CYBER SECURITY AND INSURANCE

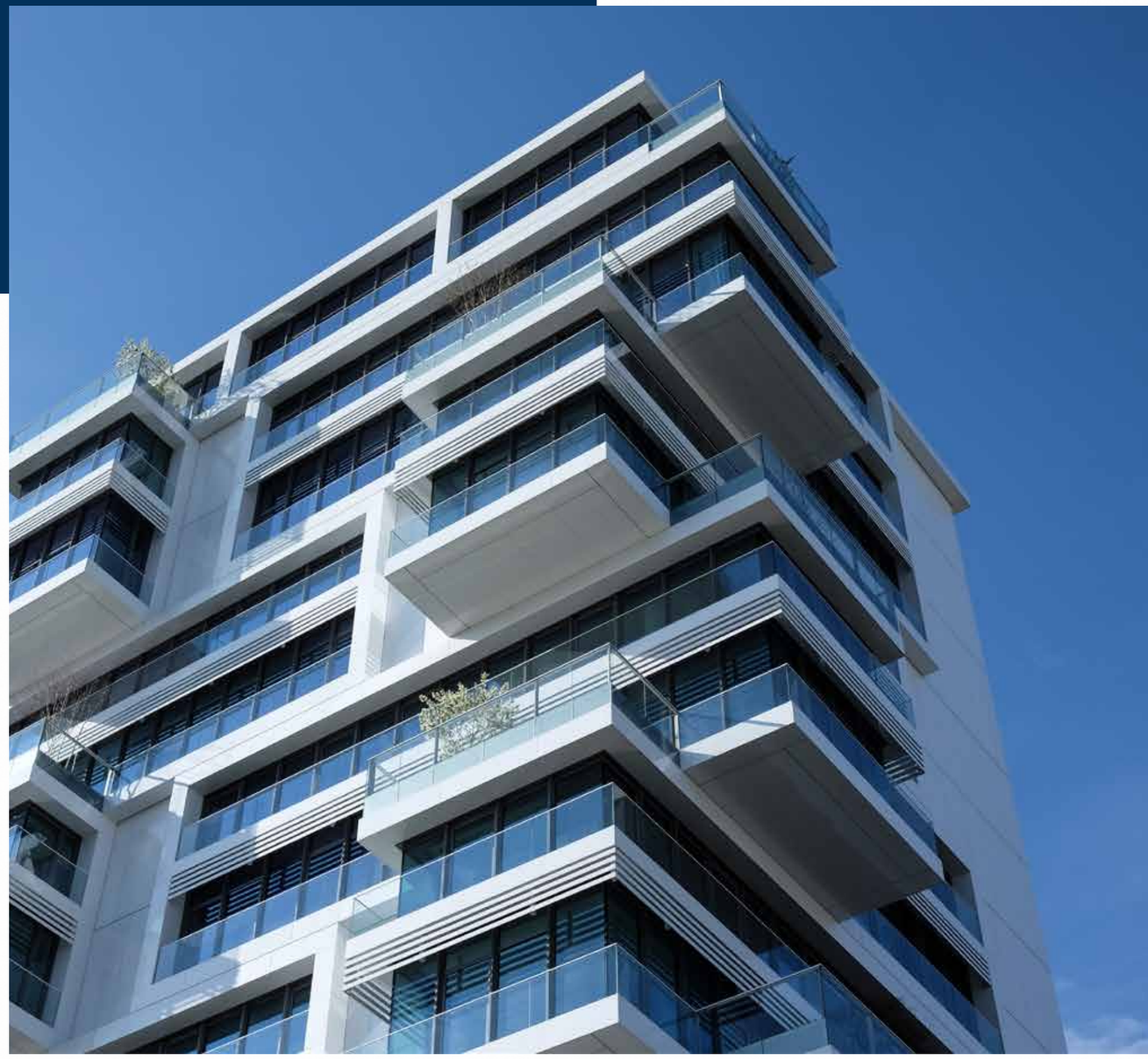
Disruption and Opportunity – Equipping the Botswana Insurance Industry for the future

SATIB Insurance Brokers
Established 1990

Presented By:
Taurai Pambweyi

+263 77 286 9242 tpambweyi@satib.co.zw

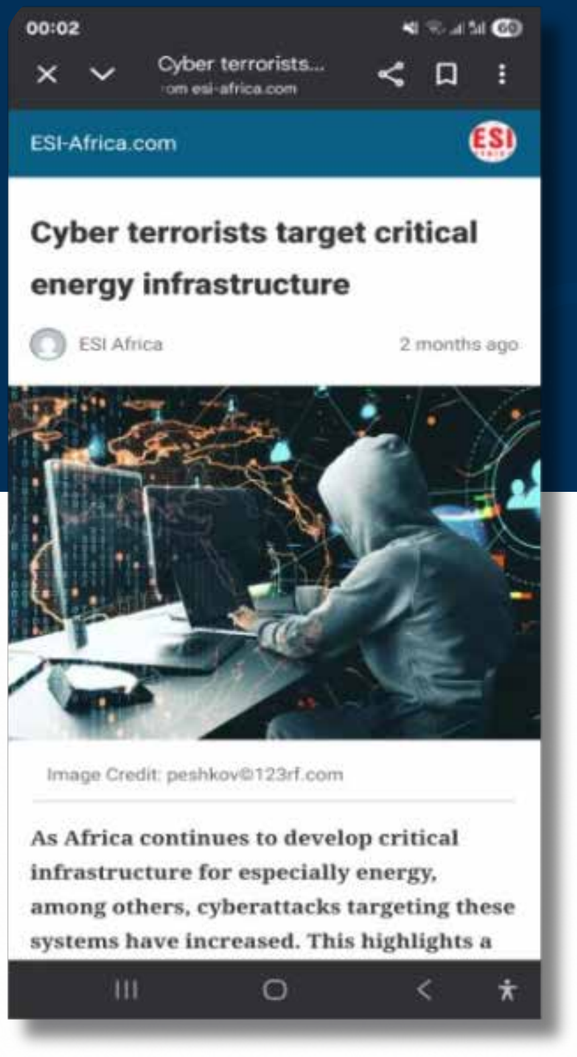
Content



CROWDSTRIKE "CROWDOUT" IT OUTAGE (JULY 2024)

- A faulty update from CrowdStrike disrupted ~8 million devices globaly
- Estimated insured losses: $400 million to $1.5 billion
- Overall economic losses for Fortune 500 firms: $5.4 billion
- Non-malicious tech failures can trigger massive business interruption claims due to the knock-on effect
- Not a direct Loss to CrowdStrike own insurance policy as essentially due to It Provider

Some Local Examples



KEY FACTORS DRIVING THE INCREASING CYBER RISK

Advancements in technology

New technologies like IoT, cloud computing, and artificial intelligence while offering benefits also introduce new vulnerabilities

Remote Work

The rise of remote work has expanded the attack surface as employees access sensitive data from various locations and devices.

Increased reliance on digital infrastructure

Critical infrastructure like power grids, transportation systems, and healthcare are increasingly digitized, making them attractive targets.

Financial incentives

Cybercrime is a lucrative business, motivating cybercriminals to develop more advanced techniques.

Artificial intelligence

(AI) is widely expected to power future ransomware attacks, with automated attack processes, more convincing phishing, and faster malware development

IMPACT OF CYBER ATTACKS

Financial loss

Direct costs (e.g., ransom payments, legal fees) and indirect costs (e.g., lost revenue, business interruption).

Reputational Damage

Loss of customer trust and confidence.

Legal Liabilities

Compliance violations and lawsuits.

Operational Disruption

System downtime and business interruptions.

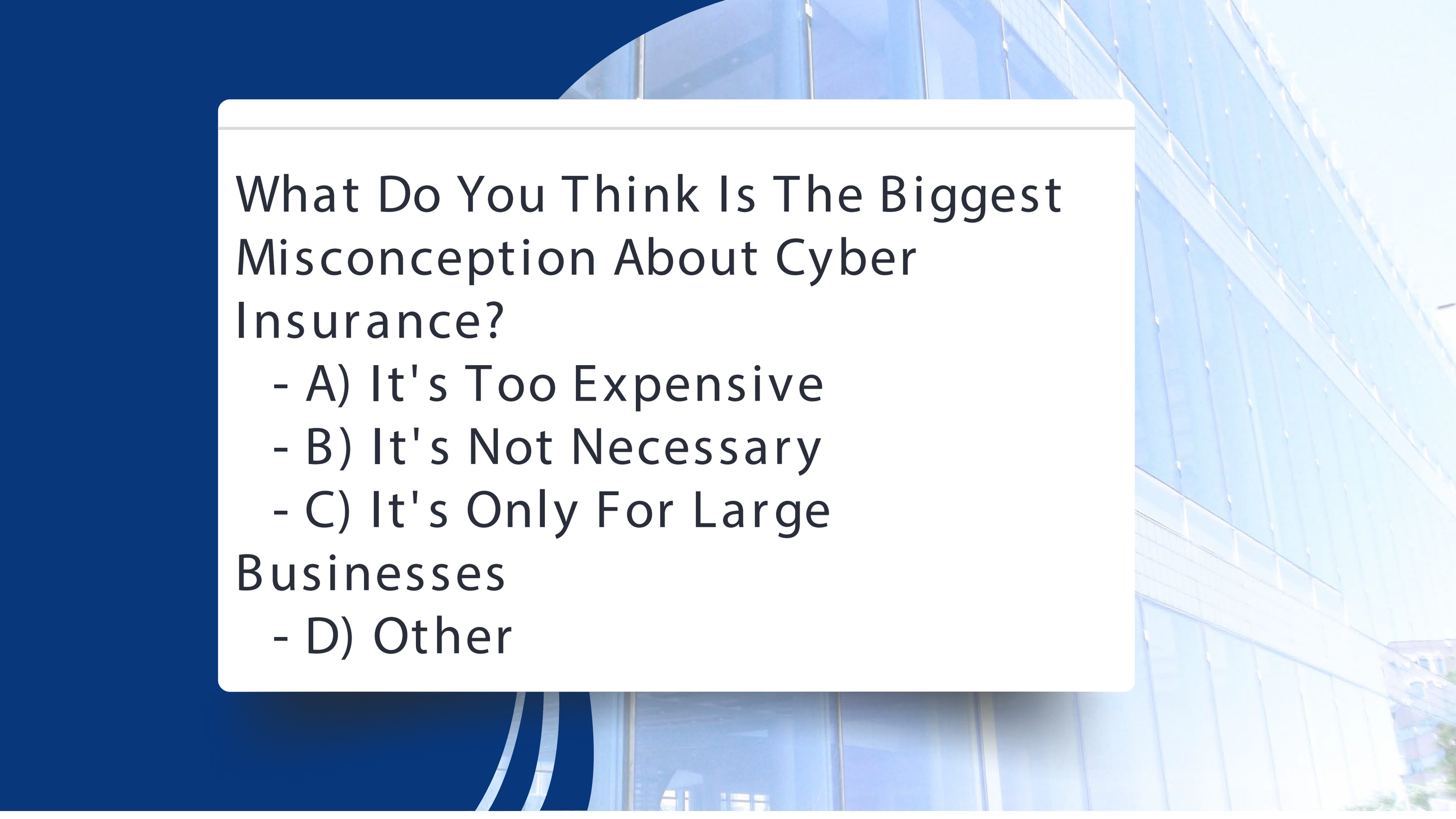
Data Loss

Loss of valuable information and intellectual property.

LETS GO LIVE

Have You Ever Received A Suspicious Email Or Message?

- A) Yes
- B) No



What Do You Think Is The Biggest Misconception About Cyber Insurance?

- A) It's Too Expensive
- B) It's Not Necessary
- C) It's Only For Large Businesses
- D) Other

How Often Do You Change Your Machine And Email Password?

- A) Daily
- B) Weekly
- C) Monthly
- D) Quarterly
- E) Rarely

How Confident Do You Feel In Your Organization's Ability To Respond To A Cyber Attack?

- A) Very Confident
- B) Somewhat Confident
- C) Not Very Confident
- D) Not At All Confident

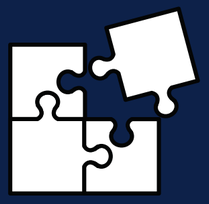
What are the most significant barriers to adopting cyber insurance in Botswana,and how can they be addressed?

What Do You Think Is The Most Common Cyber Threat Facing Businesses Today?

LETS INTERACT

Lucrative Business?
Is there a market for such in Botswana?

Why is penetration low?



What are some of the challenges we face in this space?

Lucr ativ e Business ?
Is ther e a mark et f or such in Bots wana ?

Somewhat

Yes

No

Submit

Loading...

CYBER LANDSCAPE

THREAT MAP

DID YOU KNOW ?

Global GWP (2024) – USD16.6 billion

Expected growth in 2025/6 – 25% annually

2030 Anticipation – USD35 Billion

STATE OF THE MARKET

STATE OF THE MARKET

Growth: $16.6 billion in 2024,

Increase In Sophistication Of Threats: Ransomware, phishing attacks, data breaches, and sophisticated malware continue to be primary loss drivers

Regulatory Fines: Expected to increase as more and more governments continue to be strict on data protection laws

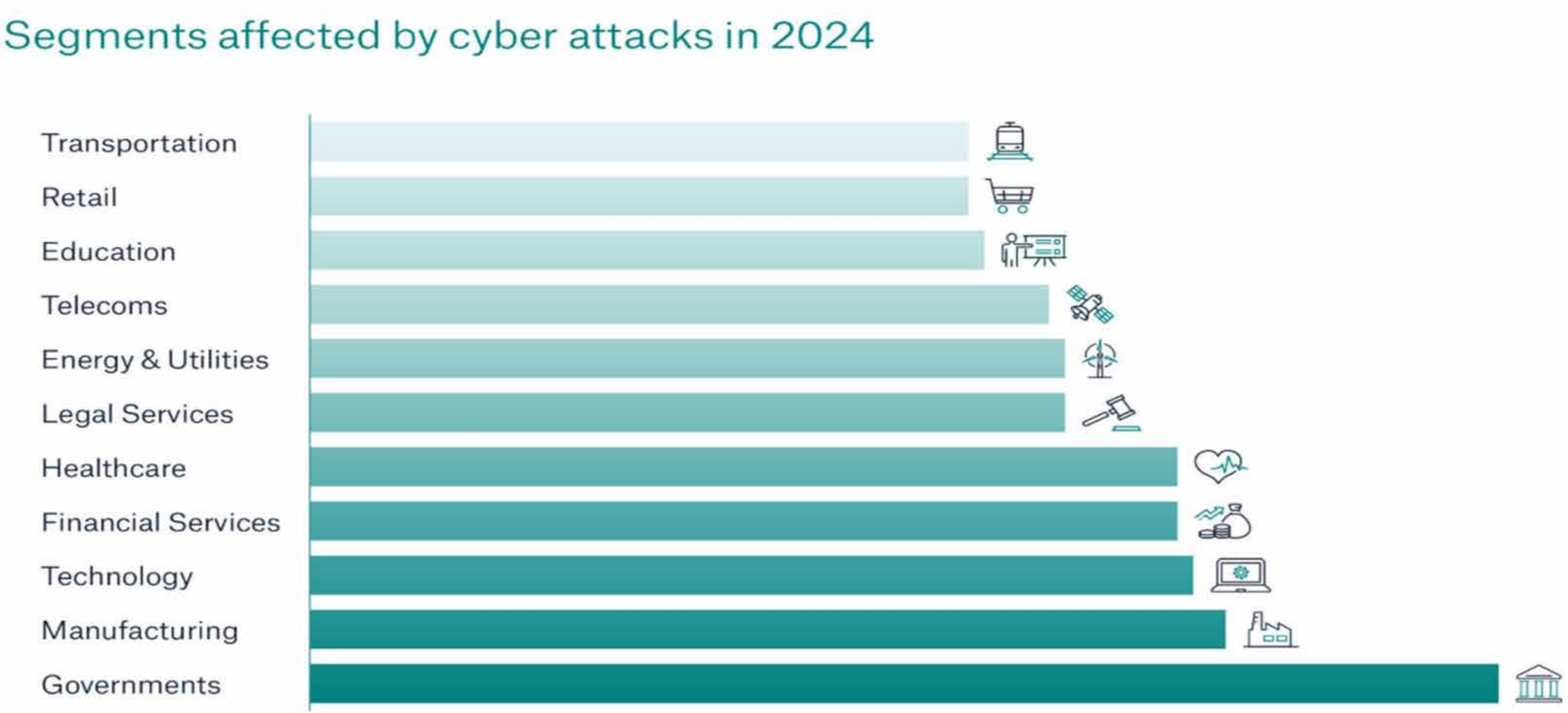
Rate Stabilisation: new entrants driving the prices down creating a near soft market

STATE OF THE MARKET

High Vulnerability and Low Penetration

Data: Global Cyber Risk and Insurance Survey by Munich Re, 2024;

STATE OF THE MARKET



CYBER LANDSCAPE

Cyber crime is anticipated to cost the global economy USD 10.5 trillion annually by 2025

Cybercrime costs are growing 15% per year

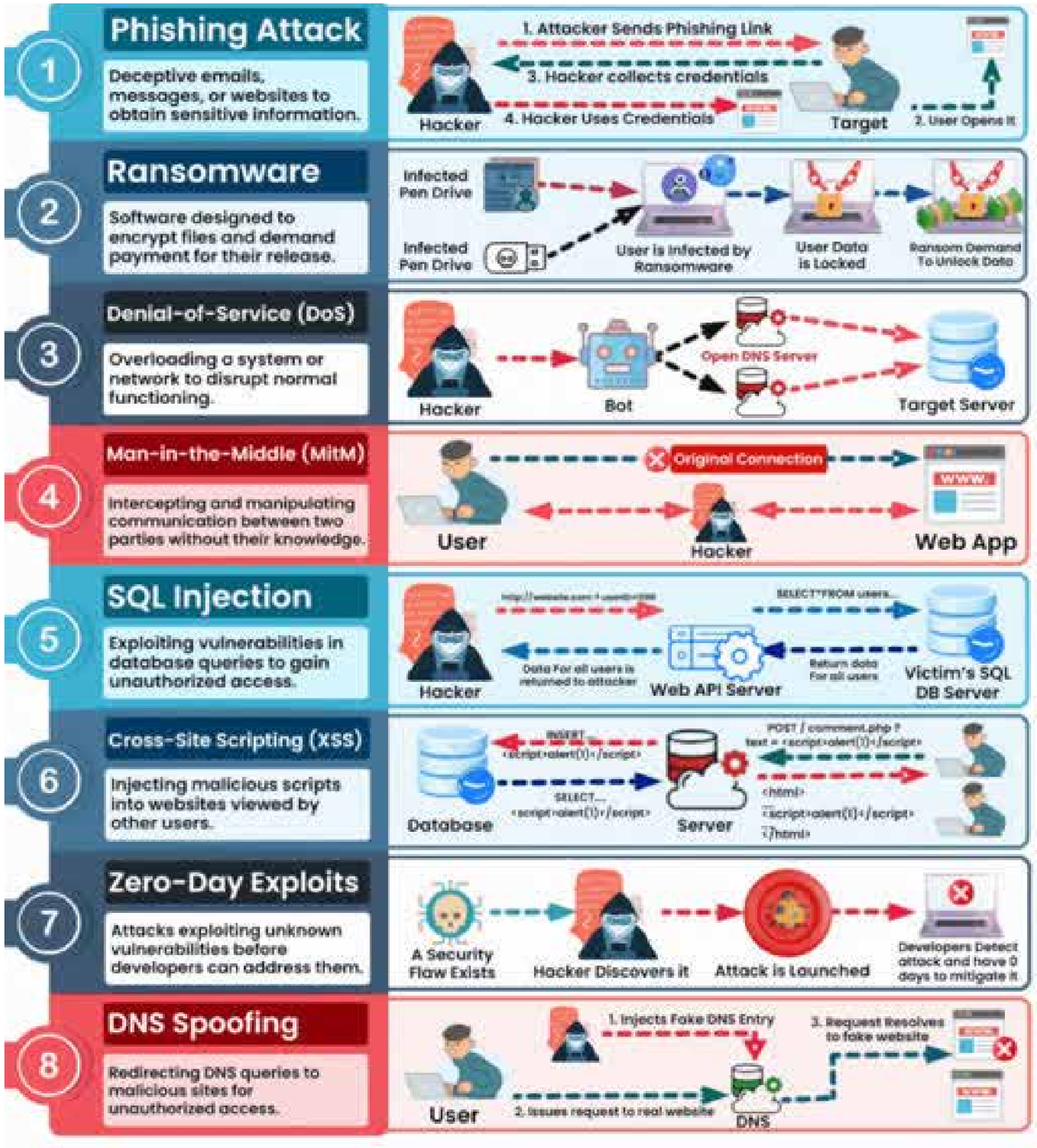
The cost of a data breach can be devastating. In fact, the average data breach cost reached approximately USD 4.45 million per incident in 2023. That is an increase from USD 4.35 million in 2022.

Experts estimate that up to 90% of cyber incidents involving smaller or medium-sized organizations may never appear in official records because some victims prefer to handle breaches quietly, fearing reputational harm or lacking confidence in legal recourse.

Studies often cite that roughly 70% of all cyber attacks specifically target small-to-midsize businesses

Growth in AI driven Cyber Attacks (deepfake extortion, GhostGPT)

TOP 8 TYPES OF **CYBER ATTACKS**



CYBER LANDSCAPE

Top 5 cyber attacks are:

1. Phishing attacks (including spear-phishing)
2. Ransomware attacks
3. Business email compromise
4. Investment fraud / investment scams
5. Identity theft

CURRENT TRENDS IN CYBER SPACE

Building more sophisticated malware

Sabotaging Machine Learning

- Convincing imitations of humans eg writing speech and images
- Deception for fraud including identity theft, financial fraud and disinformation

Enhanced Phishing emails

- Draft emails mimicking common terms and tone to specific recipients

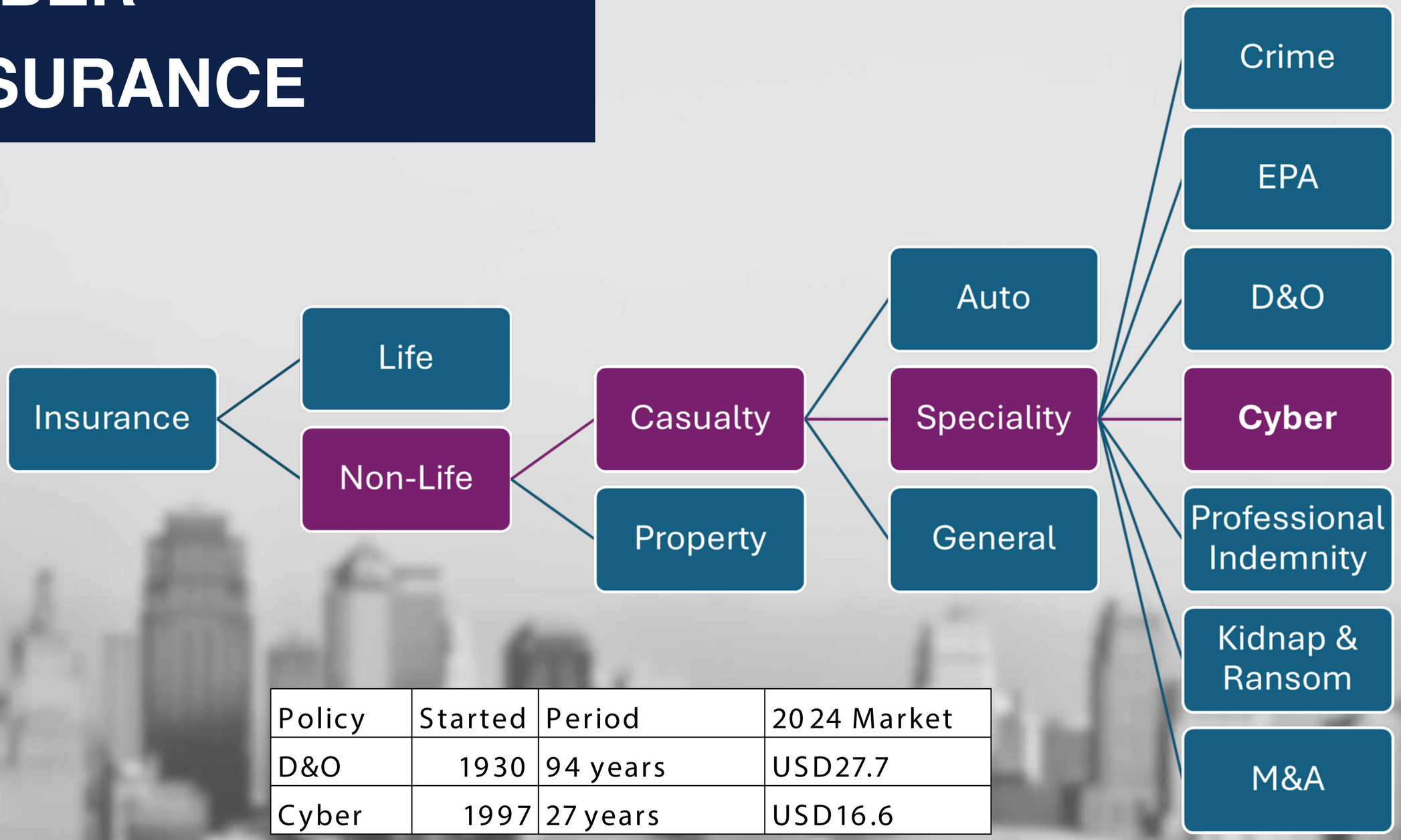
Cracking Captchas and brute force password attacks

- Advanced password guessing

CYBER INSURANCE

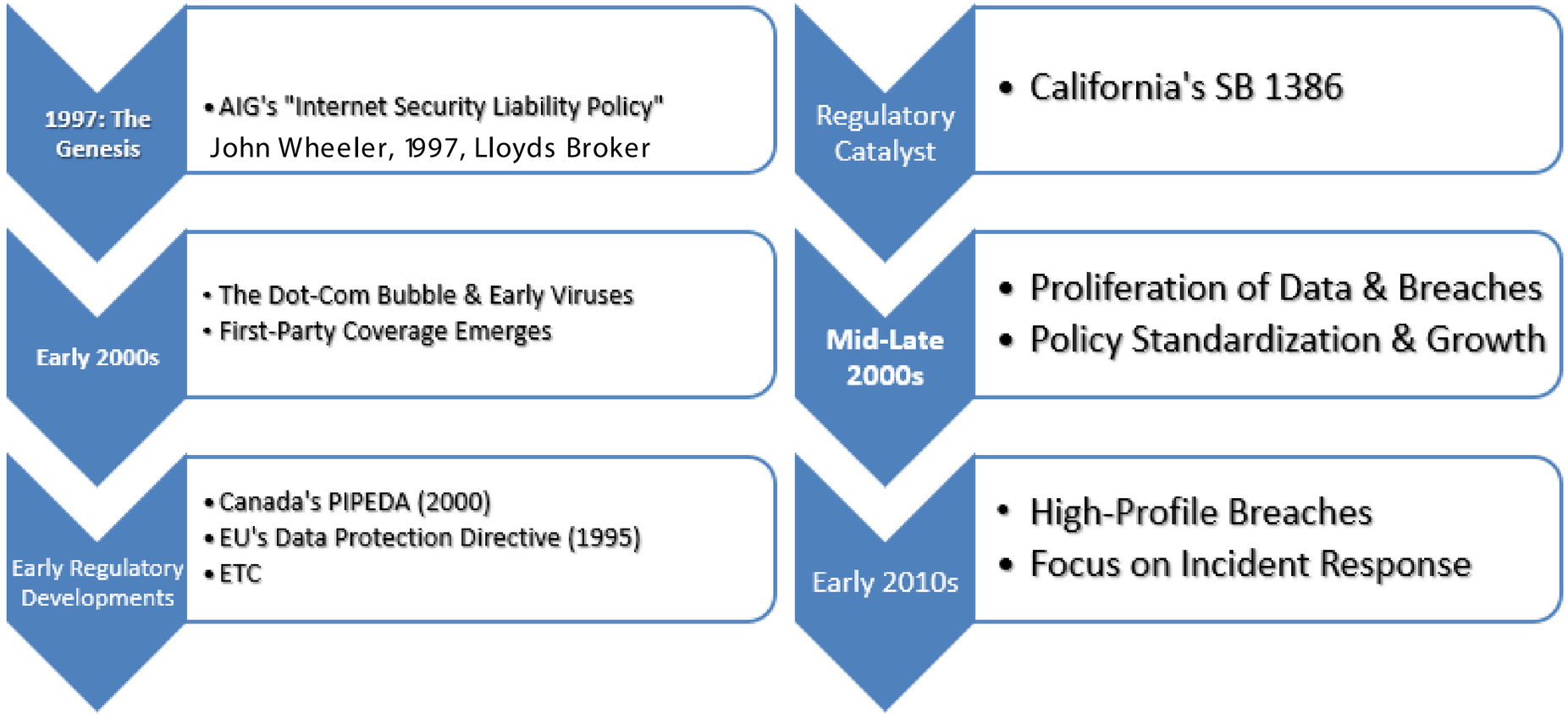
A CLOSER LOOK

CYBER INSURANCE



Policy	Started	Period	2024 Market
D&O	1930	94 years	USD27.7
Cyber	1997	27 years	USD16.6

EVOLUTION OF CYBER INSURANCE



EVOLUTION OF CYBER INSURANCE

Mid-Late 2010s

- Global Regulatory Avalanche

Late 2010s - Early 2020s

- The Ransomware Epidemic
- Hardening Market & Underwriting Scrutiny

CURRENT STATE

- Comprehensive & Proactive Cover
- Risk Management Partnership

WHAT IS CYBER INSURANCE?

- Cyber insurance fills the gaps in both traditional first-party and third-party liability policies
- Cyber insurance provides protection for companies who:
- Have access to private, confidential information about their customers or employees and have a responsibility for keeping it safe
- Have a web presence with emerging content exposures
- Have a dependency on technology and have emerging transactional exposures
- It is not Technology Errors and Omissions
- John Wheeler, 1997 - Lloyds Broker

WHAT IS CYBER INSURANCE?

Cyber insurance (also known as cyber liability insurance or cyber security insurance or network security and privacy insurance or Cyber Crime) is designed to protect businesses against the financial loss (first and third party) resulting from a range of cyber threats and exposures, including cybercrime, data breach and system interruption

CYBER INSURANCE TYPICALLY COVERS

Coverage Area	Example (Real or Fictitious)	Example (Real or Fictitious)
Incident Response & Forensics	Covers the cost of hiring forensic experts to identify and contain breaches, plus legal & crisis management advice.	In the 2023 MGM Resorts breach, forensics and PR support costs exceeded $15 million (KrebsOnSecurity, 2023)
Data Breach Liability	Third-party liability for unauthorized disclosure of PII/PHI. Includes legal defense, fines (if insurable), and settlements.	A Zimbabwean private hospital leaks patient records due to an outdated firewall. The insurer covers legal and regulatory costs.
Cyber Extortion (Ransomware)	Covers ransom payments, negotiation services, system decryption, and extortion-related costs.	In the Colonial Pipeline attack (2021), the company paid a $4.4M ransom to restore access (CISA, 2021).
Business Interruption (BI)	Lost income and extra expenses from cyber incidents causing network/system outages.	A South African logistics firm loses $500K in income after malware halts shipment tracking. Insurer pays BI claim.
Contingent BI	Downtime due to cyber events at third-party vendors (e.g., AWS, payment processors).	Retailers experienced revenue loss after AWS outage in 2020. Many had no coverage.
Digital Asset Loss / Restoration	Covers data recovery, software restoration, reconfiguration, and reinstallation of IT assets.	A Zimbabwean retail chain's ERP system is corrupted by malware—insured pays for full system rebuild.
Reputational Harm & PR	Crisis comms, media strategy, and brand rebuilding after a public cyber incident.	British Airways spent millions on PR after their 2018 data breach affecting 500,000+ users (ICO, 2019).
Regulatory Fines & Penalties	Coverage for non-compliance fines (subject to legal permissibility). Often covers GDPR-like laws.	H&M (2020) fined €35M for employee surveillance. Cyber insurance can cover legal & regulatory response
	Coverage for deception-based fraud if explicitly endorsed. Often sub-	A Zimbabwean insurer is tricked into paying US$250,000 via spoofed

STRUCTURE OF CYBER COVER

First Party Losses

- Direct Network Interruption and Business Income
- Contingent Network Interruption and Business Income
- Bricking
- Reputational Business Income
- Cyber-Extortion and Ransom
- Privacy Regulatory Defense and Penalties
- PCI Expenses and Penalties
- Hacker Theft

Third Party Losses

- Privacy and Data Breach
- Network Security Liability
- Multimedia Liability

STRUCTURE OF CYBER COVER

Root cause

- Data Breach
- Network Failure

Resolution

- Remediation Costs
- BI
- Liability

EXAMPLE

Coverage Description	Limit	Deductible
A. Breach Response - Covers costs related to responding to a data or security breach.		
A.1 Breach Response Services	USD 1,000,000	USD 20,000
A.2 Breach Notification and Credit Monitoring Costs	USD 1,000,000	USD 20,000
A.3 Breach Response Legal and Forensic Costs	USD 1,000,000	USD 20,000
B. First Party Loss		
B.1 Data Recovery Costs	USD 1,000,000	USD 20,000
B.2 Business Interruption Loss	USD 1,000,000	USD 20,000
B.3 Dependent Business Interruption Loss	USD 1,000,000	USD 20,000
B.4 Cyber Extortion Loss	USD 1,000,000	USD 20,000
C. Liability - Covers damages and legal expenses from		
C.1 Privacy and Security Liability	USD 1,000,000	USD 20,000
C.2 Regulatory Defense and Penalties	USD 1,000,000	USD 20,000
C.3 Payment Card Liabilities and Costs	USD 1,000,000	USD 20,000
C.4 Media Liability	USD 1,000,000	USD 20,000
D. eCrime		
D.1 Funds Transfer Fraud	USD 100,000	USD 20,000
D.2 Telephone Fraud	USD 100,000	USD 20,000
D.3 Phishing and Social Engineering	USD 100,000	USD 20,000
E. Criminal Reward - Covers rewards for information leading to the arrest of cybercriminals.		USD 20,000
E.1 Criminal Reward Costs	USD 100,000	USD 20,000

WHAT DOES CYBER INSURANCE COVER?

What Are Remediation Costs?

Remediation costs are the expenses incurred to restore systems, data, and operations after a cyber incident.

Covered Remediation Costs May Include:

- Forensic Investigation:

Analyzing how the breach occurred and assessing the scope of damage.

- Data Restoration:

Recovering or recreating lost or corrupted data.

- System Repairs:

Repairing or replacing compromised hardware and software.

- Crisis Management:

Public relations, legal advice, and communication efforts to mitigate reputational damage.

- Compliance & Notification:

Notifying affected parties and regulatory bodies as required by law.

These costs can be immediate and significant.

Without insurance, businesses often struggle to manage the financial and operational impact.

Cyber insurance helps minimize downtime, protect reputation, and ensure regulatory compliance.

WHAT DOES CYBER INSURANCE COVER?

•What Is Business Interruption (BI) Coverage?

BI coverage compensates for lost income and extra expenses when a cyber incident disrupts normal business operations.

When Does It Apply?

- Cyberattacks: Ransomware, DDoS attacks, or data breaches causing system downtime
- System Failures: Outages due to malicious or accidental disruptions
- Cloud Provider Failures: Downtime from third-party service interruptions

What Does It Cover

- Lost Profits: Revenue lost due to business downtime
- Operating Expenses : Rent, payroll, utilities during the interruption period
- Extra Expenses: Costs to continue operations (e.g., temporary systems, staff overtime)

Why It’s Critical:

- Many businesses can't operate without their digital infrastructure
- BI losses can exceed direct remediation costs
- Coverage helps maintain financial stability during and after a cyber crisis

WHAT DOES CYBER INSURANCE COVER?

What Are Liability Claims?

Liability claims arise when a third party (e.g., customer, partner, or regulator) holds your organization legally responsible for a cyber incident.

When Do They Occur?

- Data Breaches: Loss of personal, financial, or health information
- Privacy Violations: Non-compliance with data protection laws (e.g., GDPR, HIPAA)
- Transmission of Malware: Your systems infecting others
- Contractual Breaches: Failing to meet cybersecurity obligations

What's Covered?

- Legal Defense Costs

Attorney fees, court costs, and settlements

- Regulatory Fines & Penalties

Where legally insurable

- Third-Party Damages

Compensation to customers, clients, or vendors

- Media Liability

Defamation, copyright infringement, or data misuse

WHAT DOES CYBER INSURANCE COVER?

What Are Liability Claims?…..C ontinued

Why It Matters:

- Legal and reputational risks are often more costly than direct damage
- Even a minor breach can lead to class-action lawsuits or regulatory scrutiny
- Liability coverage protects your business from external claims and financial ruin

INCIDENT RESPONSE: IMMEDIATE ACTION & COSTS

What it Covers: Reasonable and necessary expenses incurred due to an actual or suspected:

- Privacy and network security event.
- Network interruption event.
- Cyber-extortion and ransom event.

Key Point: Covers costs for "first responder services" by designated providers without the deductible.

When it Applies: Events first identified and reported during the policy period (or extended reporting period).

Network Interruption & Loss of Income:

Contingent Network Interruption and Business Income (Relying on Others)

What it Covers: Same as Direct Network Interruption (loss of income, restoration, business continuity).

Trigger: Network interruption event affecting the computer system of a service provider you rely on.

Key Point: Crucial for businesses dependent on third-party IT or cloud services.

Network Interruption & Loss of Income:

"Bricking" Protection

•What it Covers: Hardware and software replacement costs.

Trigger: A network interruption event or cyber-extortion/ransom event that renders your systems unusable ("bricked").

Key Point: Directly addresses the cost of replacing damaged or destroyed IT infrastructure.

Network Interruption & Loss of Income:

•Reputational Business Income (Protecting Your Reputation)

•What it Covers: Loss of business income due to reputational damage.

•Trigger: Reputational damage caused by a privacy and network security event or a network interruption event.

•Key Point: Recognizes that cyber incidents can impact public perception and, consequently, your revenue.

CYBER-EXTORTION & RANSOM

•What it Covers: Reimbursement for cyber-extortion and ransom expenses (where insurable by law).

Conditions for Payment:

- Prior written consent from the insurer.
- Confidentiality of coverage terms.
- Taking all reasonable steps to terminate the event without payment, if possible.
- Cooperation with governmental authorities.

Key Point: Focuses on mitigating and responding to ransomware and other extortion attempts.

REGULATORY FINES & PENALTIES

Data Privacy Compliance

What it Covers: Privacy regulatory defense costs and penalties.

Trigger: Regulatory action against you arising from a privacy and network security event.

Key Point: Addresses the financial burden of fines and legal costs related to data breaches and privacy violations.

Important: Only where insurable by law and compliant with sanctions.

Payment Card Industry (PCI)

What it Covers: PCI expenses and penalties.

Trigger: PCI action against you arising from a privacy breach.

Key Point: Specifically covers costs associated with non-compliance with Payment Card Industry Data Security Standard (PCI DSS) after a breach.

Important: Only where insurable by law and compliant with sanctions.

PRIVACY & NETWORK SECURITY LIABILITY

Third-Party Claims

What it Covers: Damages and claims expenses you are legally obligated to pay.

Trigger: Claims made against you arising from an actual or alleged privacy and network security event.

Key Point: Protects against lawsuits and legal costs brought by third parties (e.g., customers, employees) affected by a data breach or security incident.

MULTIMEDIA LIABILITY

Content & Communication Risks

What it Covers: Damages and claims expenses you are legally obligated to pay.

Trigger: Claims arising solely from your release or transmission of multimedia content, resulting in an actual or alleged multimedia wrongful act.

Examples: Defamation, copyright infringement, invasion of privacy through published content.

Key Point: Broader coverage for risks associated with content creation and distribution online.

E-CRIME (HACKER THEFT COVER) ADD ON

Cover for this is worded as below:-

“The insurer shall indemnify the insured for its one IT Theft Loss sustained as a direct result of IT Theft first Discovers During the Insurance Period”

Coverage is usually sub-limited for this section but will be part of overall aggregate

As you can see coverage is very limited to third party hack only and does not cover any other form of crime.

E-CRIME / HACKER THEFT IN COMPARISON WITH CRIME SPECIFIC COVERS

BBB vs Commercial Crime

For Financials Institutions equivalent of Commercial Crime policy is BBB policy which includes the below clauses within:

- Insuring Clause 1 : Employee Dishonesty
- Insuring Clause 2 : Premises and in Transit
- Insuring Clause 3 : Transit
- Insuring Clause 4 : Forged Cheques
- Insuring Clause 5 : Forged Securities
- Insuring Clause 6 : Counterfeit Currency
- Insuring Clause 7 : Offices and Contents

Crime Policy for Non-Financial Institutions with standard clauses as per below:-

1. Infidelity of Employees
2. Loss on Premises
3. Loss in Transit
4. Forgery and Securities Fraud
5. Counterfeit Currency
6. Computer Systems Fraud
7. Funds Transfer Fraud
8. Corporate Card Fraud

90% of CRIME LOSSES ARE UNDER CLAUSE 1

Instead of the above E crime Cover add on coverage we will always recommend a separate Commercial Crime Policy

Electronic And Computer Crime Policy

The Electronic and Computer Crime Policy has been developed as a companion policy to the BBB. It is designed to cover the Assured for Direct Financial Loss resulting from the third party intrusion into the Assured's computer systems which causes the Assured to transfer funds or Property or to believe that they have received funds or Property from a third party.

CYBER AND CRIME POLICIES CONTRAST

SCENARIO	HOW CRIME POLICY RESPONDS	HOW CYBER POLICY RESPONDS
Hacker breaches your server to steal your bank login and wires money out.	Responds to the direct loss of the money under its Computer Fraud insuring agreement.	May not respond to the direct loss of money, but will respond to the costs of the breach itself (forensics, data restoration, etc.).
Employee is tricked by a phishing email into wiring money to a fraudster.	A crime policy will respond to the lost funds. This is now often sub-limited.	Many Cyber policies do not specifically include Social Engineering coverage. It is in a grey area
Data Breach	Not Intended to be covered	Intended to be covered
Loss Of Funds	Intended to be covered	Not Intended to be covered

CYBER CLAIMS

- It is estimated that Catastrophic events (systemic attacks / hackers) could cause $20–46 billion In potential insured losses
- Global average for cyber claims in 2024: ~$115,000+
- Average ransomware payouts: ~$492,000 per incident, with data breaches averaging $600,000, and financial sector claims as high as $1.2 million alone under a cyber policy
- Business Interruption claim / loss for the business will be in addition to the above, size is dependent on revenue / turnover, Time system is down ETC

Target Data Breach ‘13

When: The breach occurred between November 27 and December 15, 2013, during the busy Black Friday and holiday shopping season.

What Happened: Attackers gained access to Target's payment systems by exploiting vulnerabilities in a third-party HVAC vendor's credentials. They then installed malware (dubbed "BlackPOS" or "Kaptoxa") on point-of-sale (POS) systems in Target stores. This malware skimmed payment card data directly from customers' credit and debit cards as they were swiped.

Data Stolen:

- 40 million credit and debit card numbers: This included cardholder names, card numbers, expiration dates, and CVV codes (though not always the full CVV).
- 70 million customer records: This included names, mailing addresses, phone numbers, and email addresses.

Impact:

- Financial Loss: Target incurred significant costs related to investigations, legal fees, credit monitoring for affected customers, and upgrades to their security systems. Estimates vary, but the total cost was in the hundreds of millions of dollars.
- Reputational Damage: Target's brand took a major hit, leading to a decline in customer trust and sales.
- Leadership Changes: The CEO, Gregg Steinhafel, eventually resigned.
- Industry Impact: The breach served as a wake-up call for retailers and the broader business community, highlighting the vulnerabilities in POS systems and the supply chain. It spurred increased investment in cybersecurity measures and greater scrutiny of third-party vendor security.

Key Takeaways

- Third-party risk: Even robust firms are vulnerable through suppliers.
- Human error: Social engineering remains a major weak point.
- Systemic resilience: Manual fallbacks essential during downtime.
- Customer communication: Post-breach transparency and password policies help rebuild trust.
- Importance of Cyber Insurance

UNDERWRITING REQUIREMENTS

WHAT UNDERWRITERS ARE LOOKING FOR?

To varying degrees depending on the individual underwriter and their perception of your exposure insurers typically look for the following security to be in place:

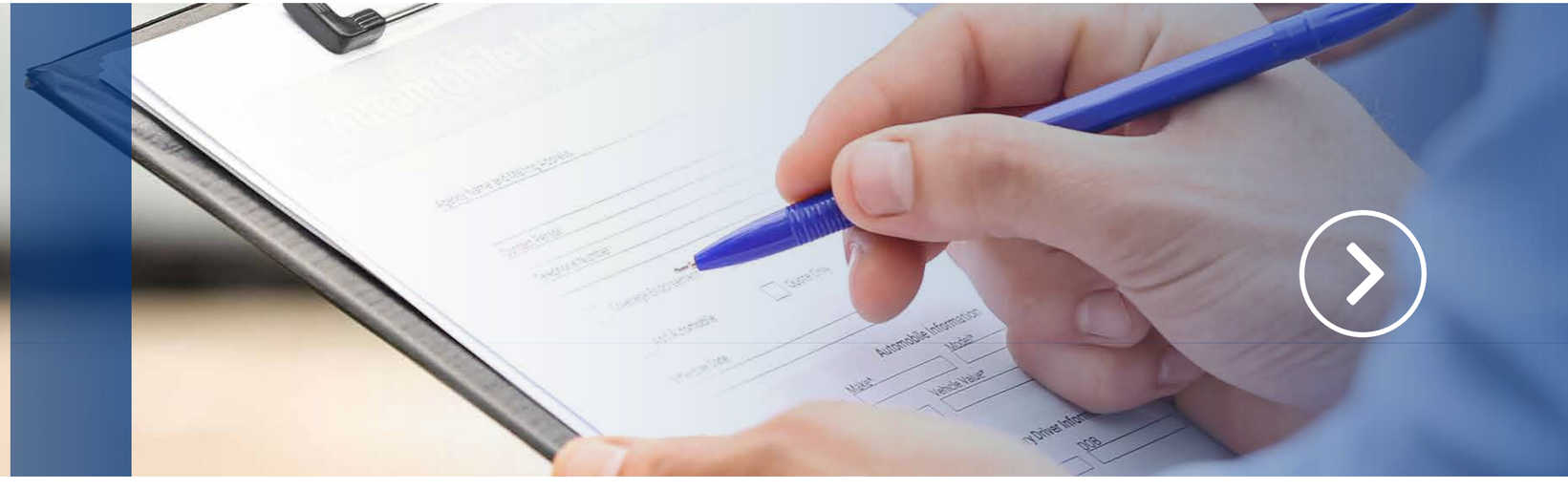
- Email filtering
- Your back-ups are done on a weekly basis, stored off-site and segregated from your usual systems
- You have firewalls and anti-virus in place and they are updated in line with recommendations
- You or your IT outsourced service provider, have a patch management policy in place to implement

WHAT UNDERWRITERS ARE LOOKING FOR?

- You encrypt sensitive information stored on portable media devices or laptops
- You have access control procedures around critical data stored on your network
- •You have (either) encryption of hard drives and/or databases containing critical data
- You have Multi Factor Authentication (with a randomly generated token) enabled for remote access

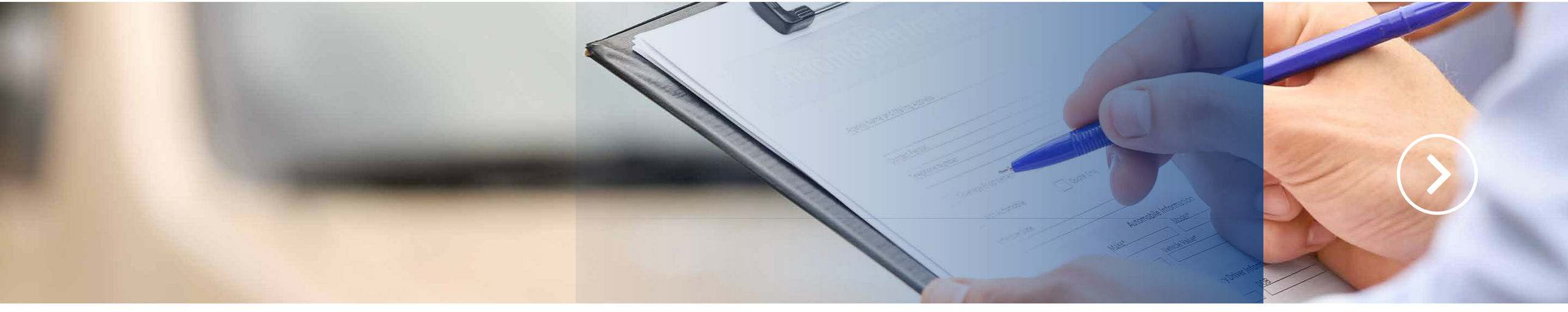
South African and Regional Market Requirements

- Do not provide a Very Rough Indication
- Require a completed proposal form, completed ransomware form as well
- No Minimum revenue requirements
- Prefer to use their own wordings



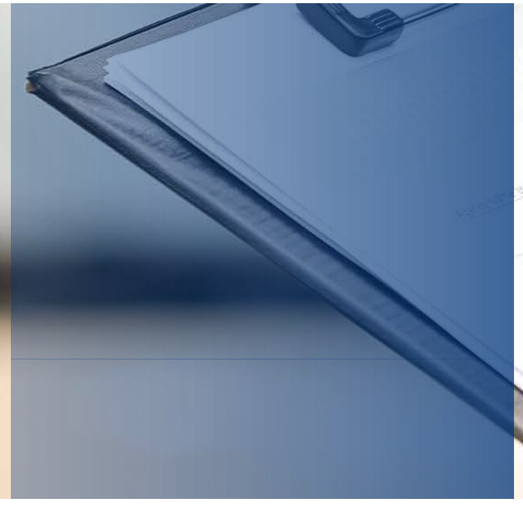
London Market Requirements

- London B+ Rated Markets
- Require Key info as a minimum to provide a Very Rough Indication (Total Staff, Total Revenue & number of records stored & processed through your system)
- No Minimum revenue requirements
- Minimum Premiums range from USD 5k – USD 10k
- Willing to use different market policy wordings



A Rated Markets

- Require their own specific wording for each policy, will not follow another market wording unless on an XS layer basis
- Also require fully completed proposal forms and annual financials
- Lloyds Syndicate Cyber markets require a minimum revenue of USD 100,000,000
- Lloyds Syndicate Cyber markets have minimum premiums in XS of USD 25,000
- A rated MGA's are available who have a lot more flexibility regarding revenues but minimum premiums usually start at USD 10,000
- But this can be reviewed on a case by case basis



THE URGENT CASE FOR A NEW APPROACH

01

Pricing Challenges: pace of the emerging new exposures with AI growth means pricing and product structure is probably lagging behind.

02

Coverage Gaps: Due to the dynamic nature of what Cyber Insurance covers and the ever changing landscape of cyber threats, this is a continuous struggle.

THE URGENT CASE FOR A NEW APPROACH

Not about simply adding cyber endorsements to existing policies

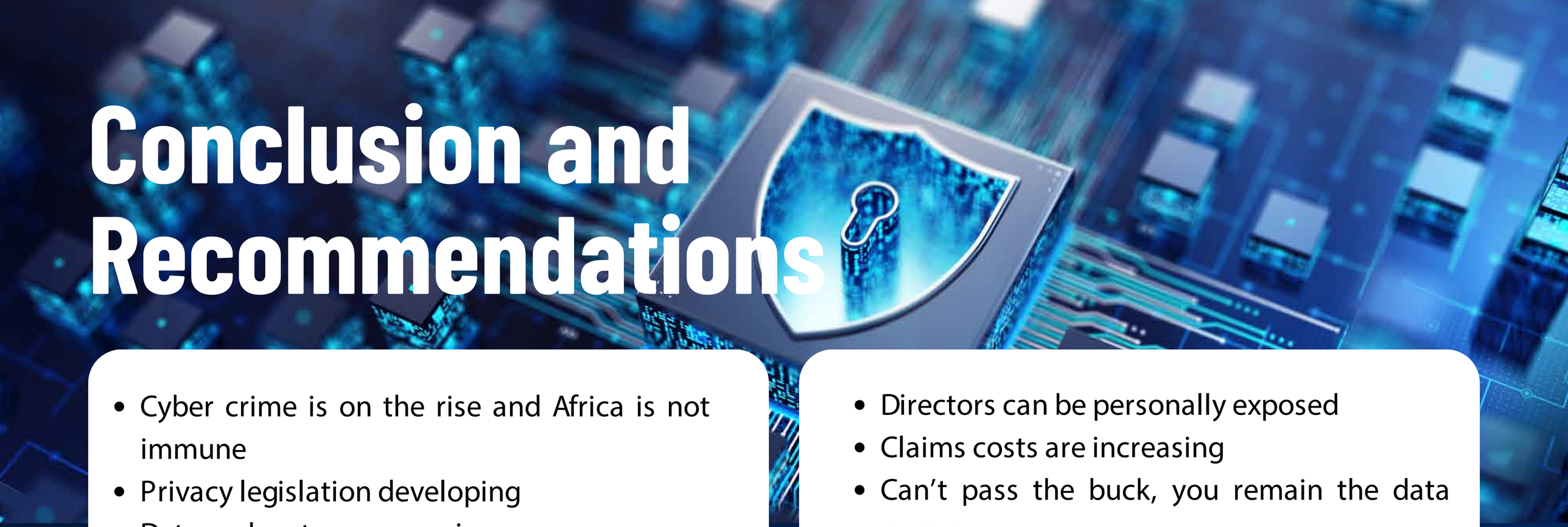
Complete reimagining of cyber risk architecture.

Solution : hybrid endorsements or integrated policies that explicitly cover cyber-physical exposures.

- Affirmative language linking cyber events to physical damage,
- Clauses covering malware-induced breakdowns or firmware corruption,
- BI coverage that includes downtime from cyber-attacks on operational technology (OT),
- And optional coverage for deepfake fraud, AI manipulation, and third-party tech outages.

“Tomorrow’s policyholder doesn’t just want a cheque after a cyber incident —they expect early detection, real-time response, and assurance of digital trust.”

—Adapted from CISA, 2023 Cyber Risk Market Study



Conclusion and Recommendations

- Cyber crime is on the rise and Africa is not immune
- Privacy legislation developing
- Data and systems pervasive:
- Cyber crime and incidents not going anywhere Incidents have broad impact and implications

- Directors can be personally exposed
- Claims costs are increasing
- Can’t pass the buck, you remain the data owner
- Effective incident response is vital

THANK YOU

tpambweyi@satib.co.zw