Cyber Insurance Coverage
How to Prepare

Overview

Many people are wondering – why are insurance companies doing this?
This is mainly due to the amount of money insurance providers have paid out in the last couple of years.

Preparing for Cyber Insurance Coverage

So, what has changed? Historically, cyber insurance applications have not required a large amount of information on security controls/policies in order to enact a cyber insurance policy. Due to the massive shift in the cyber landscape, providers now want more detail to better understand risks of insuring your organization.

They want to understand processes and controls your business has deployed to protect itself from cyber threats. Additionally, new cyber insurance policies have more detail on what is actually covered – and what is not covered. Thus, the importance of reading through your entire cyber insurance policy to understand the requirements.

1) Endpoint Detection Response/Managed Detection Response

Both of these tools monitor parts of your environment and can include advanced threat detection controls. They can identify and often mitigate threats.

Important to note – despite their similar names, these two tools are not the same. EDR is specific to the protection of the endpoint, while MDR monitors your entire network, from the endpoint to the server to the perimeter

2) Multi-Factor Authentication (MFA)

MFA is the practice of adding an additional authentication tool on top of a password. MFA helps to prevent a simple password breach from spreading to your entire network. If a password is compromised and the organization does not have MFA, the hacker could log in as the compromised user and send malicious emails that seem completely legitimate to the entire company; not to mention the overall access to the network. With MFA, this is prevented as the hacker does not have access to the user's cell phone.

3) Managed Threat Response

Managed Threat Response is similar to MDR and EDR. It provides a detection platform using Artificial Intelligence (AI), behavioral analytics, and signature controls, to detect threats. MTR has a security operations center (SOC) behind it and has the capability of notifying you of a threat as well as executing a remediation effort.

4) Policy Management

Security policies are being looked at more closely now by insurance providers. They want to understand your security planning, including disaster recovery and backup, with tested response strategies like a test incident response plan. Network segregation and due diligence on your vendor security measures are important as well.

5) Social Awareness

Insurers want to see that you are actively training end users to recognize cyber threats to protect your organization. Training should be continual throughout the year, not a one-time training, and tests should be administered to ensure training is effective. An end user's ability to recognize malicious items, like phishing emails, can mean the difference between keeping your organization safe and a complete breach of your systems.

How to Prepare for Cyber Insurance

The most important first steps are to gather your entire team – not just IT, but legal, compliance, HR, and more – and then consolidate all the security information about your organization. This way you can present all current security controls to the cyber insurance provider who is creating your policy, identifying vulnerabilities, and making a plan to address them. If you're looking for a cyber insurance provider after you've prepared, talk to your current business insurance provider to see what options they have.

The important part of getting cyber insurance coverage after these changes, is not having everything be 'perfect'. It is about demonstrating that you have proper security controls in place or are taking steps to add more controls.

How we can help

Over the past 5 years we have worked through the most complex cyber insurance requirements and remediation task.

We provide the complete approach combining cyber security and IT services to complete the coverage requirements.

This is delivered on our 24/7/365 active monitoring platform.

"Outstanding! Already there is a clear and profound difference over what they have received in the past. Thank you so much!"

-Leading Logistics Firm

Cloud1Solutions