FrontLine Cyber Solutions

Cyber Security – What we as an industry are doing wrong?

Mr. William Hoffman

Who am I

- Co-Founder & CSO at FrontLine Cyber
  - https://www.frontlinecyber.com
- Exploit research and development
- Red Team and Blue Team
- 25+ years in Cyber Security
- William Hoffman @ LinkedIn
- whoffman@frontlinecyber.com

Today's Topics

- Quick history of Cyber Security.
- Attackers.
- Breaches.
- What we as an industry are doing wrong?
- Leveraging AI in Cyber Security
- Questions?

Quick History of Cyber Security

- We will start in the 1970s with ARPANET
  - Creeper (virus) / Reaper (antivirus)
  - Unauthorized access to systems
  - Password authentication
  - Unix OS
- Moving on to the 1980s
  - TCP/IP becoming widely used
  - Commercial antivirus created
  - Backdoors in software (War Games)
- Moving on to the 1990s
  - Systems move on to the World Wide Web (www)
  - Early Phishing Attempts
  - Creation of DefCon Security Conference – June 1993
  - L0pht Heavy Industries founded in 1992 (Testified in front of Congress in 1998 on the topic of 'Weak Computer Security in Government)

FRONTLINE CYBER SOLUTIONS

Throwback

Peiter “Mudge” Zatko

L0pht Co-Founder vs CIO of DARPA

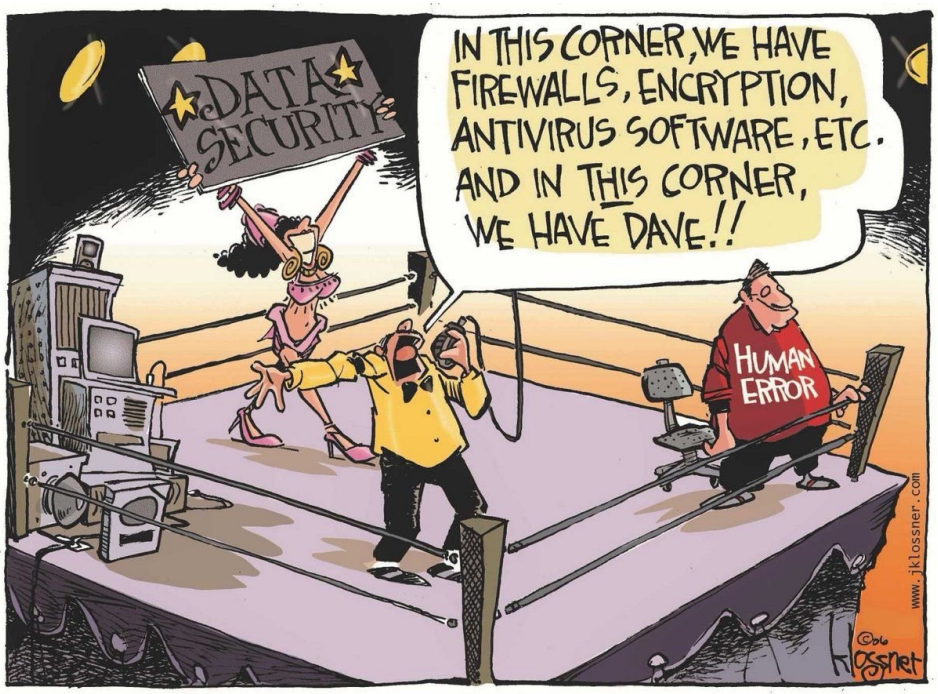
Quick Look at the 2000s

Year	Threat / Malware	Type / Vector	Key Impact / Significance
2000	ILOVEYOU	Email worm	Massive spread via Outlook; millions infected.
2001	Code Red	Web server worm	Exploited IIS; fast spread; DDoS attacks (e.g. White House).
2003	SQL Slammer	Database worm	Spread in minutes; global network slowdowns.
2008	Conficker	Botnet worm	Huge botnet across many countries; showed persistence.
2010	Stuxnet	ICS/SCADA worm	First major state-sponsored infrastructure attack; damaged centrifuges.
2017	WannaCry	Ransomware worm	Used EternalBlue; hit 200,000+ systems, including hospitals; huge financial damage.

Attackers

- Today we are seeing attacks come from all different kinds of threat actors.
  - Nation States
  - Ransomware Groups
  - Corporate espionage
  - Ecoterrorism

What about Dave? (Human Error)



Attackers cont…

So, what about Dave?

- We have seen systems that are not fully hardened.
- Misconfigured systems deployed to production.
- User not following security awareness training.

- Security risk assessments over the past 4 years, we have seen a lack in security approach.
  - Missing security patches
  - Missing endpoint protection
  - No central monitoring (Security operations center or SIEM)
  - 3rd party vendors not allowing systems to be updated
  - Normal users have admin rights
  - Users clicking on links and submitting creds.

Breaches

- Salesforce
  - The attacks did not exploit a vulnerability within the core Salesforce platform, but relied on compromised OAuth tokens for Salesloft Drift, a third-party AI chat bot.
- Akira Ransomware
  - Targeted organizations using SonicWall Gen 7 firewalls with SSL VPN enabled, initially suspected as exploiting a zero-day vulnerability, but later traced to the known CVE-2024-40766
- NPM Packages / CrowdStrike
  - An ongoing supply chain attack has compromised multiple npm packages published by CrowdStrike, extending a malicious campaign known as the “Shai-Halud attack”.

Sidenote

- On July 23, 2025, CrowdStrike put out the following –
  - CrowdStrike Falcon Prevents Supply Chain Attack Involving Compromised NPM Packages
- On September 16, 2025
  - A new supply chain attack has compromised multiple npm packages maintained by the crowdstrike-publisher account, marking a worrying continuation of the so-called “Shai-Halud attack.”
  - Developers and organizations using these packages should take immediate action to safeguard credentials and prevent unauthorized code execution.

What we as an industry are doing wrong

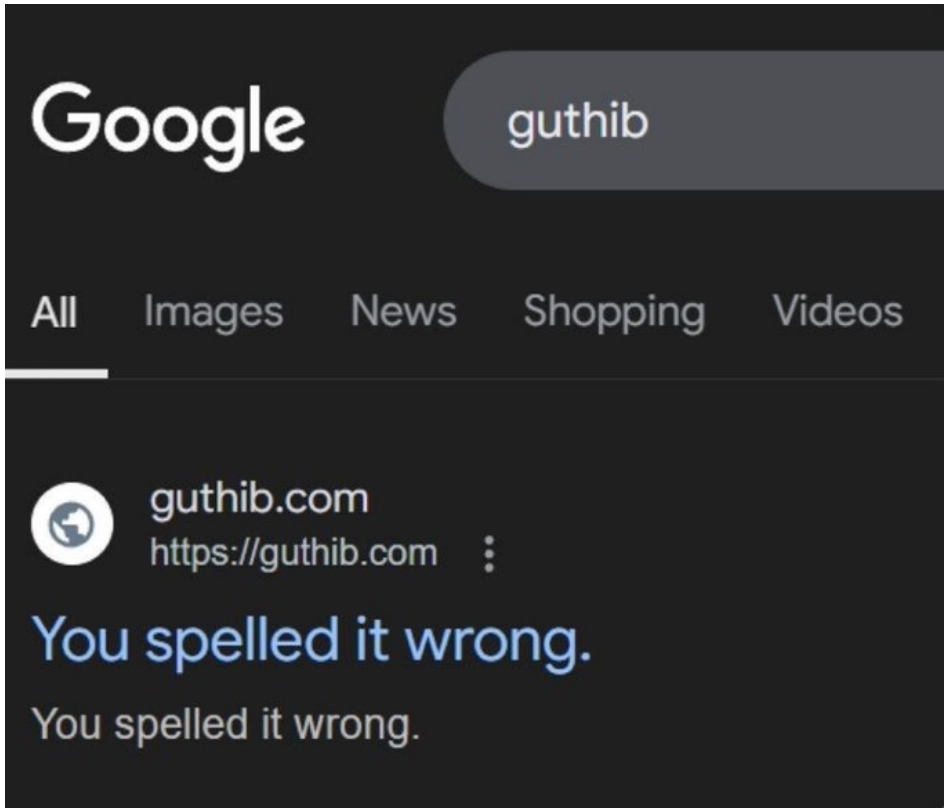
- Since the 1980's we have been fighting cyber attacks
- Since the 1990's with DefCon and Conferences for security awareness

- What are we missing? We are seeing the same type of attacks since then, and we have had "Standards / Framework" since 2005

  - NIST 800-53 – Started in 2005
  - NIST SP 800-171 - Started in 2015
  - Now we have CMMC
- Five areas where all three overlap
  - **Cryptographic, Access Control**, **Configuration & System Hardening**, **Protection of Data in Transit**, **and Auditability & Compliance**

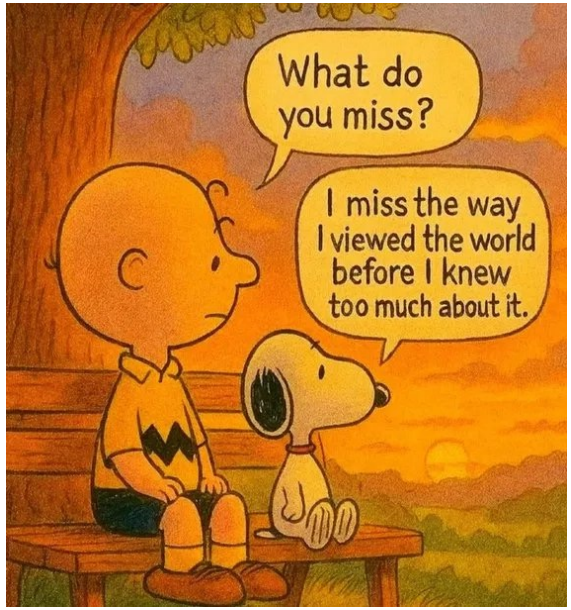
What we as an industry are doing wrong cont…

- Cyber Security 101 – Know thyself.
  - We come across so many companies that have no asset list, asset information or know what is on their network.
- Normal users with Domain level access.
- Unsecure software – Bad software development and bad coding practice
- User still clicking on links, installing software, reusing password, and sharing creds with attackers.



How do we fix this issue?

- Asset inventory
- Hardening systems
- Patching systems and firmware
- System monitoring and reporting
  - (Attacks will happen, we need to detect them)
- Endpoint protection
- Secure Software development and testing
- Tabletop exercises
- BC/DR Plans
- Playbooks (Formerly Runbooks) – Old School SOPs
- **Important number 1 – Security awareness training**
- **Important number 2 – Executive Team buy in**



Leveraging AI in Cyber Security

Pros

1. **Threat Detection at Scale**
AI can analyze enormous volumes of network traffic, logs, and endpoint data much faster than human analysts.

2. **Predictive Capabilities**
By identifying patterns of attacker behavior, AI can forecast likely attack paths or detect early indicators of compromise (IoCs), giving defenders more time to react.

3. **Automation of Repetitive Tasks**
AI reduces analyst fatigue by automating routine tasks like malware classification, triage of alerts, and patch prioritization. This allows human teams to focus on higher-level investigations and strategy.

4. **Improved Accuracy Over Time**
Well-trained AI models can adapt to evolving threats by continuously learning from new data, reducing false positives compared to rule-based systems.

5. **Faster Incident Response**
AI-driven security orchestration and automated playbooks enable quicker containment and remediation (e.g., isolating compromised endpoints within seconds).

6. **Insider Threat & Anomaly Detection**
AI excels at spotting subtle deviations in user or system behavior, which is crucial for detecting insider threats or compromised accounts.

Cons

1.**Adversarial Attacks Against AI**
Attackers can manipulate AI models with adversarial inputs (e.g., data poisoning, evasion techniques) to bypass detection or cause misclassification.

2. **High False Positives / Negatives if Poorly Trained**
If not properly trained on diverse, high-quality datasets, AI can overwhelm analysts with false alerts or miss sophisticated threats.

3. **Cost and Resource Intensive**
Building, training, and maintaining AI systems requires specialized talent, computational power, and ongoing investments—barriers for smaller organizations.

4. **Lack of Explainability**
AI decisions (especially deep learning models) are often “black boxes.” This lack of transparency makes it harder for analysts to trust or validate alerts.

5. **Data Privacy Risks**
AI systems require large datasets for training, which may involve sensitive user or organizational information. Improper handling can lead to compliance issues.

6. **Dependence and Overconfidence**
Organizations may become overly reliant on AI tools and underinvest in human expertise, leaving them vulnerable if the AI is compromised or fails.

Questions?

whoffman@frontlinecyber.com