
aliv business
CYBER SECURITY SUMMIT 2026
CYBER RESILIENCE
DEFENDING THE DIGITAL FRONTIER
EMPOWER, PROTECT, EVOLVE
The New Cyber Frontier:
From Threat Intelligence to National-Scale Resilience

Who am I?

- Offensive Security Researcher: I love everything **Hacking**
- **Tribe of Hackers**: Blue Team 2020
- **Global Advisory Board**:
  - EC-Council for **C|TIA & C|PEN**
  - USIU-A ICT
  - Ushahidi
  - CyberSafe Foundation
- Blockchain Investigator
- Senior Technology Advisor to the Attorney General of Kenya
- **C.E.O Cyber Guard Africa**
- **Founder** of Cyber Collective, **Africahackon**
- Presented at over 420 Cyber Security conferences
- **Adjunct Professor,** Cyber Security - **Strathmore University**
- Practice Kung Fu

CYBER SECURITY TRENDS & CHALLENGES IN 2026

Increased Regulation and Enforcement

Private sector companies and critical infrastructure providers will face unprecedented demands for product security, intelligence sharing, and transparency on data security

Regulatory scrutiny continues, with new rules requiring public companies to disclose material security incidents

Ransomware Remains a Threat

Ransomware attacks are as intense as ever, affecting organizations across the Pacific region.

Policies and regulations around ransom payments are expected to evolve, but specifics remain uncertain

Secure by Design and Incident Reporting

The industry emphasizes secure design principles to prevent vulnerabilities.

Compliance regulations drive incident reporting and transparency

AI-Based Social Engineering

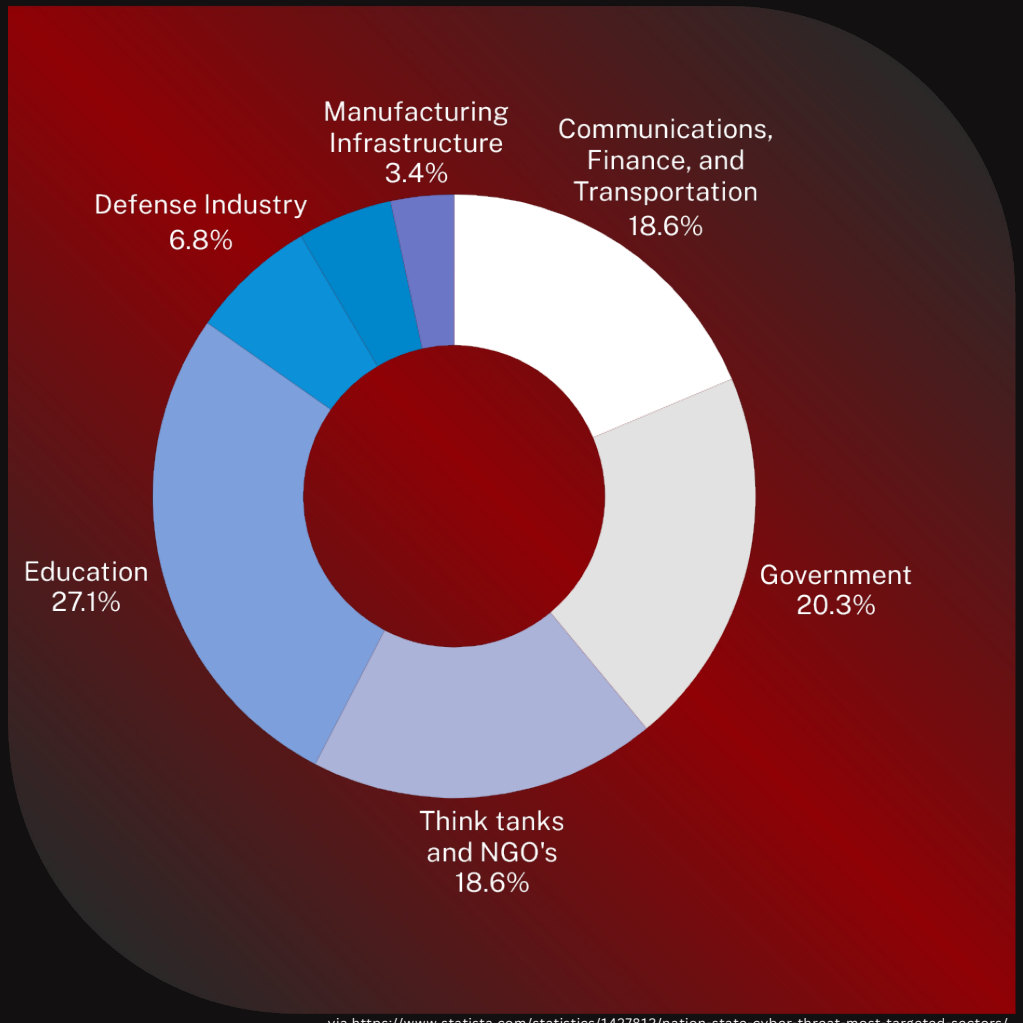
Cybercriminals leverage AI for personalized phishing campaigns at scale.

AI-driven attacks exploit human weaknesses like impulsiveness, greed, and curiosity

LOOKOUT: 2026 COMMON THREATS

- BEC attacks Vs Sophisticated Malwares (Silent password stealers)
- Fully Undetectable (FUD) malwares - Stealth Game

- Automated Attacks with AI Engines
- API Exploitation for data exploitation- Cloud, Mobile Applications & Web
- Ransomware



via https://www.statista.com/statistics/1427812/nation-state-cyber-threat-most-targeted-sectors/

Nation State Attacks Statistics

The proportion of cyber-attacks perpetrated by nation states targeting critical infrastructure jumped from 20% to 40%

The Facts for 2025/2026

Attack Sophistication: Increase of 79% of 2024–2025 attacks were malware-free, with actors increasingly "living off the land" using legitimate admin tools to evade detection.

AI Integration: By 2025, 33.5% of security leaders suspected AI involvement in attacks, with AI-enabled phishing up 202% between June–November 2025.

Dwell Time: Breaches take an average of 241 days to identify and contain.

Ransomware Link: Nation-state actors — particularly North Korea — are increasingly deploying ransomware as a revenue generation tool.

Supply Chain Attacks: More than tripled, from 13 incidents/month in early 2024 to 41 by October 2025.

As AI Gains a Voice and a Face… So Do Cybercriminals

The line between real and artificial is blurring, bringing with it new risks, new deception tactics, and new levels of urgency for cybersecurity.

WHY AI MATTERS

- Efficiency gains: 20-40% reduction in routine tasks - Automate repetitive work like data entry, document formatting, and status updates, freeing your team to focus on strategic relationships and value-added activities

- Better decision-making through data insights - AI analyzes vast amounts of historical data to identify patterns, predict risks, and recommend optimal pricing or delivery strategies you might otherwise miss

- Competitive advantage in proposal development - Generate tailored, high-quality RFP responses faster, allowing you to bid on more opportunities while maintaining personalization and quality

- Enhanced customer service and responsiveness - Provide instant answers to common queries, faster quote turnarounds, and proactive communication that strengthens buyer relationships

THE REALITY CHECK: UNSEEN RISKS

While AI tools offer immense productivity gains, our observations highlight critical security gaps in their use within workflows. Many of these risks go unnoticed until a breach occurs.

What We've Observed:

- Users inadvertently uploading sensitive documents to public AI platforms.
- Exposure of passwords, credentials, and other secrets.
- Proprietary thought processes and business ideas are becoming publicly accessible.
- Potential training data contamination from sensitive uploads.

The Stakes are High:

- Severe data breaches and regulatory violations (GDPR, PCI DSS).
- Irreparable intellectual property theft leading to competitive disadvantage.
- Significant reputational damage and loss of customer trust.

UNDERSTANDING AI PLATFORMS: PUBLIC VS. PRIVATE

The first step to secure AI integration is understanding the fundamental differences in how various AI platforms handle your data.

Always verify the data privacy policies and terms of service before using any AI tool, especially for work-related tasks.

PUBLIC AI PLATFORMS

- Free/Low-cost access.
- Data often used for model
- training.
- Conversations logged and
- potentially accessible.

Examples:
ChatGPT (free), Claude (web), Gemini, Copilot (public repos).
Public AI Platforms

Risk Level: HIGH

PRIVATE/ENTERPRISE AI

- Data Processing Agreements & privacy guarantees.
- No training on customer data.
- Enhanced security controls.

Examples: ChatGPT Enterprise, Claude for Work, GitHub Copilot Enterprise.

Risk Level: MODERATE (with proper config)

ON-PREMISES/SELF-HOSTED

- Complete data control.
- No external data transmission.
- Higher setup/maintenance
- costs.

Examples: Ollama, LocalGPT, Code
Llama self-hosted.

Risk Level: LOW (with proper Security)

ATTACK VECTORS & LOOPHOLES

AI-Powered Phishing via Voicebots

- Sophisticated robocalls that mimic real people
- Adaptive, interactive AI voice engines
- Example: Fake tech support bots posing as Apple/Microsoft

Synthetic Identity Fraud

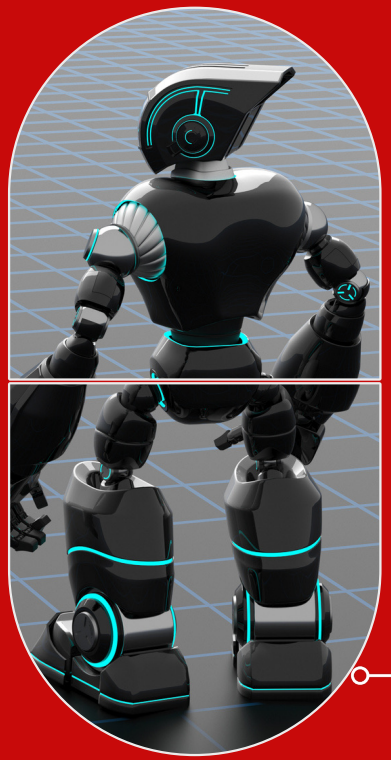
- Merging AI-generated content with real stolen data
- Used to pass KYC, job interviews, or access secure systems
- Very hard to trace or verify in real time

Real-Time AI Translation Exploits

- AI-based interpreters (e.g., in multilingual meetings)
- Potential vulnerability to man-in-the-middle manipulation
- Risk of real-time interception or message tampering

AI Powered Hacking Assistants

GhostGPT / DevilGPT / WormGPT / Venice AI



ATTACK VECTORS & LOOPHOLES

Voice Cloning Attacks

- Vishing attacks using synthetic voices
- Just seconds of recorded audio are enough
- Undermines voice-based authentication systems
- Example: $35M bank fraud via cloned CEO voice (2023)

Deepfake Video Attacks

- From crude edits to nearly undetectable fakes
- Tailored impersonation targeting public figures or executives
- Audio-video sync increases believability

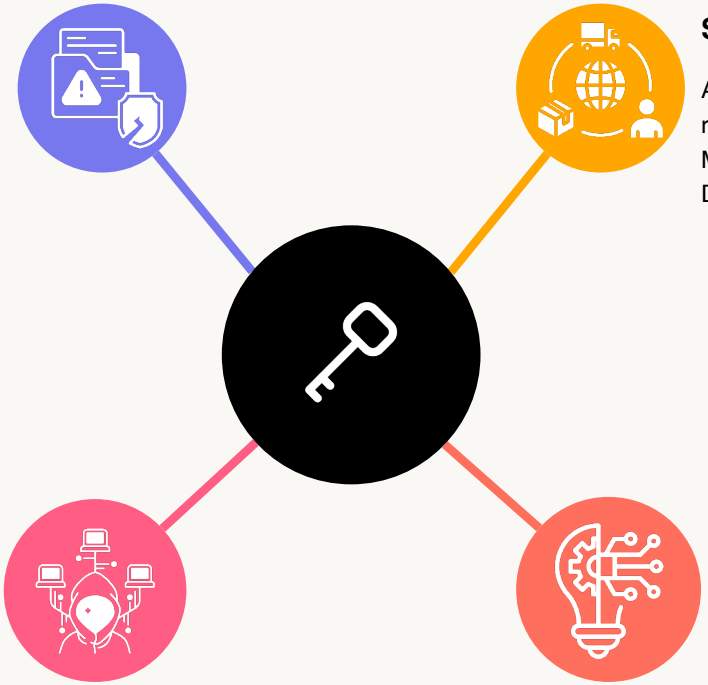
Examples:
Zelensky deepfake urging surrender (2022)
G20 movie, US secretary of state, Marco Rubio (2025)

Key AI Security Risks & Threat Vectors

Beyond direct data exposure, AI tools introduce new attack surfaces and risks that users must be aware of.

Data Exposure Risks

Credential leakage in document uploads. Proprietary company data disclosure. Customer data exposure through examples. Infrastructure details revelation



Supply Chain Risks

AI-generated output with wrong references
Malicious code (macros) suggestions
Dependency confusion attacks via AI.

Training Data Contamination

Your content becomes part of AI training data. Potential information disclosure to other users. Intellectual property ending up in public models.

Advanced Threat Scenarios

Prompt Injection: Malicious prompts to extract sensitive data.
Model Poisoning: Compromised training data affecting outputs.
Inference Attacks: Extracting training data from model responses.

What are the *priorities* today?

- **Cyber Resilience**
- **Predict, Protect, Detect, Respond & Recover to attacks across your hybrid IT environment**

1. **APPLICATIONS**
   that deliver the outcomes you want
2. **DATA**
   compliant, protected, accessible, backed up
3. **USERS**
   an engaging experience everywhere they work
4. **CUSTOMERS**
   a differentiating experience across every channel
5. **THINGS**
   connected to realise your IoT strategy

Expense in Depth:
Cyber Resilience is Everyones Responsibility

WHAT IS SECURITY SPENDING?

SECURITY MANAGER

CFO

CEO

BOARD MEMBER

IMPORTANCE OF UNDERSTANDING YOUR ENVIRONMENT

1. Asset Identification

To decisively allocate spending, knowing what lies within your domain is crucial. It's about mapping all assets, digital or otherwise, to assess what requires protection.

2. Threat Awareness

Environment-specific threat analysis helps to pinpoint where security measures should be heightened. Different sectors face distinct threats, requiring tailored solutions.

3. Compliance Standards

Regulatory compliance dictates certain security mandates. Understanding your sector's legal requirements can drive focused investments and avoid financial and reputational risk.

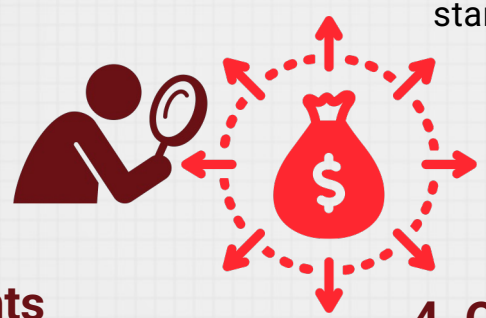
FACTORS TO CONSIDER WHEN EVALUATING SECURITY SPEND

1. Risk Appetite

Every company has its threshold for risk. Balancing your risk appetite with spend efficiency is a dance that demands precision and a substantial understanding of your tolerances.

2. Industry Benchmarks

Comparing your security investments to those of peers can illuminate overspending or underspending, and benchmarking against industry standards keeps you competitive.



3. Technology Advancements

With technology evolving at a breakneck pace, it's essential to consider future-proofing security measures and allotting resources for emerging tools and defenses.

4. Operational Resilience

Investing in security should enhance and not hinder operations. Evaluating the impact of security on operational resilience is vital.

ASSESSING THE CURRENT SECURITY LANDSCAPE

THREAT TYPE	PREVALENCE	IMPACT
MALWARE	HIGH	SEVERE
PHISHING	WIDESPREAD	MODERATE TO SEVERE
RANSOMWARE	RISING	CRITICAL
INSIDER THREATS	VARIABLE	MODERATE TO HIGH
DISTRIBUTED DENIAL OF SERVICES (DDOS)	INCREASING	HIGH

LEVERAGING STRATEGIC INTELLIGENCE TO REDUCE EXPENSE IN DEPTH

1. Context Centric

Provides information to make informed decisions regarding threats that target organizations

2. Risk Mitigation Driven Investment

Drives and justifies investments in people, process and technology to mitigate business risks

3.Answers Key Business Risk Questions

WHO would target us?

WHY would they target us?

4. Feeds Cyber Security Strategy

Edifies cyber security strategies by introducing visibility into the changing threat landscape and risk factors as a result of the changes.

IMPLEMENTING STRATEGIC INTELLIGENCE APPROACH

1. Understand Business Revenue Points

Understand how the business generates revenue. Map out risk factors that can impact revenue generation.

2. Threat Modelling

Who - Adversary

Why - Intent

How- Capability

What - Targeting

3. Prioritization

Use strategic intelligence to prioritize budgeting

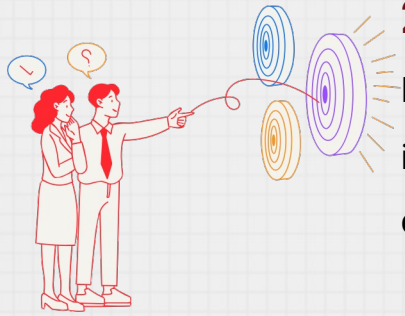
e.g What is you paint point? Where can you spend effectively to reduce the risk?

example phishing is a common entry point, targeting external public applications

DETERMINING THE ROI OF SECURITY INVESTMENTS

1. Cost-Benefit Analysis

Scrutinizing the costs against the benefits of each security measure can reveal the quantitative and qualitative returns on your security investments.



2. Incident Reduction

Monitoring the decrease in security incidents post investment gives clear indicators of success and contributes to ROI calculations.

3. Enhanced Reputation

Improved security protocols contribute to heightened customer trust and brand credibility, indirectly boosting the financial bottom line.

CYBER GUARD AFRICA LIMITED

Building an Environment to Support Threat Hunting Simulations for Bahamas

CYBER GUARD AFRICA LIMITED

Know Yourself

- Knowing your environment better than any **INSIDER THREAT** or **EXTERNAL THREAT** actors.
- If you **REALLY** want to protect your environment, you **REALLY** have to know your environment better than anyone.

CYBER GUARD AFRICA LIMITED

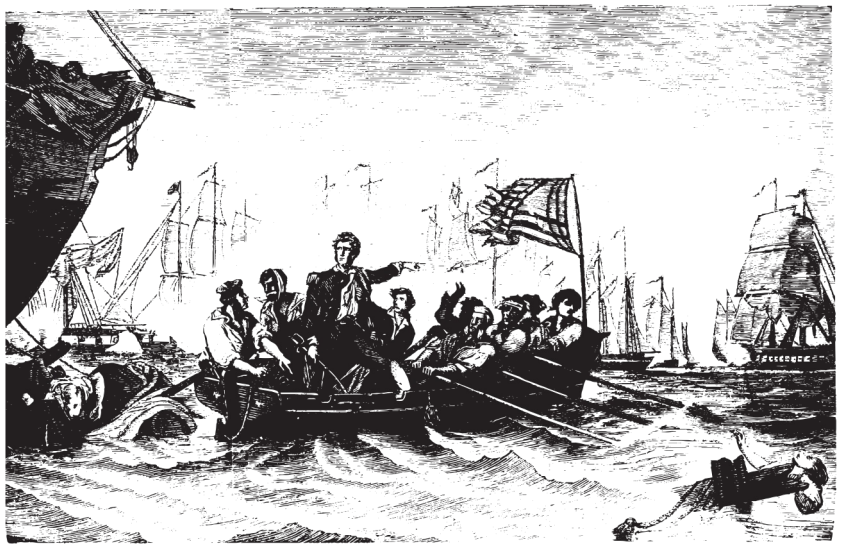
Know Your Enemy

- Define your enemies, are they internal, external or both
- What is their capability? What motivates them?, What do they target?

Know Your Battles

CYBER GUARD AFRICA LIMITED

- Why will they target us? How can they impact our vision, mission?
- What will they target ? What are our crown jewels?
- How will they target? Have we seen attempts before?
- Where are we exposed? How does our attack surface reflect?



CYBER GUARD
AFRICA LIMITED

Threat Hunting Simulation with the 3K's

CYBER GUARD AFRICA LIMITED

Know Yourself

- Consistently run hunt exercises and how often they'll be carried out to accurately understand your environment.

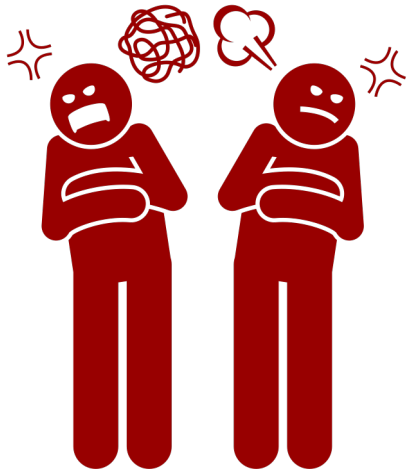
- Define your hunt mission name: e.g Understanding our Critical Assets

- Define your hunt description

CYBER GUARD AFRICA LIMITED

Know Your Enemy

- Identify attackers activities you would like to hunt for in your environment



Know Your Battles

CYBER GUARD AFRICA LIMITED

- Identify the attack path the attackers will follow to target your critical assets
- Identify opportunities to detect attacker activity through your hunts
- Network Traffic Hunting
  - Failed traffic analysis
  - Abnormal traffic patterns
  - Abnormal protocol usage
- Endpoint Activity Hunting
  - Abnormal process hunting
  - Remote Access Anomalies
  - Windows Services Anomalies
  - Suspicious Executables Anomalies

How do we move on from here?

Governance & Policy:
National cybersecurity strategies, CERT/CSIRT establishment, legislative frameworks and their implementation methods

Threat Intelligence Sharing:
How countries can operationalize intelligence at a national level.

Critical Infrastructure Protection:
Identifying national crown jewels (telecoms, energy, finance, health) and applying tiered resilience planning

Cyber Workforce Development:
A country cannot be resilient without a pipeline of skilled defenders.

WAY FORWARD

Capacity Building through university and college programs

Collaboration among other organisations in your domain

More R&D
More Bug Bounty Programs

Public vs Private Partnerships

Involvement in Cyber security communities across the Caribbean


THANK
YOU
WWW.CYBERGUARDAFRICA.COM
WWW.BRIGHTZEED.COM
BRIGHT.GAMELI@CYBERGUARDAFRICA.COM
+254712421951