esentire®

Cybersecurity for Insurance Providers

Insurance providers are at risk

The insurance industry is built on trust. Unfortunately, this trust can easily be lost in the event of a cyber breach. The insurance sector has fallen behind in its adoption of cybersecurity technologies. Although banks and other financial institutions were among the first to come under the attack of cybercriminals, they're now among the most secure. Cybercriminals have moved on to easier targets, which is where the risk lies for insurance providers.[1]

Hackers have identified the insurance industry as one that handles extremely sensitive information, but has yet to put effective measures in place to safeguard against cyber-attacks.[2] Furthermore, with an increasingly-distributed workforce, employees are accessing the network from unprotected locations, exposing firms to additional threats.

Only 20% of insurance CEOs believe their firm is prepared for a cybersecurity event, yet 42% realize that cybersecurity is their most serious concern – outweighing regulatory risk by a significant margin.[3]

Cybercriminals are targeting insurance providers for confidential customer data including finance and health information, insurance claim files, trade secrets, business assets and more.

The potential effects of a breach include:

- Financial loss
- Disruption of operation
- Compromised confidential information
- Reputational damage
- Challenges with regulatory bodies

Threats targeting insurance providers

According to eSentire Threat Intelligence[4], common attack methods used against the greater finance industry include:

Phishing: Which could indicate a lack of security among all employees.

Coin Miners: Which could indicate a lack of acceptable use policies and technical controls.

Tech Support Scams and Fake AV Social Engineering: Which could indicate a lack of employee awareness and the use of appropriate technical controls.

These methods – if successful – can cause serious business disruptions and extensive costs if not detected and responded to quickly.

Cybersecurity compliance requirements

Depending on your region and business activities, your firm may be required to comply with specific cybersecurity regulations from regulators like NAIC or other federal or state/provincial regulations.

Contact a security expert today to discuss your compliance requirements ▶ www.eSentire.com/get-started

The faster the firm catches the threat, the lower the impact

The costliest types of attacks for insurers are denial of service, phishing and social engineering and malicious insiders.[5] Because many firms have limited resources and defenses in place, protecting against these threats can be a challenging task.

Fortunately, the next victim doesn't have to be you. According to Aberdeen's Monte Carlo analysis, being twice as fast at threat detection and incident response lowers the business impact of a cyber-attack by approximately 70%.[6] The only way to avoid an incident and react quickly is to have a certified Security Operations Center (SOC) with human analysts hunting and responding to threats on your network 24x7x365.

We defend against the threats facing insurance providers

eSentire Managed Detection and Response™ (MDR) keeps insurance providers safe from cyber-attacks that other technologies miss. Our 24x7 Security Operations Centres (SOC) are staffed by elite security analysts who hunt, investigate and respond to known and unknown threats in real time.

With **MDR**, you'll experience:

- **24x7x365** continuous hunting and monitoring
- **Detection of unknown attacks** leveraging patterns and behavioral analytics
- **Human-led investigation** utilising always on full packet capture, logs and event data
- **Full forensic analysis** to confirm threats and eliminate false positives
- **Isolation and communication disruption** of the threat on your behalf, with no retainer fee
- **Full remediation support** until the threat is eliminated, not just alerting and guidance

We prepare insurance providers for complex compliance and regulatory requirements

Beyond MDR, our dedicated security experts help firms assess risks, address known gaps and build a comprehensive cybersecurity program that meets stringent regulatory requirements.

With **eSentire Advisory Services**, you'll have access to:

- Security Program Maturity Assessments
- Security Policy Guidance
- Security Incident Response Planning
- Security Architecture Review
- Health Checks
- Executive Briefings
- Penetration Testing & Vulnerability Assessments
- Risk Assessments
- Phishing Campaigns

[1] http://businessworld-usa.com/cyber-security-risks-facing-insurance-companies-2017/
[2] https://www.cloudsecuretech.com/information-security-breach-in-the-insurance-industry/
[3] http://businessworld-usa.com/cyber-security-risks-facing-insurance-companies-2017/
[4] 2017 Threat Report
[5] https://www.insurancejournal.com/news/national/2018/02/15/480708.htm
[6] https://www.mcafee.com/in/resources/reports/rp-aberdeen-cybersecurity-2017-summary.pdf

About eSentire

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Centre (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise grade protection and the ability to comply with growing regulatory requirements.For more information, visit www.eSentire.com and follow @eSentire.

esentire®