How to Implement Cyber Insurance

Cyber Insurance for Small Healthcare Organizations

HHS 405(d)
Aligning Health Care
Industry Security Approaches

What is Cyber Insurance?

Cyber Insurance is one option that can help protect your business against losses resulting from a cyber–attack. Cyber insurance is an on-going partnership between you and your insurance company, used to continually improve your organization's security and ensure that needed protections are present and available in the event of a cyber attack. Working in partnership with your insurance company can help augment your organization’s practices to address security requirements, while effectively managing your premium costs.

Why is it important?

Due to the increase in targeted attacks on the healthcare sector, having added protection can potentially ensure you will not have to shut your doors if you become the victim of a cyber attack. Cyber insurance can help protect your organization from excessive costs that can occur in the event of a cyber attack. It can prevent your organization from potentially going out of business due to a successful attack. This is even more impactful for small organizations that may have limited resources.

How will this keep my organization safe?

If your organization becomes the victim of a cyber attack cyber-insurance can provide your organization with access to third-party breach specialists including forensics, independent legal counsel working on your behalf, and possible reimbursement of loss of business coverage or revenue.

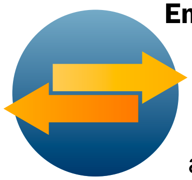
Threats Cyber Insurance Mitigates:

- Social engineering
- Ransomware attack
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss
- Attacks against network connected medical devices that may affect patient safety

Implementation Tips:

Have a minimum level of security controls in place. Be advised that many policies require you have a minimum level of security controls in place. You should not secure a cyber insurance policy in lieu of implementing cybersecurity practices. The HICP publication can be utilized as an outline in your search for security policies that could satisfy this requirement.

Discuss which policy would best fit your company’s needs. If you are thinking about cyber insurance, discuss the policy that fits your company’s needs with potential Insurance providers. This should include whether you should go with first-party coverage, third-party coverage, or both.



Ensure your policy includes cyber attacks on your data held by vendors and other third parties’. Third-party vendors that require access to provide services to your organization can also be a liability to your network. Their connection can be used by an attacker to take down your network. Ensuring that they are also included in your cyber insurance policy will provide you with an additional layer of protecting your valuable health information.

Include Cyber-attacks aided by insiders both intentional and unintentional in your policy . Insider threats involve people who typically have legitimate access to your computer systems and network. Whether through negligence or malice, insiders can compromise your patient and enterprise data over short or extended periods of time. This has serious repercussions for the patients, their security, and overall quality of care delivery. Therefore, it is important to include internal vulnerabilities as well into your cyber-insurance policy.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, X, LinkedIn and Instagram!*