



REVOLUTIONCYBER

PART II - SUPPLY CHAIN RISK MOVES FAST - GET ON YOUR FEET & RUN

2024 Supply Chain Risk
Trends & Transformations

PRESENTED BY: JULIET OKAFOR, JD
CEO & FOUNDER, REVOLUTIONCYBER

Agenda

- 🌸 Welcome & Introduction
- 🌸 2024 Trends & Transformations
- 🌸 Trend #1: Hyper-Automation
- 🌸 Trend #2: AI as New WatchDog
- 🌸 Trend #3 The Power of Humans
- 🌸 Trend #4: 5G's Need for Speed
- 🌸 Trend #5: Smarter Smart Grids
- 🌸 Trend #6: The Rise of Zero Trust
- 🌸 Trend #7: Steel-Fortified Chains
- 🌸 Trend #8: Insider Threat Focus
- 🌸 Trend #9: Eco-Secure Cyber
- 🌸 Q&A / Closing Remarks



SPEAKER: JULES OKAFOR, JD

- **Attorney, CEO & Founder, RevolutionCyber, we build Human-Enabled Digital Ecosystems.**
- **Bestselling Author: Securing our Future, Embracing the Resilience and Brilliance of Black Women in Cyber**
- **Former SVP, Global Security Solutions, Fortress Information Security - Led the team that built the foundation for the widely used automated security questionnaire process utilized by many of the largest Energy, Manufacturing Companies & Government Agencies**
- **Partner of Traxiom Security, the first of its kind, Software Trust-as-a-Service Company**

2024 Supply Chain Risk Trends & Transformations

Critical Infrastructure heavily impacted by external factors



- Illuminating the way for future trends
- Showcasing the importance for energy and manufacturing providers

[BACK TO AGENDA PAGE](#)

Manufacturers and Suppliers

- Responsible for producing and supplying essential components and systems that make up critical infrastructure.
- Form the backbone of critical infrastructure

Utility Providers (e.g., Electricity, Water, Gas)

- Operate and maintain the essential services that are vital to daily life and the economy
- Continuous delivery of services like electricity, water, and gas

Government Agencies and Regulators

- Set standards, regulations, and guidelines to ensure the security and resilience of critical infrastructure.
- Key role in establishing policies, conducting oversight, and enforcing compliance

Transportation and Logistics Providers

- Responsible for the movement and distribution of goods and materials necessary for the operation of critical infrastructure.
- Ensure the timely and secure delivery of critical supplies.

Cybersecurity and IT Service Providers

- Technology and expertise needed to protect critical infrastructure from cyber threats.
- Play a pivotal role in safeguarding the digital aspects of critical infrastructure.

[BACK TO AGENDA PAGE](#)

Maintenance and Emergency Response Teams

- These teams are responsible for the ongoing maintenance, repair, and emergency response for critical infrastructure. They ensure operational continuity through regular upkeep and are crucial for rapid response and recovery in the event of failures, attacks, or natural disasters.

Trend #1: Hyper-Automation

- Whoa! The use of hyper-automation tools for keeping our infrastructure's supply chain risks in check has shot up by 20% this year alone!
- These slick tools don't just make risk management more efficient but also enable a proactive approach to tackling the challenges.
- Plus, they cut down the time and resources spent on traditional manual risk assessments.

[BACK TO AGENDA PAGE](#)



Trend #2: AI as the New Watchdog

- Cracking the Code: How to Read the Icons of AI and Cybersecurity
- Cutting Response Times in Half: The Powerful Impact of AI
- Futuristic Scenarios: Where AI Could be Headed



Trend #3: The Power of Humans: Quicker Decisions & Training

[BACK TO AGENDA PAGE](#)

AI-Powered Crystal Balls

Imagine if AI could predict cyber threats like a fortune-teller with a crystal ball, and data crunching. It's like having a psychic in your supply chain, but one that's really good at math!

Human Intuition: The Secret Sauce

Humans add that secret sauce to AI's data stew – intuition. When AI says, “This looks odd,” humans chime in with, “Odd like my uncle's dance moves or odd like a cyber threat?”

Not Your Average Cyber Drill

Remember school fire drills? Instead of ‘Stop, Drop, and Roll’, it's ‘Stop, Think, and Don't Click That Suspicious Link’. Plus, you don't have to leave your comfy office chair!

Lightning-Fast Decisions

AI + Human Training is like putting rocket boosters on decision-making. AI can process security data at the speed of light, but a human can say, “Hold up, let's not invite that Trojan horse to the party.”

Trend #4: 5G's Explosive Connectivity Rapidly Expands Risk



- Increased connectivity, increased vulnerability
- Faster data transmission, quicker responses
- Enabling advanced IoT integration:
- Opportunities for enhanced remote monitoring and improved oversight

Trend #5: Smarter Smart Grids



When cyber threats emerges, the grid can respond quickly and efficiently, minimizing potential disruptions or damages

- Enhanced Detection and Response Capabilities
- Self-Healing Systems Lead to Improved System Resilience and Adaptability
- Advanced Encryption and Secure Communication

Trend #6: The Rise of Zero Trust



- Standard, non-negotiable element in procurement processes
- Ensuring every network interaction is verified, regardless of origin
- Policy Integration and Compliance that move towards trust, but verify.
- Regular audits and compliance checks, ensuring that every link in the supply chain meets the security benchmarks
- Stricter access controls and continuous monitoring

Trend #7: Steel-Fortified Supply Chains

- 60% of suppliers enhancing basic security controls and hygiene
- Supply chain continuity & Closed Digital Ecosystems vital to resilience
- Largest organizations are using technology to better understand risks across supply chain and apply controls
- Investments in operationalizing HBOM & SBOM increasing



Trend #8: Insider Threat Focus

[BACK TO AGENDA PAGE](#)

WFH Background Checks

- Enhance security by ensuring remote environments meet stringent cyber security standards, Pivotal in mitigating risks associated with remote work setups

Integration of AI + Machine Learning

- Integration of AI and machine learning into insider threat programs aids in sifting through massive data sets to identify subtle signs of malicious or risky activities. This allows for quicker, more efficient, and more accurate detection

Holistic Employee Monitoring & Wellness

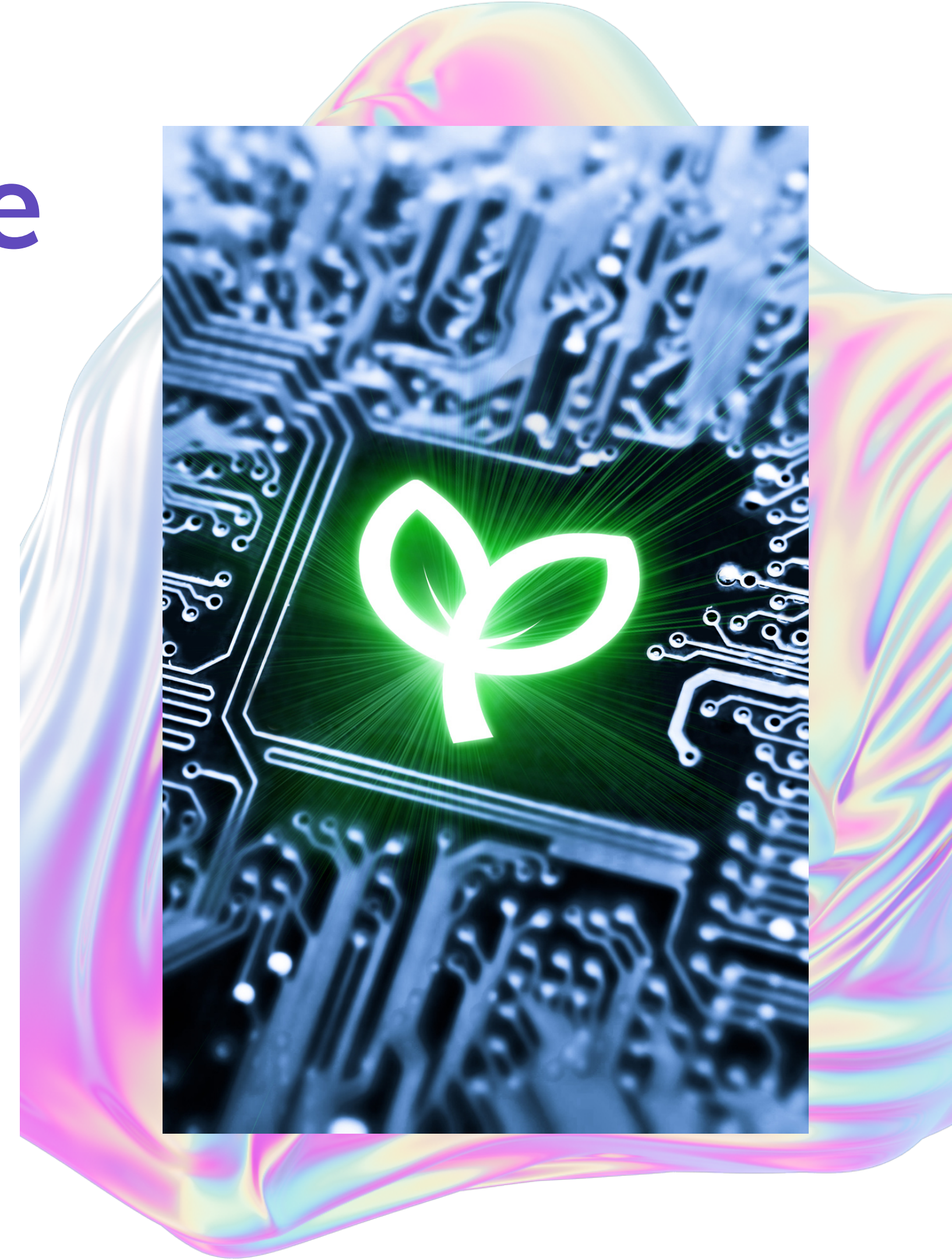
- Growing recognition that insider threats are not always malicious but can stem from employee dissatisfaction or mental health issues. More companies will focus on overall employee wellness. Aim to provide support and intervention strategies, reducing unintentional acts

Cross-Functional Insider Threat Teams

- Build cross-functional teams, including HR, IT, cybersecurity, and legal departments. This collaboration ensures a comprehensive approach to managing insider threats, combining expertise from different areas of the organizations.

Trend #9: Eco-Secure Cyber

- 90% of Green Energy Suppliers are increasing their spend on cybersecurity measures.
- Federal government is actively investing in green energy firms developing tech integral to the grid.
- Crucial for integrating sustainable technologies into the existing grid infrastructure.
- Growing importance of focus on cyber hygiene
- Need to fortify cyber defenses to meet industry standards and secure min. insurance protections



Q&A / Closing Remarks

QUESTIONS

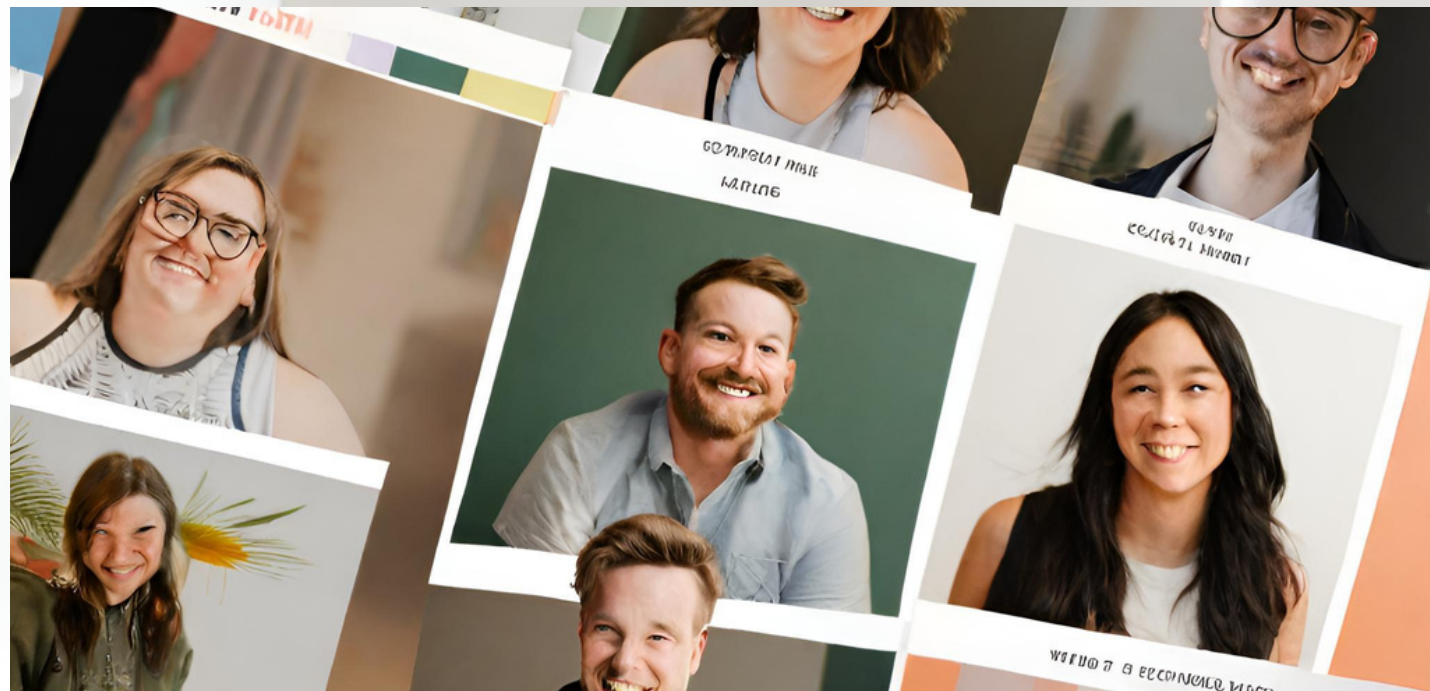
ANSWERS

"As we race ahead in the digital transformation marathon, remember – in the world of cybersecurity, if you're not running with the pace of technology, you're just jogging with the risk of being lapped!"

- Jules Okafor, JD

Tip: As we wrap up our discussion on the rapid transformation of supply chain dynamics in relation to cybersecurity, I'd love to hear your insights or suggestions on other factors that you believe are significantly impacting this evolving landscape.

About RevolutionCyber



Security Culture & Comms
Cyber Workforce Development
SDLC & Software Trust

Digital Supply Chain Resilience
Executive Branding & Coaching
Incident Response & Crisis Comms

Contact Me Today

Juliet “Jules” Okafor, JD

Email

ceo@revolutioncyber.com

LinkedIn

[linkedin.com/in/julesmgmt](https://www.linkedin.com/in/julesmgmt)

RevolutionCyber Website

www.revolutioncyber.com



[BACK TO AGENDA PAGE](#)