

The State of Cybersecurity in 2026

Threats, Trends, and What Comes Next

GEORGIA GMIS 2026 FALL CONFERENCE
DULUTH, GA



What to Expect

- ▶ 45-minute briefing
- ▶ From awareness, preparedness to continuous resilience
- ▶ Audience: IT, cybersecurity, and executive leaders

Executive Message

SECTION SUBTITLE

The threat environment has accelerated

- ▶ Attackers are compressing the time from access to impact.
- ▶ Identity, cloud, third parties, and AI are converging into one attack surface.
- ▶ AI is a force multiplier for both adversaries and defenders.
- ▶ Resilience—not prevention alone—must become the operating objective.

Key 2026 Metrics

- ▶ **Breakout time:** Dropped to an average of **29 minutes** (fastest observed at 27 seconds), shrinking handoff times to seconds.
- ▶ **AI-enabled attacks:** Surge of **89%** by adversaries; prompt injection and GenAI tool abuse function as new malware.
- ▶ **Malware-free intrusions:** Account for **82%** of detections, heavily driven by credential and identity abuse.
- ▶ **Zero-day / rapid exploit spike:** Zero-day exploitation rose **42%** prior to disclosure; time-to-exploit for critical CVEs dropped to hours/days.
- ▶ **Machine-to-human identity ratio:** Machine identities outnumber humans **109:1**, with 9 out of 10 organizations facing an identity breach

The attack lifecycle is getting faster

- ▶ Reconnaissance and target selection are increasingly automated.
- ▶ Attackers can personalize phishing and social engineering at scale.
- ▶ Stolen credentials may bypass malware-focused controls.

The defensive question: can we detect and contain activity before impact?

Ransomware and extortion: the business interruption problem

- ▶ Encryption is only one component; data theft and coercion remain central.
- ▶ Backups are necessary but not sufficient—recovery must be tested.
- ▶ Privileged access, segmentation, and identity controls reduce blast radius.
- ▶ Prepare communications, legal, continuity, and executive decision paths in advance.

AI-enabled cyber threats

- ▶ More convincing phishing, voice cloning, and executive impersonation
- ▶ Automated reconnaissance, exploit research, and attack-path planning
- ▶ AI-assisted malware variation and evasion
- ▶ Prompt injection and tool abuse against AI-enabled workflows
- ▶ Human verification and strong authorization remain essential.

Agentic AI: the emerging control challenge

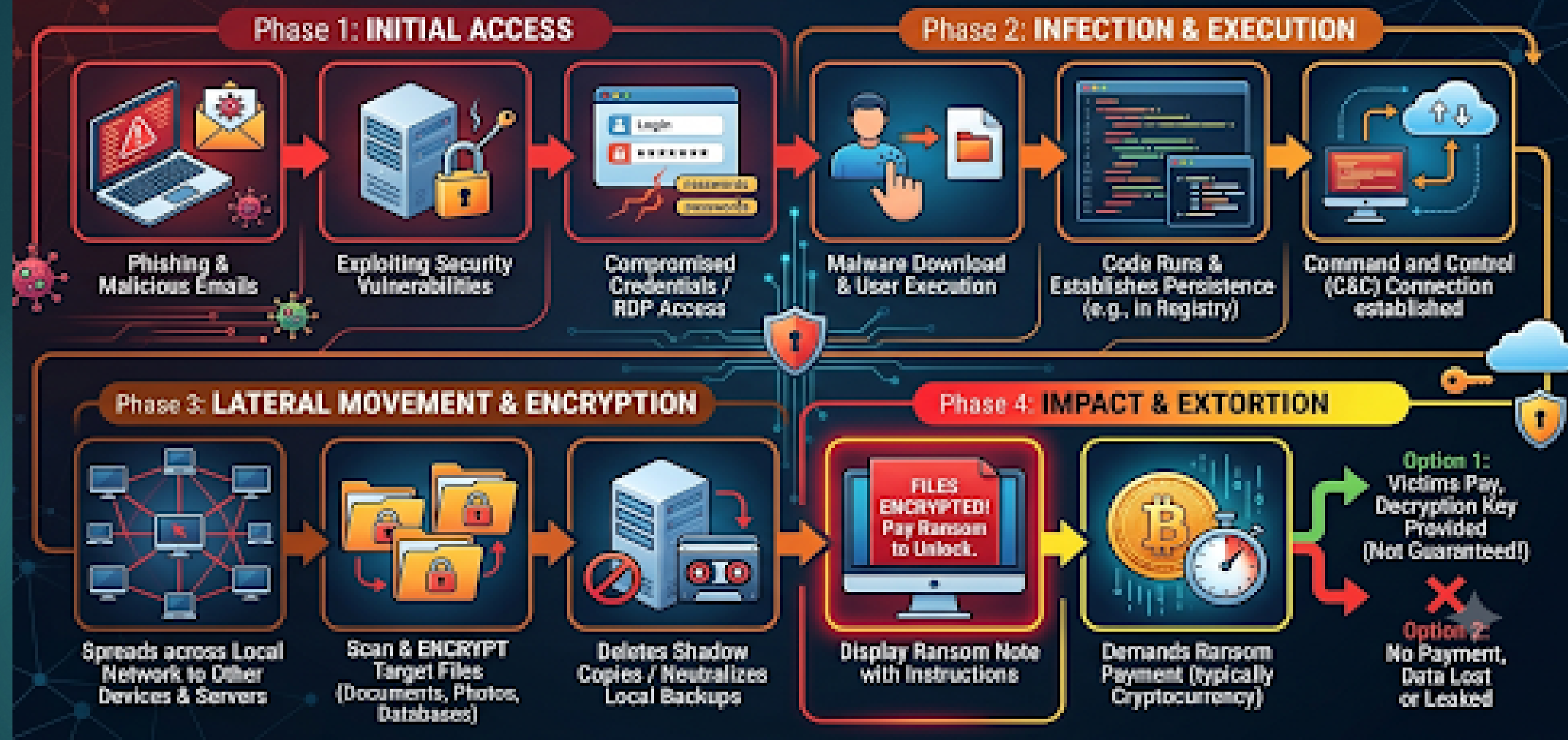
- ▶ Agents can plan, call tools, access data, and take multi-step actions.
- ▶ Security boundaries must include the model, tools, memory, data, and runtime.
- ▶ Use sandboxing, approval gates, capability-based access, and monitoring.
- ▶ Separate experimentation from production systems.
- ▶ Require human accountability for consequential actions.

Cybersecurity is a process!

Short Version

- ▶ **Infection & Access:** Malware enters via phishing, exposed RDP, or vulnerabilities
- ▶ **Setup & Spread:** Attacker steals credentials, deletes shadow copies/backups, and moves laterally across the network.
- ▶ **Encryption & Theft:** Files are encrypted (hybrid symmetric/asymmetric) and sensitive data is exfiltrated for double extortion.
- ▶ **Demand:** A ransom note appears with a payment timer and threats of data leaks or permanent loss

BASIC PROCESS FLOW OF A RANSOMWARE ATTACK



Now What?

Awareness, Preparedness and Resilience

- ✓ Awareness
- ✓ Preparedness
- ✓ Resilience

Security operations must evolve

- ▶ Move from alert volume to attack-path and business-impact prioritization.
- ▶ Integrate endpoint, identity, cloud, network, email, and SaaS telemetry.
- ▶ Use AI to summarize, correlate, investigate, and recommend—not blindly decide.
- ▶ Build playbooks for common scenarios and validate them through exercises.
- ▶ Track mean time to detect, contain, recover, and learn.

Zero Trust + continuous verification

- ▶ Never assume trust based on network location or prior access.
- ▶ Verify user, device, workload, session, and context.
- ▶ Segment critical systems and limit east-west movement.
- ▶ Continuously evaluate risk and revoke access when conditions change.
- ▶ Start with high-value applications, privileged users, and sensitive data.

Top 10 actions leaders should take now

1. Confirm crown-jewel systems and mission-essential services.
2. Enforce phishing-resistant MFA for privileged access.
3. Establish complete asset and identity inventories.
4. Reduce standing privilege and segment critical systems.
5. Test backups and full restoration.
6. Implement AI use policy, inventory, and risk review.
7. Prioritize internet-facing and actively exploited vulnerabilities.
8. Exercise ransomware, third-party, and cloud-outage scenarios.
9. Measure detection, containment, and recovery performance.
10. Fund people, process, and technology as one program.

What Comes Next:

2027 AND BEYOND

What comes next: 2027 and beyond

- ▶ Security becomes more continuous, identity-centric, and automation-enabled.
- ▶ AI agents will create new productivity opportunities and new control requirements.
- ▶ Cryptographic agility and post-quantum planning become more relevant.
- ▶ Regulatory, contractual, and insurance expectations will continue to evolve.
- ▶ Organizations that connect cyber risk to mission outcomes will make faster decisions.

Closing: cybersecurity must evolve now

- ▶ The environment is moving at machine speed; governance and resilience must keep pace.
- ▶ Technology alone will not close the gap.
- ▶ The winning operating model combines visibility, identity security, Zero Trust, skilled people, and tested recovery.
- ▶ The question is not whether an organization will face disruption—it is how prepared it will be to limit impact and restore trust. PROACTIVE!

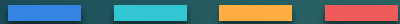
Proactive Tasks

1. Inventory assets
2. Assess and prioritize risk.
3. Patch and harden systems.
4. Strengthen identity security with MFA and least privilege.
5. Protect sensitive data and backups.
6. Monitor continuously.
7. Secure email and endpoints.
8. Manage vendor and external exposure.
9. Prepare and practice incident response.
10. Measure performance and improve continuously.

THE CYBER KILL CHAIN

How cyberattacks progress—and where defenders can break the chain

A defensive briefing for IT teams, security staff, and government leaders



DEFEND EARLY • DETECT FAST • CONTAIN QUICKLY

GEORGIA
GMIS

The 7 stages at a glance

The Lockheed Martin model is a framework—not a guaranteed sequence.



Defenders can interrupt the chain at any stage; real attacks may skip, repeat, or overlap stages.

Stages 1–3: Prepare and deliver

Defensive goal: reduce exposure and prevent the initial foothold.

01 Reconnaissance

Attacker learns about people, systems, vendors, and exposed services.

DEFENSIVE CONTROLS

Reduce public exposure • protect staff details • monitor external assets

02 Weaponization

Attacker prepares a lure, exploit, or malicious file/tool.

DEFENSIVE CONTROLS

Harden endpoints • filter risky files • use threat intelligence and application controls

03 Delivery

The attempt arrives via email, web, compromised software, removable media, or another path.

DEFENSIVE CONTROLS

Email/web filtering • phishing-resistant MFA • safe reporting and verification

Stages 4–7: Gain access, persist, and act

Defensive goal: detect suspicious behavior, limit privilege, and contain impact.

04 Exploitation

A weakness or user action enables code execution or access.

DEFENSIVE CONTROLS

Patch management • secure configuration • exploit protection

05 Installation

Malware or another foothold persists in the environment.

DEFENSIVE CONTROLS

EDR • application allowlisting • least privilege • persistence monitoring

06 Command & Control

Compromised systems communicate with attacker infrastructure.

DEFENSIVE CONTROLS

DNS/web monitoring • egress controls • network detection

07 Actions on Objectives

Attacker pursues theft, fraud, disruption, espionage, or encryption.

DEFENSIVE CONTROLS

Data controls • segmentation • backups • incident response

Example: a phishing-led ransomware incident

Illustrative scenario—map controls, telemetry, and response owners.



Where defenders break the chain

Layer controls so one missed signal does not become a major incident.

Before delivery

Asset inventory • reduce exposure • secure email/web • phishing-resistant MFA

At exploitation

Rapid patching • secure baselines • EDR • least privilege

During command & control

DNS and egress monitoring • network segmentation • alert triage

Before major impact

Protected offline/immutable backups • data access controls • rehearsed response



Measure outcomes: time to detect • time to contain • recovery time • tested restore success

GMIS

Key takeaways and discussion

Use the kill chain to improve prevention, detection, response, and recovery.

The kill chain gives teams a shared language for describing attacker progress.

It is a model—not a prediction; attackers can skip, repeat, or combine stages.

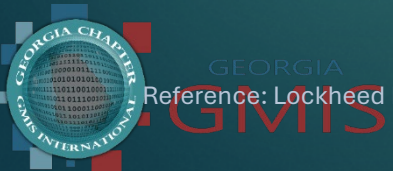
Map each stage to controls, log sources, alert owners, and response actions.

Practice scenarios with IT, security, communications, legal, leadership, and business owners.

Prioritize controls that prevent initial access, limit privilege, detect lateral movement, and protect recovery.

DISCUSSION

Where is our weakest link today—and what evidence would prove the control works?



Reference: Lockheed Martin Cyber Kill Chain®; pair with MITRE ATT&CK for detailed adversary behaviors.

The goal is not to create a security program that assumes it will never be breached. The goal is to build an organization/system that can prevent what it can, detect what it misses, contain what happens, and recover with confidence.

Stay Frosty...

Stanton Gatewood

THANK YOU!