LogRhythm®
The Security Intelligence Company

The confidence game:
Cybersecurity and insurance

LogRhythm
The Security Intelligence Company

The confidence game

Insurers are intimately acquainted with risk. It's their business. They need to assess, rate and price risk. They advise clients how to reduce risk. They buy and sell risk. Unfortunately, many of them are at risk and don't realise it.

Business growth, increased IT complexity, changing regulations and expectations of anywhere/anytime customer service are making it harder for insurance companies to keep client data accessible and compliant and, simultaneously, secure.

A survey by Accenture found that 79 per cent of security executives at large insurers were confident in their cybersecurity strategies[1]. This would seem to bode well for these insurers and their stakeholders. Unfortunately, the same survey reports that the typical insurance organisation will face 113 targeted cyberattacks every year, a third of which will be successful. Clearly, confidence is no substitute for competence.

Recognising the risks

No insurer would write a policy without a thorough understanding of the risk they were taking on. Actuaries and algorithms have long been insurance industry fixtures because they allow the business to make better decisions. Why, then, are information security decisions made without the same due diligence? It may be that the scope seems overwhelmingly large. A KPMG report says that any insurer that is serious about improving cybersecurity must first assess its current status and suggests a five-point approach[2]:

1. **Ownership:** realise cybersecurity is a business issue, not an IT issue
2. **Capabilities:** take stock of what you do well and expand those best practices across the business
3. **Awareness:** understand who has access to your data, how they are using them and from where
4. **Organisation:** establishing protocols and processes that will work across the business, leaving no weak links
5. **Preparedness:** testing, drills and audits ensure that what you have built will work and staff stay sharp

Valuable targets:

Why would an attacker go after an insurance organisation when there are banks and trading houses to target? Because insurers have an incredible amount of valuable data. Thieves, competitors, money launderers and terrorists all have their eyes on the information in your system.

- Medical records
- Client financial information, including banking and credit details
- Information on client physical facilities, including security measures
- Financial information, the release of which could violate regulatory requirements
- Client contact information and passwords
- Proprietary information, including financial projections, sales and marketing plans, and new product information

Keeping up with business challenges means automating manual processes and integrating fragmented systems. The complexity of the task introduces risks at every turn. Business needs pull in different directions: Clients that want fast, seamless access versus stringent privacy regulations; global markets running 24/7 versus national regulators versus pan-national compliance; always-on cross-platform connectivity versus securing data.

[1] Insuring your Future: Cybersecurity and the Insurance Industry, Accenture, 2017. http://ins.accenture.com/rs/897-EWH-515/images/Accenture-Security-Report-2016-Key-Insights-for-Insurance-POV.pdf
[2] Facing the cyber threat in the insurance sector, KPMG, 2017. https://home.kpmg.com/qm/en/home/insights/2017/01/facing-the-cyber-threat-in-the-insurance-sector.html

LogRhythm
The Security Intelligence Company

Taming tech with tech

As counterintuitive as it might seem, the solution to the challenges that digitalisation and technology have brought is technology—if it's the right technology.

Addressing the threat of external attackers is the most obvious example of cybersecurity and intrusion detection and it's an essential first line of defence. However, it's not enough.

Harvard Business Review says that insiders are a "more pernicious threat[3]" that can often do more damage to an organisation because of the easier access they have. User and entity behaviour analytics (UEBA) can detect and flag and respond automatically not just to intrusion attempts but also to unusual behaviour from staff or partners. For example, if an employee is accessing a much larger amount of client information than he normally would on clients with whom he does not work and saving those files to his laptop, he may be preparing to jump ship to a competitor, taking valuable data with him. UEBA can identify this anomaly, flag it for investigation and suspend access until the investigation is completed.

Monitoring across systems also protects against viruses and ransomware that can spread throughout an organisation if even one machine on that network becomes infected. The WannaCry ransomware[4] outbreak of 2017 infected more than 200,000 machines and affected individuals and companies around the world. Recovering from the loss or compromise of data can cost millions and take months. There can also be severe reputational damage, a major concern for insurers, companies that depend on the trust of their clients to maintain and grow business.

In addition to providing effective protection against intruders, malicious insiders, viruses, ransomware, malware and other threats, intelligent, system-wide automated monitoring can help meet regulatory and compliance requirements. Whether it's the Prudential Regulation Authority, PCI DSS or the Sarbanes-Oxley Act, having clear, complete, and documented proof of data integrity and regulatory compliance reduces the risks of infractions and makes audits easier.

What LogRhythm brings to the table:

LogRhythm offers an integrated approach capable of addressing all common requirements and needs, including:

- Intelligent automation
- Real-time data management and network monitoring
- User authentication, verification and monitoring
- Regulatory and compliance demands
- Monitoring of privileged users with access to sensitive information
- UEBA (user and entity behaviour analytics)
- Rapid detection, mitigation and auditing of threats
- Digital chain of custody

Designed for the payment card industry (PCI) environment, LogRhythm's solutions provide visibility across networks and notify users immediately when suspicious activity is detected. They also deliver additional insights for other performance issues, such as remote access connection failures or missed scheduled software updates.

LogRhythm's solutions support insurance industry auditing requirements through Compliance Automation Suites with embedded content and enable long-term and secure data storage as well as wizard-based data recovery. Other capabilities include privileged user monitoring, web application defence, rapid forensics and advanced correlation and pattern recognition.

Collectively, LogRhythm's offerings provide insurance companies with industry-leading automation, compliance and auditing support, comprehensive reporting, and protection against advanced threats, delivering reward from risk.

[3] The Danger from Within, Harvard Business Review, 2014. https://hbr.org/2014/09/the-danger-from-within
[4] Inside the digital heist that terrorized the world—and only made $100k, Quartz, 2017. https://qz.com/985093/inside-the-digital-heist-that-terrorized-the-world-and-made-less-than-100k/

The complete solution

LogRhythm provides a complete, integrated solution to information security that fits the needs of the insurance industry. The LogRhythm NextGen SIEM Platform provides infrastructure monitoring to detect malicious activity – whether from outsiders or insider threats – on the network. Among its capabilities are user and entity behaviour analytics (UEBA) to detect anomalous activity and respond with alerts and automated mitigation. Security automation and orchestration (SAO) frees up time so in-house IT teams can focus on other important tasks and improve operational efficiency.

Network and data monitoring also support automated, real-time reports to verify activities and security for regulatory compliance and auditing requirements.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralising damaging cyberthreats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA) and security automation and orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations centre (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

LogRhythm®

The Security Intelligence Company

Security. Made Smarter.

Contact us

UK: **+44 (0)1628 918 330**
Germany: **+49 89 919292 - 200**
Middle East & North Africa: **+971 55 6422224**
europe@logrhythm.com | **www.logrhythm.com**

LogRhythm, Clarion House, Norreys Drive, Maidenhead, SL6 4FL, United Kingdom.