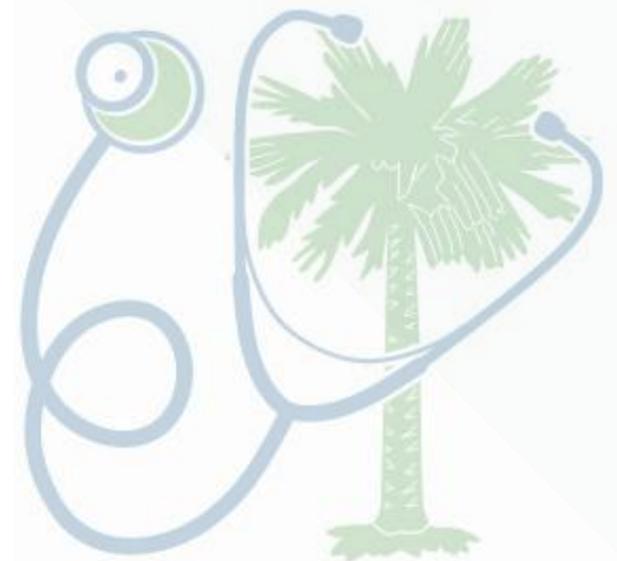# CIO Report

Presented by:
Tim Anderson
November 24, 2025

Clinical Inclusion in IT

- Our EHR Clinical Support Specialist is now a member of the IT department.

- Combining clinical and technical EHR support analysts in the same department is leading to faster resolution of clinical tickets and improved workflows and provider support experience.

Cybersecurity Landscape

- **Ransomware remains the dominant threat**, driving major EHR outages, operational disruption, and large-scale data exposure across the sector.

- **Hacking/IT incidents continue to rise**, with 364 breaches affecting over 33 million people reported to HHS in the first 9 months of 2025.

- **AI-enhanced phishing and social engineering** are rapidly increasing credential theft, making email compromise a leading entry point for attackers.

- **Third-party/vendor breaches** are accelerating, causing cascading impacts across the healthcare sector.
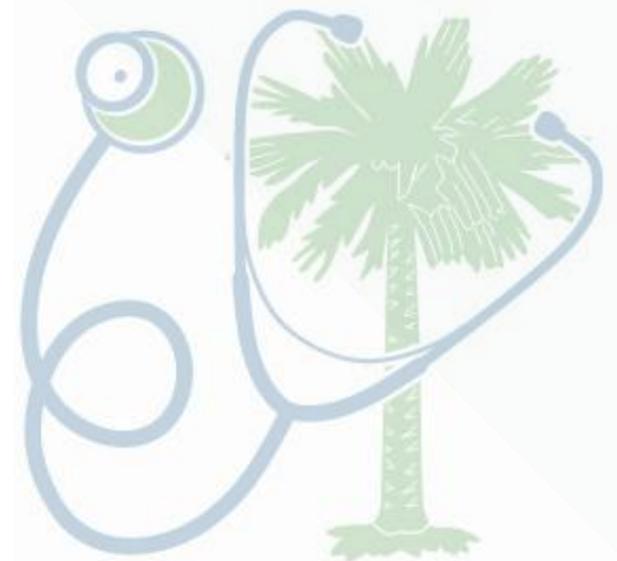
Email Security – Last 30 Days

First Layer of Defense – Microsoft 365 Defender

Phish / Malware Efficacy ⓘ

93.8%
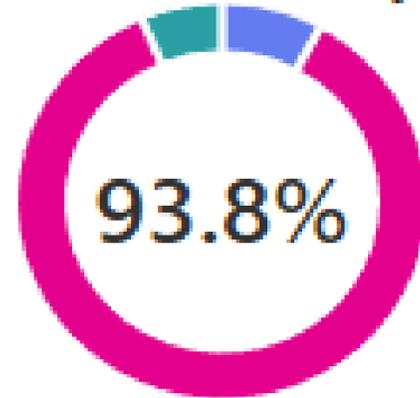
● Post-Delivery ● Pre-Delivery

● Uncaught

Learn more

Threat Detections ⓘ

2,027

○ Malware ● Phish ○ Spam

○ Impersonation ○ Detonation

○ Zap

Learn more

Email Security – Last 30 Days

Second Layer of Defense – Darktrace Antigena

THREATS SEEN

🔗 Phishing Link	58	▽
❓ Solicitation	44	▽
🏷 Fake Account Alert	41	▽
📎 Credential Harvesting	30	▽
🏷 Multistage Payload	24	▽
📎 Document Anomalies	23	▽
⋯ Others	105	

Internal IT Impersonation
800% ↑

Phishing Attachment
500% ↑

Brand Impersonation
140% ↑

Endpoint Protection

First Layer of Defense – Carbon Black App Control
Second Layer of Defense – Sentinel One

EXECUTIVE INSIGHTS

Report period: 30 days starting October 21, 2025

Created at: 21:14 November 20, 2025

SentinelOne

KEY FINDINGS

9

Threats found

Total threats since deployment: 58

● 2 (22%) Mitigated threats

● No Not Mitigated threats

● 7 (78%) Marked as Benign threats

Mitigated: The Quarantine mitigation action completed successfully. The same status shows if Remediate or Rollback also completed.

Not Mitigated: No mitigation actions were completed, or the threat was killed but no other action was done.

Marked as Benign: Your security team marked this threat as benign (the Analyst Verdict is False Positive).

Outside Resources

We recently joined the South Carolina Critical Infrastructure Cybersecurity Program (SCCIC).

Key aspects of the program include **free** access to:

1. **Risk Assessments**: Conducting thorough cybersecurity risk assessments for critical infrastructure sectors to identify vulnerabilities.

2. **Training and Awareness**: Providing cybersecurity training for infrastructure operators and public sector workers to improve awareness and readiness.

3. **Information Sharing**: Facilitating real-time information sharing about cyber threats and vulnerabilities between government and private sector entities.

4. **Incident Response**: Developing and coordinating response protocols for handling cybersecurity incidents that affect critical infrastructure, ensuring a quick and efficient recovery.

5. **Collaboration with Federal Agencies**: The program often collaborates with national entities like the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) to align state efforts with federal cybersecurity initiatives.

IT Projects

- **Windows 11 Migration Completed**
  Successfully upgraded **730+ computers** ahead of Microsoft's deadline; required significant device replacement, resulting in a higher-than-usual IT spend this year.

- **Welcome Tablets Pilot Deployment**
  Launched at **Lakelands Pediatrics** to streamline patient questionnaires; providing **major time savings**, improved data accuracy, and planned expansion to additional sites with future self-check-in capabilities.

- **Barcode Medication & Immunization Inventory Tracking**
  Implementing barcode scanning within Epic to **increase documentation accuracy**, improve pharmacy inventory control, and reduce clinical risk from medication errors.

- **Local Hyperspace Migration (Replacing Citrix/Slingshot)**
  Transitioning to Local Hyperspace to avoid **300% Citrix cost increase** and to significantly improve performance—saving users **~1 minute per Epic launch** and preventing session disconnects.

- **MyChart Direct Scheduling**
  Enabled patient self-service appointment scheduling in MyChart; **pilot underway at Hometown**, with broader rollout planned.