Entrepreneurship as Responsibility

William Paterson University
Computer Science Colloquium 2026

Megan Restuccia

Build What's Next:
Turning Ideas into Startups in an Age of AI, Cyber Risk, and Quantum Computing

Innovation and Facing Fears

Who am I?

WPUNJ Graduate

Collective Technologies

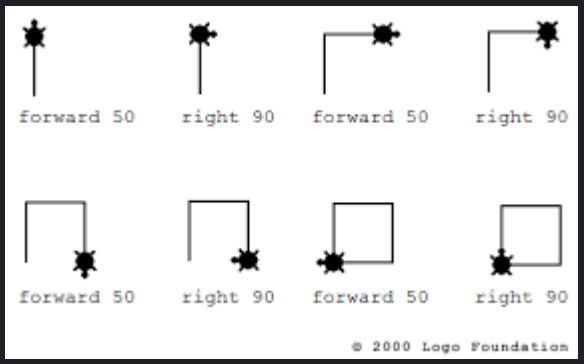
Columbia MBA

Qual-IT.net Owner

Financial Services

Specialties in Architecture, Infrastructure Engineering & Security.

My early days



The Era You're Entering

Every generation of technologists inherits a defining shift.

- The early technologist built compute.
- The early internet generation built connectivity.
- The mobile generation built accessibility.
- The cloud generation built scalability.
- The AI generation is building autonomy.

https://www.computerhistory.org/timeline/memory-storage/

Forces Converging

- Three forces are converging:

1. AI systems are making decisions at scale
2. An explosion in ransomware and cyber extortion
3. The approaching reality of quantum computing disrupting cryptography

And inside that complexity lies extraordinary entrepreneurial opportunity…

Evolving Companies

Amazon/AWS
1997

Online Bookstore to Cloud Provider to home automation to AI

CrowdStrike
2019

Endpoint Security to Ransomware specialist

Nvidia
1999

Video card manufacturer to AI powerhouse

Cyber Risk

Attackers innovate like startups

Ransomware Is a Business Model

Ransomware Concerns

In 2025, **78%** of organizations reported being victims of a Ransomware attack - which was up **32%**. The average ransom payments are down 50% to $1M with an average cost of recovery of $1.5M. 47% of attacks were US based, 93% of victims had data stolen. 83% of companies that paid the ransom were attacked at least one more time.

Attackers have productized extortion:

- They run affiliate programs.
- They operate like venture-backed startups.
- They optimize conversion funnels.

So if you want to build a startup in 2026, understand this:

- You are not just competing against other startups.
- You are building in an ecosystem where adversaries innovate just as aggressively as founders do.

Core security concepts

Security risk management involves identifying threats, understanding vulnerabilities and knowing your assets. Companies manage risk by reducing it with compensating controls, avoiding it by removing the threat or the vulnerability, transferring it, or accepting the risk.

Intractable Problems

A computational or real-world problem that is impossible to solve within a reasonable timeframe.

- Complex cryptography – large integer factorization
- Human problems – trust – phishing or insider threats

Attack Vectors

Specific path, method or entry point a threat actor uses to gain unauthorized access.

- Pivoting
- Phishing/Social Engineering
- Improper configurations (trust relationships)
- Patching

Threat Actors

Any person or group that performs malicious actions either intentionally or accidentally

- Insider Threat
- Cybercriminals
- Nation-state or APT
- Hacktivists
- Script Kiddies

Key Security Considerations

- Script Kiddies are no longer Human and have a lot of potential knowledge
- AI Models are closed systems that do not expose the internal mechanics – this includes ongoing learning data and inputs/outputs to the prompts
- Chaining of low risk or "risk accepted" issues to bypass legacy controls
- Time between identification of a vulnerability until the exploit is seen in the wild is now minutes not months or weeks
- Inventorying of all of the agents and code written is becoming increasingly difficult
- AI models are trained on human behavior and don't always "follow the rules"

The entrepreneurial insight:

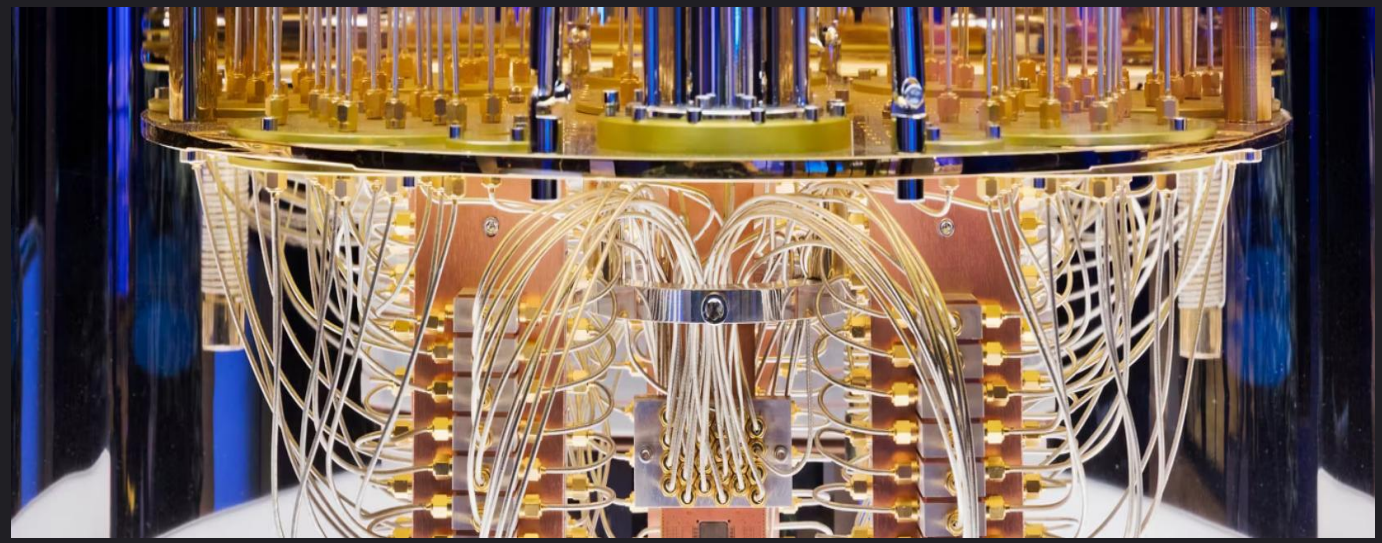
The cybersecurity practice has many areas of opportunity:

- Focusing on the next generation of security analysis
- Security Operations Automations
- Proactive Protections and Guardrails to disrupt

Startups have emerged and will continue to evolve to improve cybersecurity landscape for companies, drive guardrail design and automate remediation, validate implementations, and audit legacy systems.

Be the disruptive force that moves security from playing defense to being an offensive player in the protection of an organizations data and systems.

Quantum Computing



https://www.nist.gov/quantum-information-science/quantum-computing-explained

Chip differences for QC

Nvidia Blackwell GPU Chips

- Processing Unit: bits (0 / 1)
- Low error rate - predictability
- Parallel ability
- Uses: AI training, Graphic rendering, HPC Grid computing calculations
- Driving AI advancement in industry currently

Quantum Processing Units

- Processing Unit: bits (0 / 1 / both) – simultaneously
- High error rate and interference
- Superposition and Entanglement coordinated states
- Uses: Simulating molecular behavior, Multi-variable large problems, Risk analysis, Cryptography
- Theoretical currently, but enables exponential processing power to focus on "hard problems" tasks

Post Quantum Cryptography (PQC)

- With the evolution and power from Quantum Computing, cryptography is a major concern for the industry.
- NIST published its first standards for PQC in 2024, focused on shifting encryption to protect from "store now, decrypt later" attacks. Main concern is the PKI infrastructure used widely across the internet today.
- Out with RSA, ECC, AES, in with ML-KEM, BIKE, and HQC algorithms designed to be quantum-resistant. TLS 1.3 support for these algorithms is a key target.
- New Timelines Published by Google and CrowdStrike – @ March 25th moves the target to 2029.

https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

The entrepreneurial insight:

The migration to post-quantum cryptography will be one of the largest infrastructure upgrades in digital history.

- Every SaaS platform.
- Every financial institution.
- Every cloud provider.
- Every embedded system.

Startups will emerge to manage that migration, automate crypto-agility, validate implementations, and audit legacy systems.

The founders in this room could build those companies.

AI

MONEY > INVESTING

How Claude Mythos Wiped Billions Out Of Cybersecurity Stocks

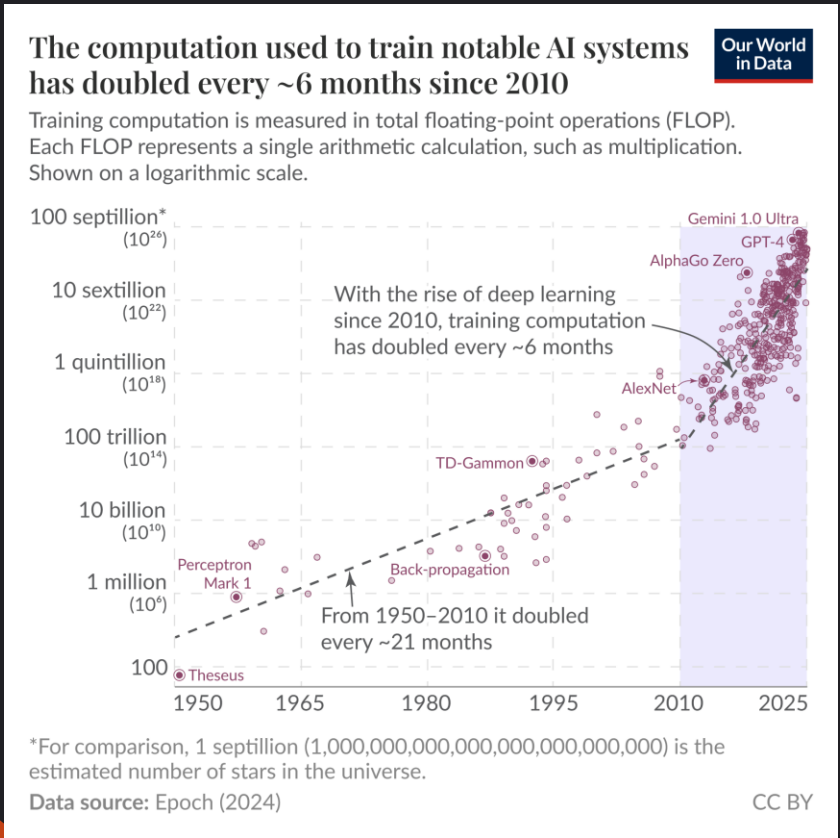
By Jon Markman, Contributor. ⓘ Analyzing tech stocks through the prism of c... Follow Author

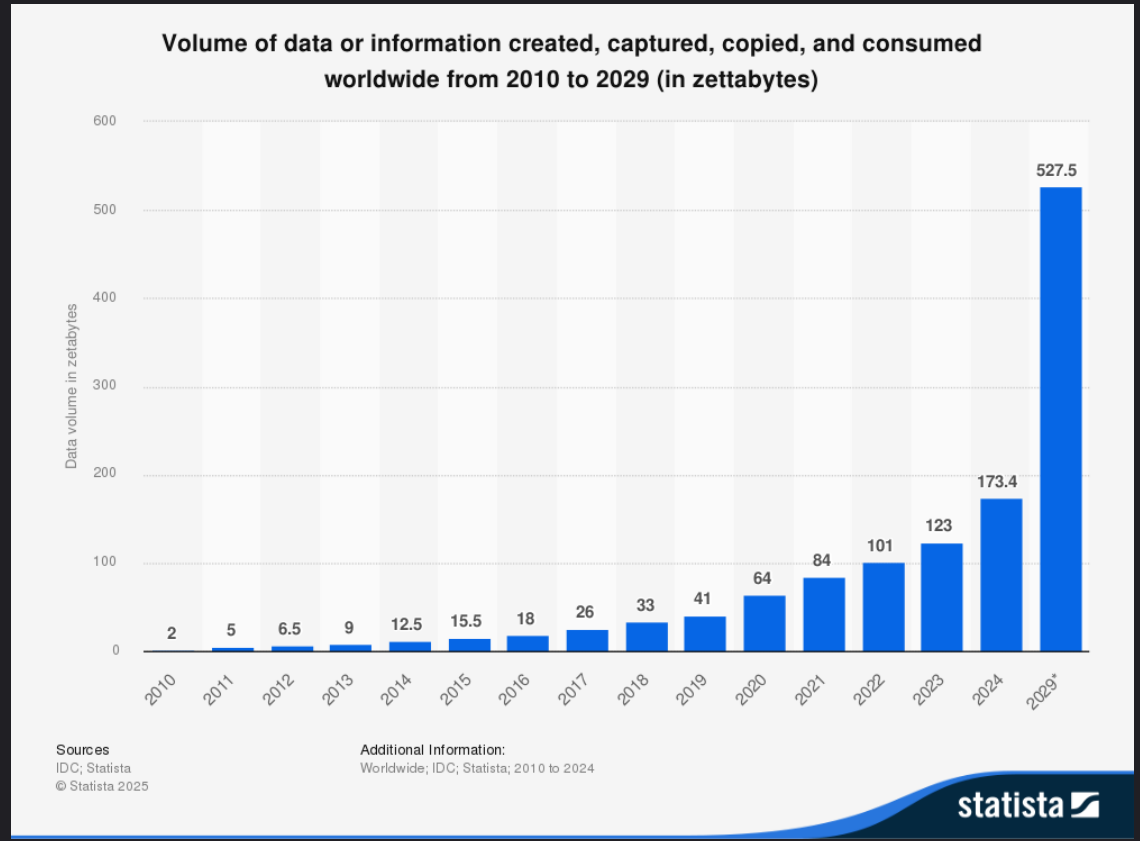
Published Apr 14, 2026, 10:26am EDT

https://www.forbes.com/sites/jonmarkman/2026/04/14/how-claude-mythos-wiped-billions-out-of-cybersecurity-stocks/
https://www.cnbc.com/2026/04/14/jamie-dimon-anthropic-mythos-vulnerabilities-cyber-attacks.html

The AI field is not NEW

AI Development spans from foundational logic theories in the 1950-60s. Neural networks foundations were published in 1958. Deep-learning break-throughs with "Big Data" happened in 2010s.





Differences between Early AI and Agentic AI

AI/ML

- Deterministic
- Purpose is to analyze, classify and predict
- Numerical values, classifications, insights
- Identify Patterns
- Needs structured data
- Rules based
- Typical Usage: Fraud Detection, demand forecasting, predictions of events.

When to use:
High Accuracy in specific, technical or niche tasks.

Generative AI

- Probalistic (with Hallucinations)
- Purpose is to create new content
- Human-like text, images, audio, code etc
- Mimic patterns for actions
- Largely unstructured data
- Tokens based
- Writing, summarizing, designing content and taking action based on the decisions or content.

When to use:
Speed content creation, automate brainstorming or create conversational interfaces to perform tasks.

Efficient Building

- AI: Amplifier of Genius – and Risk
  - Lower barriers of entry for builders and attackers
- Security for AI-Native Startups
  - Security is a design philosophy – built from the ground-up
- Move fast – but build trust
  - Crypto-agility, assume everything can be breached, threat model the AI
- Corporate Responsibility
  - Drive a culture of ethical responsibilty

Advice

Stay open-minded

The world is changing fast

Be Curious

Ask Questions and dig in to learn more

Identify Painpoints

Reflect on what you wish you could do faster/better or what are limitations others highlight

Don't be Afraid

Make the best decisions with the information you have at the time. Pivot and expand your business as needs change

Say Yes

Opportunity comes when you might not expect it

Final Thoughts

- Build boldly.
- Design responsibly.
- Secure relentlessly.

The future startups that change the world may begin with you — right here at William Paterson University.