Cybersecurity Questions Every Business Should be Asking Before an Attack

iSymplify™

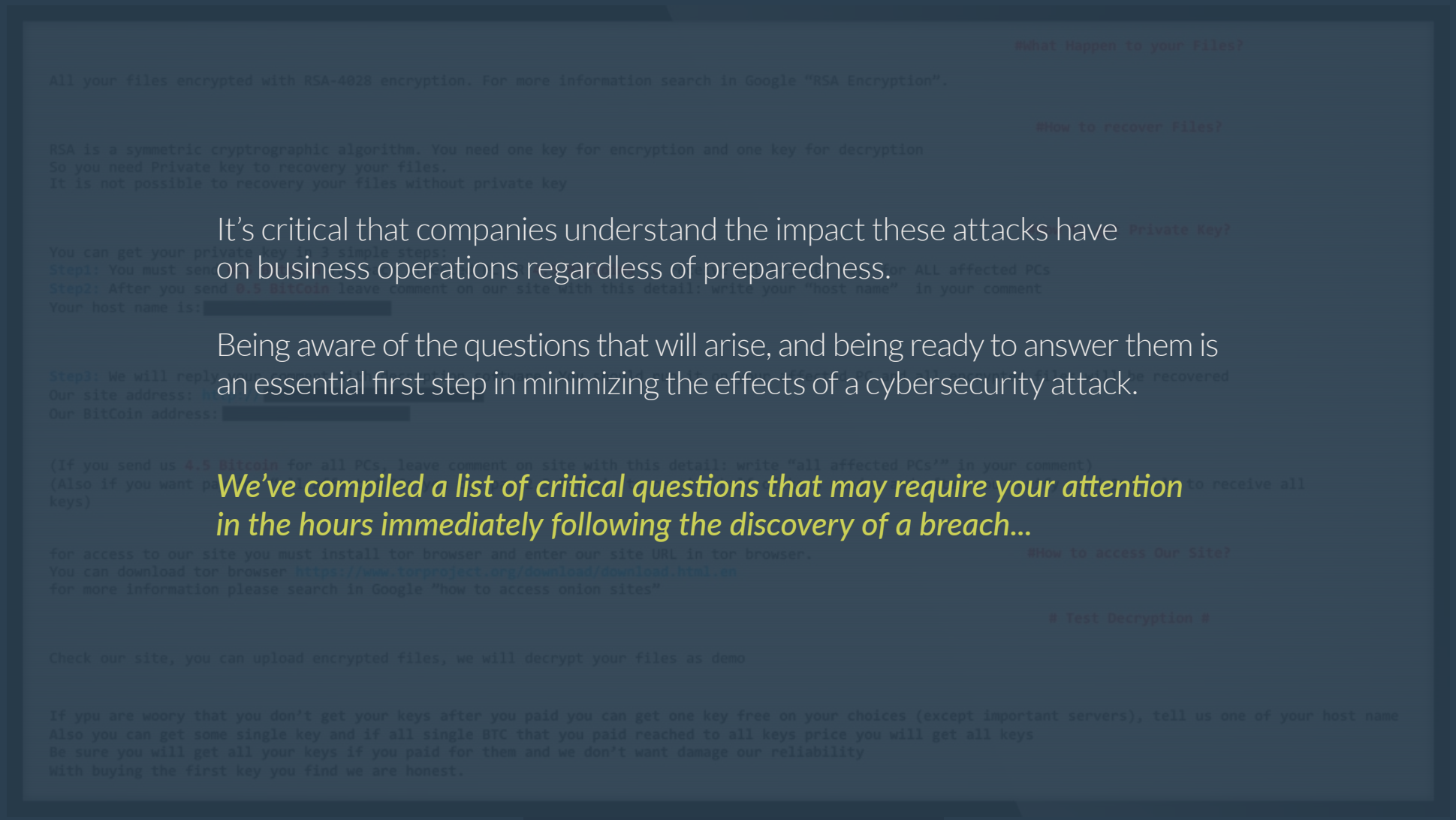
Tomorrow morning you get into the office, or turn on your computer, and discover the following message is on some or all of your computers:

How do you react?

How prepared is your company?

Attacks like these happen **every single day** to companies of all sizes.

This year they occur **about every 11 seconds**—more than **4000 times daily**.
Recovery can take weeks, sometimes months.



It's critical that companies understand the impact these attacks have on business operations regardless of preparedness.

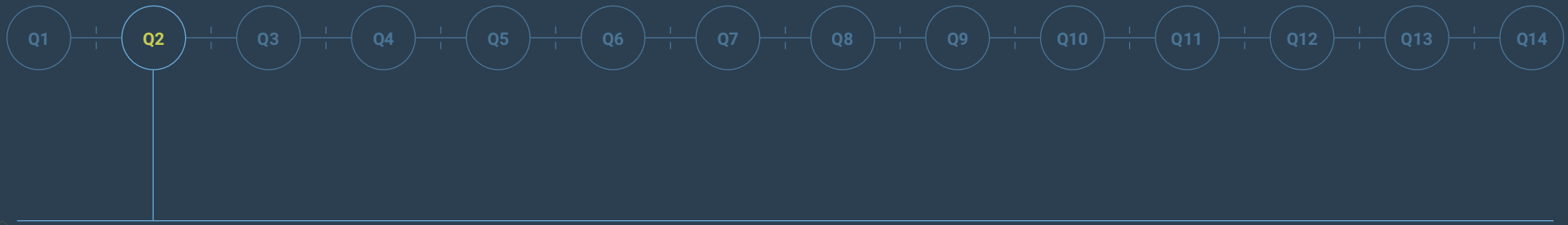
Being aware of the questions that will arise, and being ready to answer them is an essential first step in minimizing the effects of a cybersecurity attack.

We've compiled a list of critical questions that may require your attention in the hours immediately following the discovery of a breach...

Question 1

Do I call law enforcement? If so, who do we call… the local police, Homeland Security, the FBI? How do I know which law enforcement agency to engage?

Laws addressing data breaches are often enforced or governed by different entities according to the nature of the business. **In the event of a breach, knowing who to contact saves critical time**.



Question 2

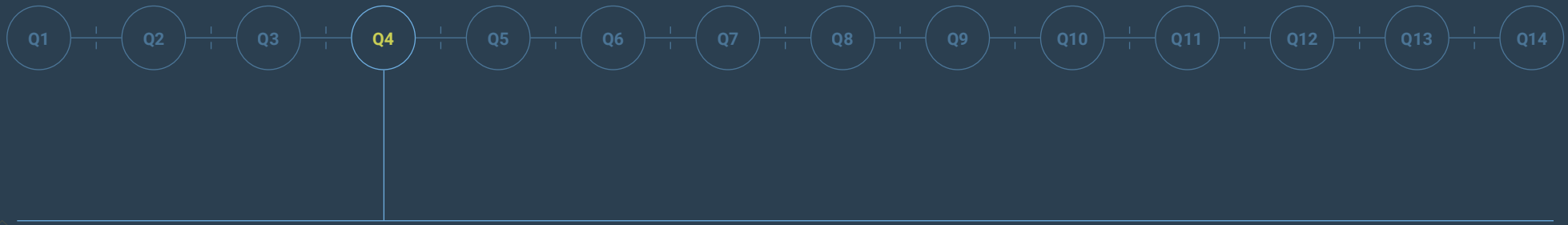
What do I do to mitigate the damage that has already been done to my information systems?

Mitigating the effects of an attack takes swift response by trained professionals. Defining those roles ahead of time can mean a faster road to recovery.

Question 3

Do I have backups of the data that was stolen and encrypted?

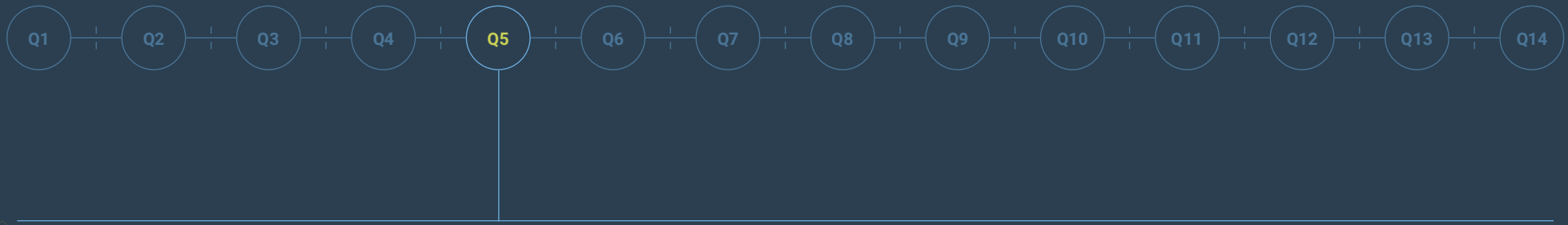
Secure backups, stored off premises, could drastically improve your company's ability to reduce the impact of a data breach. **If you have questions or concerns about your backups, address them now**.



Question 4

Exactly what data was compromised?

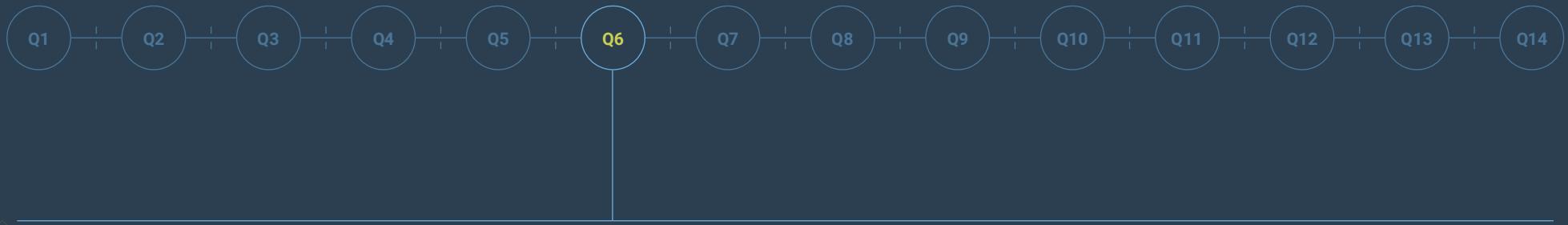
Know what data is stored within your network. You will need to determine if you have exposure to any privacy laws within the data that was compromised. Having a policy around where data is stored, and a retention policy for that data, is critical when responding to a breach.



Question 5

What do I need to tell customers whose information may have been compromised?

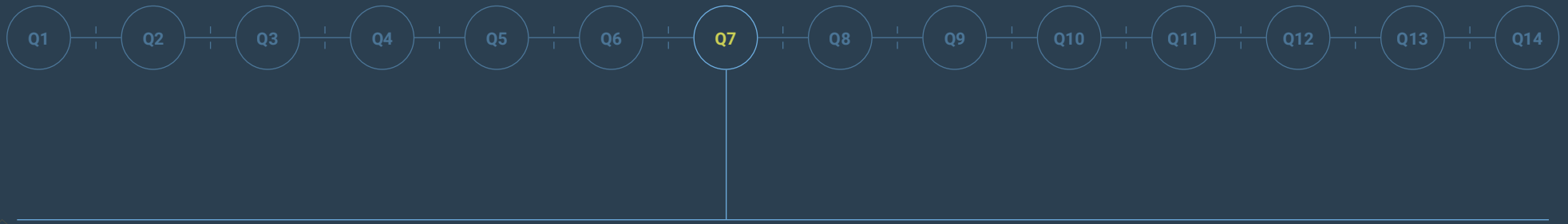
Your responsibility to your customers and their privacy could be the most damaging component of a cyberattack. Having a plan for taking the required action will help to ensure compliance with applicable law, and ideally minimize the impact on your clients.



Question 6

Do I have insurance against a cyberattack?

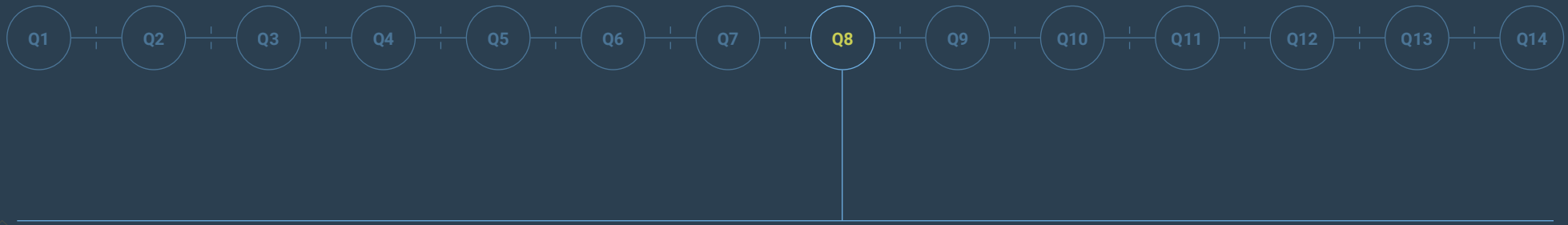
Breaches are costly. They can impact your ability to conduct business and lead to revenue loss. Breach remediation firms are also very costly, and without proper insurance coverage, your business will be responsible for any ransom payments deemed necessary.



Question 7

What exactly does the insurance cover?

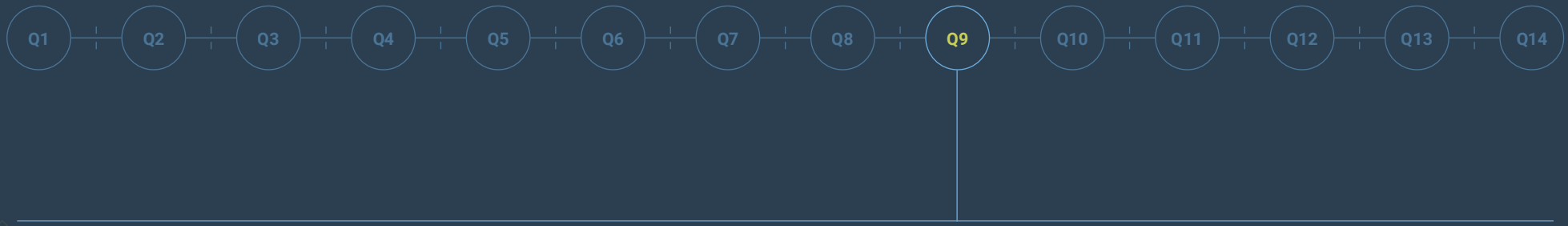
A cybersecurity insurance plan could be a business saving asset in the event of a breach. **You should know the answer to this question before an attack, not after.**



Question 8

What do I tell my employees?

A cyberattack can be emotionally and mentally taxing on your staff. Instilling confidence and a sense of control over the situation may reduce panic and improve critical collaborative efforts necessary to respond quickly and effectively.



Question 9

What is the plan for restoring my business to a pre-attack state?

Understanding who owns what responsibilities in responding to an attack is critical. Defining these roles after an attack can delay critical decisions which could prevent full recovery.

Have a proper plan. Know your internal resources, and identify any external dependencies on vendors. This will strengthen the success of your response in returning your business to normal operations.

Question 10

How do I determine how my systems were breached so that I can reduce the possibility of a future attack?

Root Cause Analysis of the attack will allow you to plug any holes in your security posture that may have led to the breach. Attackers will often create alternative paths into a breached environment in the event their exploit is discovered. Understanding who on your network has access to privileged accounts and when they were last accessed is critical.

Question 11

How long will a recovery take and what resources will I need to get back to an operational state?

Although not even the best plans can guarantee an answer, most qualified remediation teams can provide a realistic timeline for recovery once the extent of the attack has been identified.

This site lists the average at **19 days**.

Question 12

Do I have liability for the data that was compromised under privacy laws?

Many of us have probably received an email stating data we have provided to a trusted vendor has been breached. Often, they offer free credit monitoring as a remedy to protect further impact from the breach. This typically comes at the expense of the business who exposed that data.

Additionally, depending on the extent of the breach, companies can often be subject to lawsuits from customers and the government for the exposure of legally protected data.

Question 13

What will this do to the credibility of my business?

Cyberattacks, especially those events that compromise the integrity of your clients' privacy, can have devastating effects.

Demonstrating the ability to minimize the impact of an attack on your company and your clients can help to restore confidence in the safety and security of your business.

Question 14

As I restore my environment what additional steps should I be taking to improve my compromised environment?

Put the correct tools in place to more accurately guard the edge of your network and the devices connected to it. Designate a service provider or internal resource to monitor security logs on a daily basis and take proactive measures to increase your security posture.

For many companies, investing time and effort in cybersecurity can be challenging. Developing and maintaining a proper security posture doesn't have to be overwhelming.

Reliable, secure solutions are available and affordable for companies of all sizes.

At iSymplify, we work with companies to define their security needs and help identify the ideal technology partners for each scenario. And, we often find savings in other technology spends that help to pay, or completely cover, the costs of security upgrades.

Check out our **Cybersecurity Checklist** for a few simple ways to get started.

If you have questions about Security services, feel free to email us at info@isymplify.com or visit our website for more information.

We're here to help.

iSymplify™