Insurance and Pensions Symposium

“Cybersecurity as a Trust Imperative: Protecting Financial Institutions in an Era of Escalating Digital Threats”

Zelina Francis – Inflection Point, Africa

25th March 2026

Inflection Point
Where leadership meets digital confidence

Presenter Profile

Many thanks to the Insurance and Pensions Commission of Zimbabwe

Zelina Francis
Practice Director

Digital Governance & Executive Learning
Inflection Point (Private) Limited

- +263 784473876 (Zimbabwe)
  +44 790 3345027 (United Kingdom)
- zelina@inflectionpoint.africa
- https://inflectionpoint.africa
- Suite 29, Arundel Village Business Center
  51 Quorn Avenue, Harare, Zimbabwe

Zelina Francis

Practice Director, Inflection Point Africa
Digital Transformation SME | Trainer, Advisory

Zelina is a digital transformation and IT strategy leader with experience across Zimbabwe, Sub-Saharan Africa, and the UK. She has held senior roles and consulting engagements with Deloitte, IT Leadership roles at Vodafone UK, RSA Insurance Group, De La Rue International, Old Mutual Zimbabwe, and BancABC, advising boards and C-suites on technology governance, value realisation, and cyber-resilient operating models.

A practiced stakeholder engager, she translates technology for directors - from board updates and investment cases to project approvals and governance reporting She also co-founded ZimSelector.com, Zimbabwe's first online insurance comparison platform.

Credentials : MSc Univ Greenwich UK,
ChMC, TOGAF Enterprise Architect, CISM

EXECUTIVE SUMMARY

Cybersecurity has become a defining issue for the insurance industry—not only as a technology concern, but as a **core trust, financial stability, and systemic risk issue**. As insurers increasingly digitise operations, the protection of customer data, financial flows, and service continuity is now inseparable from the ability to manage cyber risk effectively.

Globally, cybercrime has evolved into a **multi-trillion-dollar economy**, growing faster than defensive capabilities. At the same time, Africa has emerged as one of the **most heavily targeted regions**, with organisations experiencing significantly higher attack volumes than the global average. For insurers, this creates heightened exposure across sensitive customer data, claims systems, payment flows, and extended partner ecosystems.

Yet, despite this elevated risk environment, Africa faces a critical constraint: a **lack of reliable, localised cyber risk intelligence**. There is limited visibility into the frequency, severity, and financial impact of cyber incidents across the region. This information gap weakens strategic decision-making, limits effective risk mitigation, and constrains the development of a sustainable cyber insurance market.

This creates a **double-edged reality** for the industry. On one hand, insurers must urgently strengthen resilience in the face of rising cyber threats. On the other, the growing digital economy presents a significant opportunity to develop cyber insurance products. However, without accurate data, insurers risk **mispricing, adverse selection, and exposure to systemic losses**.

The challenge is compounded by broader structural constraints, including **skills shortages, fragmented knowledge, under-reporting of incidents, and limited collaboration across the ecosystem**. Institutions are often responding to a shared threat in isolation, reducing collective effectiveness and slowing learning across the sector.

Addressing this requires **coordinated leadership at both regulatory and institutional levels**. Boards and executives must elevate cyber risk to a strategic priority, while regulators must enable greater transparency, reporting, and collaboration across the industry.

A key recommendation to Regulators/Leaders is the establishment of an :

African Insurer Cyber Think Tank and Centre of Excellence

—to aggregate intelligence, pool scarce expertise, build capability, and support the development of Africa-specific risk models and underwriting frameworks. This collective approach would strengthen resilience, improve pricing accuracy, and protect both **policyholder funds and national savings**.

Ultimately, cyber risk is a **shared threat**, and must be addressed through **shared intelligence, shared capability, and shared accountability**. Africa cannot afford to insure what it does not understand. Closing the cyber intelligence gap is essential to protecting trust, strengthening resilience, and securing the future of the insurance industry.

Check Point Software Technologies threat reports

Cyber Security as a Trust Imperative for Africa's Insurance Industry

Inflection Point
Where leadership meets digital confidence

Key issue

Africa sits at the intersection of rising cyber threat and limited risk visibility - making it both

- one of the most exposed regions globally and
- one of the greatest opportunities to build , data-driven cyber risk and insurance market > YET we have an information Gap

CYBER SECURITY IN INSURANCE SECTOR

CONTENTS

1

Global Threat Landscape

An overview of the evolving cyber threat environment and the trends shaping cyber risk today.

2

Why Insurance Sector is a Target

What makes insurers and financial service providers increasingly attractive targets for cybercriminals.

3

Why Africa is the hottest Target

What makes African businesses more prone to attack

4

Information Gap

Significant gaps remain in the availability of reliable data on cyber security threats, incidents, costs, and impacts across Africa.

5

Cyber Risk Management Strategies

Practical approaches regulators and industry champions can take to strengthen cyber resilience, governance, and incident response capabilities industry wide and regionally.

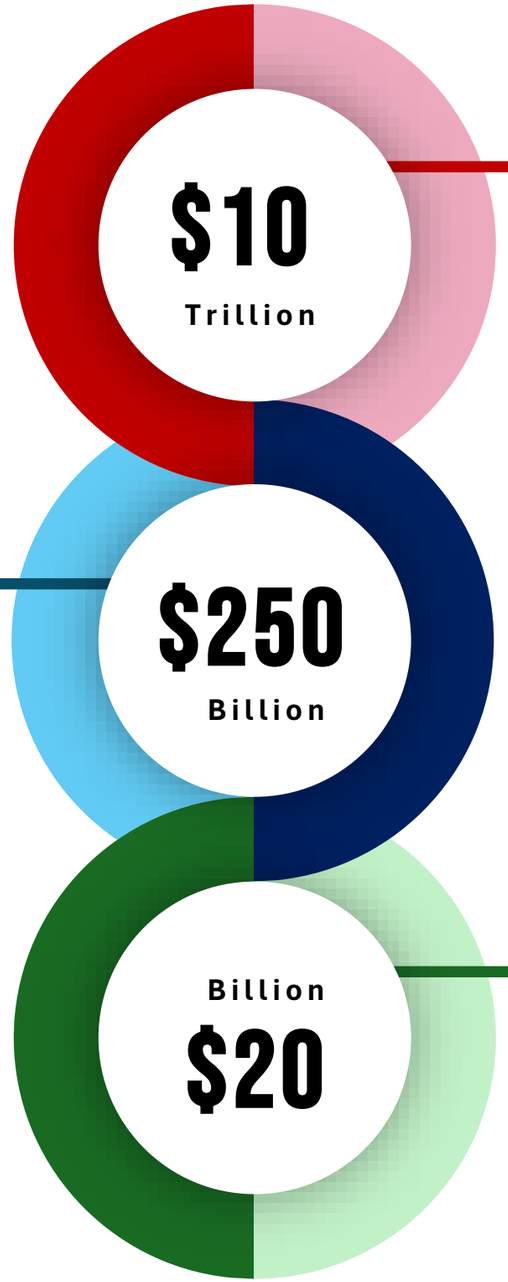
6

Closing the Gap

Bring on ideas for how we can collaborate as an industry to close the information gap and synergise strategies to protect our industry from threats.

GLOBAL CYBER ECONOMY – VALUE OVERVIEW

The global cyber economy is asymmetrical
While organisations spend hundreds of billions defending themselves, cybercrime is already a multi-trillion-dollar economy, growing faster than defence capabilities.



Cybercrime Economy (Adversary "Market")

- Estimated at **~$9–10 trillion annually (2024–2025)**
- Projected to exceed **$13 trillion by 2028**

👉 Would rank as:

- **3rd largest economy globally** (after US and China)

👉 Includes:

- Fraud and financial theft
- Ransomware payments
- Data theft and resale
- Business disruption costs

Cybersecurity Industry (Defence Spend)

- Estimated at **~$220–250 billion (2025)**
- Projected to reach **~$350–500 billion by 2030**

👉 Includes:

- Security software
- Cloud security
- Managed security services
- Identity & access management

Cyber Insurance Market

- Estimated at **~$15–20 billion globally**
- Expected to grow to **~$50–70 billion by 2030**

👉 Still significantly **underpenetrated**, ***especially in Africa*** and emerging markets

“TRUST”
our most valuable asset in Insurance

Let’s Get Started

In the insurance business, trust is our most valuable asset. As our industry becomes more digital, protecting that trust increasingly depends on

how well we manage cyber risk.

Why the Insurance Sector is a Prime Target

Insurers hold high-value data

- national ID and KYC data
- medical and health records
- payment details
- payroll-linked information
- beneficiary information
- claims history
- underwriting data.

Insurers process financial flows

They manage:

- premium collection
- claims disbursement
- pension and benefit payments
- broker commissions
- investment-linked transactions.

Attackers understand insurer vulnerabilities. Insurance organisations are often seen as:

highly data-rich

operationally dependent on uptime

less cyber-mature than banks

reliant on multiple third parties.

Cyber security is no longer just an IT concern; it is a **core business risk that affects trust, operations, compliance, and financial performance in the insurance sector**

Why Cyber Security matters for Insurance Industry

CUSTOMER TRUST

01. A cyber breach can expose sensitive customer and medical data, quickly damaging trust and confidence in the insurer

OPERATIONAL CONTINUITY

02. Cyber incidents can disrupt critical systems such as claims processing, policy administration, and customer services

CLAIMS ADMINISTRATION

03. Insurance claims systems are prime targets for fraud, payment manipulation, and data exploitation.

04. Cyber incidents can trigger regulatory scrutiny, compliance investigations, and potential penalties.

REGULATORY EXPOSURE

05. Reputational damage from a breach can take years to repair and may result in loss of customers and partners.

REPUTATION

06. Cyber attacks can cause direct financial losses through fraud, operational disruption, legal costs, and system recovery.

FINANCIAL IMPACT

Major Global Insurance Industry Cyber Breaches – Key Cases

The worst breaches in the insurance sector are not just data events - they are systemic business events, capable of disrupting claims, exposing national identity data, and triggering long-term financial and reputational damage.

1. Anthem Health Insurance (2015)

Impact: ~78.8 million customers affected

- **Data compromised: Names, Social Security numbers, addresses, employment data**
- **Cause: Stolen administrator credentials (no encryption on sensitive data)**
- **Cost: ~$115 million settlement (largest at the time)**

👉 **Insight: Even large insurers failed to protect core identity data—highlighting systemic weaknesses in cyber controls.**

2. UnitedHealth / Change Healthcare (2024)

Impact: ~100 million individuals affected (largest healthcare breach in US history)

- **Impact type: Massive disruption to claims processing nationwide**
- **Financial impact: Hundreds of millions in losses and emergency funding support**

👉 **Insight: Cyber attacks can paralyse the insurance value chain, not just steal data.**

3. Allianz Life (2025)

Impact: >1 million customers affected

- **Attack vector: Social engineering via third-party cloud CRM**
- **Data compromised: Personally identifiable information (PII)**

👉 **Insight: The weakest link is often third-party ecosystems, not core systems.**

4. Experian / Credit Data Ecosystem (Multiple incidents)

Impact: Tens to hundreds of millions of records exposed globally

- **Example: ~220 million Brazilians' data leaked**

👉 **Insight: Identity and underwriting data ecosystems are high-value systemic targets.**

5. Equifax (2017 – Adjacent to Insurance Risk)

Impact: ~147 million people affected

- **Data compromised: Full identity records (SSNs, DOBs, addresses)**
- **Cause: Unpatched vulnerability + long undetected breach**

👉 **Insight: Demonstrates catastrophic systemic exposure of identity data, directly relevant to underwriting and fraud risk.**

Across these breaches:

a) **Data is the primary target (identity, health, financial records)**

b) **Access is often legitimate (stolen credentials, social engineering)**

c) **Third parties are major vulnerabilities**

d) **Detection is often delayed (weeks to months)**

e) **Impact extends beyond IT → operations, claims, trust, liquidity**

CYBER THREAT EVOLUTION

2000s
Opportunistic attacks
In the early 2000s, attacks were largely opportunistic -driven by curiosity or reputation rather than profit. Self-replicating worms and viruses such as *ILOVEYOU* and *Code Red* exploited weak system configurations but inflicted limited economic loss.

2010
Early Industrialisation
By the 2010s, cybercrime had begun to be industrialised.

2017
Globalised impacting threats
The 2017 *WannaCry* and *NotPetya* outbreaks marked a watershed moment. These attacks demonstrated how a single vulnerability could cascade through global supply chains, disrupting hospitals, logistics companies, and governments (IBM Security, 2024). The estimated global cost of *NotPetya* exceeded USD 10 billion, highlighting the systemic risk of interconnected IT ecosystems

2020
Crimeware as-a-service
The emergence of *crimeware-as-a-service* markets allowed even unskilled actors to rent botnets, phishing kits, and ransomware platforms on the dark web . This period also saw the professionalisation of organised cybercrime groups, many operating with quasi-corporate structures and affiliate programs.

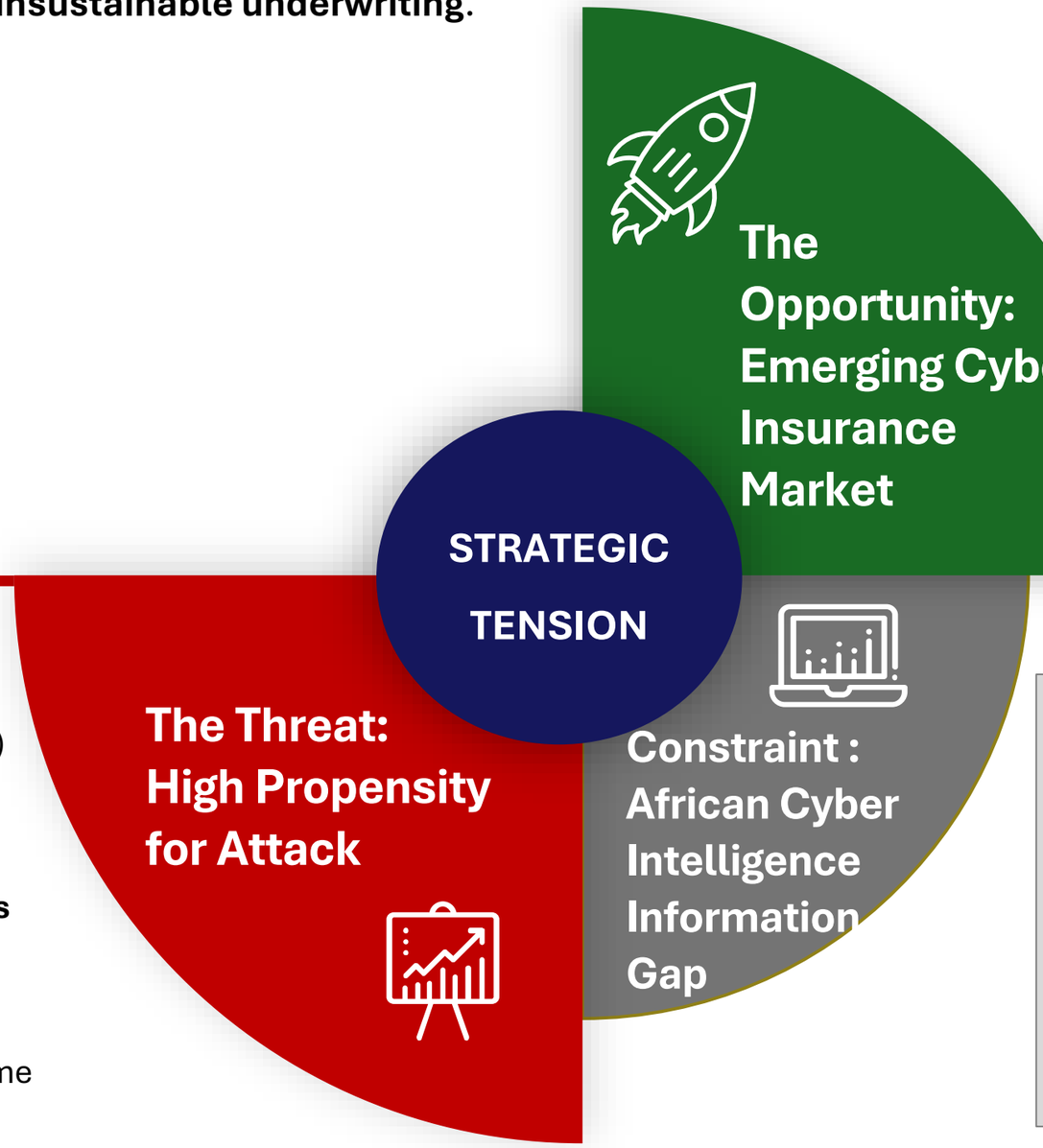
2020s
Cyber economy
By the early 2020s through COVID pandemic, cybercrime had become the world's third-largest economy by value, behind the United States and China, projected to inflict over USD 10 trillion annually in damages by 2025 (Cybersecurity Ventures, 2025). The post-pandemic era amplified risk: remote work, rapid cloud adoption, and digital payments expanded the attack surface

2026
AI fuels threats
Today, AI-enabled phishing, deepfakes, and model-poisoning attacks represent the new frontier of digital risk, challenging both technical and ethical governance frameworks.

The past two decades have witnessed a radical transformation in the scale and sophistication and financial consequences of cyber threats.

Cyber Risk in Africa – A Double-Edged Opportunity

African insurers are **both highly exposed to cyber risk and uniquely positioned to insure it**—but without reliable data, they face the risk of **mispricing, adverse selection, and unsustainable underwriting**.



- A rapidly expanding digital economy is increasing **demand for cyber protection**
- Organisations across sectors are:
  - More exposed
  - But Less aware of cyber risk
- Creates a **significant opportunity** for insurers to:
  - Develop cyber insurance products -Capture a growing, underpenetrated market

👉 **Implication:** a **high-growth, strategic product opportunity**

- African organisations face **some of the highest cyberattack volumes globally**
- Insurers are exposed across:
  - Customer data (health, financial, ID)
  - Claims and payment systems
  - Broker and partner ecosystems
- Increased likelihood of:
  - **Fraud, ransomware, data breaches**
  - **Operational disruption and reputational damage**

👉 **Implication:** African insurers must assume they are **high-probability targets** and strengthen resilience accordingly.

The Constraint: Lack of Local Risk Intelligence

- Limited Africa-specific data on:
  - Frequency and severity of attacks
  - Financial impact and loss patterns
- Reliance on **imported or generic risk models**

👉 **Result:**

- Difficulty in:
  - Accurate pricing
  - Risk selection
  - Portfolio management

Key Cyber Risks facing Insurers

The threat landscape is no longer dominated by a single actor type AND neither is it focused on the data center the surface has expanded —**insurers face a layered risk from organised crime, insider exposure, and ecosystem vulnerabilities**, with Africa-specific risks amplified by **fraud syndicates, identity weaknesses,& extended broker networks**.

1. Organised Cybercriminal Groups (Global & Regional)

Highly structured, profit-driven groups behind ransomware, data theft, and payment fraud targeting insurers for financial gain.

2. Ransomware-as-a-Service (RaaS) Affiliates

Decentralised actors using rented ransomware tools to launch attacks, often targeting organisations with weaker defences.

.

3. Third-Party & Ecosystem Exposure

Brokers, Agents, Vendors, TPAs, fintech partners, and service providers expand the attack surface, with weaker links exposing core insurer systems.

4. Insider Threat Actors (Employees, Contractors, Agents)

Individuals with legitimate access who intentionally or inadvertently expose systems, data, or financial processes.

5. Nation-State & State-Sponsored Actors (Global)

Advanced threat actors targeting financial systems and sensitive data, sometimes for intelligence gathering or economic disruption.

6. Supply Chain incl Cloud Platform Attackers

Actors compromising software vendors, cloud providers, or service partners to gain indirect access to insurer systems.

7. Opportunistic Cybercriminals

Lower-skilled attackers exploiting common vulnerabilities, phishing, or weak controls—particularly prevalent in under-secured environments.

8. AI-Enabled Threat Actors

Both organised and opportunistic attackers using AI to scale phishing, automate fraud, and enhance social engineering attacks.

BOARD & C-SUITE CYBER AWARENESS CHALLENGE

Cyber resilience requires astute and aligned leadership - **Boards set direction and accountability, while Executives operationalise resilience**. Together, they enable organisations to lead with **digital confidence in an increasingly hostile threat environment**.

BOARDS

Set strategic direction and accountability for cyber risk as a core business issue:

- Elevate cyber risk to **board-level priority alongside financial and operational risk**
- Ensure **robust governance frameworks, policies, and risk appetite definitions**
- Demand **transparent reporting on cyber exposure, incidents, and resilience posture**
- Oversee **investment in cyber capability, data integrity, and system resilience**
- Hold management accountable for **cyber preparedness and regulatory compliance**

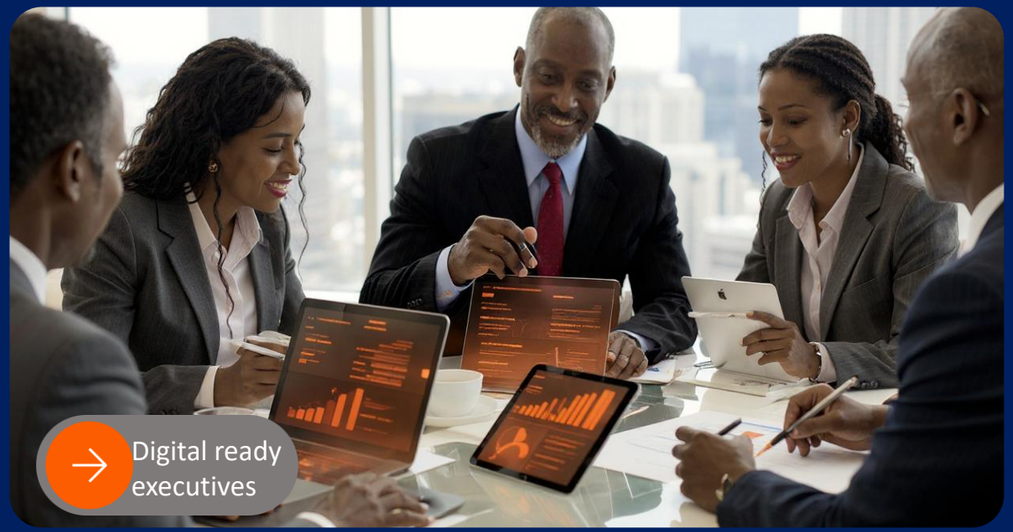
👉 **Board Mandate:**
Set the tone for **risk-aware, digitally confident governance**

C-SUITE EXECTUIVES

Translate strategy into **practical resilience and organisational capability**:

- Embed cyber risk into **day-to-day operations, decision-making, and culture**
- Strengthen **systems, data quality, and digital platforms** to reduce vulnerability
- Drive **incident readiness, response capability, and recovery planning**
- Ensure **ecosystem risk management** across brokers, partners, and vendors
- Build **organisation-wide cyber awareness and accountability**

👉 **Executive Mandate:**
Deliver **secure, resilient, and trusted operations**



If you are not a cyber-ready executive, secure the right training and advisory support because

THE THREAT IS REAL AND GROWING

Global Threat Landscape

The year of the evasive adversary

According to the **CrowdStrike 2026 Global Threat Report**, the current cyber threat landscape is increasingly shaped by **evasive, fast-moving, AI-enabled adversaries**.

Key threat themes

- Adversaries are leveraging **AI to enhance and accelerate operations**.
- Ransomware actors are expanding **cross-domain tradecraft**.
- Threat actors are targeting **network perimeter devices for initial intrusion**.
- Supply chain attacks are increasingly used to **evade traditional controls**.

Implications for insurers

Insurers are especially vulnerable because they combine:

- sensitive personal data
- health information
- financial workflows
- digital customer channels
- complex partner ecosystems.

89% increase in attacks by AI-enabled adversaries

Average eCrime breakout time dropped to **29** minutes, a **65%** increase in speed from 2024, and the fastest breakout time was only **27** seconds

82% of detections in 2025 were malware-free, up from **51%** in 2020

24 new adversaries tracked by CrowdStrike, raising the total to **281**

China-nexus activity increased **38%** across all sectors, with an **85%** increase in logistics

42% increase in zero-day vulnerabilities exploited prior to public disclosure

Valid account abuse accounted for **35%** of cloud incidents

37% rise in cloud-conscious intrusions, with **266%** increase by state-nexus threat actors

Threat actors increase in efficiency with AI

Breakout Time:
The Race Against Adversaries

Once adversaries gain initial access, their next objective is to “break out” and move laterally from the initial foothold to high-value assets. The speed of this “breakout time” determines how fast a defender must respond to reduce the costs and damages associated with an intrusion.

Breakout time has been steadily decreasing over the past five years, roughly a **70% reduction** from 2021 to 2025. Adversaries are getting significantly faster at expanding their foothold after initial access.

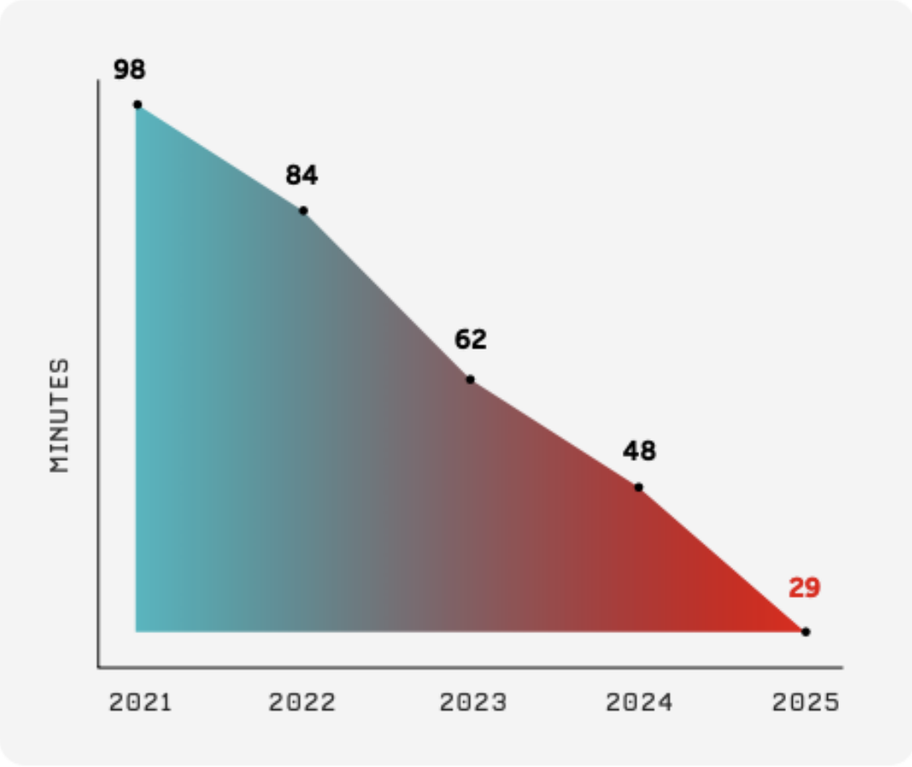


Figure 3. Average eCrime breakout time, 2021-2025

Breakout Time Defined : The time it takes for an attacker to move from the first compromised system to other systems within a network. Breakout time is like a fire spreading in a building — the faster it spreads, the less chance you have to contain it.

Interactive intrusions

African organisations are operating in a high-intensity threat environment, experiencing nearly double the attack volume of developed markets, placing them at the frontline of global cyber risk.

Global Average

- ~2,000–2,100 attacks per organisation per week
- By Region (Latest Benchmarks) **Latin America: ~3,100+ attacks/week *(highest globally)***
- **Asia-Pacific (APAC): ~3,000+ attacks/week**
- **Africa: ~2,900–3,000 attacks/wk (off unreliable data Africa is hit 30-50% more than Europe/USA**
- **Europe: ~1,700–1,800 attacks/week**
- **North America: ~1,400–1,500 attacks/week**

Key Insight **Africa is not the highest, but consistently among the most targeted regions globally**

- **Attack levels in Africa are:**
  - **~40–100% higher than Europe and North America**
  - **Comparable to APAC and just below Latin America**

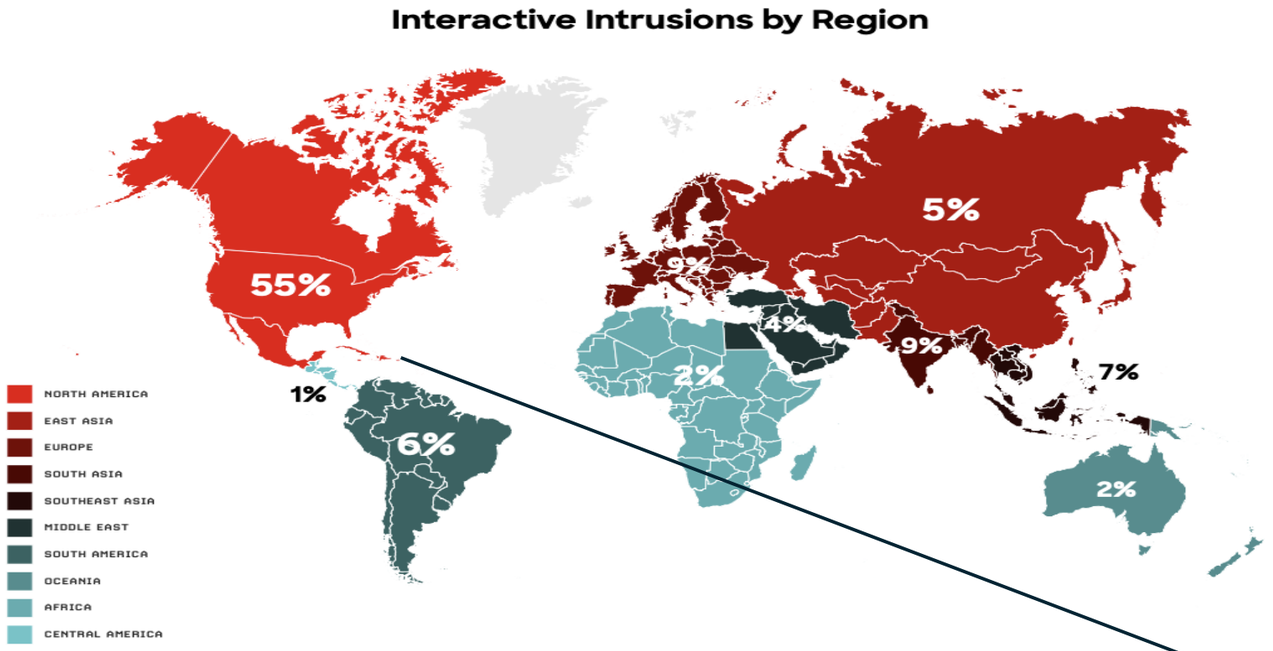


Figure 1. Interactive intrusions by region, January-December 2025

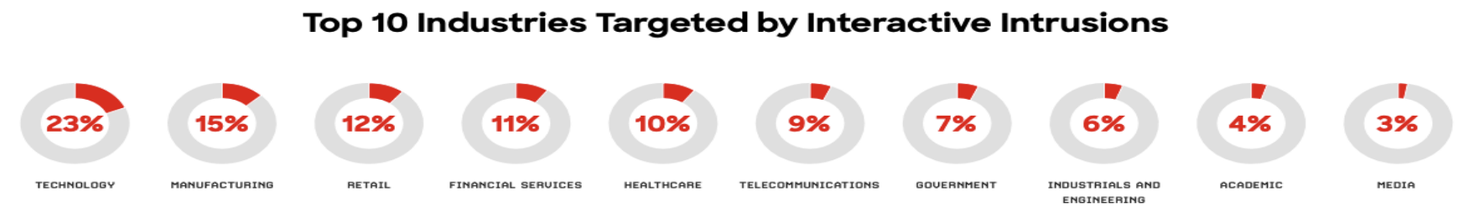


Figure 2. Top 10 industries targeted by interactive intrusions, January-December 2025

Don’t believe the 2% - we just don’t measure or report cyber incidents enough in Africa!

While global data on “success rates” is limited, all indicators point to a higher likelihood of successful attacks in Africa—driven by lower cyber maturity, human-factor vulnerabilities, and limited detection and reporting.

The African Visibility Gap

The challenge

One of the major obstacles in Africa, including Zimbabwe, is the **limited public visibility of cyber incidents**.

We often do not know:

- how many insurers have been attacked
- how often incidents occur
- how much loss has been suffered
- whether data was exposed & whether customers were notified
- what corrective action followed..

Likely reasons for under-disclosure

In practice, public underreporting in African markets is often driven by:

- reputational concerns
- fear of customer panic
- weak or inconsistent disclosure norms
- limited mandatory public reporting
- low sector cyber maturity
- preference for private handling of incidents.

Strategic consequence - This secrecy has costs:

- leaders underestimate the threat & boards fail to prioritise cyber investment
- institutions repeat the same mistakes & Regulators lack visibility
- the public remains uninformed & the sector loses collective learning.

SUPPORTING AFRICAN CYBER RESILIENCE: INTERPOL AFRICA CYBER SURGE OPERATION SURGE II

INTERPOL supports African cyber resilience through partnerships, platforms, and capability-development activities.

A prime illustration of this is Operation Africa Cyber Surge II:

- INTERPOL Gateway and the World Economic Forum's Cybercrime Atlas partners provided essential information that was crucial for the operation's success
- The use of CCP – Operations by participating countries for information exchange and operational coordination
- A series of pre-operation training sessions aimed at enhancing the skills of investigators in various domains of cybercrime investigation

3. Coordination challenges across the cyber ecosystem

Establishing and strengthening open, inclusive, and diverse partnerships is key to fostering effective cooperation in the fight against cybercrime.

However, African member countries reported challenges in fostering collaboration between law enforcement and the relevant stakeholders in the cyber ecosystem.

Working with service providers, especially when located overseas, appears to remain a major difficulty for cybercrime investigations. Meanwhile, it was reported that public-private cooperation is often conducted on an ad hoc basis rather than through established, standardized frameworks.

Why Greater Disclosure Helps the Sector

Yes, disclosure carries short-term reputational risk.

But long-term silence creates a larger strategic risk by normalising complacency .

The advantages of transparency far outweigh the risks of silence.

Secrecy protects image in the short term, but weakens resilience in the long term.

Bottom Line :

This is not about shaming institutions. It is about improving sector resilience. If incidents remain hidden, executives convince themselves the problem is small. Public enforcement, public breach reporting, and visible penalties in other jurisdictions have helped boards take cyber risk seriously. Africa needs a more mature disclosure culture, because secrecy delays learning.

Raises leadership awareness

Executives act faster when consequences are visible.

Strengthens regulatory deterrence

Public disclosure of incidents and penalties reinforces accountability.

Promotes sector learning

Institutions can improve faster when they know what has gone wrong elsewhere.

Encourages investment

Boards are more likely to fund cyber resilience when risks are concrete and evidenced.

Protects customers

Disclosure improves trust when accompanied by timely remediation.

Cyber Insurance – Pricing

Without reliable data on cyber incidents and propensity, accurate sustainable product pricing is not possible

Strengthens Regions $ Stability

enables insurers to better protect policyholder funds and institutional reserves - safeguarding **national savings + long-term financial security** against cyber-related loss

Reduces Systemic Industry Risk

allows insurers and reinsurers to manage aggregate risk more effectively—protecting the industry from **cascading losses and systemic instability in the face of escalating cyber threats**.

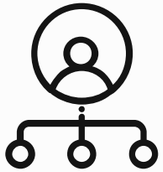
CALL TO ACTION : Collective Defence – A Cyber Think Tank & Centre of Excellence

Cyber risk is a shared threat—our response must be shared.
By combining **intelligence, capability, and collaboration**, we become stronger together - protecting not only our institutions, but the financial security of the nations we serve.

THE REALITY

- African insurers face a **common and escalating cyber threat**
- The industry is **collectively under-resourced**, with:
  - Scarce and expensive cyber skills
  - Fragmented knowledge and intelligence
  - Limited local data to guide decision-making

👉 We are **fighting the same enemy, with similar constraints, in isolation**



THE OPPORTUNITY

Act Together, Not Alone
(Strategic Layer)
Establish -African Insurer Cyber Think Tank

- Develop **shared intelligence on threats, incidents, and emerging risks**
- Shape **Africa-specific cyber risk strategies and underwriting frameworks**
- Drive **policy alignment and regulatory engagement**
- Enable **collective foresight and coordinated response**

CENTER OF EXCELLENCE

Establish Centre of Excellence
(Capability Layer)

- Pool **scarce cyber expertise across the industry**
- Provide **technical advisory, incident support, and best practice guidance**
- Build **skills, training, and executive cyber literacy**
- Support insurers with **practical tools for resilience and response**

The Resilliant Insurer's – Must Do Checklist

1. Governance & Leadership

- Board-level oversight of resilience and cyber risk
- Defined accountability (CIO, CRO, Risk, Operations)
- Regular resilience reporting to ExCo

2. Critical Business Services

- Identify **core services** (e.g. claims, policy admin, payments)
- Map dependencies (systems, people, third parties)
- Define acceptable downtime (impact tolerances)

3. Cyber Security Controls

- Multi-factor authentication (MFA) in place
- Endpoint detection and monitoring (EDR)
- Regular vulnerability assessments and patching
- Identity and access management controls

4. Data Protection & Recovery

- Regular, tested backups (including offline backups)
- Data encryption for sensitive information
- Clear data classification and access policies

5. Incident Response & Crisis Management

- Documented incident response plan
- Defined escalation procedures + Crisis communication plan (internal + external)
- Regular simulation exercises (cyber drills)

6. Third-Party Risk Management

- Due diligence on vendors and partners
- Security requirements in contracts
- Monitoring of third-party access
- Contingency plans for critical suppliers

7. Operational Continuity

- Business Continuity Plan (BCP) in place
- Disaster Recovery (DR) capabilities tested
- Alternative processing arrangements
- Remote working capability if systems fail

8. Regulatory & Compliance Readiness

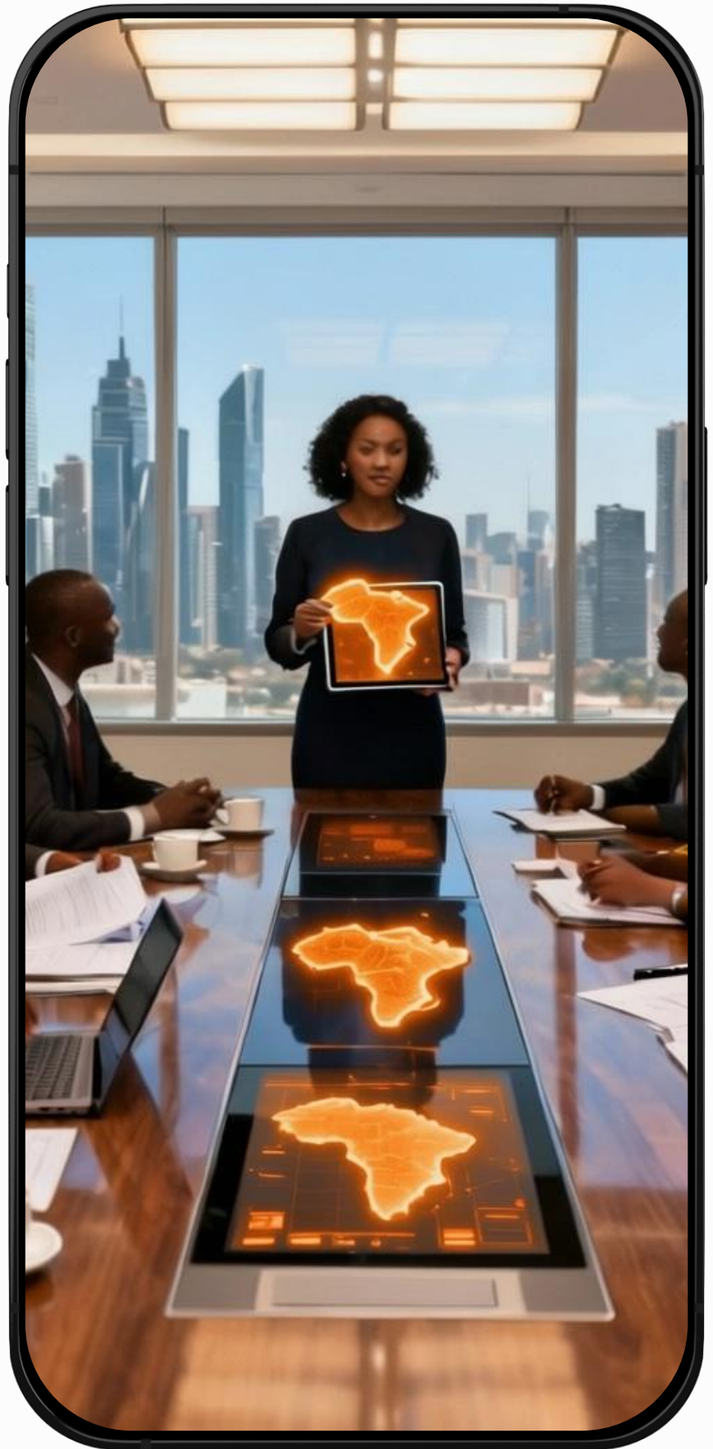
- Alignment with data protection laws
- Incident reporting procedures defined
- Audit trails and documentation maintained

9. Staff Awareness & Training

- Regular cyber awareness training
- Phishing simulation exercises
- Clear policies for password and access management

10. Testing & Continuous Improvement

- Regular resilience testing (BCP, DR, cyber scenarios)
- Lessons learned from incidents
- Continuous improvement programme



THANK YOU FOR YOUR TIME AND ATTENTION

Do reach out should you have any feedback or queries regarding training or advisory on cyber resilience for your organisation.

&

View our full Profile online

Zelina Francis
Practice Director

Digital Governance & Executive Learning
Inflection Point (Private) Limited

- +263 784473876 (Zimbabwe)
  +44 790 3345027 (United Kingdom)
- zelina@inflectionpoint.africa
- https://inflectionpoint.africa
- Suite 29, Arundel Village Business Center
  51 Quorn Avenue, Harare, Zimbabwe

Thank You

Protecting The Interests
Of Insurance And Pension Consumers

enquiry@ipec.co.zw 0772 154 281 www.ipec.co.zw

@ipeczw

Cyber Imperative : Presenters supporting slides

What is “Malware-Free Detection”?

Malware-free detection refers to identifying cyber attacks **that do not rely on traditional malicious software (malware)**.

In simple terms, it is the ability to detect attackers who are using **legitimate tools and normal system behaviour** to carry out attacks instead of installing viruses or malicious files.

How These Attacks Work

Instead of using malware, attackers:

- use **stolen usernames and passwords**
- log in like legitimate users
- use built-in system tools (e.g. PowerShell, admin tools)
- move through the network quietly
- avoid triggering traditional antivirus systems

These are often called **“fileless attacks”** or **“living off the land” attacks**.

Why It Is Important

1. Traditional security tools may miss them

Most legacy security systems are designed to detect **malicious files**, not suspicious behaviour.

2. These attacks are increasing

Modern attackers prefer stealth. Many advanced breaches today are **malware-free**.

3. Harder to detect

Because attackers look like normal users, it is difficult to distinguish:

- legitimate activity. vs malicious activity.

4. Faster and more damaging

Attackers can: move quickly across systems + access sensitive data + initiate fraud before detection occurs.

“Malware is like a burglar breaking a window. Malware-free attacks are like someone using a stolen key - everything looks normal, but they shouldn’t be inside.”

“The most dangerous attacks today often don’t use malware at all - they use your own systems, your own tools, and your own credentials against you.”

Ransomware Affiliate : Chatty Spider

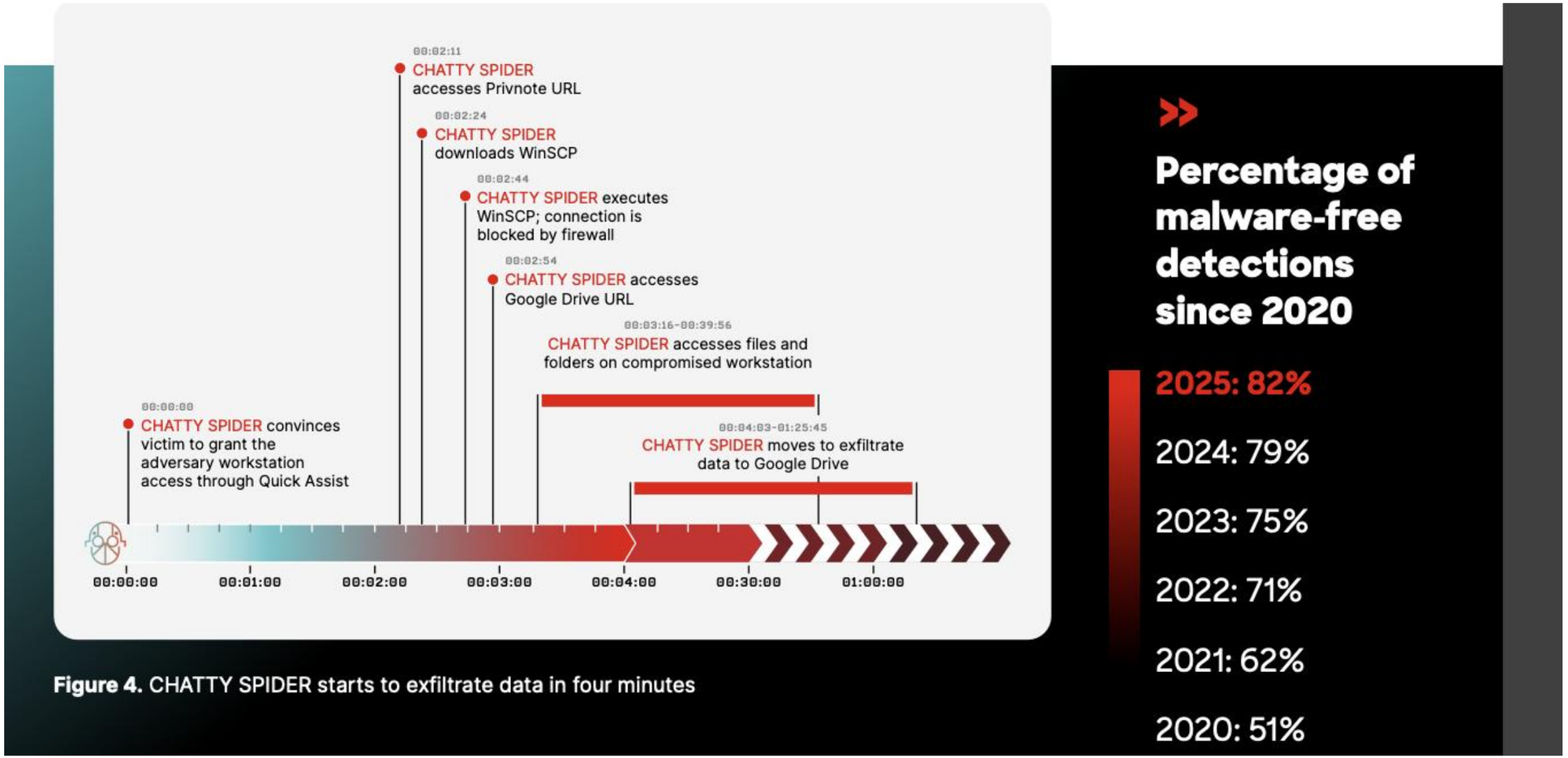


Figure 4. CHATTY SPIDER starts to exfiltrate data in four minutes

Chatty Spider is a financially motivated cybercrime group that specialises in manipulating people (not just systems) to gain access to organisations.
It is part of a broader ecosystem of **ransomware affiliates and cybercrime-as-a-service operations**.

Fake CAPTCHA Campaigns Surge in Popularity During 2025

In 2025, many criminal actors shifted from malicious browser update-related lures to fake CAPTCHA lures to entice victims to download and execute malware. Figure 5 highlights adversaries' rapid adoption and persistent use of fake CAPTCHA lures (compared to malicious browser update lures) over the past two years. In comparison to 2024, CrowdStrike Intelligence observed a 563% increase in incidents using fake CAPTCHA lures in 2025.

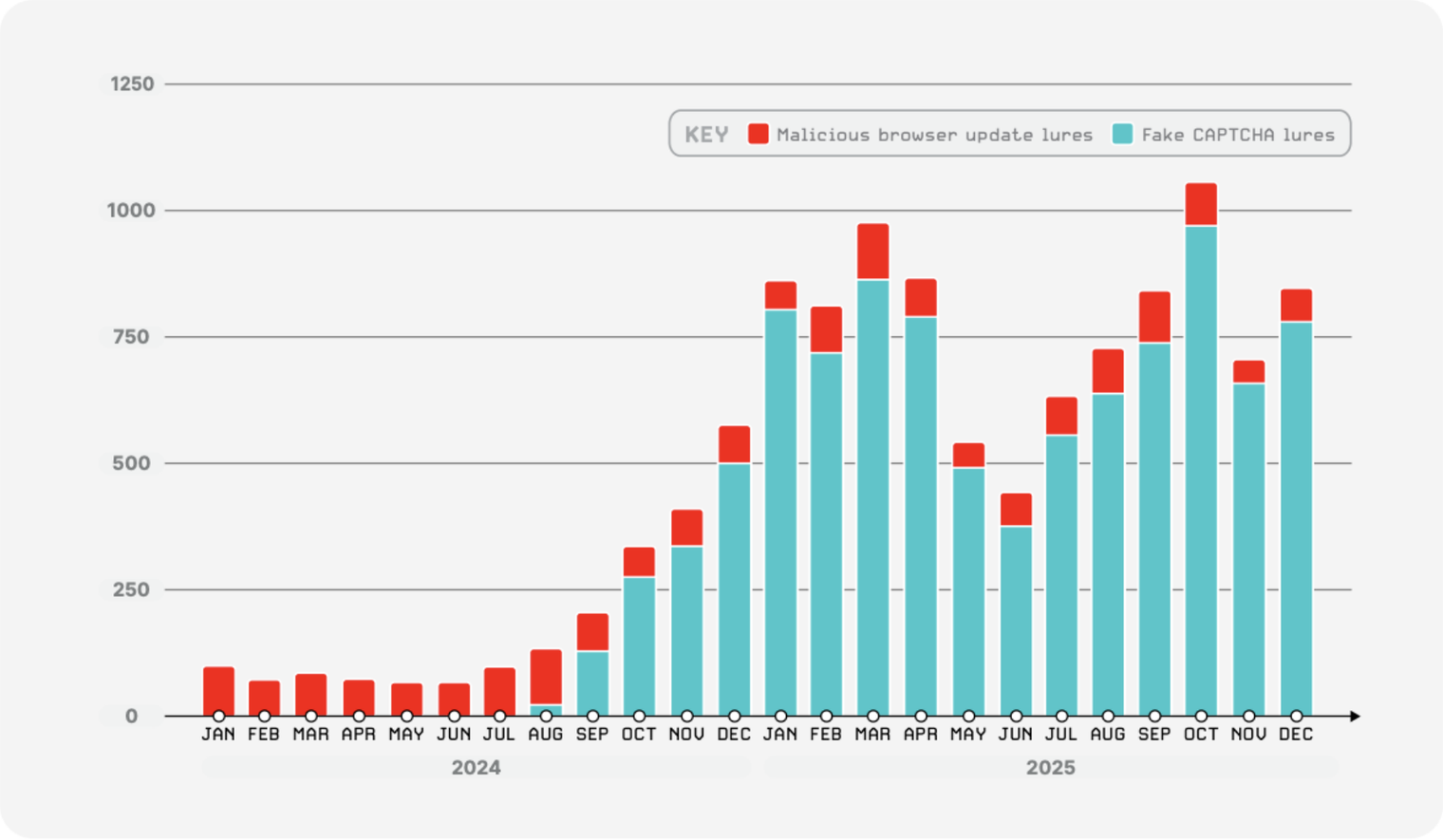


Figure 5. Criminal use of malicious browser update lures and fake CAPTCHA lures, January 2024-December 2025

China Nexus - feared or revered

What is "China Nexus"?

In cyber security, **"China Nexus"** refers to:

Cyber threat activity that is linked to, originates from, or aligns with Chinese state interests or actors.

This does **not always mean direct government control**, but typically includes:

- state-sponsored groups
- state-aligned cyber actors
- advanced persistent threat (APT) groups operating in China's strategic interest

These groups are often associated with **espionage, data collection, and long-term access**, rather than quick financial gain.

How China Nexus Actors Operate

China Nexus groups typically focus on:

1. Long-term access (stealth over speed)
They aim to stay inside systems for extended periods without detection.

2. Data exfiltration
They target large volumes of data such as:

- personal records + financial data + health information + corporate intel

3. Supply chain infiltration
They often compromise:

- software providers + IT vendors + infrastructure partners

to gain access to multiple organisations.

4. Low-noise, malware-light techniques
They increasingly use: legitimate system tools + credential compromise + subtle persistence methods

"Not all cyber threats are about immediate financial loss - some are about long-term access to data and insight. For insurers, that makes them an unexpected but valuable target."

Insurance organisations must defend against both fast, visible financial attacks and slow, invisible strategic intrusions.

Zero-Day Vulnerabilities

A security flaw in software or systems that is unknown to the vendor or developers — meaning there is no fix (patch) available yet.

Why is it called “zero-day”?

Because:

- The software vendor has **“zero days” to fix it**
- Attackers can exploit it **before anyone knows it exists**

How it works

1. A weakness exists in software (e.g. operating system, application, platform)
2. Hackers discover it before the vendor does
3. They exploit it to gain access, steal data, or disrupt systems
4. No patch or protection exists at that time

Why Zero-Day Vulnerabilities Are Dangerous

1. No immediate defence
Since the vulnerability is unknown, there is **no patch or signature to detect it**

2. Highly valuable to attackers
Zero-days are often used by: advanced cybercriminal groups and state-linked actors (e.g. China Nexus-type threats)

3. Difficult to detect – Attacks - look like normal system behaviour

Insurance Sector Relevance, a zero-day attack can:

- compromise **claims systems or policy databases**
- expose **customer and medical data**
- disrupt **core operations**
- create **regulatory and reputational risk**

“A zero-day vulnerability is like a hidden door in your building that even the owner doesn’t know exists — but an intruder has already found it - most dangerous because organisations are exposed before they even know there is a problem.”

Valid Account Abuse – when hackers don’t break in they “Log In”

The use of legitimate user credentials (usernames and passwords) by attackers to gain access to systems and carry out malicious activities.

How It Happens

Attackers obtain valid credentials through:

- phishing emails
- social engineering (e.g. impersonating IT support)
- password leaks or data breaches
- weak or reused passwords
- credential stuffing attacks

What Attackers Do Once Inside

Because they are using valid accounts, they can:

- access systems without raising alarms
- move across networks (lateral movement)
- escalate privileges - manipulate data - initiate fraudulent transactions - extract sensitive information

Why It Is So Dangerous

1. Looks like normal activity
Security systems may not flag the activity because it appears legitimate.

2. Bypasses traditional defences
No malware is required, so antivirus tools may not detect anything.

3. Enables fast escalation
Attackers can move quickly once inside — reducing response times

Insurance Sector Relevance

Valid account abuse is particularly high-risk for insurers because attackers can: - access **claims systems -** change **beneficiary or payment details -** manipulate **policy records -** extract **customer and medical data -** initiate **fraudulent payouts**

“Valid account abuse is like someone using a stolen ID card to walk into your office - everything looks normal, but they shouldn’t be there.”

“Today’s attackers don’t always hack systems- they log in using stolen identities, making detection much more difficult.”

Cloud-Conscious Intrusions

Attacks specifically designed to exploit cloud systems, focusing on **identity, access, and misconfigurations** rather than traditional infrastructure.

Key Characteristics

- Target **user accounts and access controls**
- Often **malware-free and hard to detect**
- Exploit **misconfigured cloud environments**
- Enable access to **multiple systems from a single entry point**

Insurance Sector Impact

- Exposure of **customer and medical data**
- Risk of **claims and payment manipulation**
- Increased **third-party and ecosystem vulnerability**
- Greater reliance on **identity as the primary security control**

As insurers move to the cloud, attackers are shifting from breaking in to simply logging in and accessing entire systems at once.

Third Parties – Manage them tightly

1. Expanded Attack Surface
Every third party (brokers, hospitals, IT vendors, payment platforms) creates an additional entry point into your systems.

2. Weakest Link Risk
Attackers often target the least secure partner to gain access to the primary organisation.

3. Access to Sensitive Data
Third parties may handle **customer, medical, and financial data**, increasing exposure if they are compromised.

4. Shared Systems and Integrations
APIs and system integrations mean a breach in one organisation can quickly spread across connected platforms.

5. Limited Visibility and Control
You do not fully control how third parties manage their security, yet their weaknesses directly impact you.

Insurance Sector Impact

- Data breaches through providers or vendors
- Fraud via compromised partners
- Disruption to claims and service delivery
- Reputational damage from incidents outside your control

Key Message : “Your security is only as strong as your weakest third-party partner.”

Secure AI Use – Opportunity vs Threat

1

Secure AI to reduce emerging business and operational risk

As AI becomes embedded in core business processes, it introduces a rapidly expanding attack surface that adversaries are already exploiting. Organizations should employ comprehensive AI security and governance measures to address threats to AI systems as well as threats posed by threat actors using AI. These should include monitoring employees' use of AI tools, enforcing access controls, and using data classification rules to prevent sensitive data leaks. These measures should also include securing homegrown AI workloads from runtime attacks (such as prompt injection), assessing the security of external vendors, and requiring secure configurations and vulnerability assessments for new AI products and their dependencies.

To defend against AI-enabled threats, organizations should develop clear incident response responsibilities and business continuity plans. Organizations can further secure their environments with strong identity verification procedures, AI-focused security awareness training, and continuous threat hunting.