Cybersecurity Landscape

Dr. Fred Cohen
CEO Management Analytics
2026-02-25
fc@manalyt.com
+1-831-200-4006

A discussion
- **I talk for a bit**
- **We discuss it**

Then, Now, and Next

- 2025-08 - The Dam Seems to be Breaking (all.net)
  - All Personally Identifiable Information has been leaked
    - All SSNs are being changed?!?
  - All widespread operating environments are breached
  - Bad advice is more widespread than good advice
  - Cognitive attacks are just beginning to emerge
    - Deep fakes, new spam, narrative attacks, LLMs
  - Automated attacks are getting easier
    - Attackers use AI to generate orders of magnitude more
  - Automated defenses are getting harder
    - We've automated for 75 years
    - But there are fundamental limits

On the other hand

- 2026 today
  - Privacy is gone but transparency is emerging (we hope)
    - It’s a lot harder to hide today
  - Emerging civil AI is going back to all/most things local
    - Sovereign AI cannon systems
  - Good advice is getting less expensive – if you can find it
    - Expertise is being automated and improved with AI
  - Cognitive defenses are starting to be noticed
    - CogSec is emerging as a discipline – not all technical
  - Attackers are not innovating as much
  - Time to adapt defenses is getting shorter
  - People are starting to ask more from big companies

What could possibly go wrong?

- At a basic level, it's this simple:
  - Assume all systems are vulnerable to arbitrary attack
    - Integrity, Availability, Use control, Accountability, Confidentiality, Transparency, Custody failures
  - Assume all systems are connected
    - You can get into anything if you know how and change anything if you don't screw up along the way
  - This is the price you pay for the benefits you get
    - So far: Longer, healthier, easier, happier life
- It's a matter of risk management:
  - Risk := uncertainty about the future
    - We can be certain we will all die → no risk: it's certain

They are also being exploited faster

Almost all of them are today

How has it helped you?
- **What would your life be like without it?**

What could possibly go right?

- At a basic level, it's this simple:
  - We usually get reasonable amounts of these:
    - Integrity, Availability, Use control, Accountability, Confidentiality, Transparency, Custody failures
  - The connectivity brings amazing capabilities
    - You can learn about anything, create a vast array of things, and change the world for the better
  - The benefits continue to accrue for now
    - So far: Longer, healthier, easier, happier life
- We are co-evolving with technology
  - We have been for a long time
    - We will continue to do so or perish over time

It has benefitted me
- **Pneumonia as a 2yo**
- **Spinal stenosis at 60**
- **The beat goes on**

Threats, Vulnerabilities, Consequences

- Threats:
  - Actors (individuals, groups, nature) acting (or failing to)
  - Intentionally or accidentally causing consequences
- Vulnerabilities:
  - When actors act (or fail to) undesired things happen
    - Your desires may not be mine.
- Consequences:
  - Bad things happen
    - Your version of bad may not be mine.
- Question:
  - Change threats, vulnerabilities, or consequences? How?

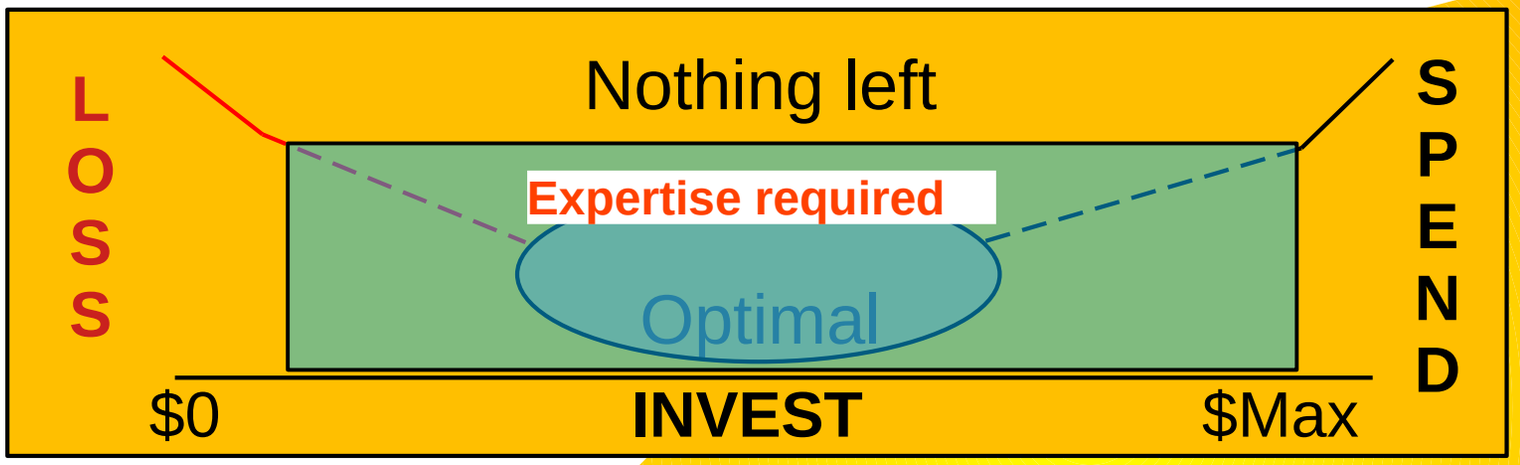
Stuxnet
- **Smashed Iran's nuclear …**
- **Good for us**
- **Bad for them**

Threats, Vulnerabilities, Consequences

- Change threats, vulnerabilities, or consequences? How?
  - People, by their nature, are imperfect
    - See “Frauds, Spies, and Lies and how to defeat them”
    - Training and awareness can only go so far
    - Why do we believe they can defend better than SW?
  - Vulnerabilities
    - Find and fix has failed for 75 years
    - We don’t have the NTSB for cyber – or much of the rest
    - Without a governance structure enforced, …
  - Consequences
    - Risk aggregation through centralization and lack of separation causes most of the large consequences

Two important concepts

- Under-invest
  - Fail
- Over-invest
  - Fail



Zero (no) trust cannot work

Unreasonable
Reasonable

Trust Architecture Works

Prudent
Imprudent

Unlimited trust doesn't work

- Trust is a core issue
  - Under-trusting
  - Over-trusting
- Trust Who/what
  - For what purpose
  - Over what time frame
  - To what extent

Conclusion: It's complicated – get expert help – keep getting more

Exaggerations

- The story of Chicken Little: The Sky is Falling!
  - It’s the end of the world as we know it
    - And I feel fine...
- Event sequences (things take time):
  - Anything is not everything (careful of viruses)
  - Attackers are not all knowing and all powerful
  - The “one mistake” fallacy
- Exaggerations:
  - Intentional, marketing to get more money from you
  - Accidental, lack of clarity and knowledge
    - Cyber Pearl Harbor? The thing that got the US to act?

What's really going on?

- Emerging attacks
  - We have been at war since
    - Information, influence, infrastructure
- If you look at US strategics...
- No longer:
  - **Post WW2 leader**
  - **World or even NATO lead**
  - **Moral high ground**
  - **Invincible against terror**
  - **Info Tech leader**
  - **Robotics leader**
  - **Manufacturing leader**

World War 3:

We are losing it
and most of us didn't even know we were fighting in it

Information Warfare Basics

by Fred Cohen, Ph.D.

Copyright (c) Fred Cohen 2006

Realities (a.k.a. Friday)

- What did you do to get here today?

CYBER THREAT BRIEF

The latest cyber threat and risk news.

New Keenadu Android Malware Found on Thousands of Devices

A new Android backdoor has been discovered by researchers. Kaspersky researchers discovered a new Android backdoor called Keenadu that was found preinstalled on many devices and also distributed through major app stores such as Google Play. The malware provides attackers full ... | **(Read More)**

French Government Says 1.2 Million Bank Accounts Exposed in Breach

French government officials have reported that millions of bank accounts have been compromised following a data breach. France's Ministry of Economy reported unauthorized access to the national FICOBA banking registry, exposing data on 1.2 million bank accounts. Stolen credentials from a ... | **(Read More)**

Nearly 1 Million User Records Compromised in Figure Data Breach

Blockchain based lender Figure has confirmed that it was the victim of a data breach. Blockchain-based lender Figure confirmed that nearly 1 million user records were exposed after an employee fell victim to a social engineering attack. The ShinyHunters group ... | **(Read More)**

German Rail Giant Deutsche Bahn Hit by Large-Scale DDoS Attack

Deutsche Bahn was the victim of a DDoS attack. Deutsche Bahn experienced a major DDoS attack that disrupted information systems, booking services, and its DB Navigator app for several hours. The attack began on February 17 and continued into February 18, ... | **(Read More)**

Name, Email Address

City/State/Zip

New login ID

Verify cognitive limitations

Verify receipt of email

Get an account

Provide a password

Sign up for further contact

Provide browser&system info

- All that for a URL!?!?
- If it's free you are the product!

Realities (a.k.a. Weekend)

Meta Director of AI Safety Allows AI Agent to Accidentally Delete Her Inbox

EMANUEL MAIBERG · FEB 23, 2026 AT 10:20 AM

Character-Level Perturbations Disrupt LLM Watermarks

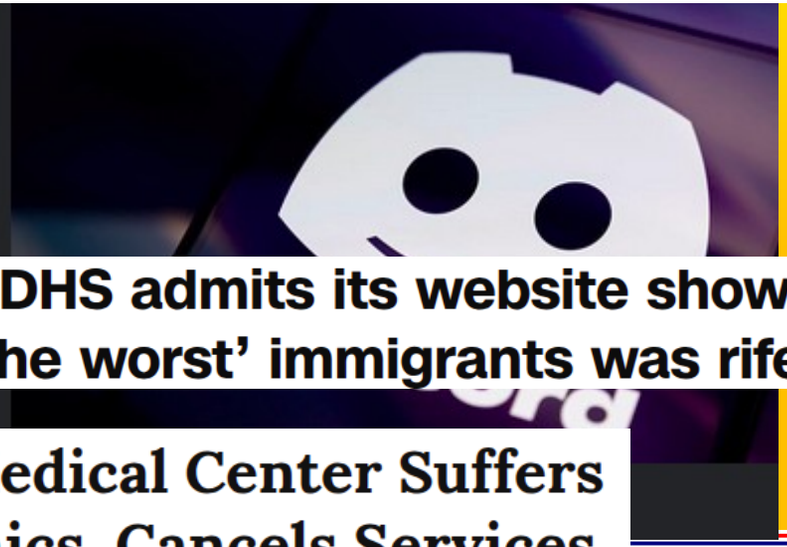
Significantly more than half of the phishing attempts I see now come from Google email servers (as proven by the top Received: header line), typically Gmail. An even larger percentage of the payloads (e.g. "click this link") for these -- closer to 75% these days -- point to GCP (Google Cloud Platform) instances (e.g. via googleapis.com). Google puts a lot of effort into detecting incoming spam and phishes (with varying success) but has become a veritable firehouse of such garbage sent to non-Gmail addresses.-L

BROKEN TRUST

Fury over Discord's age checks explodes after shady Persona test in UK

Persona confirmed all age-check data from Discord's UK test was deleted.

ASHLEY BELANGER –



Exclusive: DHS admits its website showcasing the 'worst of the worst' immigrants was rife with errors

University of Mississippi Medical Center Suffers Cyberattack, Closes All Clinics, Cancels Services

Realities (Privacy)

I VERIFIED MY LINKEDIN IDENTITY. HERE'S WHAT I ACTUALLY HANDED OVER.

FEB 16, 2026 · 10 MIN READ · PRIVACY, LINKEDIN, BIOMETRICS, GDPR, CLOUD-ACT, IDENTITY

- My **full name** — first, middle, last
- My **passport photo** — the full document, both sides, all data on the face of it
- My **selfie** — a photo of my face taken in real-time
- My **facial geometry** — biometric data extracted from both images, used to match the selfie to the passport
- My **NFC chip data** — the digital info stored on the chip inside my passport
- My **national ID number**
- My **nationality, sex, birthdate, age**
- My **email, phone number, postal address**
- My **IP address, device type, MAC address, browser, OS version, language**
- My **geolocation** — inferred from my IP

And then there's the weird stuff:

- **Hesitation detection** — they tracked whether I paused during the process
- **Copy and paste detection** — they tracked whether I was pasting information instead of typing it

Behavioral biometrics. On top of the physical biometrics. For a LinkedIn badge.

// THEY ALSO CALLED THE

Persona didn't just use what I gave them. of trusted third-party data sources":

- Government databases
- National ID registries
- Consumer credit agencies
- Utility companies
- Mobile network providers
- Postal address databases

I scanned my passport for a checkmark. T

Realities (This morning)

Hundreds of FortiGate Firewalls Hacked in AI-Powered Attacks: AWS
FortiGate devices have been compromised in a global campaign using generative AI to exploit vulnerabilities. More than 600 Fortinet FortiGate devices were compromised in a global campaign relying on generative AI to exploit exposed management ports and weak passwords. Attackers ... | **(Read More)**

PayPal Data Breach Led to Fraudulent Transactions
A PayPal data breach lead to a small number of unauthorized transactions. PayPal disclosed that an application error in its PayPal Working Capital loan system exposed customer data for nearly six months. The exposed information included names, contact details, birthdates, phone ... | **(Read More)**

US Healthcare Diagnostic Firm Says 140,000 Affected by Data Breach
US based healthcare firm Vanta Diagnostics has been the victim of a ransomware attack. Nearly 140,000 individuals had their personal and medical data compromised in a breach involving Vikor Scientific, now rebranded as Vanta Diagnostics. The breach originated not from ... | **(Read More)**

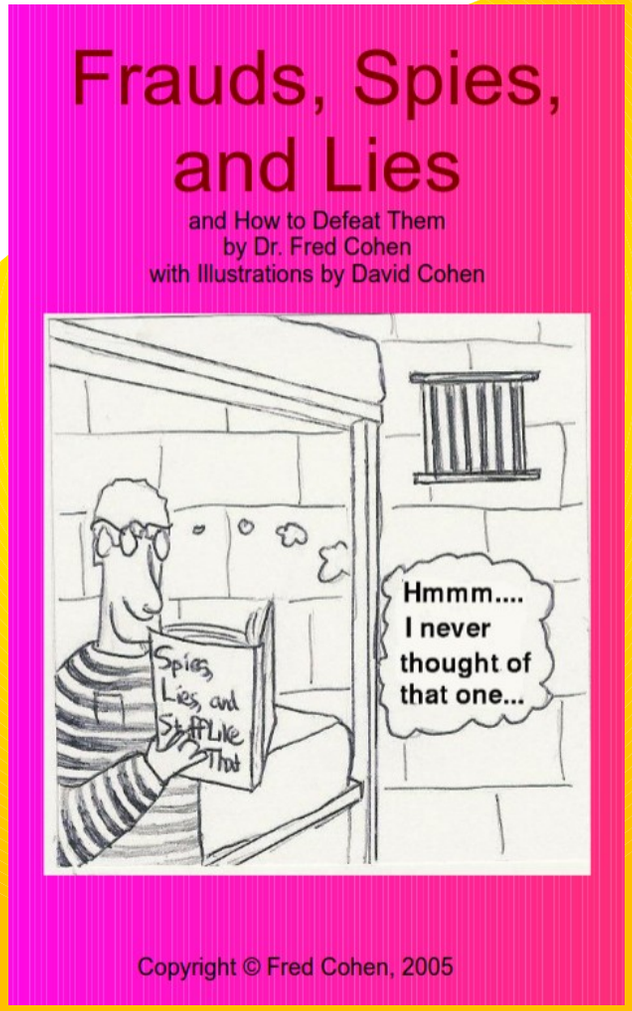
Mississippi Hospital System Closes All Clinics After Ransomware Attack
A ransomware attack forced a Mississippi hospital system to shutdown nearly all operations. A ransomware attack forced the University of Mississippi Medical Center to shut down all 35 of its clinics and cancel elective procedures statewide. Officials warned the outage could ... | **(Read More)**

New Keenadu Android Malware Found on Thousands of Devices
A new Android backdoor has been discovered by researchers. Kaspersky researchers discovered a new Android backdoor called Keenadu that was found preinstalled on many devices and also distributed through major app stores such as Google Play. The malware provides attackers full ... | **(Read More)**

- Once site updating this morning with a few new items from yesterday…
- It’s just another day
- And it will continue day after day
- Most of these are easily preventable
- But most entities don’t know how to defend themselves
- ~120,000 experts today

What can you do about it?

- Some recent stuff
  - Everyone is an insider
  - Narrative viruses
  - AI for attack and defense
  - Extortion (a.k.a.) / ransomware
- Evolution
  - Job losses and the newer economy?
- Continue the mission?
  - What's my mission?
  - What do you want yours to be?
  - **Our mission is to help you achieve yours**



Thank You

Trusted Advisors Since 1977

Management Analytics

Boots2Bytes®