SKURIO

THE MULSANNE INSURANCE STORY

CASE STUDY

Protecting the business from increasing threats

Today's insurance sector has come a long way from the clipboard-carrying reps that collected premiums on the doorstep in the 1970s. A digital revolution has turned insurers, brokers, claims specialists and comparison sites fundamentally into technology businesses. These companies trade on a foundation of trust and efficiency. Attracting and retaining customers depends on their ability to provide differentiated customer service whilst guaranteeing the highest levels of data security.

Established in 2010, Mulsanne Insurance is a motor insurance disruptor, focused on the high-premium sector. The business operates in a highly networked and distributed market, using comparison websites to attract new business and reputable intermediaries for policy generation.

Insurers process vast amounts of data to understand the risks that apply to their policies. This data is highly sensitive too. It includes financial details and personal information that must be protected at all costs. And, this is the challenge, the very data used to operate their business is highly prized by threat actors and fraudsters. It's hardly surprising that insurance business incidents accounted for nearly a 5th of all ransomware attacks in the UK last year. The figure could have been higher still, if it weren't for companies like Mulsanne and its Insuretech parent, Abacai, going to great lengths to lower risk, mitigate threats and proactively prevent incidents from happening in the first place.

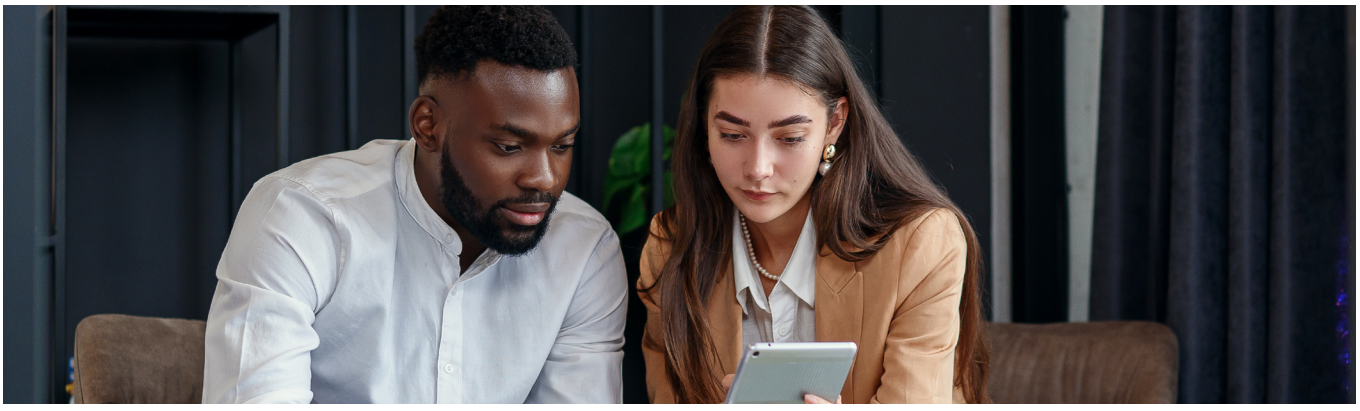
PROTECTING DATA ACROSS THE DIGITAL SUPPLY CHAIN

Mulsanne's IT Leader, James Borne, has responsibility for information security across the group. He identified an opportunity to improve the company's cybersecurity strategy by adding an external threat monitoring capability three years ago. The Skurio platform was selected to identify compromised data and potential threats with automated surface, Deep and Dark Web monitoring. Key factors in James' selection criteria included onboarding speed, ease of use and value for money.

Keeping it lean

To remain agile in such a fast-moving industry, Mulsanne operates with a "lean team of high-powered individuals". The company discounted threat detection solutions that would have required them to devote time and specialist skills to maintain. "We didn't want a massive overhead," explains James, "With Skurio, we can easily keep on top of incoming alerts and investigations using a lean team without impacting their other day-to-day responsibilities". Skurio improves team productivity by automating intelligence gathering, allowing security operations staff to focus on investigations and incident response.

> "We didn't want a massive overhead. With Skurio, we can easily keep on top of incoming alerts and investigations using a lean team without impacting their other day-to-day responsibilities."



Reducing the human factor

James' philosophy on cybersecurity is pragmatic and technology-centric. "You can spend a lot of time developing and documenting security policies, but you cannot rely on humans to adhere to them. By using the right technology solutions, threats can be mitigated or avoided without expecting staff to be consistently faultless."

Securing every link in the chain

Adding new partners to an extended digital supply chain increases risk. It's vital to ensure that any new partner takes digital risk and cybersecurity as seriously as Mulsanne does. Using Skurio, the IT team can understand the digital footprint of consenting suppliers, enabling them to make smarter decisions on which partners to select.

Specialists in listening

Skurio is used to detect compromised credentials, monitor for attack planning, identify potential typosquatting domains and protect the personal information of senior management. Real-time alerts are sent by email and requests or incidents are raised for any that require more detailed investigation. Crucially, James' request to include additional details in these alert notifications led to the feature being added to the Skurio solution. With an ever-evolving threat landscape, this was a critical success factor for him. "Skurio configuration was simple and quick. We've optimised our alerts and added use cases as we've progressed," says James, "Having regular catchup sessions with our Skurio success manager has been instrumental to us getting even greater value from the product. The Skurio team always listen to our ideas and that's essential to us."

BENEFITS OF DRP

The Skurio Advantage

Skurio surface, deep and Dark Web monitoring, data breach detection and cyber threat intelligence compliments existing operational systems and are simple to use and have been easily integrated.

Skurio enables IT operations staff to mitigate threats before they cause incidents and impact IT users. Automated intelligence gathering and real-time alerts improve productivity and help teams work smarter.

The Skurio Customer Success team stay in touch regularly to explain new features, review configuration and optimise investment in the platform. Features are added to the Skurio roadmap based on customer feedback and shared knowledge of the challenges customers face from evolving threats.

Simple powerful tools

Reducing human factors

A responsive relationship

"Skurio configuration was simple and quick. Having regular catchup sessions with our success manager has been instrumental to us getting even greater value from the product. The Skurio team always listen to our ideas and that's essential to us."

James Borne, Head of IT Operations

DIGITAL RISK IN THE INSURANCE SECTOR

A recent study of data breaches in the financial sector found insurance companies to be the most heavily-targeted organisations. They accounted for 23% of tracked financial data breaches between 2018 and 2022. Whilst cyber attack methods continue to evolve, attacks targeted at the insurance sector are increasing. An important factor that makes insurance companies an irresistible target is that they collect considerable amounts of sensitive data to calculate premiums, including payment and contact information.

Types of cyber risk for insurance firms

Business impersonation

Criminals can dupe customers into giving sensitive information and payment diversion scams using phishing campaigns that rely on typosquatting domains.

Data breaches

If sensitive information is stolen or compromised in a data breach, it can lead to identity theft, financial fraud, and reputational damage.

Ransomware attacks

A successful ransomware attack can disrupt an insurance company's operations, cause financial losses, and damage the company's reputation.

Business email compromise (BEC) attacks

Insurance companies are particularly vulnerable to BEC attacks because they often deal with large sums of money and have complex payment processes.

Third-party vendor risk

If a third-party vendor experiences a data breach or cyber attack, it can compromise the insurance company's sensitive data and systems.

Insurance businesses can act faster to mitigate threats and reduce risk if they monitor for data breaches and malicious domain registrations.

ABOUT US

Skurio creates innovative cybersecurity software to help you protect your organisation from digital risks. The Skurio Digital Risk Protection platform combines automated, round-the-clock monitoring of the surface, deep and Dark Web with powerful analytics capabilities for cyber threat intelligence.

hello@skurio.com www.skurio.com