Looking Back to Look Forward!

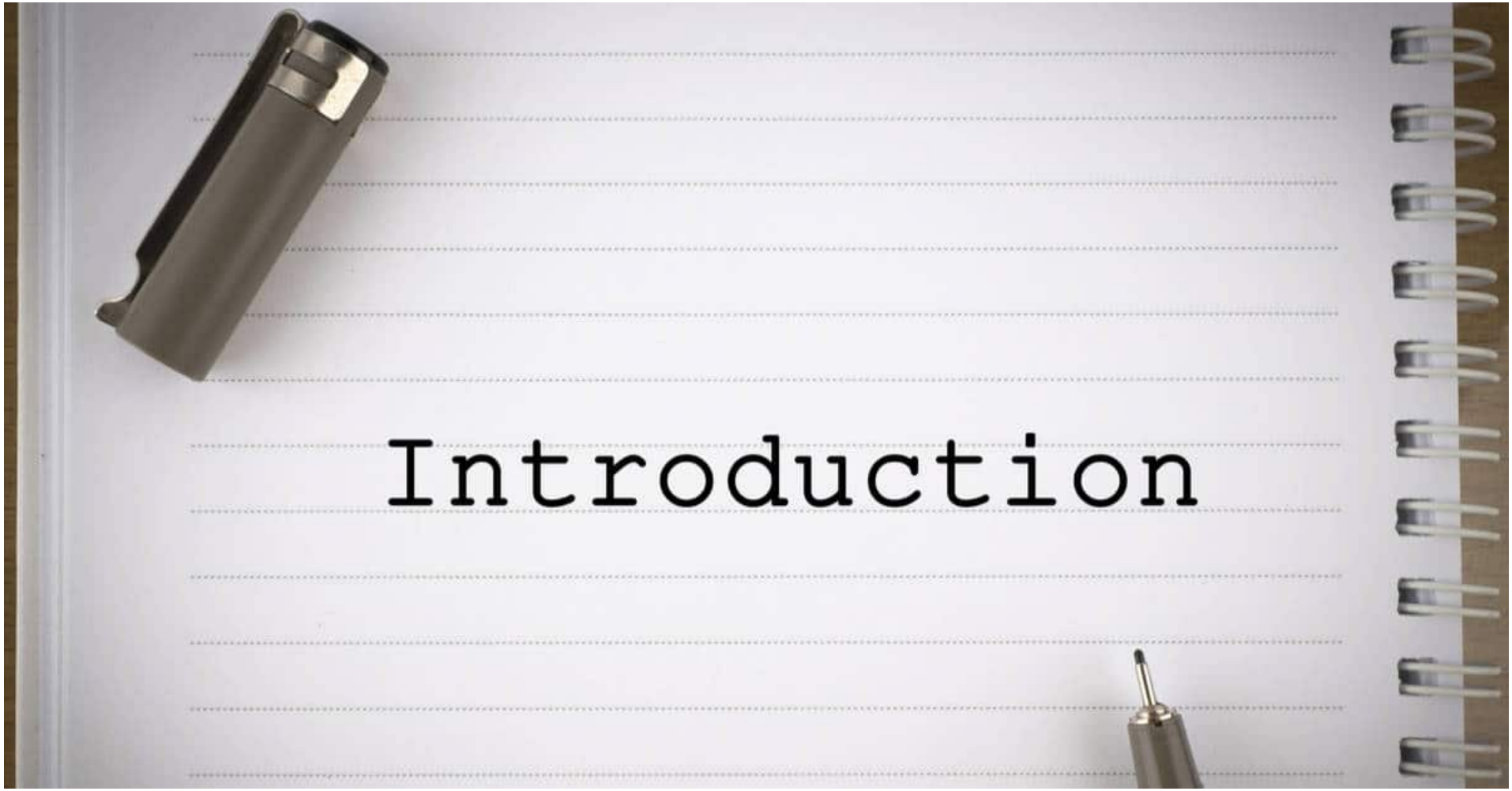
Mark Wilson
Technical Director

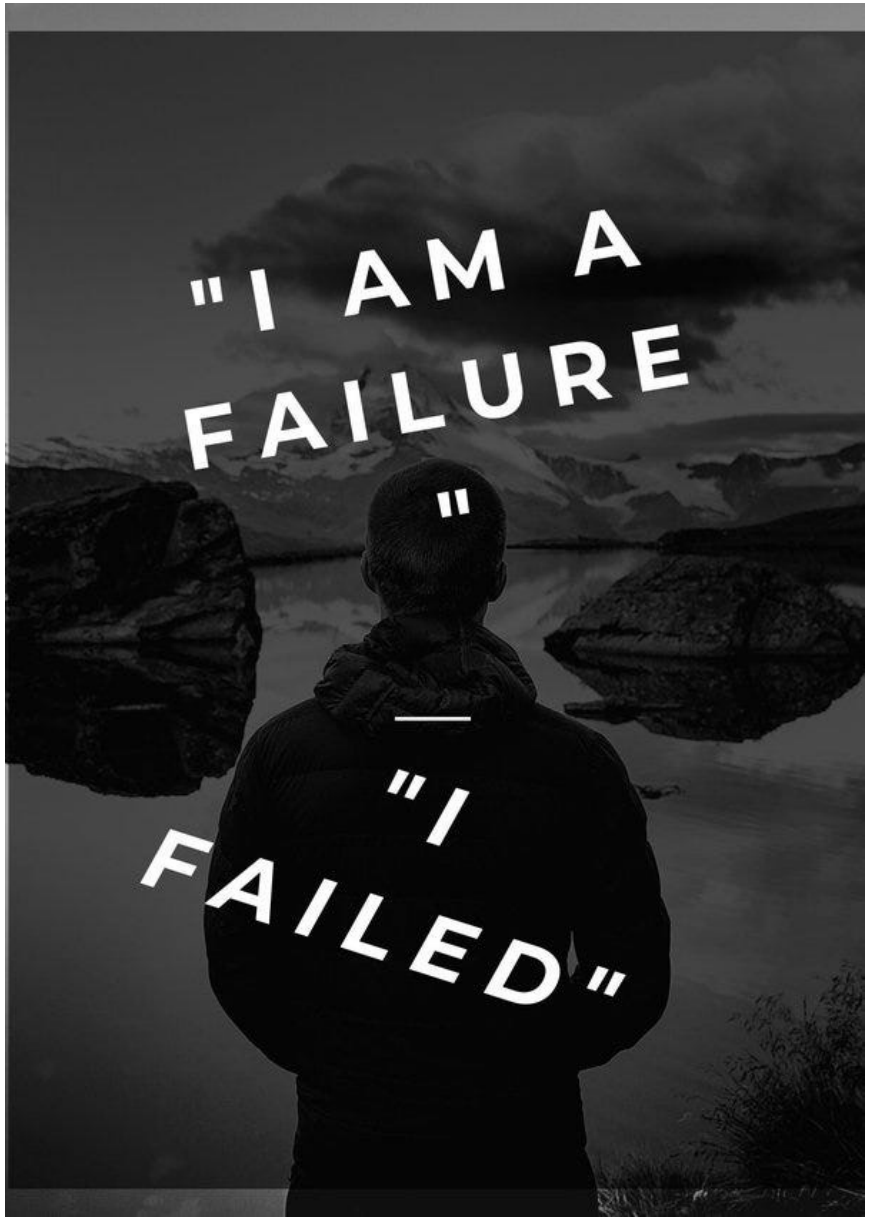
Your feedback is important!

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation


Introduction


"I AM A FAILURE"
—
"I FAILED"

Introduction

GS-UK Board Member

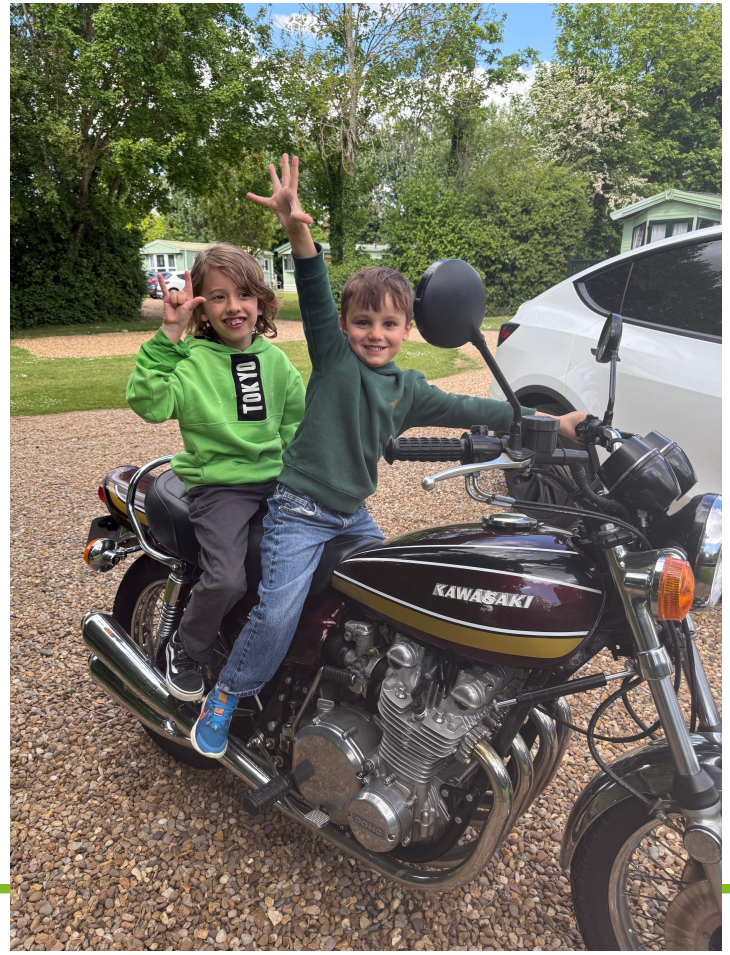
Technical Director at Vertali

Editor Cheryl Watsons Tuning Letter

I am a mainframe technician with some knowledge of Mainframe Security and other Mainframe Stuff

I have been doing this for over 45 years!

Outside Of Work



VERTALI

Have Often Been Told.... That.....

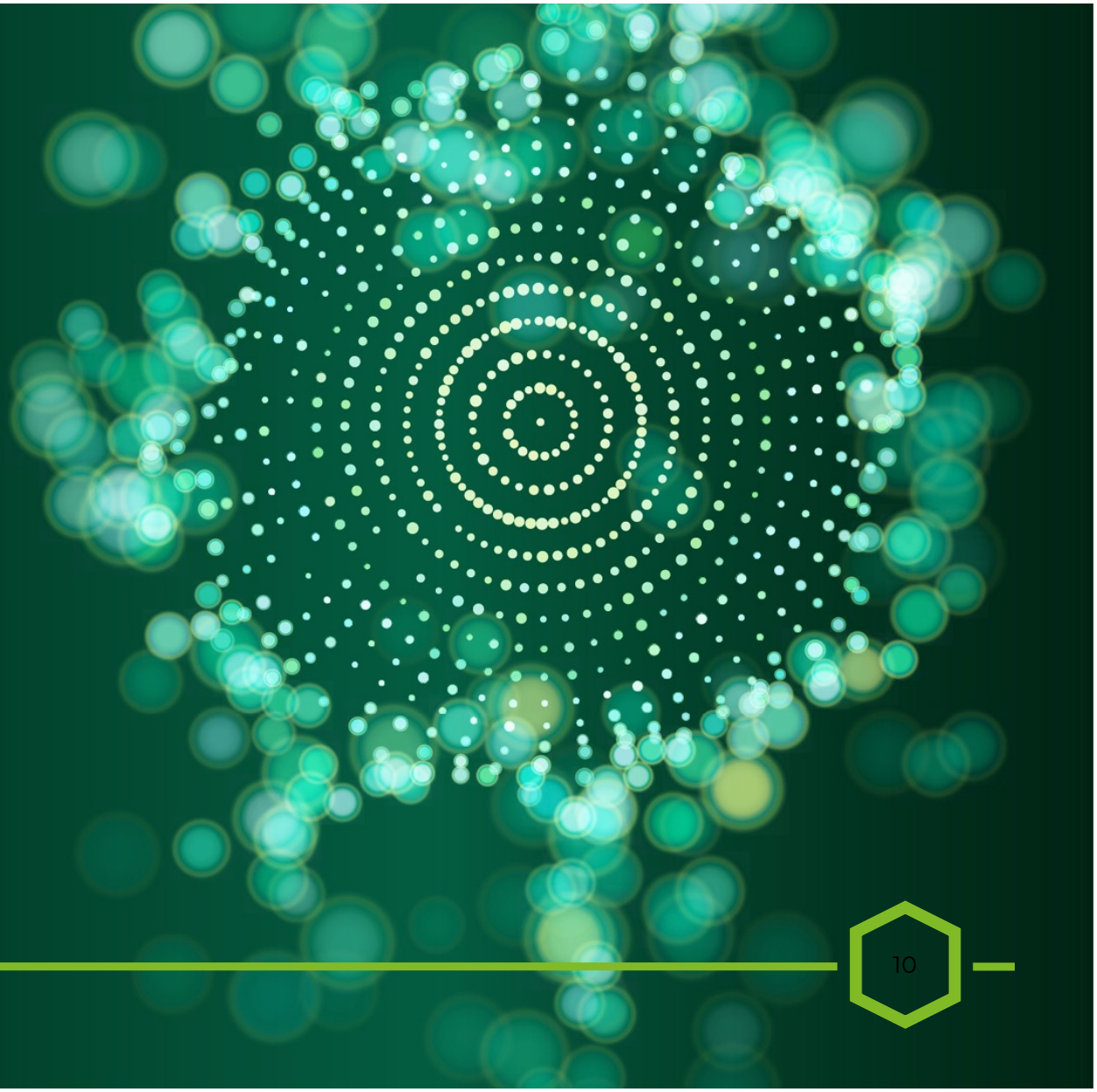
VERTALI


SO YOU CAN IMAGINE MY SURPRISE
WHEN I FOUND OUT

Agenda

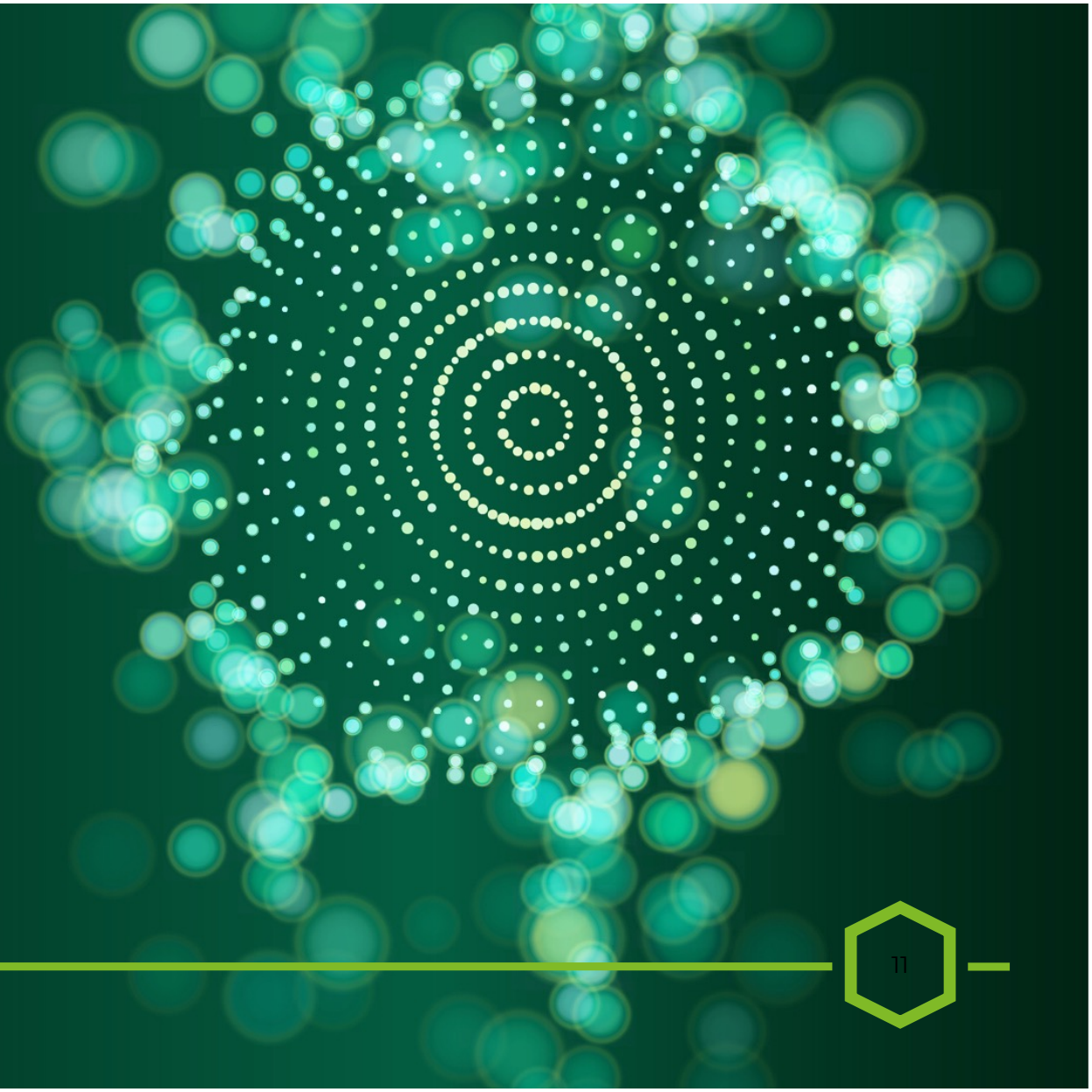
01	Challenges we saw in 2025
02	AI In Cyber Security
03	Mainframe Security Basics
04	Complexity and Observability
05	Looking Ahead

Our World is Changing



VERTALI

Our World Has Changed



VERTALI

Mainframe Security

- Countering New Threats, Using AI, and Getting the Basics Right

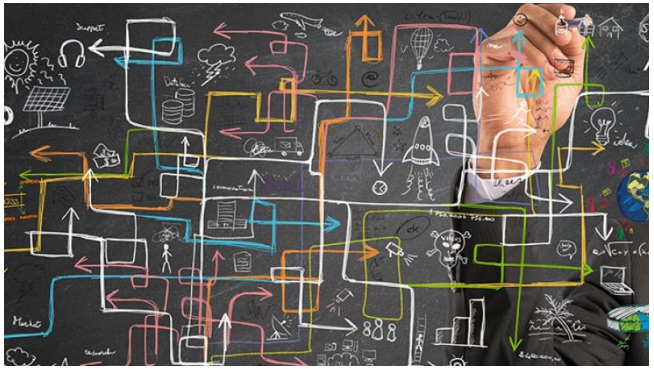
- In 2025, many security teams focused on Zero Trust and AI to address risks from code vulnerabilities, supply chain issues, and insider threats

- In 2025, the worldwide average cost of a data breach hit USD 4.88 million, rising 10% from 2024, highlighting increasing risks.

VERTALI

Mainframe Security Challenges in 2026

- Evolving Threat Landscape
- Vulnerabilities and Risks
- Increased Complexity



VERTALI

Cyber Threat Landscape

- Evolution of Cyber Threats
  - Cyber resilience professionals face major challenges in a world of increased inter-connectivity.
  - Organizations' digital transformations introduce vulnerabilities and risks.
  - The need for robust risk management practices is critical in addressing these evolving threats.

- Challenges for Professionals
  - The cyber threat landscape evolves rapidly, reflecting advancements in technology.
  - Cyber security risks are dynamic; new threats and attack vectors emerge constantly.
  - IT security attacks have shifted from isolated incidents to targeted, complex threats.

Slaying The Cyber Beast

- Threats multiply like a Hydra, cut one head and two more appear, driven by creativity and new tech.
- Targeted attacks are escalating: from individuals to corporations, governments and critical infrastructure.
- Sprawling connectivity & IoT create backdoors, fridges, exercise bikes and smartphones are attack vectors.
- Unknown unknowns: plan for the worst while hoping for the best.

VERTALI

A Changed World

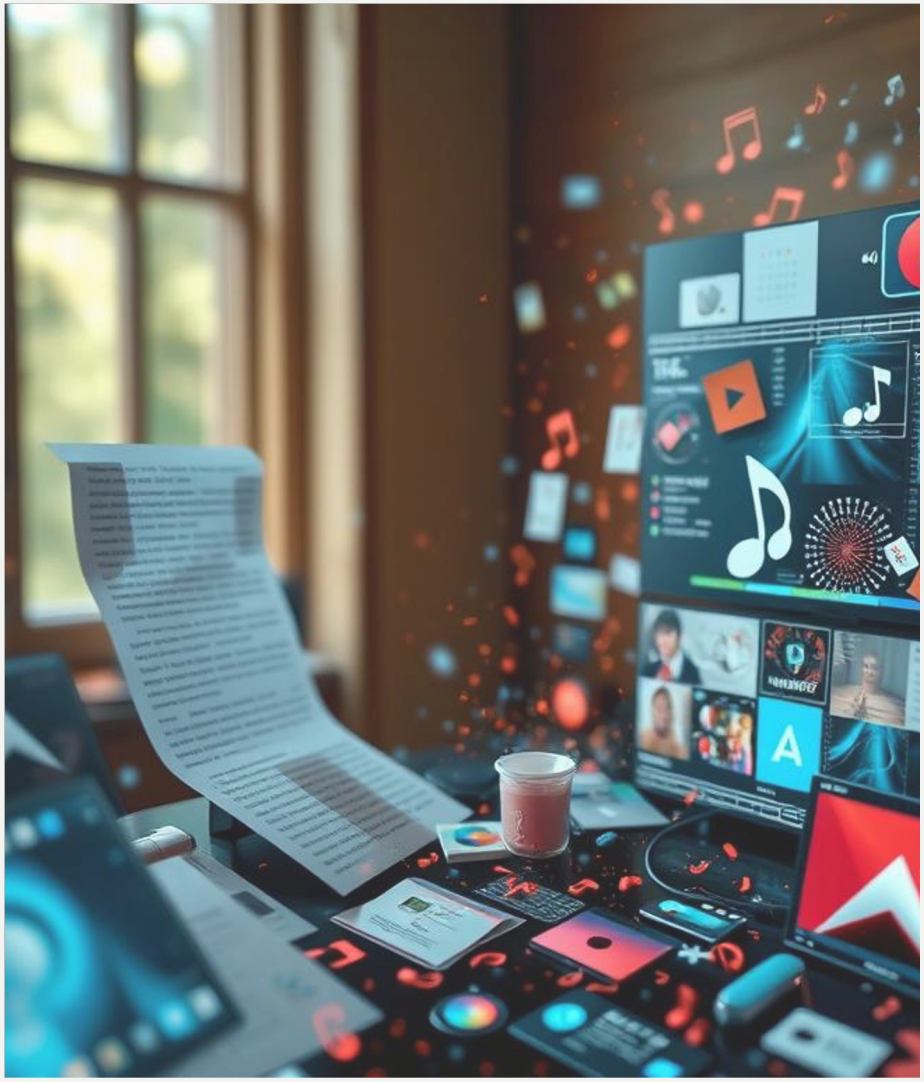
- **Evolution of IT Security Attacks**
  - In recent years, IT security attacks have shifted from isolated incidents towards targeted and complex threats at personal, corporate, and national levels.
- **Impact of Digital Transformation**
  - New digital technologies have introduced vulnerabilities, as organizations continue their digital transformation, leading to major risks associated with increased connectivity.
- **Remote Working Challenges**
  - The pandemic highlighted that cyber attack methods didn't change, but the scale increased as individuals adapted to remote, home, and hybrid working environments.

VERTALI

Generative AI

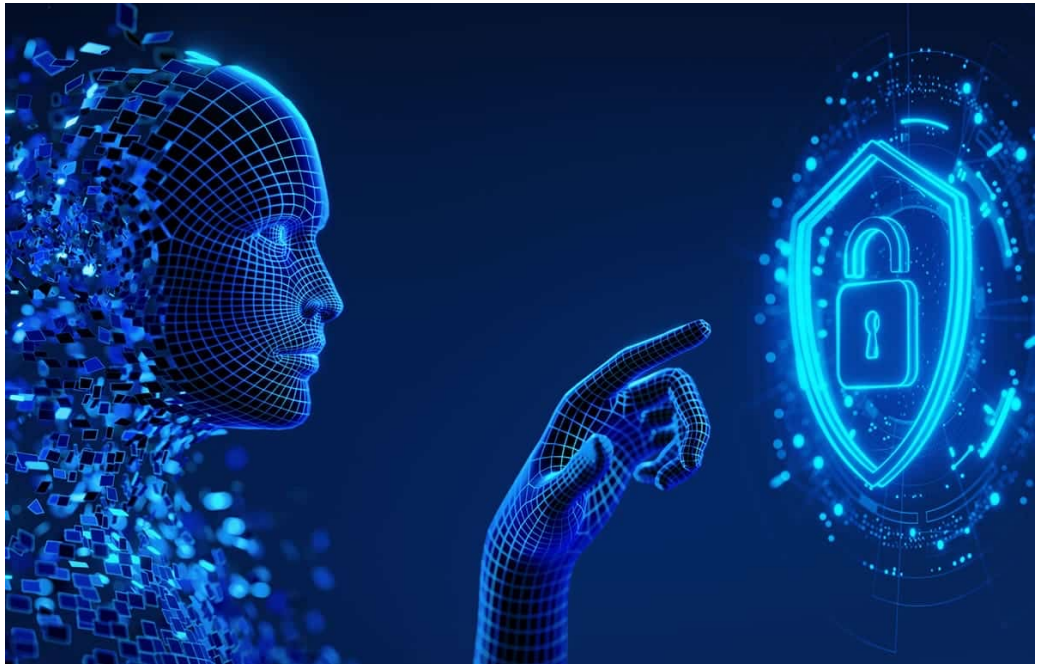
- Generative AI is a type of artificial intelligence that creates content, including images, music, text, videos, and audio

- Popular examples of generative AI include ChatGPT, which generates text-based responses, and DALL-E, which creates images from textual descriptions



VERTALI

The Good: AI in Cybersecurity



Enhanced Threat Detection

AI-powered security analytics can analyze vast data volumes to identify patterns and anomalies, enabling proactive threat detection and faster responses to potential breaches.

Automated Security Responses

Generative AI can automate incident responses, reducing the time between detection and action, such as isolating affected systems or swapping out concerning address spaces.

Vulnerability Management

AI can predict and identify vulnerabilities by analyzing system behaviors and configurations.

The Bad: AI-Driven Attacks

AI as a Tool for Cybercriminals

Attackers utilize AI technologies to identify system vulnerabilities at an unprecedented speed

Phishing attacks have become more sophisticated through AI

AI can automate the exploitation of security flaws

VERTALI

Generative AI: Risks & Challenges

AI-Driven Attacks

- Attackers use AI to craft phishing and identify vulnerabilities.
- Sophisticated exploits are automated and already underway.

Complexity & Over-Reliance

- Integrating AI requires significant time, people & resources.
- Over-reliance may lead to complacency; human oversight remains vital.

Compliance & Skills

- AI adoption must meet regulatory requirements & be transparent.
- Historic skills gap: need experts versed in mainframe & AI.

VERTALI [16] [17] [18] [19]

The Double-Edged Sword of AI in Cybersecurity

↗ Opportunities

- Enhanced threat detection and prevention
- Automated security responses
- Improved encryption and data privacy
- Advanced vulnerability management

↘ Risks

- AI-powered criminal activities
- Complex integration with mainframes
- Significant resource investment
- Risk of over-reliance on automation

Security Fundamentals

Mainframe Security Basics

01	Authentication	Accountability is assured only if you can confirm that whoever accesses your system is who they claim to be. Do you enforce the use of MFA?
02	Access Management	Insider threats combined with phishing and ransomware pose serious risks; no encryption can prevent someone with valid access from misusing data. Consider data ownership and role-based access control.
03	Encryption	Regulations increasingly require encryption. Key management and protection of cryptographic services are critical risks that need to be addressed.

Security Fundamentals

Authentication

- Strong passwords & MFA ensure you know who is connecting.
- Encrypt authentication secrets; rotate keys frequently.

Access Management

- Role-based controls restrict access to what's necessary.
- Enforce least privilege & approval workflows.

Privileged & JML

- Rigorous Join–Move–Leave processes reduce dormant accounts.
- Recertify privileged access and implement break-glass procedures.

Dealing with Complexity and Ensuring Observability

1. **Increasing Complexity**

   Mainframes at the center of complex application and service webs

2. **AIOps Integration**

   AI and automation tools to streamline systems management

3. **360-Degree Observability**

   Extending visibility across multi-cloud, on-premises, and hybrid environments

4. **AI as a Golden Thread**

   Integrating AI throughout security and observability processes

VERTALI

Towards the Unknown

Understanding Cyber Threats

- As the landscape evolves, there are 'known knowns; things we know we know.'
- There are 'known unknowns; some things we do not know.'
- However, there are also 'unknown unknowns - the ones we don't know we don't know.'

Importance of Preventative Actions

- Make informed predictions and plans through research and understanding the current threat landscape.
- Engage with external experts and invest in practical activities such as security assessments and penetration testing.
- Implement robust policies and technologies to mitigate risks and defend against emerging threats.

VERTALI

Real-World Impact & Costs

Once attackers gain mainframe access, damage can be catastrophic, they create backdoors even after fixes.

Penetration testers prove mainframes are hackable within minutes when not secured.

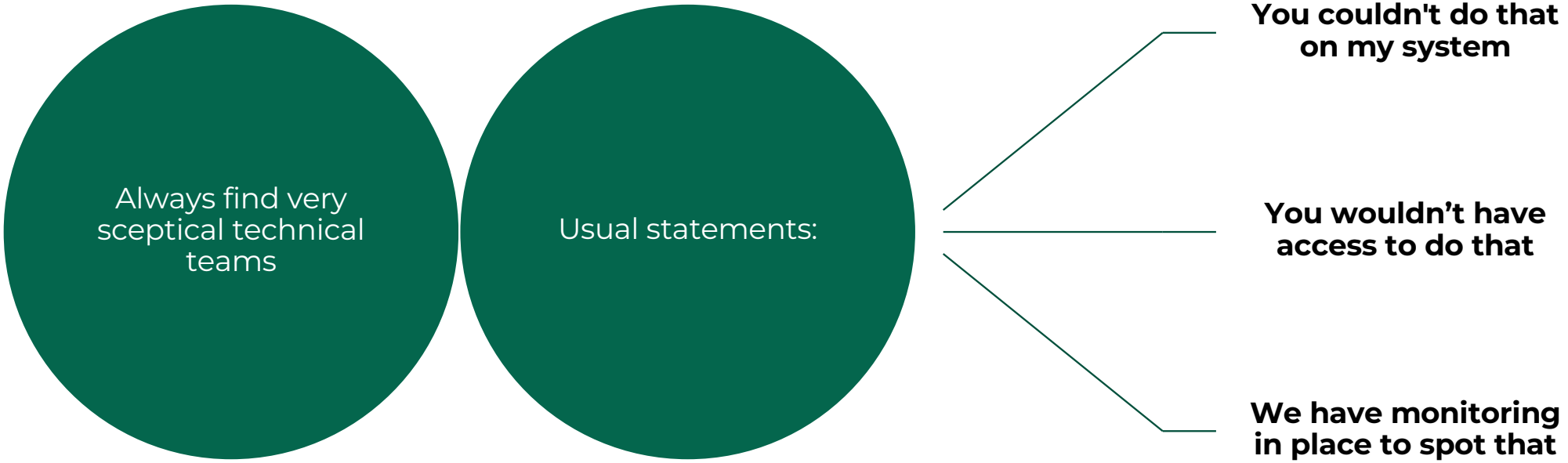
Average cost of a data breach in 2024: US$4.88M, a 10% increase year-on-year.

VERTALI

Still Our Biggest Risk: Insider Threats

- Users with:
  - Elevated Security authority Special, Operations, Non-CNCL, Security, etc
  - UID(0) in USS
- Risks:
  - Reading/Updating or Deleting sensitive system and business datasets
  - Creating hidden backdoor IDs
  - Disabling logging
  - Manipulating transactions
- Because it's "authorised access," it often bypasses perimeter detection

Still Our Biggest Risk: Insider Threats



VERTALI

VERTALI

Flight To Bolivia Anyone!

- Not an Un Typical Sysprog Response....
- So, I Said, What if **you** did it?
- Would anyone notice?
- How About.....

VERTALI

Modern Defence Strategies

VERTALI

Modern Defence Strategies

VERTALI

Key Recommendations

Zero Trust & Basics

- Implement strong auth, MFA & least privilege.
- Get the fundamentals right before chasing shiny objects.

AI with Oversight

- Invest in AI for detection & response.
- Maintain human oversight & meet regulatory standards.

Secure Mobile & IoT

- Define robust BYOD policies & protect all devices.
- Monitor and log access continuously.

Culture & Resilience

- Foster continuous training & cross-team collaboration.
- Conduct assessments, pen tests & resilience planning.

Looking Ahead: Mainframe Security in 2026

As we look towards 2026, the landscape of mainframe security continues to evolve. The integration of AI, the pursuit of Zero Trust security, and the need for comprehensive observability will likely remain key focus areas.

While new technologies and threats emerge, the importance of maintaining strong foundational security practices cannot be overstated. The future of mainframe security lies in balancing innovation with tried-and-true security principles.

Conclusion

Mainframes are integral to our digital world and must not be ignored

AI brings both opportunity and risk, leverage them wisely

Strong fundamentals, Zero Trust and continuous vigilance are essential

Start your journey today: assess, adapt and evolve your security posture

VERTALI

VERTALI

Your feedback is important!

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation