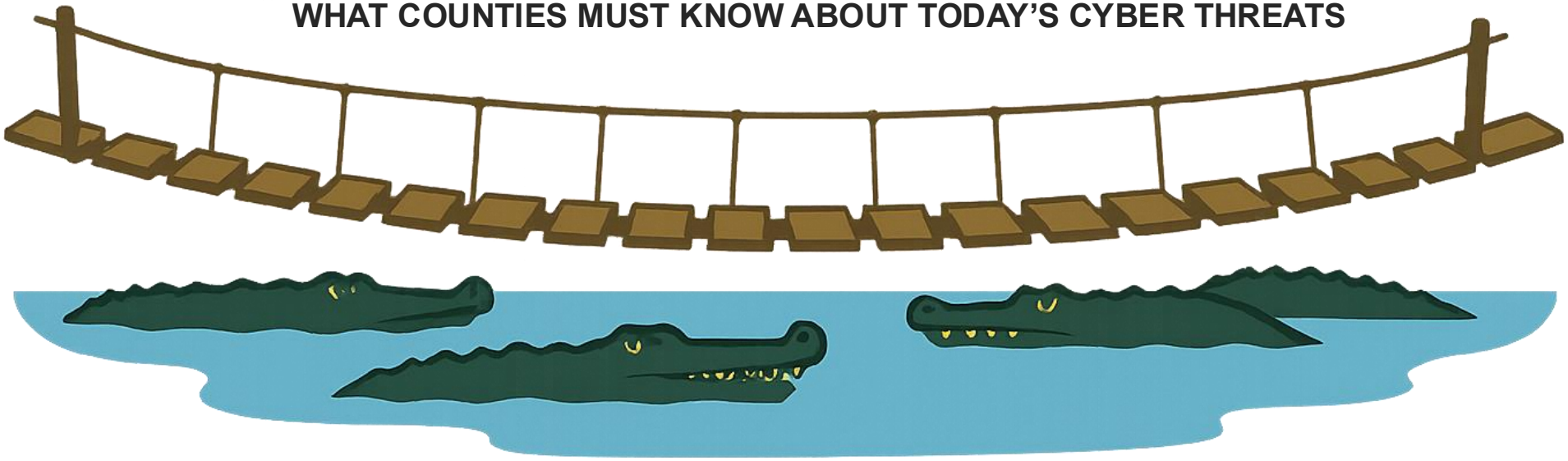
CYBER THREAT LANDSCAPE & TOP CONTROL RECOMMENDATIONS

WHAT COUNTIES MUST KNOW ABOUT TODAY'S CYBER THREATS



NOVEMBER 19, 2025

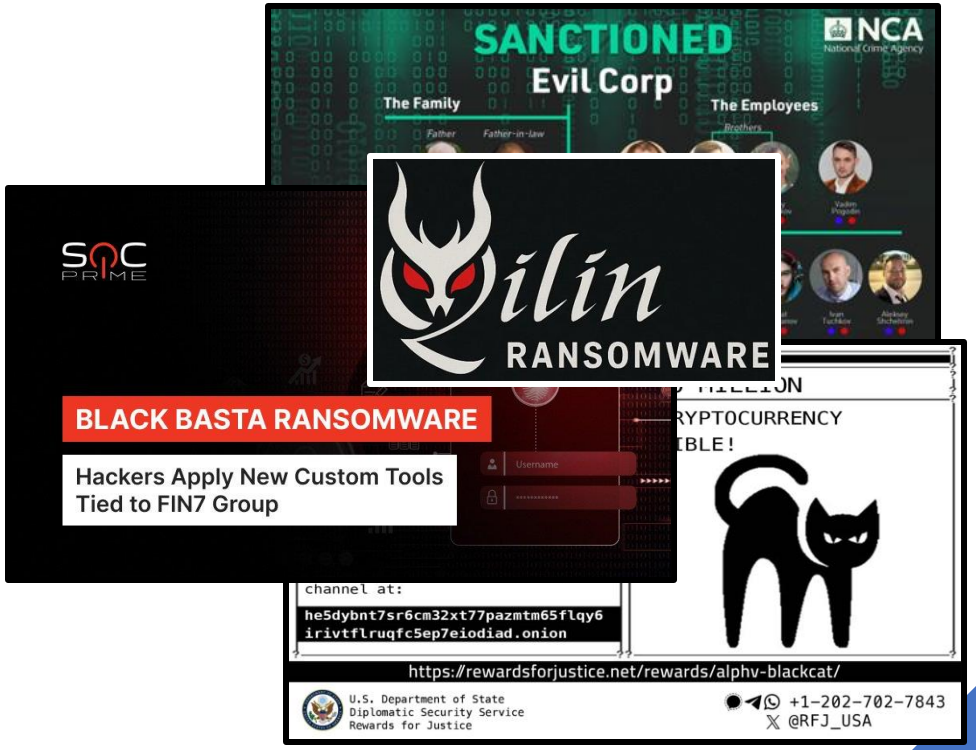
01

CURRENT THREAT LANDSCAPE

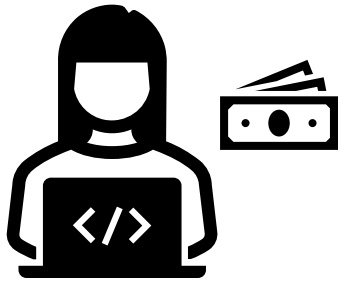
THREAT ACTORS

- Nation States

- Organized Crime
  - Qilin
  - Scattered Spider
  - Fin7
  - BlackCat
  - EvilCorp
  - cl0p
  - Revil
  - Akira
  - Vice Society



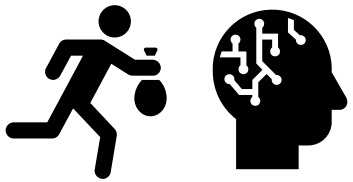
CURRENT THREAT LANDSCAPE



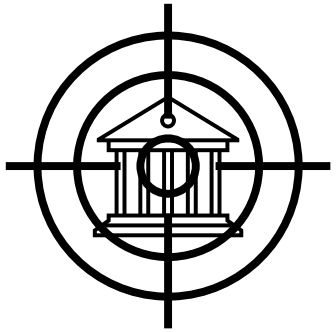
Smarter Adversaries

- Cybercriminals and nation-state actors are more organized, patient, and well-funded.
- Social engineering is the #1 tactic—not just technical exploits.

Evolving Tactics, Techniques & Procedures (TTPs)



- Shift from ransomware-only to **multifaceted extortion**, **B.E.C.**, and **supply chain attacks**.
- Cybercriminals use AI and automation to scale attacks faster than defenders can respond.



Government & Public Sector = Prime Targets

- Local governments are attractive: high trust, lower budgets, and lots of sensitive data.
- Legacy systems, limited MFA, and lack of user training widen the attack surface.

02

2025 COUNTY INCIDENT EXAMPLES

REAL INCIDENT EXAMPLES

November 2024 Incident – Nation State

- No MFA on VPN
- IOT device exploded (public utilities affected)
- RAT installed on multiple servers (ghostly mouse!)
- Purposefully no ransom or large data exfil

March 2025 Incident – Vendor Ransomware

- Vendor hardware the entry point
- Didn't inform county
- Flat network – TA moved around environment
- Data exfil & encrypted entire environment
- No backups

April 2025 Incident – MSP

- VM Level Encryption on MSP
- Data exfil of county data
- Ransom as a service model
- County had backups but still paid
  - Why: Data sensitivity

May 2025 Incident – Data Exposure

- Accounting folder on web server not private
- Exposed to internet
- ChatGPT ingested data

June 2025 Incident – Ransomware

- VPN Access – No MFA
- Viable Backups
- County had backups but still paid
  - Why: Data sensitivity

July 2025 Incident - BEC

- "Vendor" requested to setup ACH
- Accounting transferred $300k to threat actors
- Discovered 3 months later

03

SO WHAT DO WE DO ABOUT IT?

SEEING PATTERNS

COMMON ISSUES

- Limited or missing logging & retention configuration
- Endpoint detection not fully deployed or misconfigured
- Flat network
- Did not adhere to least privilege
- No immutable backup solution
- Improper MFA configuration (and bad passwords)
- Unpracticed IR process or no IR plan at all

TOP CONTROL RECOMMENDATIONS

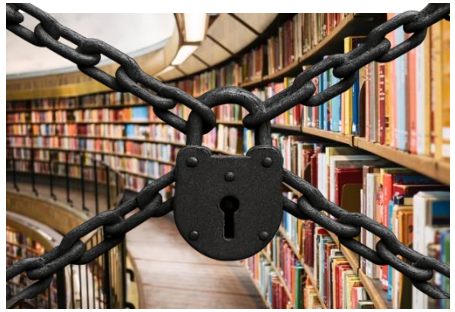
What would have stopped some of these attacks?

1. <u>STRONG</u> MFA with Conditional Access *Everywhere*

2. Network Segmentation

3. EDR/XDR + 90-day logging

4. Practice! (IR Tabletops)

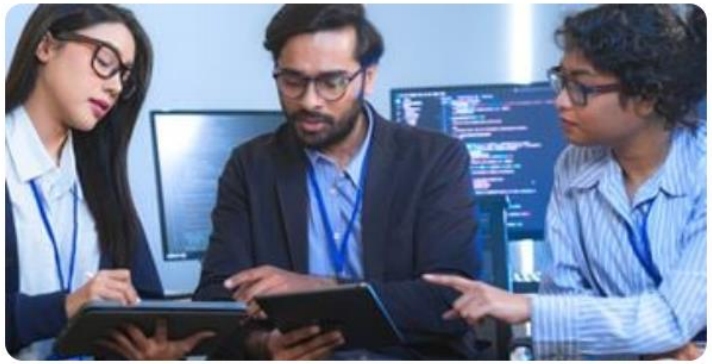


5. *Tested* Immutable backup solution

STAY AHEAD OF THE THREAT

Mitigating the Risk of Triple-Extortion Ransomware Attacks

Organizations can protect against triple-extortion ransomware attacks by understanding the complexity of the threat and investing in cyber resilience.



Cybersecurity on a Shoestring Budget

A Crowe cybersecurity specialist details free cybersecurity resources and tools that can help security teams build maturity despite limited resources.

Password Security Best Practices for 2025

Password security best practices, such as password managers, MFA, biometrics, and passwordless options, can help users stay safe online.

Thank you

Michael Salihoglu

Cyber Senior Manager and Penetration Tester

Crowe LLP

Michael.Salihoglu@crowe.com