Protecting Global Insurance Institutions with the **ARM Methodology** of Cyber Security

ACTIONABLE INSIGHT FOR INSURANCE SERVICE ORGANISATIONS

This paper represents our methods for improving the cyber security posture through the implementation of the ARM method.

GBMSTECH

SECURED BUSINESS CONTINUITY

www.gbmstech.com

Introduction

Cyber Attacks **Against Insurance Institutions**

Cyber-attacks against insurance institutions are becoming increasingly frequent and often very sophisticated. 2015 and 2016 have seen some of the biggest cyber-attacks ever on Global Insurance Providers.

Data breaches at healthcare insurers such as Anthem, Premera, Blue Cross, and CareFirst, resulted in a total loss of personal information of over 100 million US policy holders.

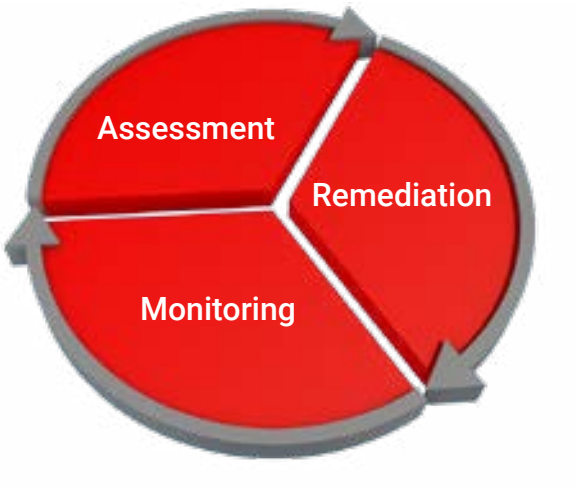
At a time of unprecedented cyber-attacks on insurers and an expanding cyber insurance market, US insurance supervisors have taken the lead in addressing insurers' cyber security risks.

Stuart Collins

All insurers **share with third parties**

All insurers, regardless of their size, complexity, or lines of business, collect, store, and share with third-parties (e.g., service providers, reinsurers) substantial amounts of private and confidential policyholder information, including in some instances sensitive health-related information.

Information obtained from insurers through data breaches or data loss may be used for financial gain through extortion, identity theft, misappropriation of intellectual property, or other criminal activities. Exposure of private data can potentially result in severe and lingering harm for the affected policyholders, as well as reputational damage to insurer sector participants. Similarly, malicious cyber-attacks against an insurer's critical systems may impede its ability to conduct business.



The objective of this paper is to raise awareness for insurers on how to approach the risks presented by cyber-attacks based around the ARM (Assess, Remediate, and Monitor) method of securing data and prevent cyber incidents.

> "From criminal syndicates, to terrorist organizations, to foreign intelligence groups, to disgruntled employees and other malicious intruders, the range of entities that stand ready to execute and exploit cyber-attacks has never been greater."
>
> U.S. Attorney General Eric H. Holder, Jr.

The **ARM Method**

The ARM methodology for protecting and preventing against cyber security attacks is a three-pronged circular methodology for employing cyber security practices at any insurance institution regardless of size.

In practice the ARM methodology employs the continual use of Assessments, Remediation, and Security Monitoring to paint a picture of the security posture.

Each step of the methodology is an important piece in the protection of the critical assets of an insurance institution.

The process is deployed in a circular format always starting with the Assessment to allow for building a complete and overall picture of the organization security posture. Following the assessment is a detailed remediation plan for correcting any vulnerabilities or security holes that are found in the assessments.

The final step

The final step in the process starts with the continual security monitoring of the insurance institutions infrastructure to continually identify any possible breaches or security incidents and act to correct them.

The ARM method is circular, meaning that the process continually runs in a circle and becomes a cycle of continual assessment, remediation, and monitoring. In today's ever-changing landscape of cybersecurity threats creating this cycle allows for the Insurance institutions to stay in front of any potential vulnerabilities, incidents, security breaches, or loss of data.

Assessment

The assessment starts the ARM method by assessing the current state of the network, business, and security policies of an insurance institution.

For any insurance institution to assess risk they need to know what assets they have, what assets are authorized to be on their network, and what assets are most important to protect.

Assessments are recognized as a crucial component of network security and are the critical first step in the ARM... method.

The assessments are performed to determine the actual security posture of the network environment. They are designed to explore whether an attack that could potentially bypass defenses and find an exploitable element in the network that could be used to steal information.

Assessment consists of:

- Penetration Testing (also called pen testing), is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit.

- Vulnerability assessment is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.

- Security Policies and Procedures Assessment is the practice of looking at the business or policy and procedure side of an organisation to determine if they are using the correct policies and if those policies are being followed.

Regulation and **compliance**

As the insurance regulatory landscape becomes increasingly complex with many States and Jurisdiction creating their own sets of regulation the risks associated with noncompliance increase and grow costlier.

Many insurance organizations and their security staff are **required to show compliance** to internal polices, federal and state regulation, and industry standard.

Current best practices indicate that a vulnerability assessment should be performed a minimum of **four times per year**, with **penetration testing done yearly**.

Remediation

Insurance institutions should be conducting regular assessments and using those assessments to identify all cybersecurity risks associated with firm assets then they should plan to prioritize their remediation of the risks.

Remediation is the second phase of the ARM method and as such takes the assessments and works with the stakeholders to identify the most important assets and the most critical vulnerabilities to fix.

Each assess/vulnerability that is identified to be updated/fixed will be completed during the remediation process and rescanned to validate that the vulnerability has been addressed.

Monitoring

Continual Monitoring is the final step in the ARM methodology for dealing with cyber security breaches. The GBMS Tech, Ltd. SOCaaS provides insurance institutions with the ability to have continual monitoring of their network and security infrastructure without the need of additional FTEs or security staff to their organization.

Due to ever increasing sophistication and persistence of malicious cyber activity combined with the sheer complexity and volume of security information, detecting security breaches requires an insurance institution to have a monitoring strategy in place to deal with the potential for malicious cyber activity.

The GBMS Tech, Ltd. SOCaaS has been developed and created to work with the institution to develop a strategy and deal with any breaches or incidents that are identified.

Once a potential breach has been identified, response timing is critical in the monitoring process.

The process, people, and technology that will respond to any breaches in accordance with the incident response plan of the insurance institution must have already been identified.

Threat Actors

ACTOR	TARGET	INSURANCE INDUSTRY
NATION STATES	• Business Plans • Trade Secrets • Disruptions	• International Plans • Access to Services
FOR-PROFIT HACKERS	• Account numbers • Personally Identifiable Information • M&A data for insider trading	• Customer Profiles • Account numbers
HACKTIVISTS	• Disruption of operation • Embarrassment	• Critical for business operations and business continuation
INSIDERS	• Theft of intellectual property • Disruption of critical systems	• Client lists • Business continuity

This guide does not address all areas of security; however, it does provide a proven method for cyber risk reduction that could allow an insurance institution to withstand or identify any potential cyber threats.

For further information, please contact us.

GBMSTECH

SECURED BUSINESS CONTINUITY

enquiries@gbmstech.com

+44 (0) 207 993 6949

www.gbmstech.com

1Berkeley Street
London, W1J 8DJ