Cyber Insurance Requirements

Ransomware Protection

What Kind of Ransomware Protection is Required to Qualify for Most Cyber Policies?

Do you have the ransomware protection policies in place to get the extra protection you need when disaster strikes? You'll need to showcase you have ransomware protection policies in place as a preventative measure. In the event of a ransomware breach, you'll need a data backup plan with minimal mean time to recovery (MTR) Below, we've listed what cyber insurers are looking for to give you the coverage you need.

Ransomware Readiness Checklist

To qualify for certain cyber policies, you'll need to attest to the following ransomware protection protocols:

What Ransomware Protection Policies and Procedures Do You have in Place?

You will need to prove adequate coverage in the following arenas.

- [ ] Email Filtering to prevent phishing
- [ ] Suspected malicious email code management
- [ ] Email content and sender authentication protocols
- [ ] Multi-factor Authentication (MFA) Procedure
  - **Learn More about MFA Requirements**
- [ ] Web and web content filtering procedures
  - **Learn More about Web Content Filtering**
- [ ] Procedure for end users remotely accessing your network
  - **Learn more about Network Access Control**
- [ ] Remote access control protocol to your network
- [ ] Remote Desktop Protocol protection in your network
- [ ] Office 365 security add-ons utilization
- [ ] Security Awareness Training/ anti phishing training.
  - **Learn more about Security Awareness Training**
- [ ] Network Access Control Procedure.
  - **Learn more about Network Access Control**
- [ ] Applications and Application Data Privileged Access Control Protocol
- [ ] Endpoint Detection and Response (EDR) Solution in place
- [ ] Open port hygiene maintenance procedure
- [ ] Network access control procedure for Managed Service Providers (MSPs)
- [ ] Vulnerability Management Procedure (includes patch updates)
- [ ] Adequate security events monitoring and logging

Additionally, you'll need to determine if you have any unsupported systems and applications in your network and if so, identify to what extent.

Ransomware Recovery Questionnaire

You will need to have satisfactory answers for the following questions to ensure you have adequate ransomware recovery policies and procedures in place.

In the event of an infection of the core network and applications:

- [x] How quickly would your business operations be impacted?
  - Not sure? **Consider a Business Impact Analysis**
- [x] What percentage of the network could be recovered from a back-up?
  - **Learn More about Disaster Recovery**
- [x] What's your network redundancy?
- [x] What's the estimated number of hours to restore your business operations?
- [x] What's your Mean Time to Recovery (MTR) estimate?
- [x] How would you describe your back-up procedure?
- [x] How often are your critical systems and data files backed up?
- [x] What back-up storage do you have?
  - **Learn More about Data Storage Solutions**
- [x] How often is your network fail-over and recovery procedure tested?
- [x] What is the extent of your disaster recovery preparedness?

Pro Tip:

If you struggle to answer any of these questions, or are concerned that you coverage is not sufficient. Invest in an Incident Response Readiness Assessment!

Security Risk Assessment

A review of your entire security posture. Helps to Identify gaps and vulnerabilities.

Learn More

Virtual CISO (vCISO)

The creation or refinement your security policies and prepare you for new compliance requirements

Learn More

Ransomware Readiness Advisor

Examines the maturity of your current Ransomware Response Plan and program capabilities.

Learn More

Need Help Checking these Boxes?

IE has a team of Cybersecurity experts certified in data center management and ransomware protection protocols. If you're unable to answer any of the above questions, struggle to define what you have in place, or know you need extra assistance qualifying for cyber policies.

In the meantime, considering boosting your security arsenal with a **free trial of Cisco ThousandEyes**. This offering can help you identify threats faster, reducing your mean time to identification.

Try Cisco ThousandEyes Free

INTERNETWORK ENGINEERING