10 Must Ask Cybersecurity & Information Security Questions

1

Question One: How well do you know your IT environment?

- Accurate inventory of devices and software.
- Accurate inventory of Internet- facing systems.

Recommendation: Perform an asset inventory.

2

Question Two: What data do the hackers want and where does it live?

- Explore not only structured data, but unstructured as well (e.g., spreadsheets, user reports, Word documents, PDFs and email).

Recommendation: Perform a data discovery assessment.

3

Question Three: If you have identified critical systems and data, how do you further protect access to it?

- Do you require complex passwords?
- Do you require two-factor authentication to critical systems and the network?
  - Email
  - VPN
  - CRM
  - ERP

Recommendation: Deploy logical access controls such as passphrases and two-factor authentication.

4

Question Four: Are your employees susceptible to being phished?

- Statistics show the answer is likely "yes".
- Have you tested/trained them?
- What technical controls have you put in place to stop it?

Recommendation: Conduct regular phishing campaigns and security awareness training.

5

Question Five: If phishing succeeds, do you have additional protection methods?

- Advanced endpoint protection complements traditional anti-virus;
- Encryption of data; and
- Whitelisting of allowed applications.

Recommendation: Deploy other security measures such as endpoint protection, data encryption, de-identification and application whitelisting.

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

For more information on Schneider Downs cybersecurity services, please visit www.schneiderdowns.com/cybersecurity or contact us at cybersecurityteam@schneiderdowns.com.

6

Question Six: Do you know where you are vulnerable?

- A large amount of breaches take advantage of unpatched operating systems and application software.
  – e.g., Equifax breach leveraged vulnerability in Apache Struts software toolkit.

Recommendation: Conduct regular network vulnerability scans and patch applications, servers and mobile devices.

7

Question Seven: Have you simulated an external attack to determine how secure/vulnerable you really are?

- Penetration tests or ethical hacking exercises are valuable because they help identify issues before the bad guys do.

Recommendation: Conduct external penetration tests and attempt to exploit detected vulnerabilities.

8

Question Eight: How prepared are you for a breach?

- Its not a matter of "IF" but, "WHEN."

Recommendation: Develop a cybersecurity incident response plan and test your data back up and recovery processes.

9

Question Nine: Are you subject to compliance with any data protection or cybersecurity regulations such as GDPR or New York Cyber Rules?

- Protect your organization and sensitive customer data.
- Avoid fines, penalties or reputation damage.

Recommendation: Conduct a Readiness examination.

10

Question Ten: Do you know what vendors have access to, or store your data?

- You can outsource certain business operations, but you can't outsource the risk.

Recommendation: Obtain SOC report from service providers and implement a third party risk management program.

COLUMBUS
65 E. State Street, Suite 2000
Columbus, OH 43215
P 614.621.4060
F 614.621.4062

PITTSBURGH
One PPG Place, Suite 1700
Pittsburgh, PA 15222
P 412.261.3644
F 412.261.4876

ASSURANCE AND TAX ADVISORS
BUSINESS ADVISORS
CORPORATE FINANCE ADVISORS
TECHNOLOGY ADVISORS
WEALTH MANAGEMENT ADVISORS