The Year in Risk

TOP THREATS AND EMERGING CYBER RISKS FOR 2025

Risk Cooperative

An Ensurise Company

01 Introduction

01

INTRO

An Ensurise Company

- Independent, MBE brokerage founded in 2014 and joined Ensurise in 2023.
- Work with organizations across all industries and revenue sizes to mitigate risk and develop robust insurance programs
- Extensive expertise across all classes of insurance including, life, health, property, casualty, specialty risks as well as excess and surplus lines of insurance
- A key focus area for Risk Cooperative is emerging risks, cyber being the top concern.
- Licensed across the U.S. with global coverage capabilities
- Offices in DC Metro area

01

INTRO

Andres Franzetti, CRM

- Vice President, Ensurise and President, Risk Cooperative division
- Specializes in helping multinational organizations address complex risk
- Industry leader in program development and innovation
- Thought leader, speaker and published author on cyber insurance and risk management
- Has worked with Fortune 500 firms, leading academic institutions and the United Nations

Ensurise

02

Setting the Stage

02

BACKGROUND

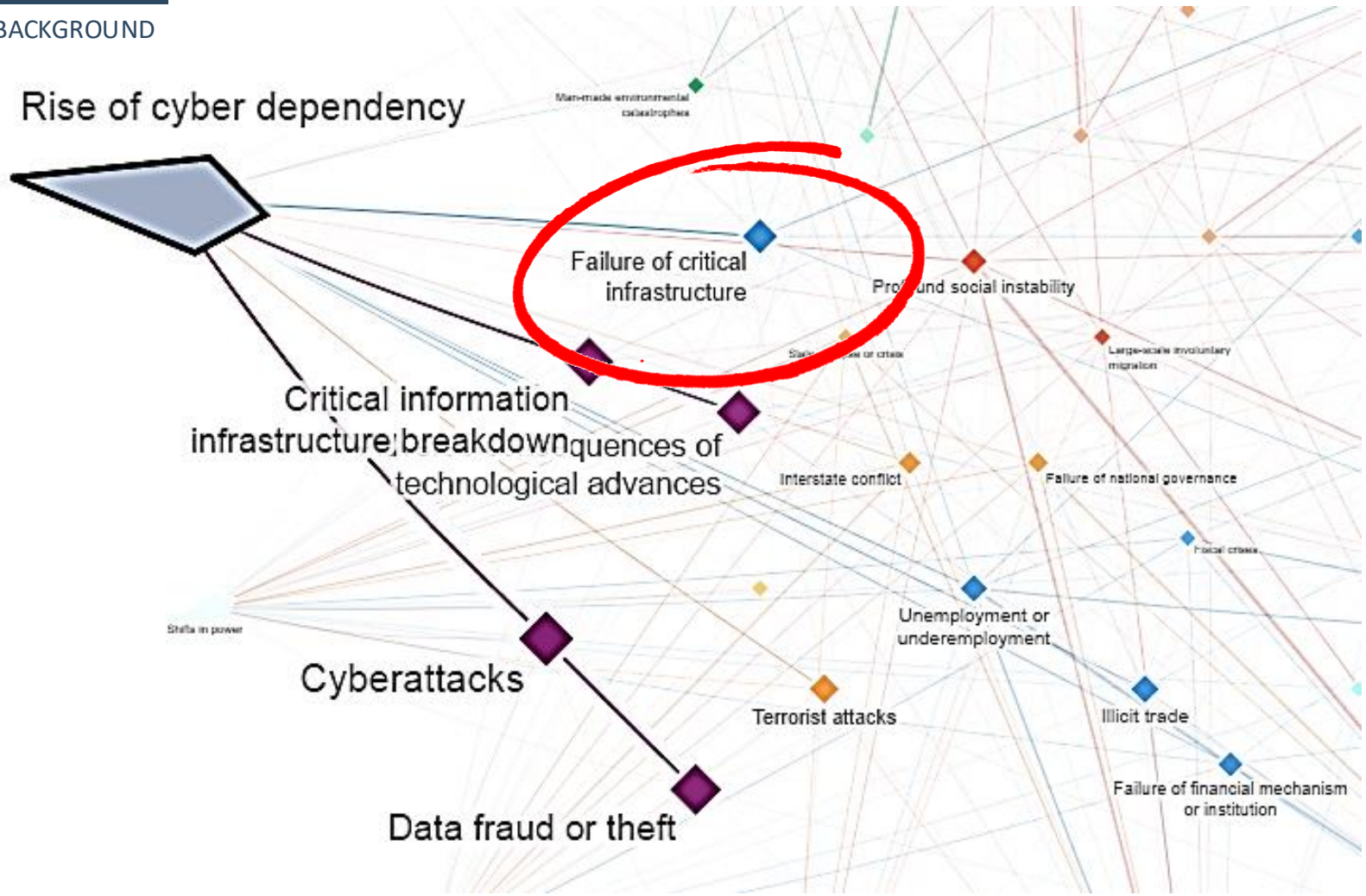
The Cyber Landscape Has Changed Dramatically

REMEMBER, TWENTY YEARS AGO…	AND, TODAY…
The ‘cloud’ did not exist	Cloud computing is poised to surpass $1T by the year 2028
There was no Internet of Things (IoT)	There are more than 75 billion connected devices globally
Gmail hadn’t been invented yet	Around the world, 28% of people work from home
No one had an iphone (invented in 2007)	7.2 billion smart phones keep people online 24/7
Businesses were afraid of computer viruses infecting their systems	MSSPs are worried about viruses infecting the organization’s entire ecosystem
IT security protected laptops and desktops	Governments are grappling with how to protect critical infrastructure.
Forensic investigations and data analytics were done onsite and manually	AI has emerged both as a threat to cyber security and as a tool to analyze cyber threats

02

BACKGROUND

Cyber State of Play

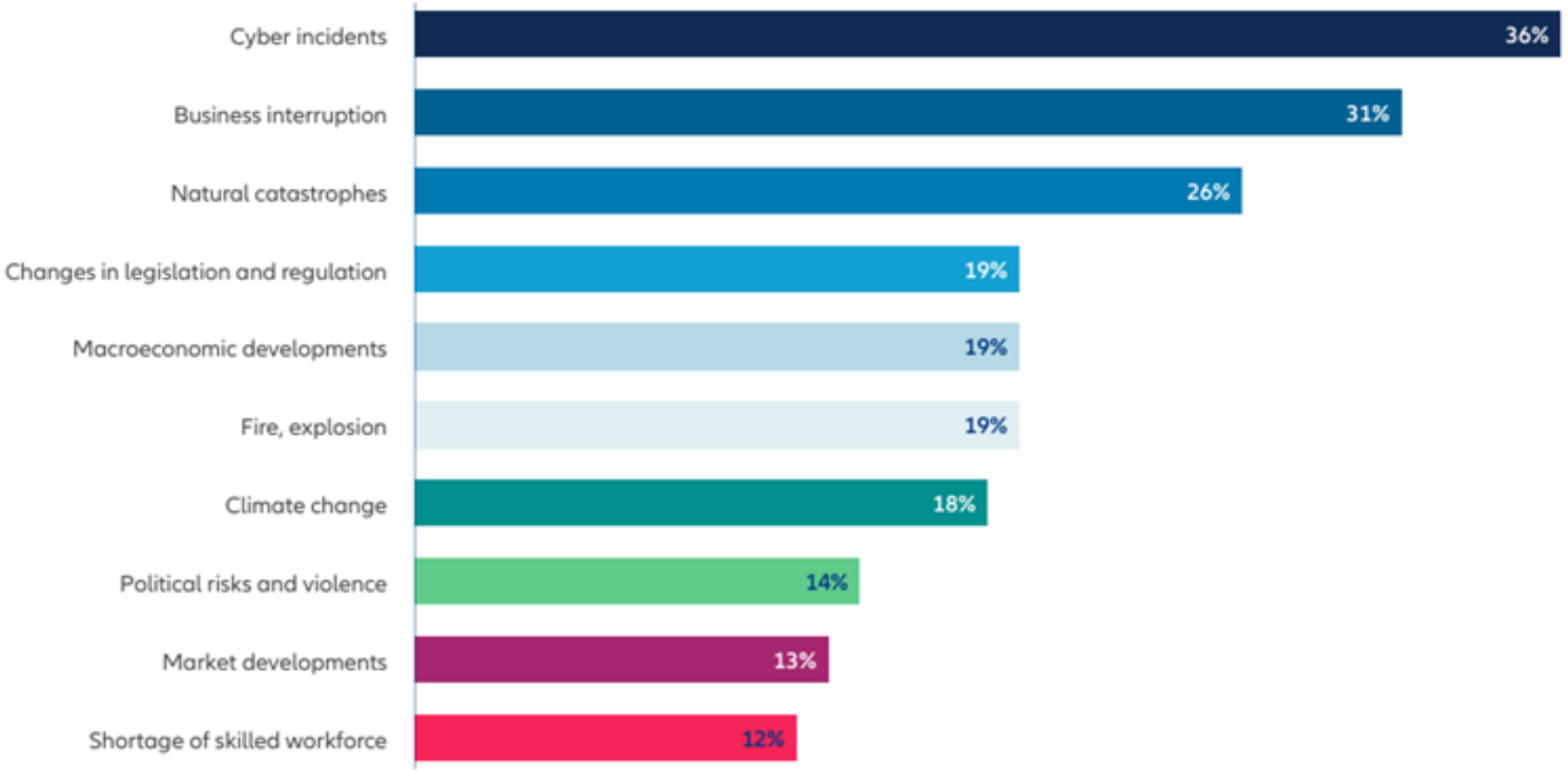


Cyber risk is increasingly defining the 21st century. Given the systemic connections, virtually every facet of the global economy exposed to this insidious threat.

- As the global economy becomes more technology dependent, cyber attacks have become the new theater of war.
- Cyber attacks are currently considered as being in the top three risks to global economic stability.
- A cyberattack occurs every 39 seconds.
- The rise of “ransomware” and business models being “kidnapped” has been steadily rising with no end in sight.
- No one is “safe”

Ensurise

2024 Top Business Risks



Allianz Commercial News & Insights

Source: Allianz

02

BACKGROUND

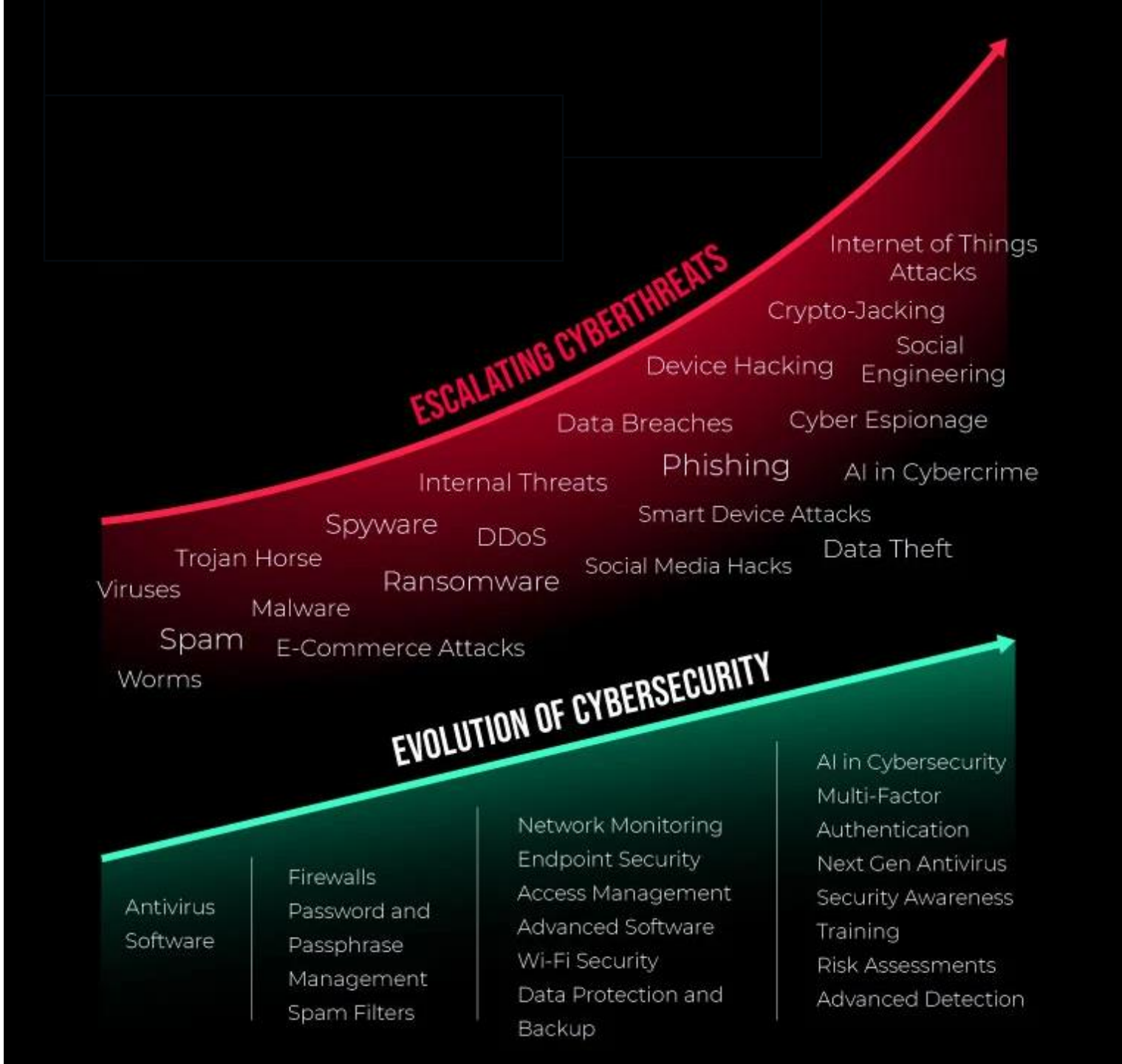
Cyber Security Evolves with Cyber Risk

To stay protected, a team of experts is required to monitor and proactively defend networks.

The amount of money spent on security or technology solutions is not a proxy for cyber-security.

Organizations with robust cybersecurity culture, and top-down enforcement of these policies are best suited to withstand and prevent attacks.

The biggest cyber risk and the most effective cybersecurity resource often lies between the chair and the keyboard.



Ensurise

03

Emerging Cyber Threats

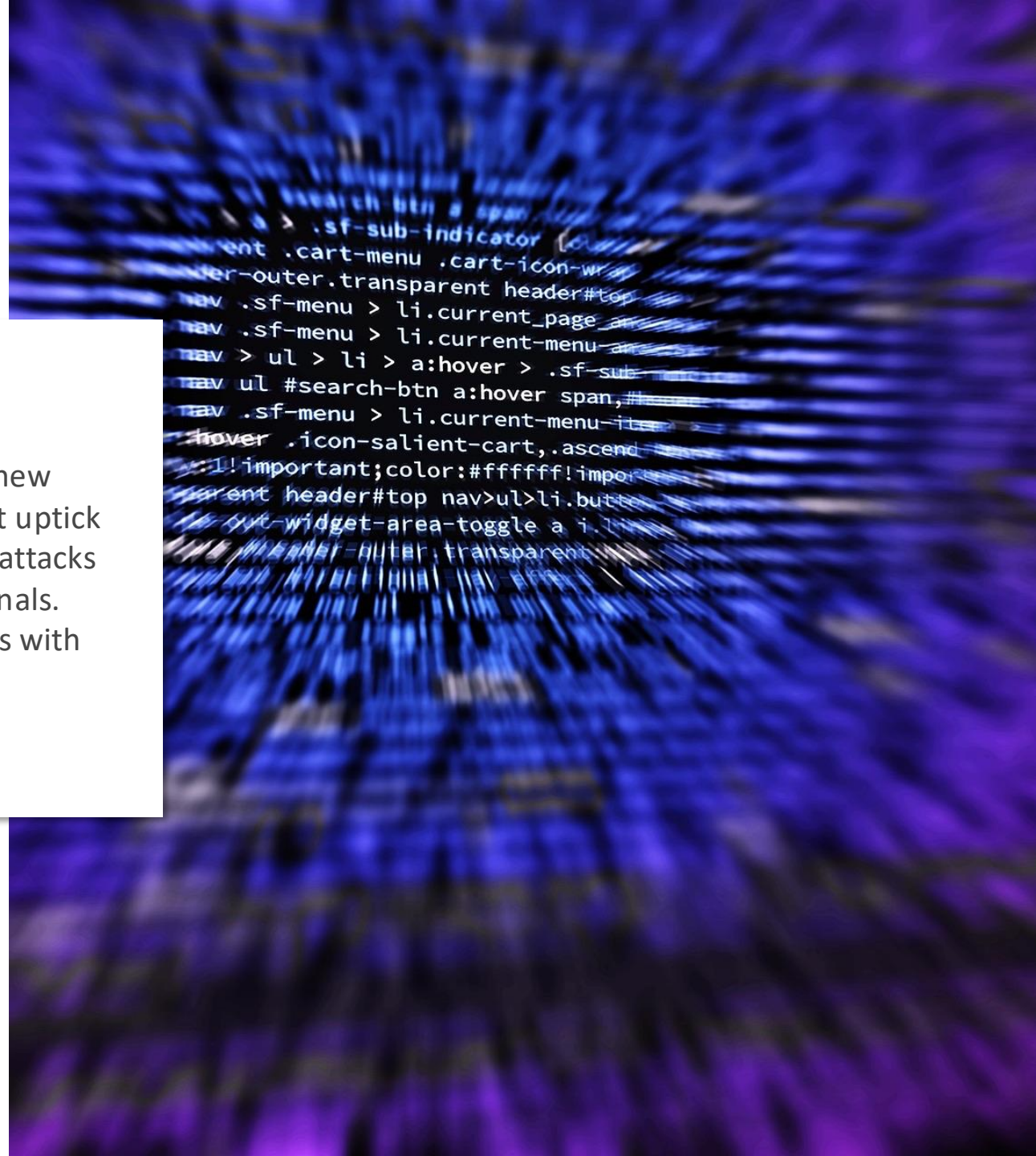
03

5 RISKS

Emerging Risk | #1 |

AI-POWERED CYBER ATTACKS

Artificial intelligence (AI) giving cybercriminals a powerful new tool to inflict devastating cyber attacks. Expect a significant uptick in AI-driven ransomware, phishing, and social engineering attacks that are sophisticated enough to catch seasoned professionals. Businesses need to adapt at the same rate as the AI threats with AI-based cybersecurity tools.



Ensurise

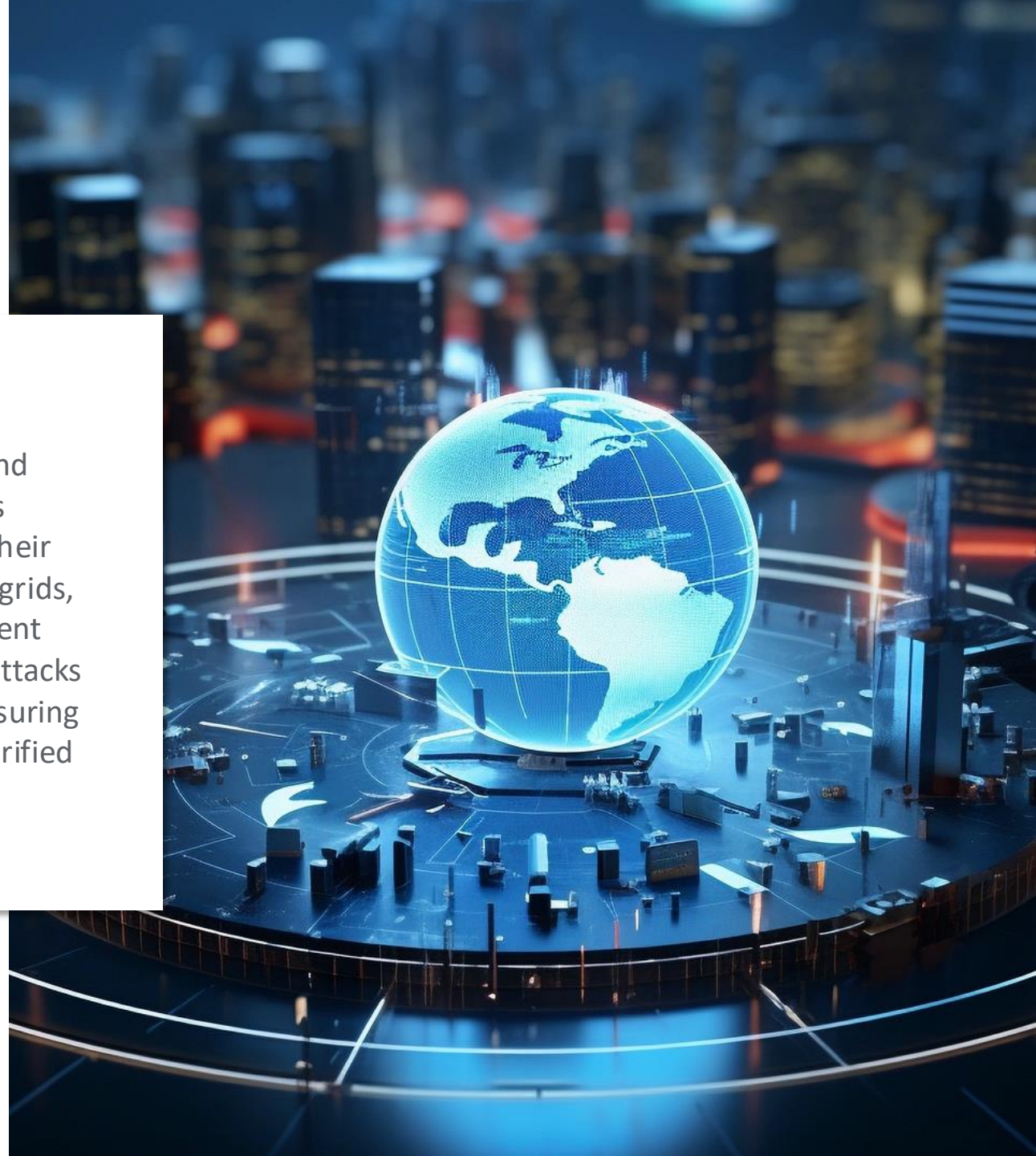
03

5 RISKS

Emerging Risk | #2 |

GEOPOLITICAL CYBER CRIME

Russia, China, Iran, and North Korea will continue to fund and implement cyber operations and misinformation campaigns designed to wreak havoc on western powers and advance their political interests. Our aging critical infrastructure – energy grids, transportation networks, healthcare systems, and government agencies – will be the targets of increasingly sophisticated attacks from threat actors abroad. Zero-trust is the standard for ensuring every user, device, or service – regardless of location – is verified before gaining access to your data.

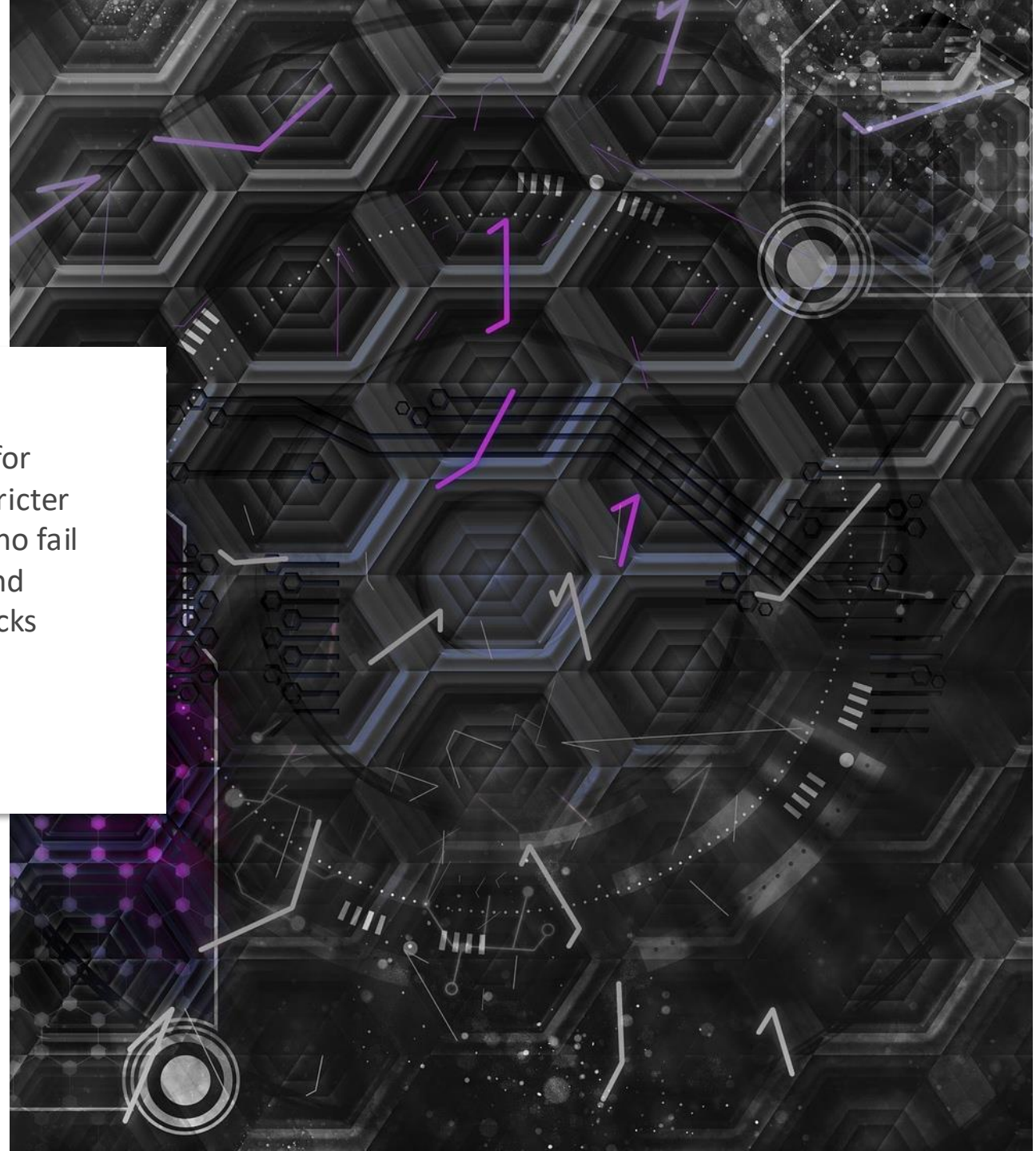


Ensurise

03

5 RISKS

Emerging Risk | #3 |



ACCESS TO CYBER INSURANCE

Robust cybersecurity protocols are already a pre-requisite for cyber insurance application eligibility, which will only get stricter as underwriters calibrate their risk tolerance. Businesses who fail to implement these practices – and maintain them – will find themselves unable to procure coverage, even as cyber attacks increase in frequency and severity.

Ensurise

03

5 RISKS

Emerging Risk | #4 |

SUPPLY CHAIN VULNERABILITY

You're only as secure as your weakest link. As vendors, cloud platforms, and digital tools help streamline operations – so, too, do they create the potential for cyber vulnerabilities. Businesses are moving more critical processes and sensitive data to the cloud, making these environments susceptible breaches from things as simple as a misconfiguration to lack of identity management. Ensure your service providers take cybersecurity seriously and maintain cyber insurance policies.

Ensurise

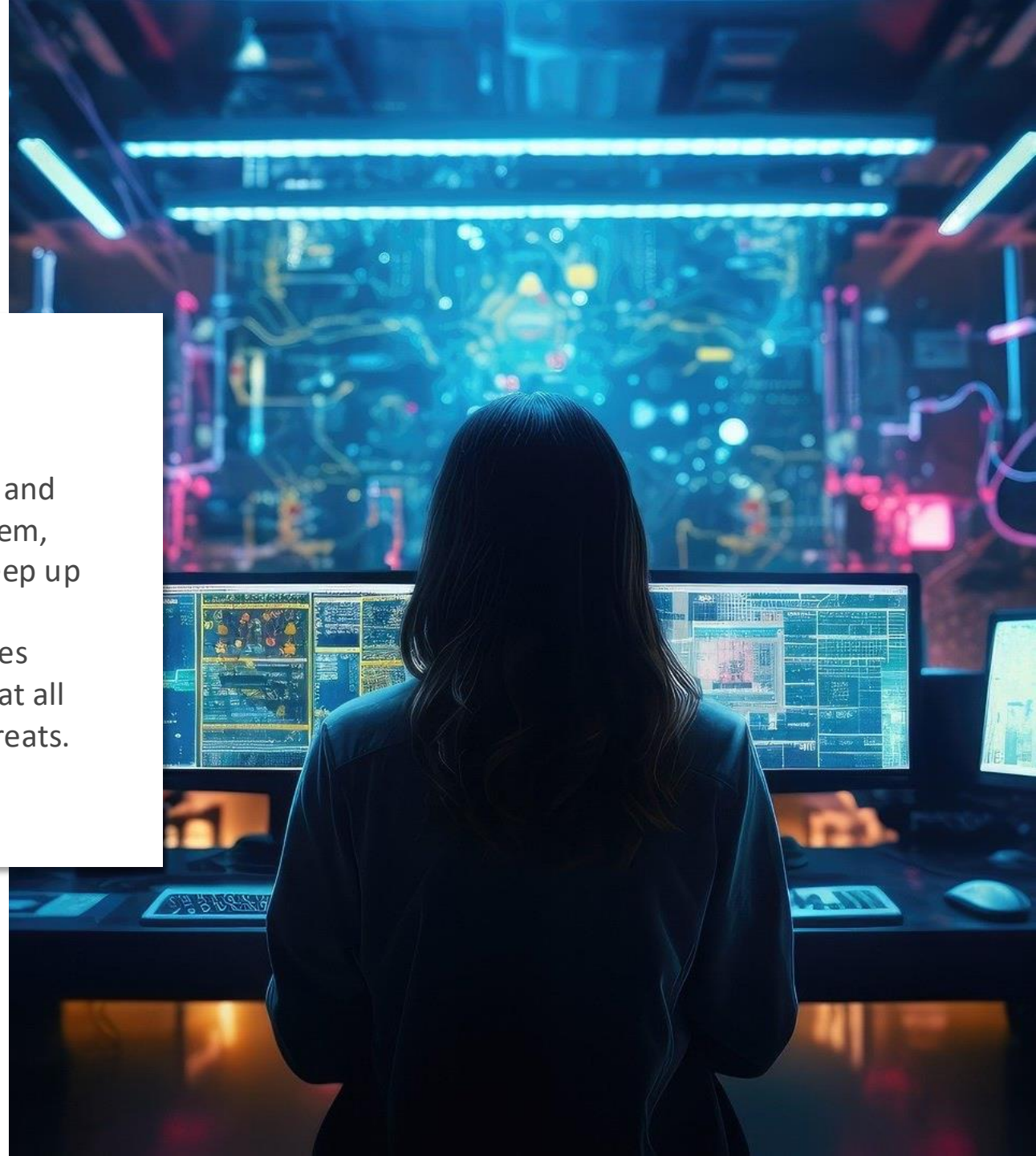
03

5 RISKS

Emerging Risk | #5 |

CYBERSECURITY TALENT SHORTAGE

While the gap between needed cybersecurity professionals and the number of jobs available has been a longstanding problem, the shortage will widen even more. The skills required to keep up with evolving threats makes these workers invaluable, and organizations will struggle to find and keep talent. Companies who invest in cybersecurity education and training for staff at all levels will be that much more prepared to face everyday threats.



Ensurise

04 Conclusion

04

TAKEAWAY

Building Operational Resiliency

A RESILIENT ORGANIZATION CANNOT RELY ON ONE SINGULAR COMPONENT.

PEOPLE

Do you have a culture of proactive cybersecurity?

Are roles, responsibilities and priorities defined?

Does your organization chart and accountabilities reflect the importance of cybersecurity to your enterprise?

PROCESSES

Do you have cybersecurity policies in place?

Do your onboarding/ termination procedures include cyber elements?

Do you have established procedures for allowing access to your networks and infrastructure?

Do you have plans and procedures for emergency response and business continuity?

Do you have cybersecurity insurance? Do you understand its requirements?

TECHNOLOGY

Do you utilize firewalls as well as anti-virus and anti-malware software?

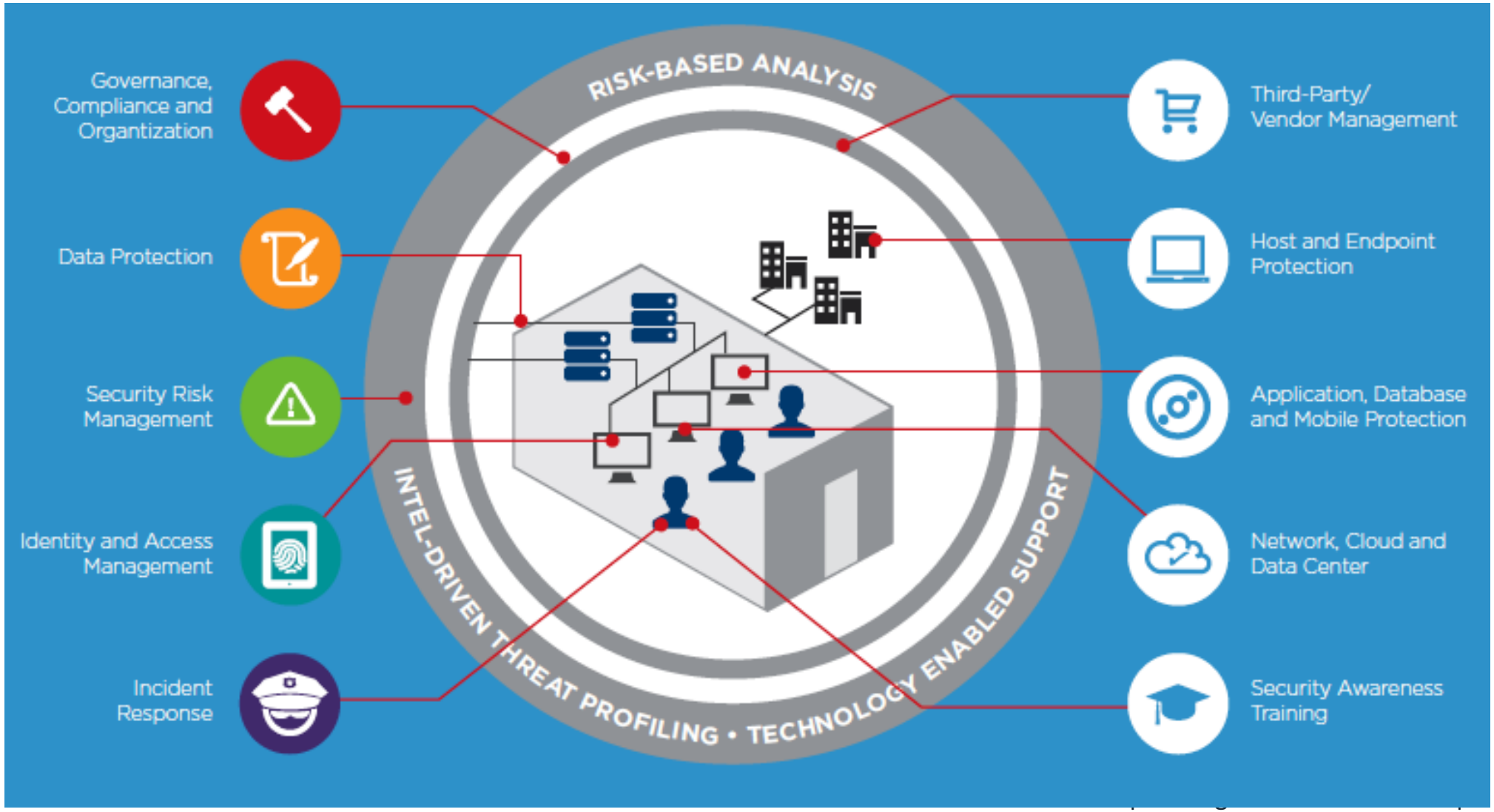
Are these technologies kept up to date?

What monitoring capabilities do you employ?

Do you encrypt data?

Do you have “tripwires” in place guarding against exfiltration?

04 Critical Cyber Security Components



Risk Mitigation Strategies

04

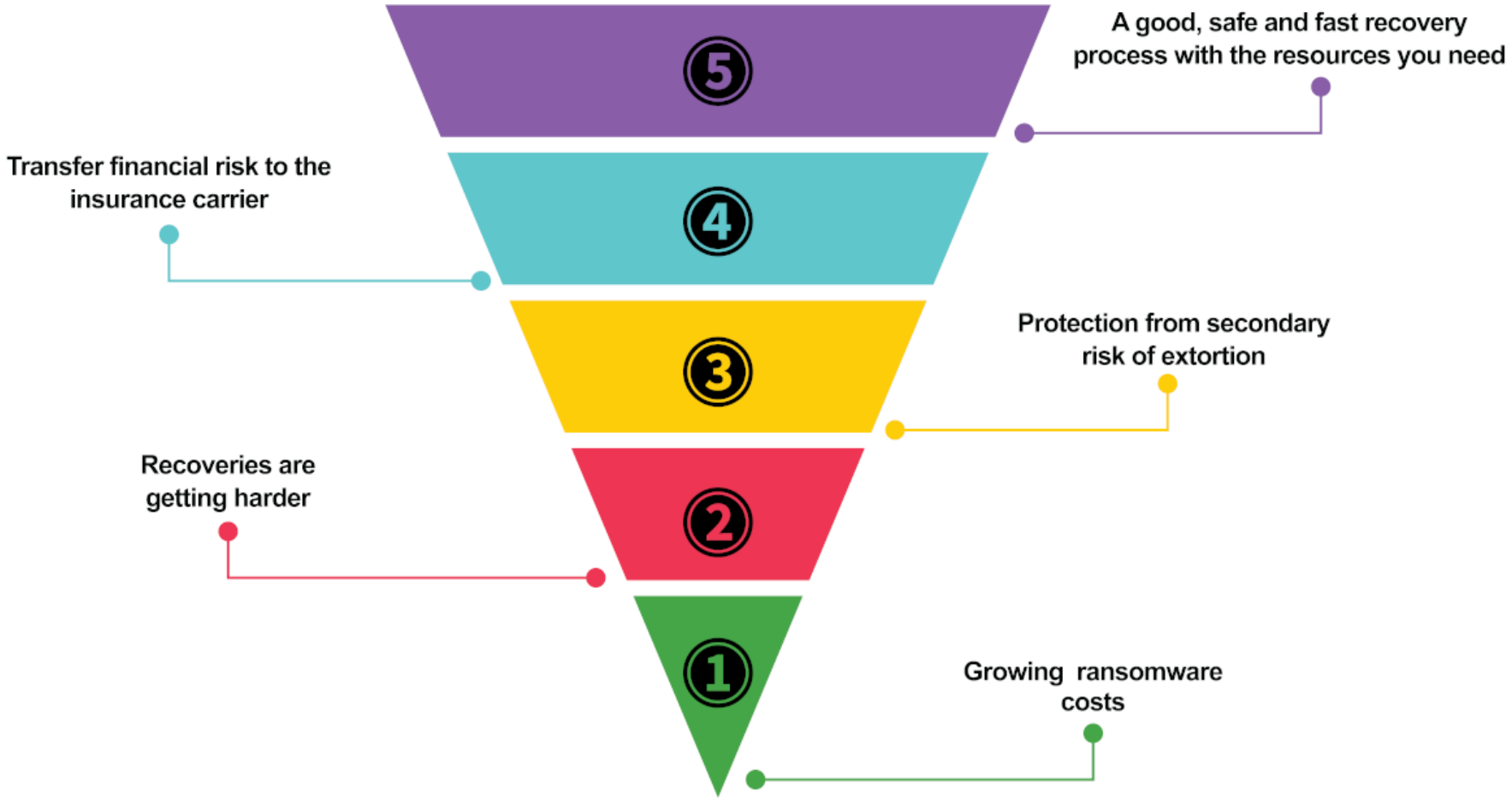
BACKGROUND

Reasons For Cyber Insurance

Cyber insurance plans go beyond financial risk transfer, they can provide a range of proactive and risk mitigation services such as training, workshops, and more.

Integration with MSSP's is another component.

The the proper type of cyber insurance can reduce the risk of interruption and losses for companies and the supply chains they comprise.

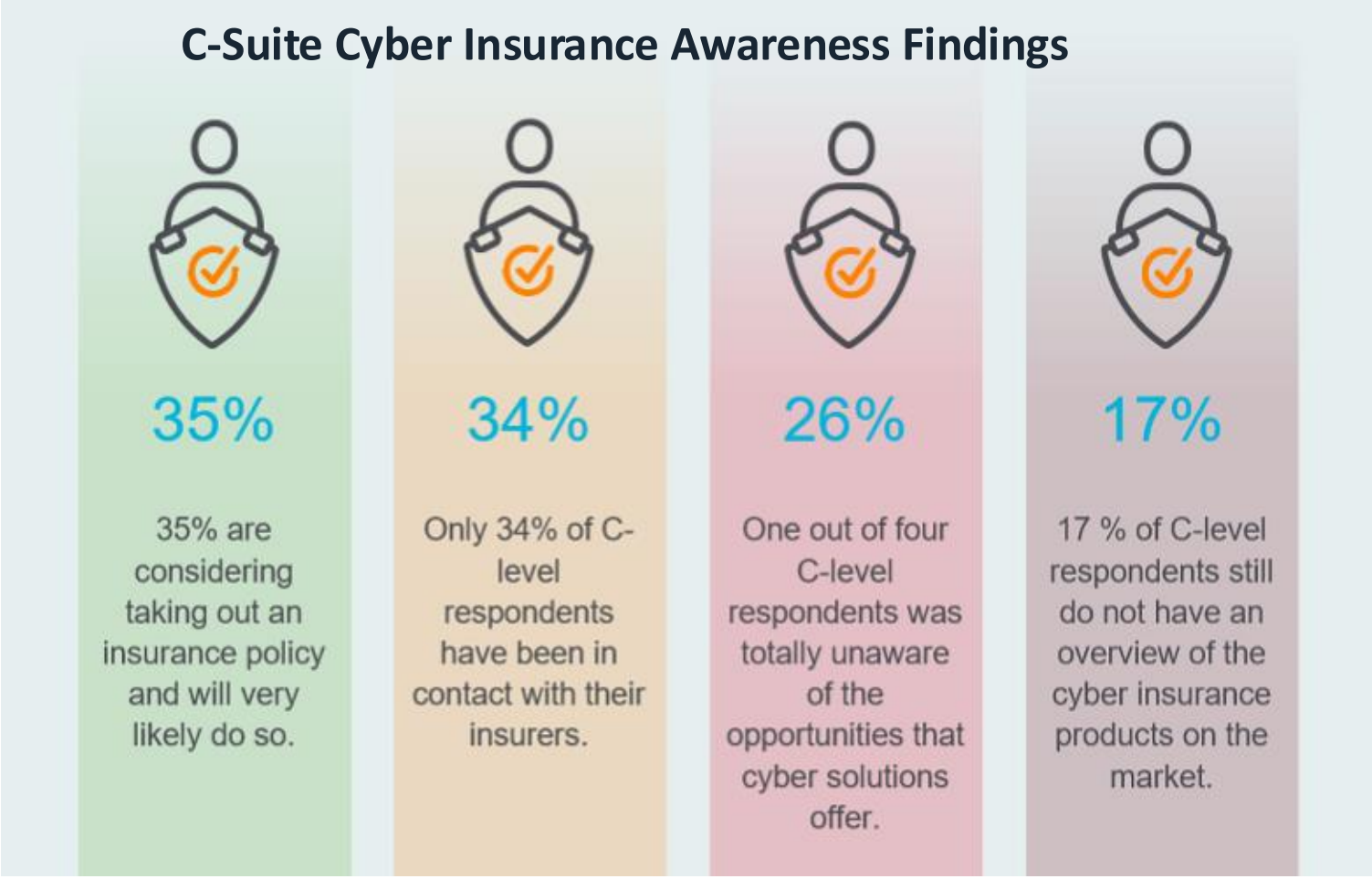


04
STRATEGIES

Cyber Insurance Awareness

Companies can use cyber insurance as a financial hedge to limit the potential liability and economic damage incurred from a cyber attack.

Yet, the cyber insurance landscape remains mysterious to many organizations. Recent surveys showed the majority of C-level executives, while concerned about cyber threats, are largely unaware of the cyber insurance products and services available on the market.



Not All Cyber Policies Are Created Equal

DANGER ZONE

BUNDLED POLICIES CAN BE A SOURCE OF CONFUSION, HIDDEN GAPS & INCREASED RISKS.

SAFE(R) ZONE

STAND-ALONE CYBER POLICIES PROVIDE THE GREATEST PROTECTION.

BUNDLED PRODUCTS

COVERAGES:

- Bundled Programs
- Directors & Officers
- General Liability
- Excess (Umbrella) Liability

DATA PROCESSING

COVERAGES:

- Electronic Data Processing Equipment
- Hardware Replacement
- Property Coverage

STAND-ALONE PRODUCTS

COVERAGES:

- Third Party Liability
- Breach Response & Notification
- Restoration
- Business Interruption
- Reputation Risk

STOP-LOSS COVERAGE

COVERAGES:

- Catastrophic Backstop
- Covers Gaps
- Meant for Large Losses When Underlying Coverage is Exhausted

Insurance Policies | Cyber

What does cyber liability insurance cover?

Cyber insurance covers incident response costs associated with data breaches and cyberattacks, including the cost of recovering important data and hiring legal representation.

There are two types of cyber liability insurance coverage.

First-Party Cyber Liability

Most businesses need first-party cyber liability insurance to defend against their own cyber risks, especially if they handle personally identifiable information (PII) for customers or other valuable data.

Third-Party Cyber Liability

Companies that are responsible for their clients' cybersecurity would need third-party cyber liability insurance to provide legal protection from client lawsuits.

Insurance Policies | Cyber

Standalone first-party cyber liability insurance provides coverage for:

DATA BREACH RESPONSE COSTS

State laws typically require a response when a business is impacted by a data breach.

Cyber insurance helps cover costs associated with hiring a digital forensic expert to investigate the breach, customer notifications, consumer credit and fraud monitoring services, as well as Payment Card Industry (PCI) compliance fines.

BUSINESS INTERRUPTION EXPENSES

When a cyber incident brings necessary systems offline or otherwise grinds business to a halt, cyber insurance can help cover business interruption expenses, such as the cost of hiring additional staff or renting equipment.

This includes purchasing third-party services, such as hiring a public relations manager or crisis management team.

RANSOMWARE PAYMENTS

If a hacker encrypts private information about your company or its employees and holds it for ransom, cyber liability insurance will help with payments to meet cyber extortion demands.

04

INSURANCE

Insurance Policies | Cyber

Third-party cyber liability insurance provides coverage for:

LEGAL DEFENSE COSTS

If a client sues your business for failing to prevent a data breach at their business, cyber liability insurance could help cover attorney's fees and other legal costs for your defense in court.

SETTLEMENTS

If your business faces a lawsuit from a client who experienced a data breach, you and the client could decide upon a settlement out of court that would amend the damages they experienced.

COURT-ORDERED JUDGMENTS

If a client accuses you of being responsible for a data breach at their business and sues your company, you may be legally obligated to pay for damages from any judgments in the lawsuit.

04

CONCLUSION

Key Takeaway

Good coverage is a force multiplier.

Applicants without detailed cyber response plans and cyber risk policies are likely to be denied coverage while those that have demonstrated cybersecurity expertise are likely to obtain more favorable cyber coverage, pricing a
limits.

Created by Risk Cooperative

DATAPRISE

INSURANCE INSIGHTS

CYBER INSURANCE

Minimum Requirements Checklist

Companies must be proactive in their cyber defense. In the evolving cyber insurance market, carriers assess client risk when they review applications for cyber coverage. The checklist below summarizes six areas for cybersecurity and the minimum standards that underwriters expect. While criteria for optimum rates and coverage is continually being updated, meeting these standards is a first step toward insurability.

Data Security

- ☐ Are automated virus scans being performed on a regular basis?
- ☐ Do you have real-time network monitoring for possible intrusions or abnormalities?
- ☐ Is there a written information security policy in place, with annual employee training and certification?
- ☐ Do you use multi-factor authentication for remote access?

Data Security

- ☐ Do you have an Acceptable Use Policy to communicate appropriate use of data to users?
- ☐ Do you conduct the following exercises to test security controls?
  - Internal vulnerability scanning?
  - External vulnerability scanning?
  - Penetration testing?

Business Interruption & Data Recovery

- ☐ Do you have the following plans in place?
  - Disaster Recovery Plan?
  - Business Continuity Plan?
  - Incident Response plan?
- ☐ Have these been tested within the past year?
- ☐ Do you have offsite (e.g. cloud) back-ups less than a month old?
- ☐ Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?
- ☐ Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months?

Questions?

Ensurise

More questions? Send us a message and we'll get you the answers you need.

Risk Cooperative | An Ensurise Company

Risk Cooperative
1835 7th Street NW #103
Washington, DC 20001

info@riskcooperative.com
P | +1.202.688.3560
F | +1 202.905.0308

Risk Cooperative is a division of Ensurise LLC, which brings together nine agencies working together seamlessly to deliver superior insurance solutions.

www.riskcooperative.com