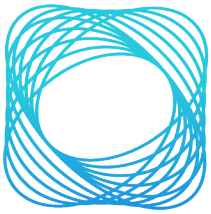
WHITEPAPER



SOTER TECH
SOLUTIONS

CYBER INSURANCE A CYBERSECURITY PLAN

Cyber Insurance is a Security Practice Every Business Should Implement into their Cybersecurity Plan.

BY: CHRISTIAN MEDEROS

Cyber insurance is a crucial, yet often neglected aspect of an organization's security posture. As cyber attacks continue to evolve and grow in volume, businesses must reassess how they incorporate cyber liability policies into their overarching cybersecurity plan. Learn how cyber insurance benefits small-medium sized businesses and how cyber liability has adapted to the new threat landscape.

TABLE OF CONTENTS

WHAT IS **CYBER INSURANCE?**

In December of 2019, several hundred employees of an Arkansas-based telemarketing firm were given a notice that they would have to find new employment due to a recent ransomware attack made against the company. The Heritage Company suffered overwhelming financial loss as well as weeks of downtime, ultimately leading to the total shutdown of the organization. You can read more about this case in detail, **here.** Unfortunately, this attack is indicative of what many businesses face as the volume of cyber-attacks increase alongside the average cost. **Verizon reports** that when targeting small businesses, threat actors are financially motivated nearly 100% of the time. If an organization finds itself in the cross-hairs of a sophisticated threat actor, it could be disastrous. Smaller organizations are more than three times more likely to permanently close following a serious cyberattack than larger organizations.

Verizon reports that when targeting small businesses, threat actors are financially motivated nearly 100% of the time.

CYBERATTACKS: WHAT IS THE SOLUTION?

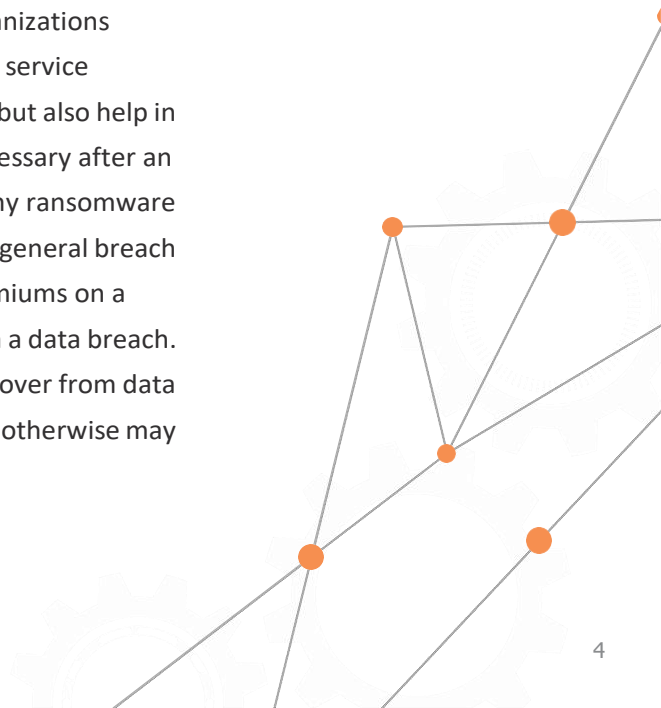
What is the solution to this ever-growing problem? Should organizations require yearly security awareness training for its employees? Is the solution implementing the strictest firewall policies available? Simply making sure every application is setup with Multifactor Authentication (MFA)? All these practices are components of what go into crafting a rock-solid cybersecurity plan. However, these controls aren't perfect, and humans make mistakes. When it comes to comprehensively mitigation an organization's cyber risk, an often-neglected concept is that of Cyber insurance. In the past, pieces of an organization's insurance risk transference strategy may have included a form of cyber policy, as an add-on to an existing insurance policy. However, due to the ever-evolving nature of cyber-attacks, how organizations address their cyber insurance and how insurers craft their policies must adapt to the times. **AdvisorSmith conducted a survey** of 1,122 U.S. based small businesses and found that only 17% had "some form of cyber insurance". With threat actors demanding more from their victims, small businesses must reconsider how they approach their cyber insurance. It is important to recognize that cyber insurance, as a stand-alone policy, is necessary in today's security environment to curb the financial risks of ransomware, data exfiltration, social engineering, and other attack vectors.

BENEFITS OF **CYBER INSURANCE**

Many organizations may ask themselves how cyber insurance benefits them. Oftentimes, cyber attacks and data breaches don't feel or look as tangible as other disasters that could negatively impact a business. Perhaps this is why cyber liability is considered "optional" rather than "necessary"? In order to better understand the current state of the cyber insurance industry and why it may be viewed as optional, an interview was conducted with John Cantrell, Certified Insurance Counselor (CIC) and owner of HB Cantrell and Co Insurance in Charlotte, NC. With thirty years of experience in the insurance industry, he was able to provide an experts insight on how cyber insurance benefits small businesses and why it is an often neglected process.

Cantrell explained that a well-defined cyber liability policy addresses multiple areas of risk consisting of ransomware, data exfiltration, social engineering, and financial loss. According to Cantrell, a separate cyber liability policy gives businesses the tools necessary to recover from a data breach that small businesses often lack the resources to utilize. This includes forensics, remediation tools, and protection against fraudulent wire transfers that may not have been accessible under a conventional property or liability policy. A strong cyber liability policy is, at the end of the day, intended to cover the financial cost of a cybersecurity incident or data breach within an organization.

According to Cantrell, a solid cyber liability policy should provide access to forensics tools to understand how the bad actors got into an organizations network, the enlistment of a data recovery specialist or managed service provider (MSP) to help with data recovery and incident response, but also help in covering the cost of any hardware replacements that may be necessary after an attack. Standalone cyber policies also offer to cover the cost of any ransomware payments that must be made, regulatory fines due to lost data, or general breach expenses. From a purely financial perspective, the insurance premiums on a cyber liability policy are far less than the expenses that result from a data breach. From a practical sense, cyber liability empowers businesses to recover from data breaches faster and more effectively by giving them the tools they otherwise may not have.



EVOLUTION OF **CYBER INSURANCE**

It is important to understand how insurance offerings have changed over the past few years. As cyber-attacks continue to evolve and bad actors develop newer and trickier tactics, the controls used to combat them must change too. It's no different with cyber insurance. John Cantrell noticed in the last 5 years that there was a change in attitude from policy holders on the necessity of a standalone policy. He stated that in 5 years it has gone from a suggestion for businesses to a requirement. To be considered "secure" a company is advised to have its own independent policy regarding cybersecurity. Organizations are now responsible for taking the next steps in securing their cyber insurance policy. Cantrell shared that businesses need to ask their insurance carriers if they have cyber, and if not, how can they get it.

> ***"As cyber-attacks continue to evolve and bad actors develop newer and tricker tactics, the controls to combat them must change too".***

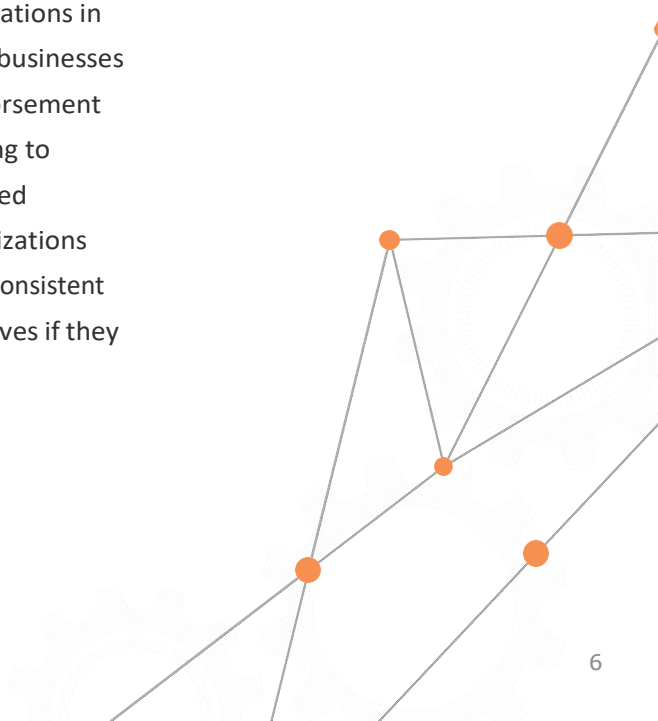
There has also been a shift in how insurance carriers measure responsibility. What is considered negligence on the policy holders account, and what falls within the bounds of a claim? As coverage broadens, more is expected from companies when implementing security controls. It's important to note that cyber insurance isn't a blank check to use if a business gets hit by a cyber-attack. Companies still need to do their due diligence in setting up protocols and security practices that reduce the probability of an attack happening at all. Many organizations may think they are covered, but when push comes to shove a neglected security control may keep them from collecting.

CYBERSECURITY ASSESSMENT

Before making any insurance related decision, your business should conduct a security assessment to get a baseline understanding of where your security posture lies. This assessment should use a recognized cybersecurity framework as a reference standard to ensure all vulnerabilities and gaps are accounted for prior to deciding. Assessing an organization's vulnerabilities using a recognized cybersecurity framework can aid businesses in making threat informed decisions about their cyber policies.

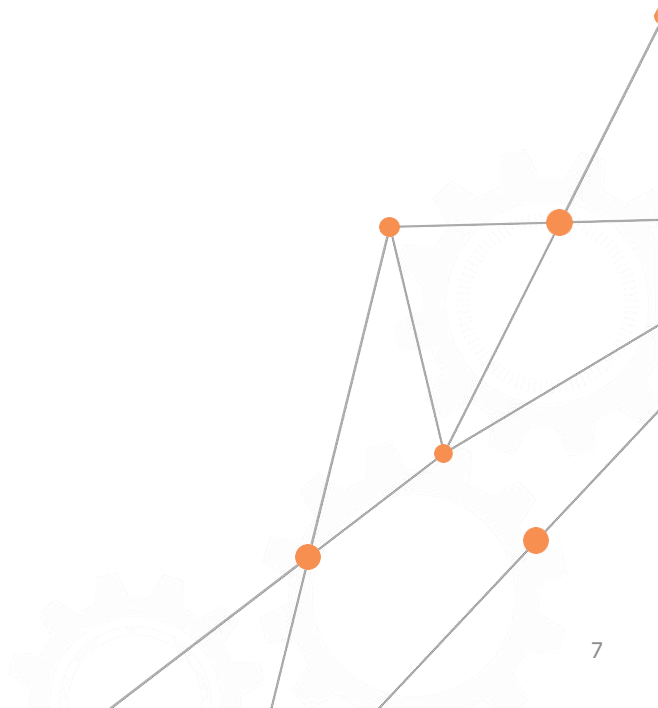
Insurers have begun to establish a more concrete metric of what coverage applies to and what responsibility the insured holds in securing their IT assets. Chubb, one of the world's largest traded property and casualty insurance companies, introduced several new endorsements in 2021 to their policies to address the rise of ransomware and other cyber risks. One such endorsement is the "Neglected Software Exploit Endorsement". Chubb's description of this endorsement states that the Neglected Software Exploit Endorsement "recognizes and rewards good software patching hygiene by providing full coverage for 45 days, and then for software that remains unpatched beyond 45 days, gradually re-weights risk sharing between the insured and insurer as time passes". What is so encouraging about this statement is that it gives companies a tangible and quantifiable time limit on how long they have to assess their organization for vulnerabilities and patch them.

A common critique of different compliance frameworks and regulations in the cybersecurity industry is how vague the time table is for when businesses need to be compliant or have certain practices in place. This endorsement from Chubb represents a monumental step forward in contributing to a security culture where both the insurer and insured have a shared responsibility to maintain security. This does mean that for organizations who haven't previously committed to vulnerability management or consistent security assessments have a larger role to play in securing themselves if they want to get the most out of their policy.



This endorsement from Chubb essentially means that if an insurer doesn't do their due diligence before those 45 days, the risk and responsibility will gradually shift back over to them. How do businesses make sure they keep full coverage under policies like these? The most sure-fire way is to implement some form of vulnerability management and patch management solution within the organization. Security isn't a one-time fix, but rather the continual process of discovering, managing, and remediating vulnerabilities in an IT infrastructure.

When addressing a company's overall security posture, cyber insurance is just one piece of all company's risk management plan, but it is an often neglected one. As the cost and volume of cyber attacks increase and the ways bad-actors infiltrate networks becomes more advanced, more businesses must consider a standalone cyber insurance policy. A common phrase used in the cybersecurity sphere is "it's not a matter of if, but when". This saying continues to ring true as we see more and more businesses fall victim to ransomware only to not have the resources to open again. Cyber insurance, like MFA or security awareness training, is a security practice that every business should implement into their cybersecurity plan.



SOTER TECH
SOLUTIONS

GET IN TOUCH

(305) 786-7490
sales@sotertechsolutions.us

Remote
Miami, FL 33176

www.sotertechsolutions.us