ICE
TRUSTED IT PARTNER

ICE's Ultimate Guide to

QUALYFING FOR CYBER INSURANCE

TOP QUESTIONS YOU NEED TO BE PREPARED TO ANSWER

How many PII records are held on your network?

If you haven't taken the time to identify and classify the information on your network, it can be practically hard to calculate. Both sensitive and non-sensitive personally identifiable information (PII) is available. Legal specifics including a person's full name, Social Security number (SSN), driver's license, mailing address, credit card number, passport number, financial information, and medical history are examples of sensitive personal information. Depending on your business and the kind of records you keep on your network, you might need to often change the items on this list.

Do you limit remote access to all computer systems by using two-factor authentication?

Given the work-from-home tasks that many of us had to perform during the epidemic, I found this subject to be intriguing. The risk of remote access is obviously recognized by insurance underwriters, who want to make sure that we have two-factor authentication (2FA) if we use credentials outside of the office to remote into the company.

Can users access email through a web application on a non-corporate device?

The appearance of this query startled me. Large corporations frequently require the usage of separate devices for office access. Phones were once a bulwark of safe access, but they are now viewed as a network security issue. Insurance companies obviously want you to utilize 2FA to protect your email if you permit access through a non-corporate device.

Do you strictly enforce SPF on incoming emails?

A method of email authentication called Sender Policy Framework (SPF) is used to stop spammers from sending emails on your domain's behalf. An enterprise can publish approved mail servers using SPF. It also questioned whether your desktop email clients or firewalls offer sandbox functionality to assess attachments.

ICE
TRUSTED IT PARTNER

Do you provide periodic cybersecurity training to employees?

By asking this question, we can make sure that we're educating our staff to spot the popular attack vectors cybercriminals are using, for example Phishing Emails that look like they are coming from the IT department, but are actually spoofed webpages to collect login information.

Do you publish, update, and maintain a network security and privacy policy?

Updating normally entails writing an updated version of your policy, publishing it, and informing your clients of the main adjustments that have been made. Most data protection rules stipulate that you must inform customers of how their personal information is used and obtain their informed consent before implementing any changes.

Do you use a commercially available firewall and anti-virus protection system for all your computer systems?

It is advised to install both an antivirus program and a firewall on your computer. A firewall can aid in the blocking of dangerous communications, but it cannot find or delete malware. On the other side, antivirus software is made to find and get rid of viruses.

Do you use intrusion detection software to detect unauthorized access to your computer systems?

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.

Do you perform regular backups and store them in a secure off-site location?

In the age of ransomware, having a technique to restore data is essential for making sure you can recover from an attack. According to reports, even after receiving the decryption key during the recent Colonial Pipeline ransomware assault, they still had to restore from backup since the decryption procedure was taking too long.

Are your backups encrypted and kept separate from the network whether offline or with a specialist cloud service?

The next query was if we had ever tested the restoration and recovery of important service configurations and data. Too many businesses wait until they are in the middle of a disaster to properly test their complete recovery plan. Ensure sure your catastrophe recovery plan has been thoroughly tested.

Do you use endpoint protection in the network? What brand?

There were multiple inquiries regarding privileged user account security. Once more, they inquired as to whether privileged user accounts were protected by 2FA.

How long does it take to install critical, high severity patches?

In my organization, we do not install updates promptly. Instead, before deploying updates, we evaluate them to rule out any negative effects.

What steps are you taking to detect and prevent ransomware attacks?

They cited network segmentation, additional software tools, and outside security services as examples.

Do you have a SOC?

A centralized unit called a security operations center (SOC) handles organizational and technical security challenges. For maintaining and improving an organization's security posture, a SOC typically consists of people, processes, and technology. Do you have a department dedicated to monitoring, detecting, looking into, and responding to cyber threats? You could have to outsource to a third-party supplier if you lack the resources for a SOC.

Network operations centers (NOCs), though well-known to many of us, are not the same as a SOC. Protecting corporate networks, systems, and data from security threats is the SOC's main objective. The NOC is in charge of the overall performance, upkeep, and availability of the network.

CONTACT US FOR A COMPLIMENTARY SECURITY POSTURE ASSESSMENT TODAY

ICE Consulting, Inc
www.iceconsulting.com
888-423-4801

ICE
TRUSTED IT PARTNER