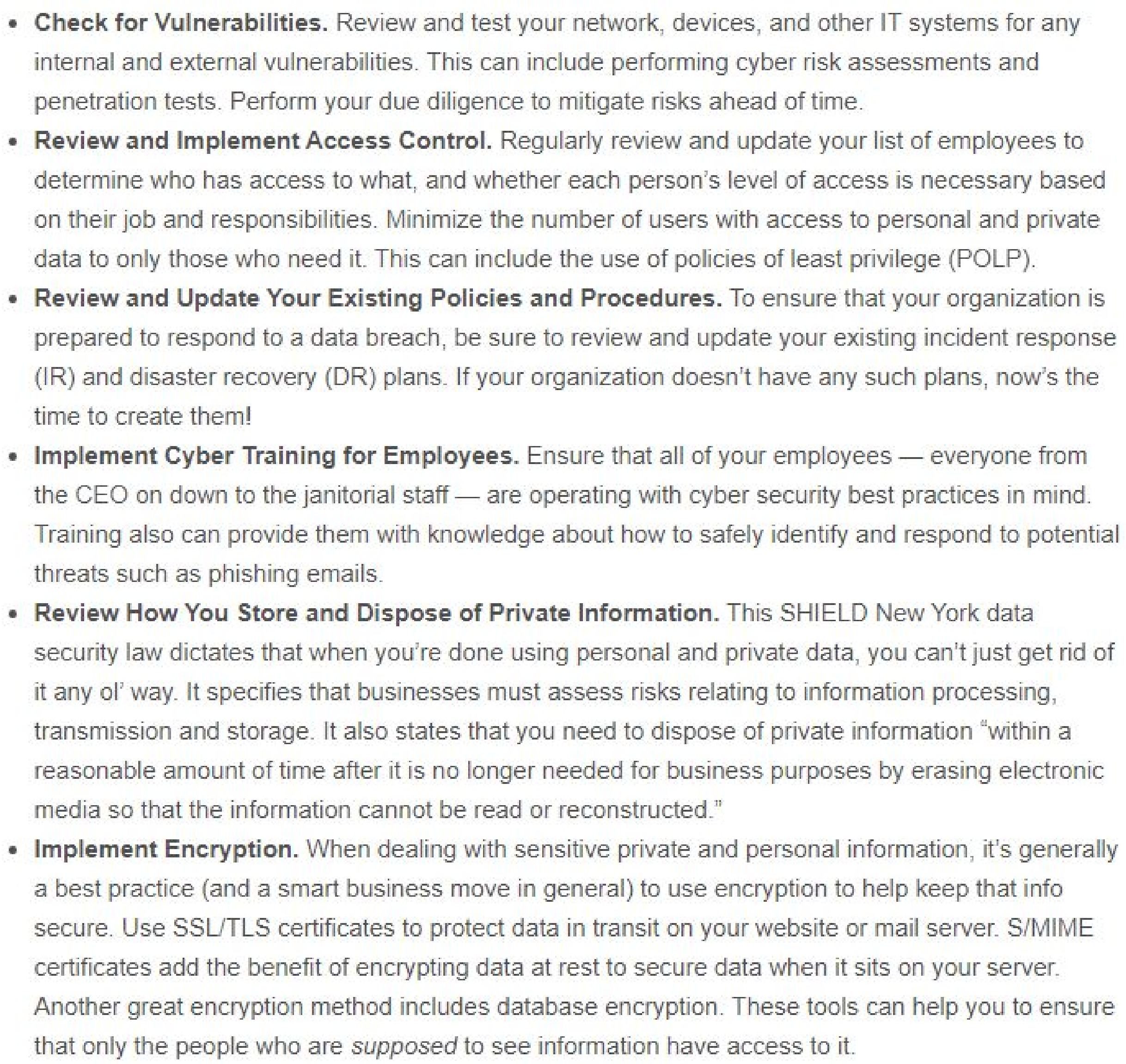
I am doing some research for a New York University program, can I ask you some questions about Cyber Security? I don't need to know your name or any personal information. (Try to see if you can use a recording app, ask for permission first)

1. Can you tell me your job title?
2. What do you know about Cyber Security?
    a. If they don't know: Cyber security is the process of protecting networks, devices, and programs from any type of cyberattack.
3. On a scale from 1 to 10, how much do you care about protecting your personal and private information?
4. Where in the real world, would you call or go to if you had Cyber Security related questions?
5. Where in the real world, would you call or go to if you need Cyber Security related services?
6. Do you know about the NY SHIELD Act?
    a. If they don't know: If your business or organization has employees or customers, you must implement security measures to protect their personal and private information or else you can face fines of $5,000 per violation up to $250,000.
7. If you own a business, how much money will you be willing to spend to secure your systems?
    a. Do you know how much it cost to hire a cyber security consultant?
        i. (After they answer): Up to $250 an hour.
    b. What would you do if you can't afford the fees to hire cyber security professionals?
8. Would be able to implement the features below on your own?



- **Check for Vulnerabilities.** Review and test your network, devices, and other IT systems for any internal and external vulnerabilities. This can include performing cyber risk assessments and penetration tests. Perform your due diligence to mitigate risks ahead of time.
- **Review and Implement Access Control.** Regularly review and update your list of employees to determine who has access to what, and whether each person's level of access is necessary based on their job and responsibilities. Minimize the number of users with access to personal and private data to only those who need it. This can include the use of policies of least privilege (POLP).
- **Review and Update Your Existing Policies and Procedures.** To ensure that your organization is prepared to respond to a data breach, be sure to review and update your existing incident response (IR) and disaster recovery (DR) plans. If your organization doesn't have any such plans, now's the time to create them!
- **Implement Cyber Training for Employees.** Ensure that all of your employees — everyone from the CEO on down to the janitorial staff — are operating with cyber security best practices in mind. Training also can provide them with knowledge about how to safely identify and respond to potential threats such as phishing emails.
- **Review How You Store and Dispose of Private Information.** This SHIELD New York data security law dictates that when you're done using personal and private data, you can't just get rid of it any ol' way. It specifies that businesses must assess risks relating to information processing, transmission and storage. It also states that you need to dispose of private information "within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed."
- **Implement Encryption.** When dealing with sensitive private and personal information, it's generally a best practice (and a smart business move in general) to use encryption to help keep that info secure. Use SSL/TLS certificates to protect data in transit on your website or mail server. S/MIME certificates add the benefit of encrypting data at rest to secure data when it sits on your server. Another great encryption method includes database encryption. These tools can help you to ensure that only the people who are *supposed* to see information have access to it.

9. If you were going to hire a security consultant, would you choose the **consultant with a Cyber Security Masters degree and no experience** or the **consultant with no degree but 3 years of professional cyber security experience**?
10. Do you think the city should be responsible for subsidizing Cyber Security services for people or businesses that can't afford them?
11. That's all the questions I have, thank you for your time!
    a. Only if they have questions about why you're asking them questions.
    b. I am helping conduct research for a non-profit startup that wants to provide **free** cyber security services for people and businesses that can't afford them. (See if they have any responses)
    c. **END RECORDING**

Bootcamp specific questions:

1. Are you willing to support a program which will bridge the gap experience recent bootcamp grads have vs the one the jobs require?
2. What would you like to see from such a program? Success metrics?
3. Are you willing to recommend us to recent bootcamp grads? Why or why not?

Cyber NYC & NYC govt:

1. How important are SMBs is in the Cyber NYC strategy? Why important or not important?
2. If there is (and we think there is) a gap b/w experience required by jobs and recent bootcamp grads lack of experience. Are you willing to support a program bridging this gap and
3. Can NYC govt provide funding for our idea? What success metrics are needed?

Small Businesses Questions

1. Would you prefer to learn how to protect your business through a presentation or a 1 on 1 consultation?
2. If the city were to provide free cyber security services to small businesses that can't afford them, what is the best way they can notify you?
    a. Email
    b. Flyer in mail
    c. On their website
    d. Phone call