# CYBER INSURANCE MANAGER

With built-in application questions taken directly from dozens of the largest cyber insurance companies, there's no guesswork when it comes to compliance with your policy terms. This module quickly reveals specific red flags that may prevent you from getting paid in the event of a claim, and tells you what to do to fix it. Then, if you ever do have the need to make a claim, you'll have proof of the Due Care necessary to compel the insurance company to pay.

With an alarming uptick in data breaches and ransomware in recent years, an increasing number of businesses have opted to add Cyber Risk Insurance to protect themselves from catastrophic loss.

But as the threat landscape continues to expand, many insurance companies are restricting payouts by creating more claim exceptions and exclusions. Some of these are clearly stated, while others are hidden within confusing policy applications. This leaves many policy-holders vulnerable to holding the short-end of the stick when the insurer looks to disqualify a claim.

Cyber Insurance Manager ensures that companies with Cyber Risk Insurance actually get paid in the event of a claim by automatically verifying the accuracy of information submitted on the original insurance application and then documenting on an ongoing basis, that the business has used "due care" to reasonably secure their computer network against a breach.

## Compliance Reports

These reports show where you are in achieving compliance with the guidelines provided by your selected Cyber Insurance carriers. In addition, these documents identify and prioritize issues that must be remediated to address related security vulnerabilities through ongoing managed services.

Response Verification Reports (AIG Application, AIG Self- Assessment, Axis, BCS, Beazley, Chubb, CNA, Travelers, XL Group, Hiscox )

With Cyber Insurance Manager, you can perform insurance assessments based on specific criteria from several different insurance carriers. Depending on the carriers you select, you will be prompted to answer various questions about your overall site and network security. This helps you know exactly how best you can improve your overall security, as well as document your compliance with the security provisions outlined by your insurance carrier. You will receive a Response Verification Report for each insurance carrier you select during the assessment. This documents your responses to the carrier-specific questions.

Personal Data File Scan Report The report identifies specific and detailed instances of personal identifiable information (PII) throughout your computer network that could be the target of hackers and malicious insider.

## Compensating Control Worksheet

The report is used present the details associated with security exceptions and how Compensating Controls will be or have been implemented to enable compliance. Here you can document any false positives. You can also indicate if you have taken measures to reduce or avoid any issues identified in the assessment that might not otherwise appear in your assessment documentation. The benefit of this feature is that it adds back in the human element into the assessment and allows for explanation of special circumstances and specific environment requirements.

## Network Assessment Full Detail Report

This report provides comprehensive documentation of the current configuration and use of the network. The report shows assets in high-level views, allowing you to easily get an overall assessment of the entire network. Discovered issues are highlighted, making it easy to spot individual problems.

## External Vulnerability Scan Detail by Issue Report

A more compact version of the External Vulnerability Scan Detail report that is organized by issues. Devices that are affected are listed within an issue type. This report is useful for technicians that are looking to resolve specific issues identified within the environment, rather than performing remediation on a particular system.

## Cyber Risk Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

## Cyber Risk Analysis

The Cyber Risk Analysis Report aggregates risk analysis from multiple assessments performed on the network, providing you with both a Cyber Risk Score and a high-level overview of the health and security of the network. This includes a summary of individual issues, as well as their severity and weighting within the risk analysis. At the end of the report, you can find a summary of the assets discovered on the network, in addition to other useful information organized by assessment type.

## Supporting Documents

These documents show the detailed information and raw data that backs up the compliance reports. These documents include the various interviews and worksheets, as well as detailed data collections on network assets, shares, login analysis, etc.

## External Port Use Worksheet

Understanding where you have ePHI Data is an important component of HIPAA compliance. The Personal Data Scan System Selection Worksheet allows you to specify which systems are scanned for ePHI during the assessment process. A comprehensive scan should be performed annually to help identify and document all potential locations for personal data as defined by HIPAA.

## Anti-virus Verification Worksheet

Compliance Manager will automatically detect any anti-virus software installed on PCs on the target network. The Anti-virus Verification Worksheet details whether each endpoint on the network has anti-virus software installed. It also displays the type of anti-virus software.

## File Scan Validation Worksheet

This worksheet details each instance of sensitive data discovered on the network. It displays the PC name, IP address, and file path where sensitive data was detected. You can verify whether the information is valid or a false positive.

## File Scan Selection Worksheet

Understanding where you have sensitive data (ePHI, Cardholder Data, and PII) is an important component of data protection security. A comprehensive scan should be performed annually to help identify and document all potential locations for sensitive data. Complete the worksheet to identify systems to run the automated sensitive data file scan on.

### User Access Review Worksheet

The User Access Review Worksheet enables you to identify each user and to document their status: Employee, Third Party, Former Employee, Former Third Party, Service Account. You can also indicate whether each user has Remote Access. This is important for understanding which users have access to the network — and especially which users have access to sensitive information.

### Cyber Liability Questionnaire

The Cyber Liability Questionnaire is used to gather information about your organization's IT Security Policies and Procedures and ongoing sensitive data protection practices. The questions in this document are based on the specific insurance carriers you select during the assessment process.

## Cyber Risk Update Assessment Reports

### External Vulnerability Scan Detail

Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

### Cyber Risk Management Plan Update

Based on the findings in the Cyber Risk Update Assessment, the organization must create a Cyber Risk Management Plan with tasks required to minimize, avoid, or respond to identified risks to IT security and regulatory compliance.

The Cyber Risk Management Plan Update contains a list of tasks that can be executed to mitigate identified IT Security risks.

### Cyber Risk Change Summary Report

Every time you use Cyber Risk Manager to run a Cyber Risk Update assessment on a given network, the Cyber Risk Manager generates the Cyber Risk Change Summary report.

This report compares the results the last Full Cyber Insurance Risk Assessment with the Risk Update Assessment's network scan, local computer scan(s), and external vulnerability scan results performed during the Risk Update Assessment process.

This report details changes in the network's User Accounts, Local Computer Accounts, Active Directory (A/D) Computers, Non-A/D Computers, Non-A/D Devices, External Vulnerabilities, along with a Windows computer Patch Summary.

## Cyber Risk Analysis Update

The Cyber Risk Analysis Update report lists IT Security risks identified during a Risk Update Assessment that impact the state of network security and Cyber Risk compliance. The Cyber Risk Analysis Update identifies what protections are in place and where there is a need for more.

The Cyber Risk Analysis Update report presents results in a list of items that must be remediated to ensure the security and confidentiality of sensitive or confidential information at rest and/or during its transmission.