ncc group

FOX IT
part of ncc group

Insurance Industry Threat Intelligence Report

Contents

Section 1

Threats to the Insurance Industry

Organisations in the Insurance industry are at significant risk of falling victim to a cyber-attack. The insurance sector remains a high-value target for a range of threat actors, including financially motivated organised criminal groups (OCGs), nation-states, and hacktivists. The industry's role within the broader Financial Services (FS) sector and its classification as Critical National Infrastructure (CNI) make it particularly attractive.

Ransomware remains a threat, with Medusa the primary threat actor targeting the industry in 2024. First observed in 2021, Medusa regularly targets CNI organisations including healthcare, manufacturing, education, and insurance.[1] They employ the hack and leak tactic, where a victim's data is encrypted and threatened to be leaked publicly unless a ransom is paid. They regularly use phishing to gain initial access and have been observed brute forcing weak passwords on services such as RDP and VPN.[2]

Insurance organisations hold extremely sensitive information which is attractive to threat actors. This includes Personally Identifiable Information (PII), sensitive medical information, and sensitive corporate information which can be used for future fraud or Business Email Compromise (BEC) campaigns. Perhaps most valuable to attackers are application forms for corporate insurance. These can assist attackers in uncovering weaknesses in the insurer's clients' defences or identify how much a potential victim is covered for, thus informing the threat actor's ransom demands.[3]

Increasing technological innovation in the industry offers incredible advantages but also introduces cyber risk. Technological innovation is integral to the automation of processes and contributes to increasing workplace efficiency. Adopting cloud services and API technologies assist in integrations and scalability of services and are crucial for embedded insurance offerings.

This significantly increases the customer experience which, in an industry where reputation is an organisation's key asset, is crucial for success. Customers are now able to use mobile apps to stay on top of every stage of their insurance journey; from applying for policies, to making and following the progress of claims, and making payments.

These developments however are a double-sided sword. Attackers abuse the same legitimate technologies used by the industry, such as generative AI to assist in the creation of believable phishing campaigns. They also regard organisations' expanded digital estates and assets as an expanded attack surface with correspondingly more opportunities to intrude upon a network.

The nature of the industry, and how it's evolving, creates a challenge for defenders. IT and cyber security teams are faced with the battle to balance operational efficiency and increasingly personalised customer experiences with resiliency and security.

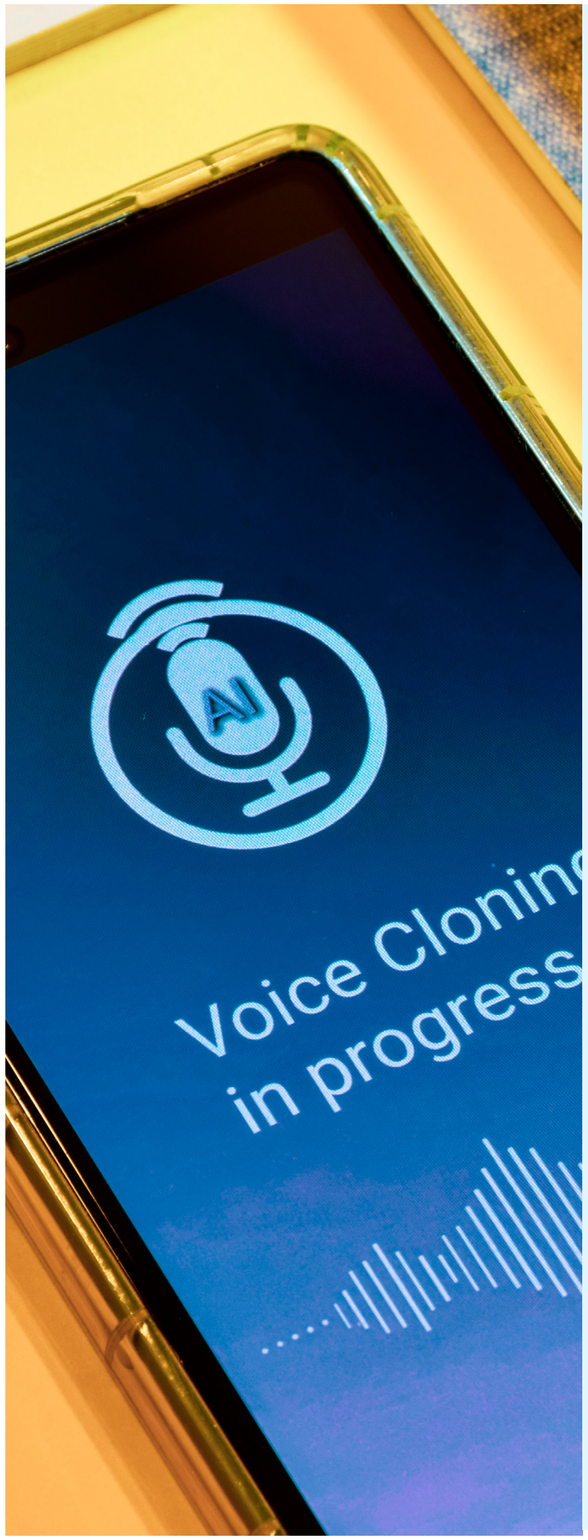
Key Tactics and Techniques in Detail – Technical Perspective

Conditional Access and MFA Gaps

As insurance organisations modernise their IT environments, many are migrating from traditional on-premises infrastructure to cloud platforms such as Microsoft 365, Azure, and AWS. While this transition offers scalability and operational efficiency, it also introduces new identity and access management challenges.

A critical vulnerability lies in misconfigured Conditional Access policies. These gaps are being exploited to bypass MFA entirely, without social engineering, by leveraging legacy authentication protocols or exploiting session token reuse.

In particular, we have seen token theft where attackers are using phishing kits or adversary-in-the-middle (AiTM) attacks to steal session tokens. Traditional MFA solutions often protect a smaller area of the attack surface leaving command-line tools (e.g. PowerShell, PsExec) and legacy systems exposed.



Emerging Threat Actor Focus: Scattered Spider

Recent intelligence indicates that Scattered Spider, a sophisticated threat group known for its social engineering capabilities, is increasingly targeting the insurance sector. Their pivot from broader FS targets to insurance is likely due to the sector's rich data stores and often inconsistent implementation of identity and access controls.

With operations largely based in the U.S and U.K, Scattered Spider is best known for highly effective social engineering tactics, including:

· **Vishing:** Impersonating staff or IT via phone to reset credentials.

· **SIM Swapping:** Hijacking mobile numbers to intercept MFA codes.

· **AiTM Phishing Kits:** Bypassing MFA by stealing session tokens.

· **Cloud Exploitation:** In 2024, they breached 165+ Snowflake customers.

· **Ransomware:** Deploying tools like ALPHV/BlackCat to extort victims.

· **ESXi Hypervisors:** Disrupting virtual infrastructure and crippling entire server environments in recent attacks.

They are known for speed and precision, sometimes deploying ransomware within 24 hours of initial access.

Motivations for Targeting Insurance

· Access to high-value data (PII, medical, policy details).
· Weak identity controls across the sector.
· Third-party dependencies, creating exploitable trust paths.

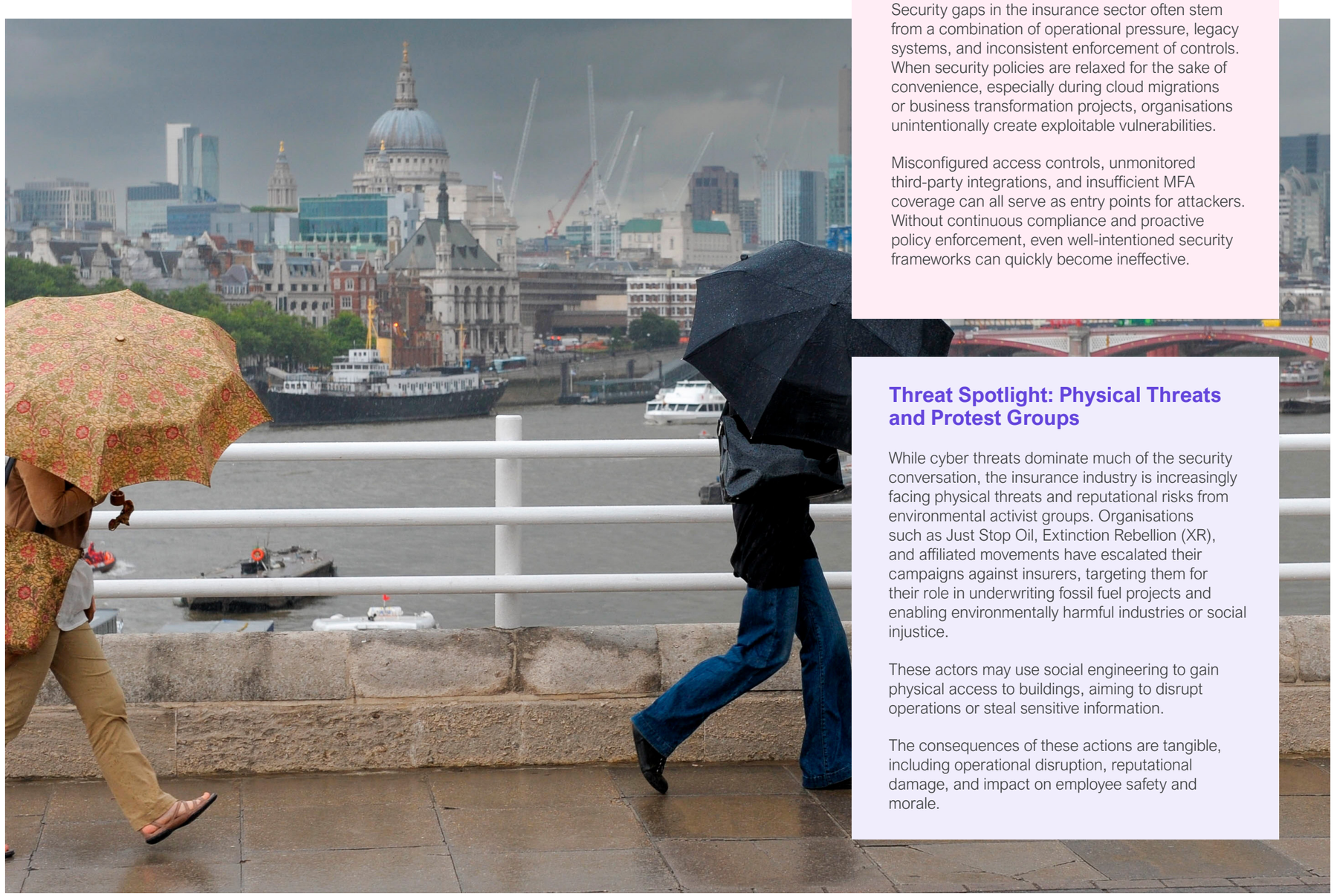
This trend highlights the urgent need for insurers to strengthen defences against identity-based threats, especially those exploiting human error and access weaknesses.

Section 2

So what? The Real-World Impact of Cyber-Attacks on the Insurance Industry

Cyber-attacks on organisations in the Insurance industry have the potential to cause significant impact:

- **Operational disruption –** attacks such as ransomware or DDoS can impede an organisation's ability to operate as normal, which can further impact the victim organisation's own clients and the service they receive.
- **Breach to confidentiality –** data breaches or leaks could expose potentially sensitive customer information. Depending on the nature of the insurance company, this could include sensitive financial, corporate, or even medical data. This data could be used by threat actors as part of future fraud or identity theft campaigns, or to inform what lures to use in phishing campaigns, for instance.
- **Financial loss –** falling victim to a cyber-attack can inflict financial damage. Should victim organisations fall short with data protection, they may face regulatory fines. Additionally, the reputational damage following a cyber-attack could influence existing customers to leave for competitors or deter future customers.



Cyber Consultant's View

As the insurance industry continues to digitise and adopt cloud-first strategies, it faces a growing array of cyber threats. Often companies neglect to implement and audit policies, procedures and the general governance of data, while being distracted by tools and technology.

Security gaps in the insurance sector often stem from a combination of operational pressure, legacy systems, and inconsistent enforcement of controls. When security policies are relaxed for the sake of convenience, especially during cloud migrations or business transformation projects, organisations unintentionally create exploitable vulnerabilities.

Misconfigured access controls, unmonitored third-party integrations, and insufficient MFA coverage can all serve as entry points for attackers. Without continuous compliance and proactive policy enforcement, even well-intentioned security frameworks can quickly become ineffective.

Threat Spotlight: Physical Threats and Protest Groups

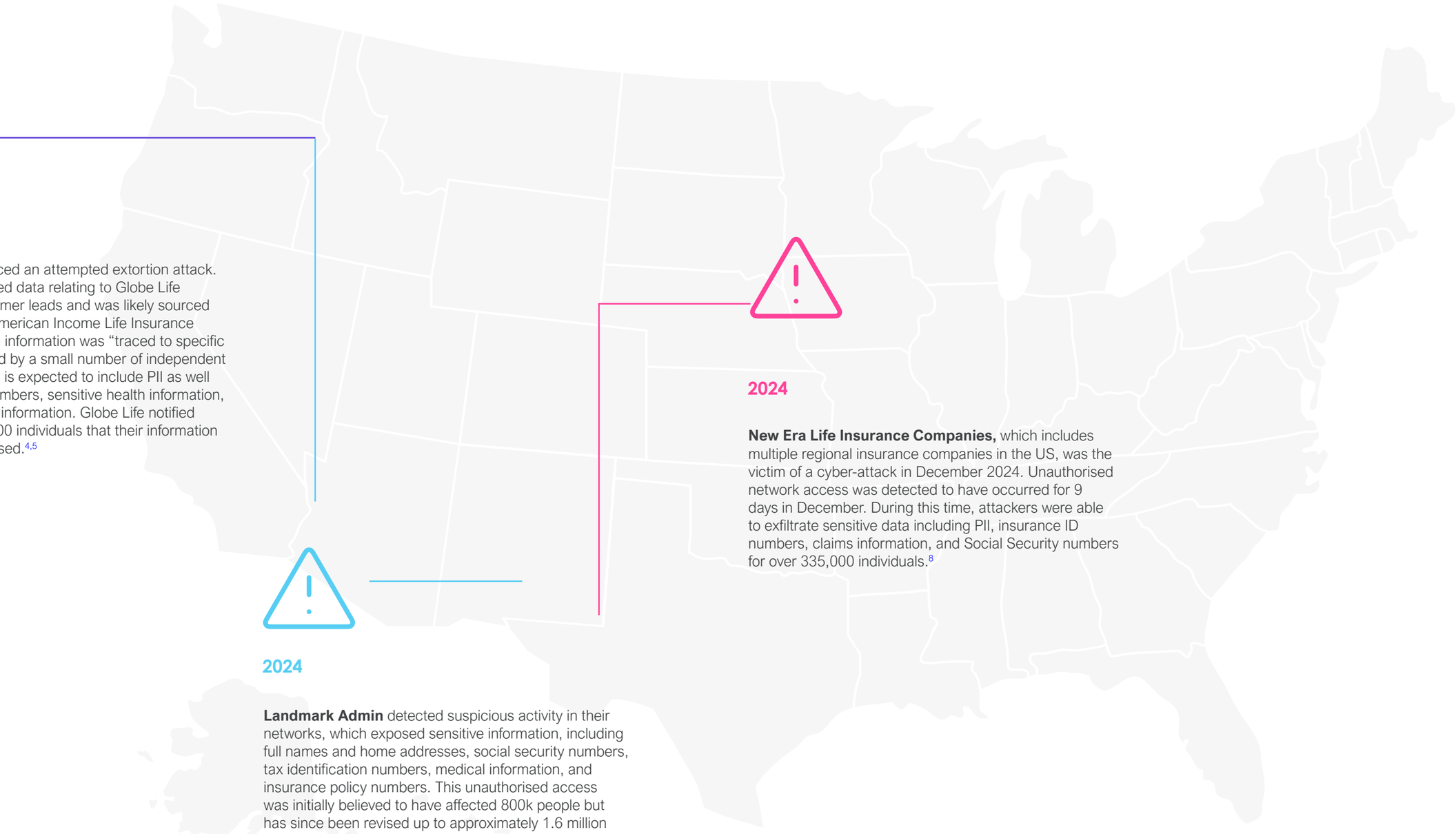
While cyber threats dominate much of the security conversation, the insurance industry is increasingly facing physical threats and reputational risks from environmental activist groups. Organisations such as Just Stop Oil, Extinction Rebellion (XR), and affiliated movements have escalated their campaigns against insurers, targeting them for their role in underwriting fossil fuel projects and enabling environmentally harmful industries or social injustice.

These actors may use social engineering to gain physical access to buildings, aiming to disrupt operations or steal sensitive information.

The consequences of these actions are tangible, including operational disruption, reputational damage, and impact on employee safety and morale.

Section 3

Recent Cyber Incidents



2024

Globe Life experienced an attempted extortion attack. The attacker exfiltrated data relating to Globe Life customers and customer leads and was likely sourced from its subsidiary, American Income Life Insurance Company. The stolen information was “traced to specific databases maintained by a small number of independent agency owners,” and is expected to include PII as well as Social Security numbers, sensitive health information, and insurance policy information. Globe Life notified approximately 850,000 individuals that their information may have been exposed.[4,5]

2024

Landmark Admin detected suspicious activity in their networks, which exposed sensitive information, including full names and home addresses, social security numbers, tax identification numbers, medical information, and insurance policy numbers. This unauthorised access was initially believed to have affected 800k people but has since been revised up to approximately 1.6 million individuals affected.[6] Though Landmark Admin is not an insurance company itself, it provides crucial services to some of the largest insurers in the US, including American Monumental Life Insurance Company and American Benefit Life.[7]

2024

New Era Life Insurance Companies, which includes multiple regional insurance companies in the US, was the victim of a cyber-attack in December 2024. Unauthorised network access was detected to have occurred for 9 days in December. During this time, attackers were able to exfiltrate sensitive data including PII, insurance ID numbers, claims information, and Social Security numbers for over 335,000 individuals.[8]

Section 4

Top Cyber Threats to the Insurance Industry

Emerging Technology

New technologies are being adopted into everyday operations and services. Telematics are used in auto-insurance to personalise premiums and offer usage-based coverage. AI is increasingly utilised, increasing efficiency and improving customer experience. Customer support chatbots, enhancing fraud detection and risk management though the analysis of historical data and comparing them to modern trends, all rely on AI.[9]

Third-party solutions are increasingly common. Cloud services and API technologies assist with integrations and scalability of services and are crucial for embedded insurance offerings. Mobile apps are increasingly being prioritised. They enable customers to take out policies, file claims, and follow its process and resolution in mere days.[10]

Advances in technology benefit attackers too, however. Attackers are creating more convincing phishing campaigns and have been spotted using AI-assisted tools to target the financial sector. Business Invoice Swapper is an AI tool sold on the dark web since at least 2023, designed to create fraudulent invoices for wire fraud and BEC scams.[11]

These innovations also expand organisations' attack surfaces, increasing the avenues for potential attackers to gain access.[12] Security teams must balance automation, operational efficiency, and customer experience, with the need to secure attack surfaces, manage vulnerabilities, and respond to incidents when they do inevitably occur.[13]

Third-Party Risk and Supply Chain Compromise

As part of the industry's move to digitisation and expanding its attack surface, organisations are also becoming more reliant on external partners. These third parties help to provide crucial services to the Insurance industry, such as cloud computing solutions and mobile and web-based app development.[14]

Whilst utilising specialist partners to provide crucial services can help organisations keep overheads down through not having to develop and maintain everything in-house, it further assists attackers in finding new intrusion vectors. Attackers seek to exploit the trusted relationship between partners, vendors, and their customers, to gain access to networks and, in turn, steal or encrypt sensitive data.

In the Insurance industry, 59% of all data breaches have been linked to external partners, highlighting the importance of vetting the security posture of third parties before entering trusted arrangements.[15]

Ransomware Attacks

Ransomware is one of the leading threats to the Insurance industry.[16]

Through being part of the financial sector, the industry automatically has a target on its back from financially motivated OCGs. Insurance companies hold large amounts of extremely sensitive data which ransomware groups attempt to exfiltrate to use for their own future campaigns, and to extort a ransom from their victim for not leaking their data online.

Sensitive information can include client's payment information, sensitive medical information, and PII. Additionally, by examining the applications paperwork for corporate clients, threat actors can potentially learn about network weaknesses prime for the exploitation of future victims.[17]

Global ransomware events have been increasing for the past few years:

- Medusa was the most prominent threat actor targeting the Insurance industry in 2024
- The Insurance industry accounted for nearly one quarter of all ransomware attacks against the financial sector in 2024
- 69 attacks were recorded in our database in 2024, down from 71 in 2023, though up 61% from the 43 observed in 2022

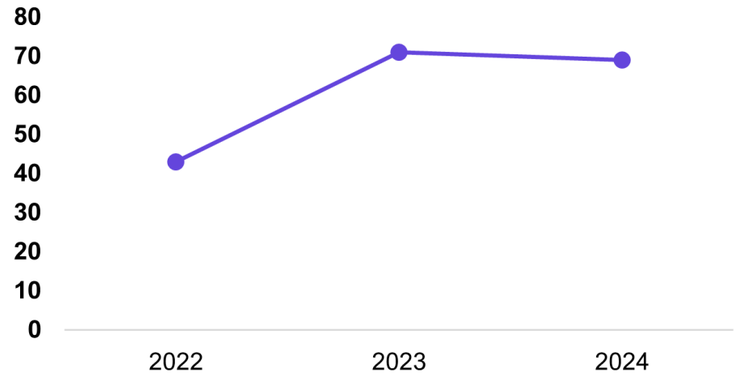


Figure 1 Ransomware Attacks against the Insurance Industry, 2024

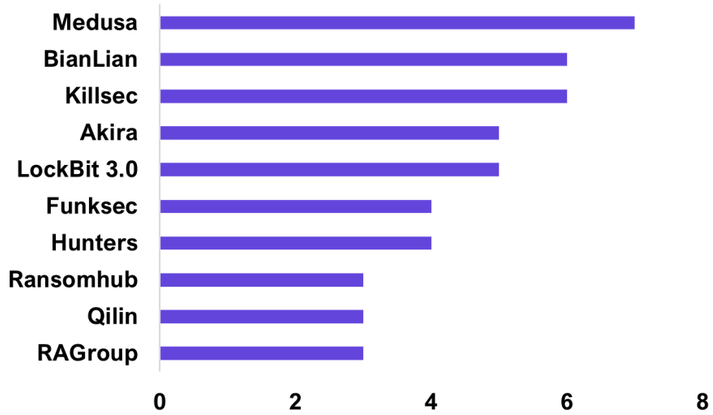


Figure 2 Top 10 Threat Actors targeting Insurance, 2024

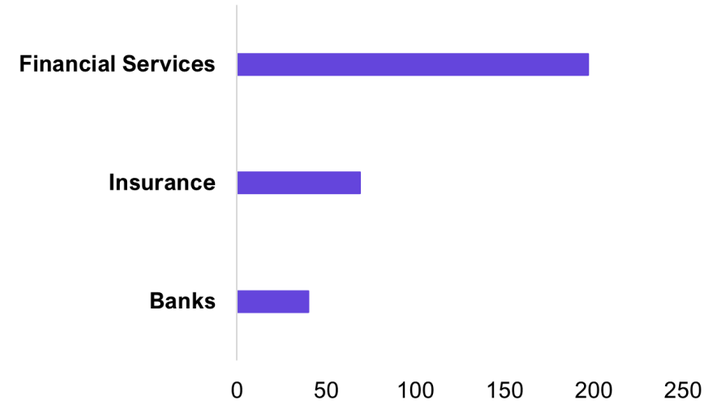


Figure 3 Number of Ransomware Attacks against the Financials Sector in 2024

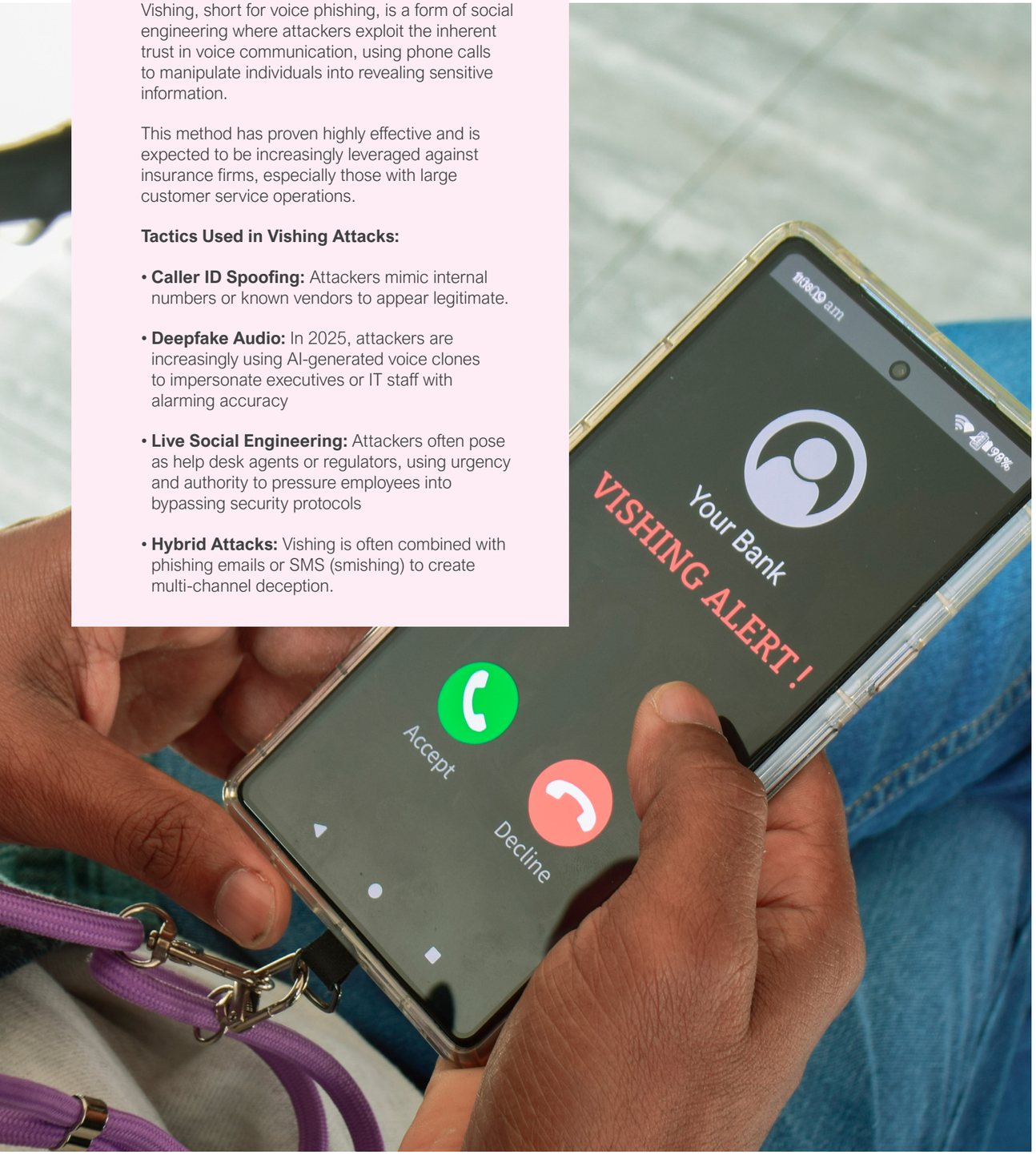
Threat Spotlight: Vishing

Vishing, short for voice phishing, is a form of social engineering where attackers exploit the inherent trust in voice communication, using phone calls to manipulate individuals into revealing sensitive information.

This method has proven highly effective and is expected to be increasingly leveraged against insurance firms, especially those with large customer service operations.

Tactics Used in Vishing Attacks:

- **Caller ID Spoofing:** Attackers mimic internal numbers or known vendors to appear legitimate.
- **Deepfake Audio:** In 2025, attackers are increasingly using AI-generated voice clones to impersonate executives or IT staff with alarming accuracy
- **Live Social Engineering:** Attackers often pose as help desk agents or regulators, using urgency and authority to pressure employees into bypassing security protocols
- **Hybrid Attacks:** Vishing is often combined with phishing emails or SMS (smishing) to create multi-channel deception.



Data Breaches

Insurance organisations often hold sensitive information which financially motivated threat actors seek to steal and either sell in the cyber-criminal ecosystem or use for future malicious campaigns. Customer PII, sensitive medical information, and direct credit card and payment information is all data which attracts threat actors to target the industry, and which have contributed to making data theft a leading threat to the industry.[18,19]

A recent SecurityScorecard report highlighted that companies which suffered from a third-party data breach often had above average scores for their security posture. This indicates that attackers can circumvent strong defences by abusing the trusted relationship between partners and customer and vendor.

Further, it emphasises the importance that attackers place on successfully "popping" insurance organisations that would not be deterred by strong defences and would instead invest the time and resources needed to successfully compromise their chosen victim.[20]

Hacktivism

Hacktivism has seen a resurgence due to Russia's invasion of Ukraine and more recently by the Israel-Hamas war.[21] This modern strain of activism is often linked to geopolitical developments, with hacktivist groups being nation-state aligned, if not officially state-sponsored. Hacktivist attacks most frequently take the form of low sophistication, but potentially high impact, DDoS attacks.

By virtue of being within the overall Financials sector, and therefore a nation's CNI, the Insurance industry is at risk of experiencing DDoS attacks. The financials sector is the preeminent target for DDoS attacks around the globe, receiving 35% of all attacks in 2023.[22] DDoS, due to their deployment by hacktivist groups, have been observed to peak during times of geopolitical instability.

Towards the end of 2023, and in the first half of 2024, DDoS attacks were observed to follow geopolitical developments in both the Middle East and Ukraine. Nations which issued statements in support of, or which delivered material support to Ukraine came under attack. These campaigns targeted government and financial entities, as well as other sectors.[23]

Looking for a wider view of the cyber threat and geopolitical landscape?

Our monthly Threat Pulse reports provide in-depth analysis of ransomware, nation-state activity, emerging threats, and other key developments shaping global security. You'll also find insights on current topics such as AI, evolving threat actors, and the trends driving change in the cyber landscape.

Learn more

Section 5

Call to Action

IT and Cyber Security Teams

- **Have third-party partners and providers undergone security audits?** Third parties must be assessed to ensure the increased efficiency of utilising specialist services does not unduly correspond with an increased attack surface.
- **Are decisions being informed by intelligence?** Regular engagement of threat intelligence and pen testing services can help identify and mitigate against any weaknesses in organisations' own networks and their supply chains. Meanwhile, incorporating threat intelligence into Cyber Security Maturity Reviews (CSRs) ensures that assessments are grounded in real-world risks, not just theoretical frameworks.
- **Are you conducting incident response planning and readiness exercises which integrate threat intelligence?** Proactive use of threat intelligence helps organisations anticipate likely attack scenarios, refine response playbooks, and test readiness against real-world threats.

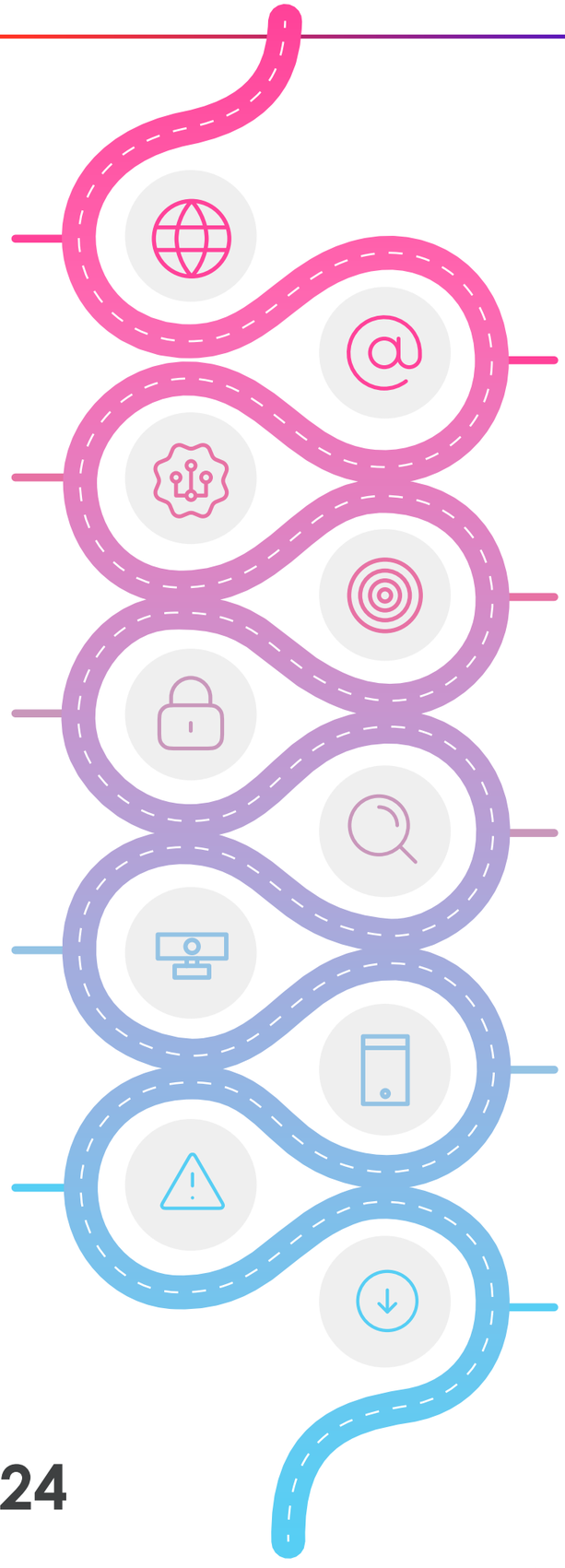
Senior Leaders and Policymakers

- **Is cyber security recognised as a priority for decision makers?** Consistent attention and commitment to cyber security awareness at the top of an organisation helps to cultivate a security-forward culture throughout.
- **Are IT and security teams adequately resourced?** These teams have the potential to increase operational resilience, thus strengthening the whole organisation. Investing resources in these business-critical functions so that they can, for instance, adopt emerging technologies, is crucial to success.

Insurance Industry Staff

- **Are Insurance industry employees sufficiently trained on common cyber threats?** All staff should be able to identify the main risks they may face in their role and have confidence in their organisation's policies and procedures which guide their response to such threats, i.e. phishing emails or accidentally installing malware.

Attack Timeline



2021

AXA offices in Asia struck by Avaddon ransomware after announcing a cessation of reimbursement for ransomware extortion payments in France.

2022

Lloyd's of London takes systems offline after detecting unusual activity within networks, though no sign of compromise after investigation.

2023

Prudential Insurance affected by the MOVEit file transfer system breach, with over 320k customers impacted.

2024

Globe Life experiences attempted extortion attack after attackers appear to source and exfiltrate sensitive data from a subsidiary.

2024

United Health hit by ransomware from BlackCat/ALPHV for roughly $22 million. Total impact over year approaches $1.5 billion.

2021

CNA Financial hit by ransomware and reportedly pays $40 million in ransom to regain access to data and systems.

2023

Sabre Insurance experiences attempted cyber intrusion but defeats the attack. Successful network segmentation ensured operations weren't disrupted.

2024

Prudential Insurance breached once again, allegedly by BlackCat/ALPHV. Approximately 2.5 million individuals are impacted.

2024

Landmark Admin, which provides crucial services to some of the largest insurers in the US, suffers a data breach affecting roughly 1.6 million individuals.

2024

Washington National Insurance senior executive targeted in SIM-swapping attack. Approximately 20k individuals affected by resulting breach.

2021-2024

About NCC Group

“People powered, tech-enabled cyber security”

We’re a people powered, tech-enabled global cyber security and resilience company with over 2,200 colleagues around the world.

For over 25 years, we’ve been trusted by the world’s leading companies and Governments to manage and deliver cyber resilience, working together to create a more secure digital future. We are proud to deliver important and groundbreaking projects for our clients.

We operate as one global business, with in-country delivery tailored to local needs and cultures, as well as a global delivery team to respond quickly to our client’s challenges. Headquartered in the UK, we also have a significant market presence in North America, Europe, and APAC.

+44 (0)161 209 5200
response@nccgroup.com
www.nccgroup.com


ncc
group


FOX IT
part of ncc group