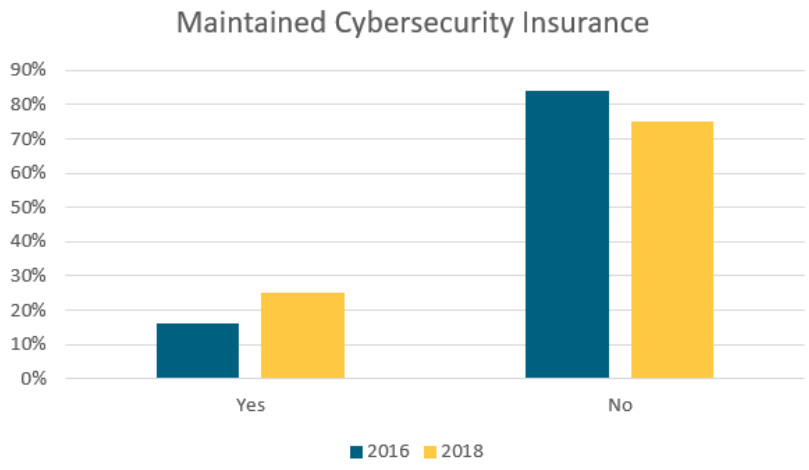
Seventy-nine percent of Nebraska advisers reported that they maintain policies and procedures regarding a variety of cybersecurity issuing including: cyberattacks, unauthorized access, data breaches, business continuity issues, and handling of devices and backups.

Conducting a risk assessment and creating strong cybersecurity policies and procedures helps firms to address risks specific to their business, plan how to protect themselves, and respond to data breaches. Cybersecurity policies should be regularly reviewed and tested to address new risks and business processes.

The biggest weakness to any firm's cybersecurity plan are the people implementing that plan. Any employee can fall for social engineering ploys used by hackers, such as phishing scams or clicking on unknown links that download malicious software. It is important train all employees on recognizing cybersecurity threats and understanding policies and procedures to address those threats.

Cybersecurity Insurance:

Another best practice is to consider carrying cybersecurity insurance to assist companies in the event of a cybersecurity event. In 2016, 16% of firms reported that they maintained cybersecurity insurance. In 2018, the number of firms reporting that they maintained cybersecurity insurance increased to 25%. The Department is encouraged that more advisers are seeking out additional protections from cybersecurity insurance.



Cybersecurity insurance can be in a stand-alone policy or as a rider to an existing policy. Cybersecurity insurance can help firms address the costs of responding to data breaches and hacks. Different policies will provide different levels of coverage. Firms should carefully review insurance policies to ensure it addresses their needs.

ADDITIONAL RESOURCES

- NASAA 2017 Investment Adviser Coordinated Exams
  http://www.nasaa.org/wp-content/uploads/2011/10/2017-IA-Coordinated-Examinations.pdf

- NASAA 2014 Cybersecurity Report
  http://www.nasaa.org/industry-resources/investment-advisers/nasaa-cybersecurity-report/

- NIST Cybersecurity Resources
  https://www.nist.gov/topics/cybersecurity

- SANS Resources
  https://www.sans.org/security-resources/

- Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006
  https://nebraskalegislature.gov/laws/statutes.php?statute=87-801

Our Vision

To Make Nebraska the Most Trusted Financial Home for People and Businesses.

Our Mission

Our mission is to protect and maintain the public confidence through the fair, efficient, and experienced supervision of the state-regulated financial services industries; to assist the public in their dealings with those entities; to assist those whom we regulate in a manner which allows them to remain competitive, yet maintain their soundness in compliance with the law; to fulfill our statutory responsibilities with regard to all licensees and registrants; and to investigate violations of the laws and cooperate with other agencies in seeking a timely resolution of problems and questions.

Contact

Claire McHenry, Deputy Director – Securities Bureau
PO Box 95006
1526 K St #300
Lincoln, NE 68508
(402) 471-3445
claire.mchenry@nebraska.gov