phuse·share
connect·share·advance

Single Day Event

Cybersecurity in Pharmaceutical Industry

Maharajan S
Navitas Life Sciences

phuse.global

Current trends - pharma industry

*Pfizer's deployed **GenAI** copilots reduced **search time by 80%** and saved over **16000** researcher hours annually.*

*NVIDIA's BioNeMo cloud platform offers **Gen AI** models for **chemistry tasks**. faster hit-to-lead cycles and improved **molecular binding**.*

*Aggressive hardware roadmaps, and regulatory alignment are accelerating **quantum computing adoption** - NVIDIA launched **BioHive-2** & Google opened **Sycamore v2***

*AstraZeneca Achieves 20x Speed-Up in **Quantum Chemistry Pipeline***

*FDA approved two investigational new drug (IND) applications for **3D-printed oral capsules**: T20G and T22 – both developed by Triastek*

***Digital twins** evolved into full-scale platforms to support **pharma factory operations, clinical development** and **real-world evidence (RWE**).*

*Fully **robotic SKAN-pod system** tailored for clinical-scale fill-finish by Selkirk Pharma. fully enclosed isolators without glove ports and **eliminate human intervention***

Investment - Pharma Industry

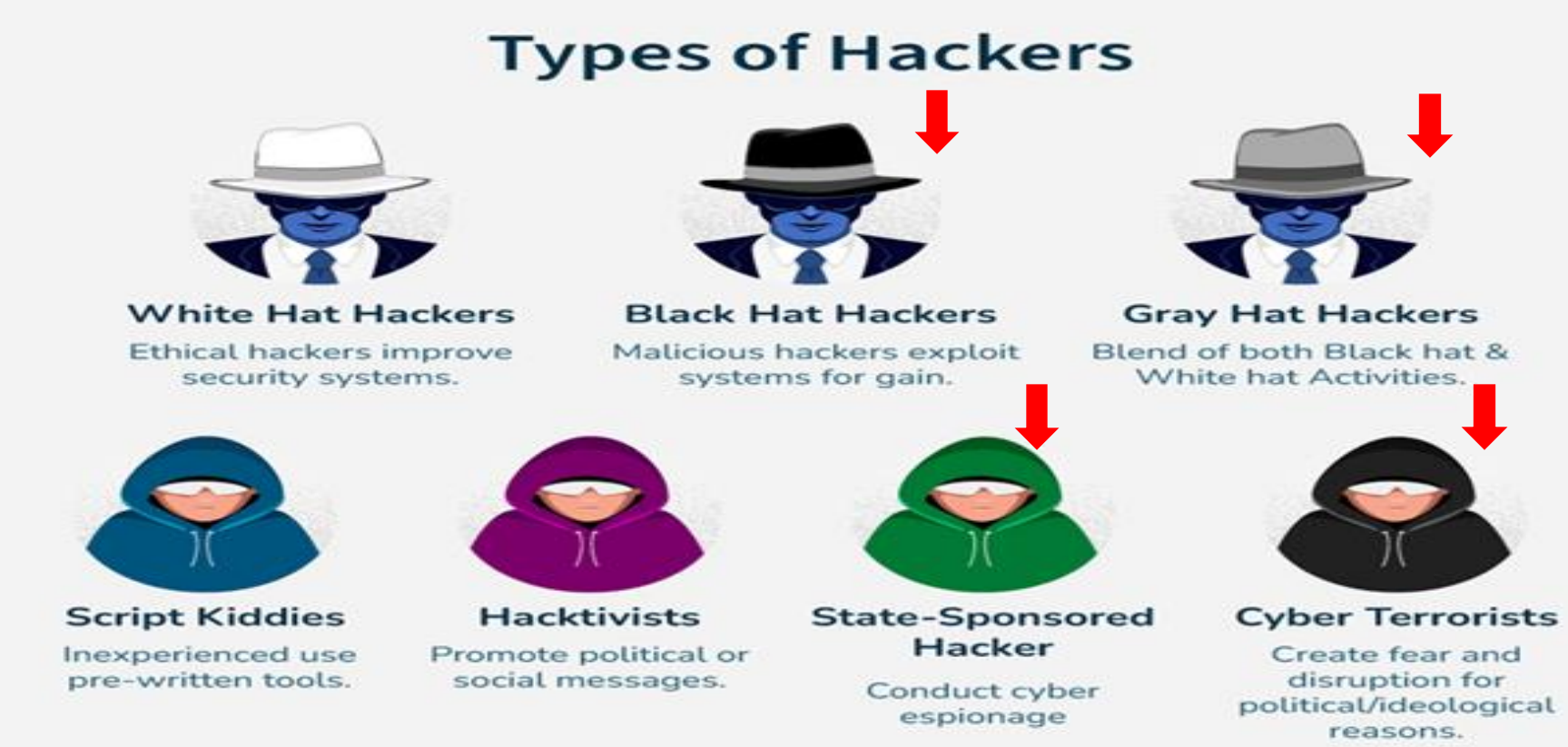
- Scalable **Cell & Gene Therapies** for common diseases; **$26B funding**.
- **Generative AI** designed drugs in trials; **$45B investment**.
- **Quantum Computing**: Speeds drug design; **$1.25B invested**.
- FDA-approved polypills by using **3D-Printed Medicines - $790M** market by 2034.
- **Robotic Fill-Finish**: reduce contamination & zero human intervention - **€1.1B** invested.
- **Digital Twins**: Boost R&D and trials; 67% faster development.
- Other major investments are in **Smart Manufacturing, Blockchain, Low-Carbon Operations, Agile Regulation…**

I am watching 😉😱😨

Cyber Crime Trends and Impact in 2025

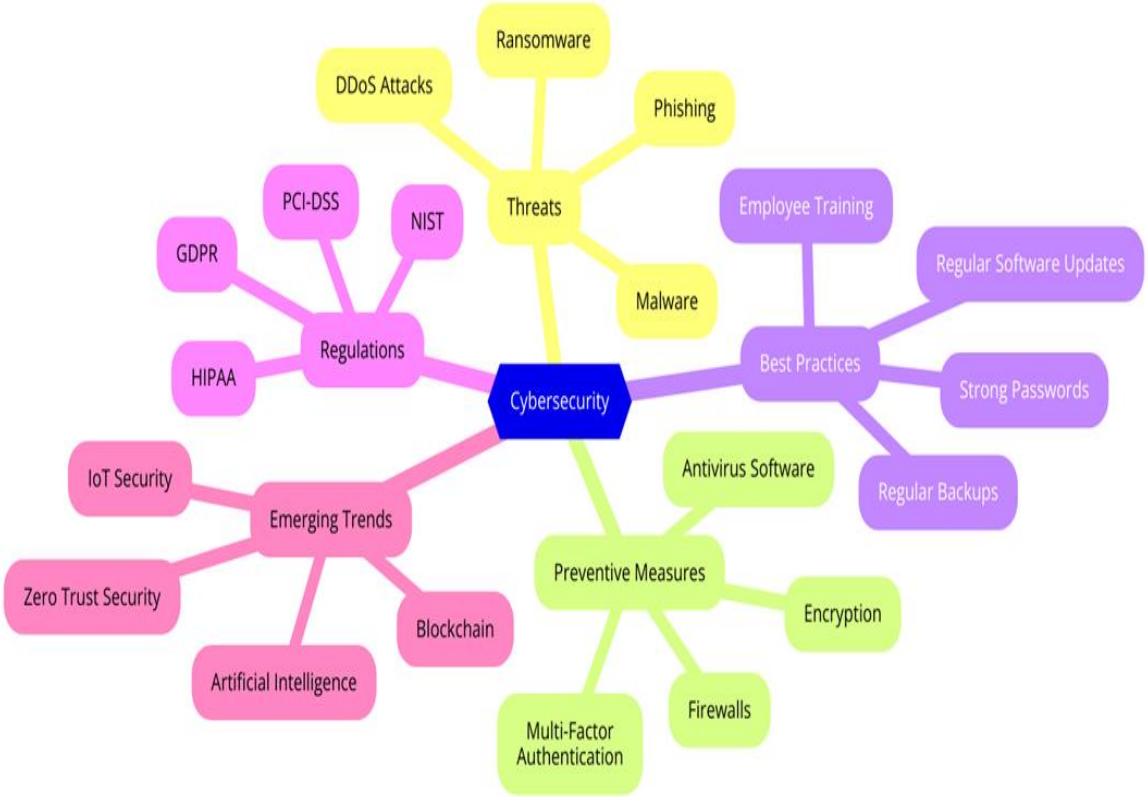
- **$12 Trillion**: Estimated global cost of cybercrime by 2025.
- **500% Increase**: Surge in median ransomware payments in 2024.
- **$1.5 Billion**: Theft by North Korean hacker group TraderTraitor from Bybit's crypto currency exchange.
- **$600**: Average price of stolen passport data on the dark web.
- **32%**: Phishing attacks in Q4 2024 exploited Microsoft's brand.
- **50%**: BEC emails were generated using generative AI technologies.

Types of Hackers



What is Cybersecurity

- ***Cybersecurity*** *is the practice of* ***protecting systems, networks, and data*** *from digital attacks, unauthorized access, and damage.*
- *Involves a combination of* ***technologies, processes, and practices*** *designed to safeguard information and ensure the* ***confidentiality, integrity, and availability*** *of data.*



Cybersecurity Incidents - Pharma

- **Sun Pharma (2023)**
  Hit by a ransomware attack that disrupted operations and exposed sensitive data
- **Pfizer Cloud Leak (2020)**
  Misconfigured Google Cloud database led to exposure of clinical trial data
- **Change Healthcare (2024)**
  Largest healthcare breach in history—190 million records compromised
- **Cencora Supply Chain Attack (2024)**
  Disrupted operations across 11 pharma companies incl, Novartis, Bayer, GSK, Abbvie etc… due to impact on supply chain vulnerabilities.
- **Merck & Co. (2017)**

  Ransomware attack disrupted **global** operations & 30,000 computers affected; $870M in damages

Dragonfly - Russia

TradeTraitor North Korea

Winnti - China

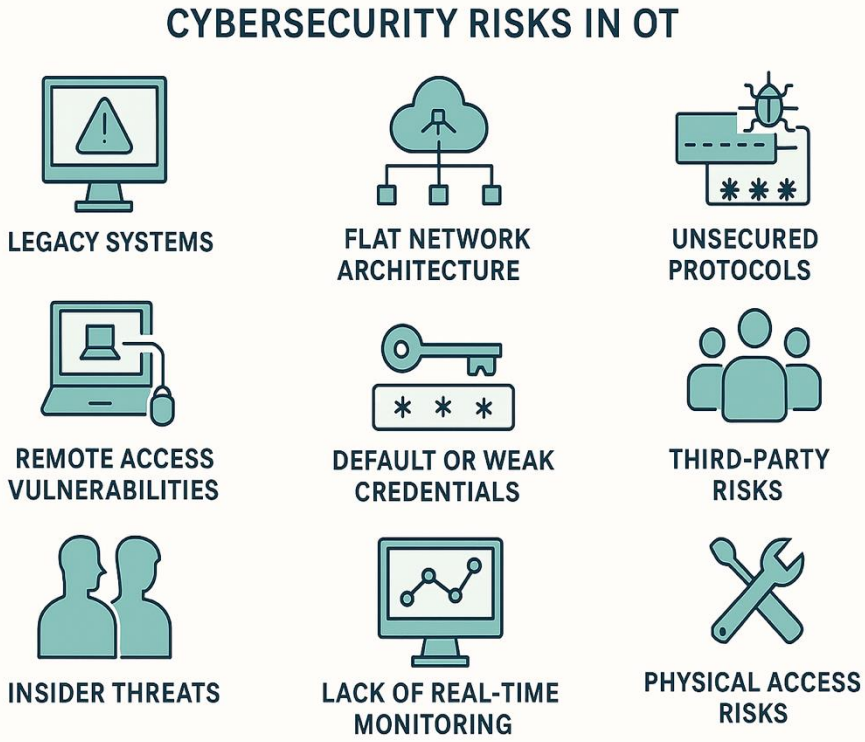
APT41 - China

Govt or State-sponsored hacker group – Called it as a Intelligence services

Cybersecurity Threats

- **Ransomware Attacks**: Encrypt sensitive data and demand payment for decryption.
- **Phishing & Social Engineering**: Trick users into revealing data or installing malware.
- **Data Breaches**: Unauthorized access to sensitive data, leading to penalties and loss of trust.
- **Supply Chain Attacks**: Third-party compromises disrupt operations and introduce malware.
- **Intellectual Property Theft**: Stealing drug formulas, clinical data, or manufacturing secrets.
- **Insider Threats**: Employees or partners cause harm—intentionally or through negligence.
- **Cyber Espionage**: Spying by competitors or state actors to gain strategic advantage.
- **Emerging Technologies**: IoT, cloud, and connected devices introduce new vulnerabilities.

Cybersecurity Risks – Pharma OT devices



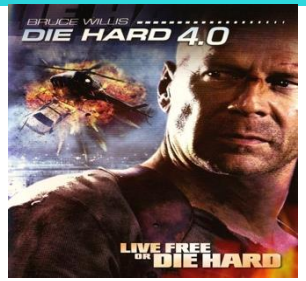
Some of the OT Systems in Pharma

- **SCADA Systems:** Used for centralized monitoring of cleanrooms, HVAC, and water systems.
- **PLC Controllers:** Manage batch processing, mixing, and packaging operations.
- **Building Management Systems (BMS):** Control environmental conditions critical for GMP compliance.
- **HMI Panels:** Human-Machine Interfaces used by operators; vulnerable to physical and network-based attacks.

Cybersecurity Risks – OT device Vulnerable

Die Hard 4.0 (Live Free or Die Hard)

- **SCADA Role**: A fictional SCADA system called *"the grid"* is used by terrorists to control traffic lights, power stations, and infrastructure.
- **Relevance to Pharma**: Demonstrates how poor SCADA security can lead to disastrous control loss

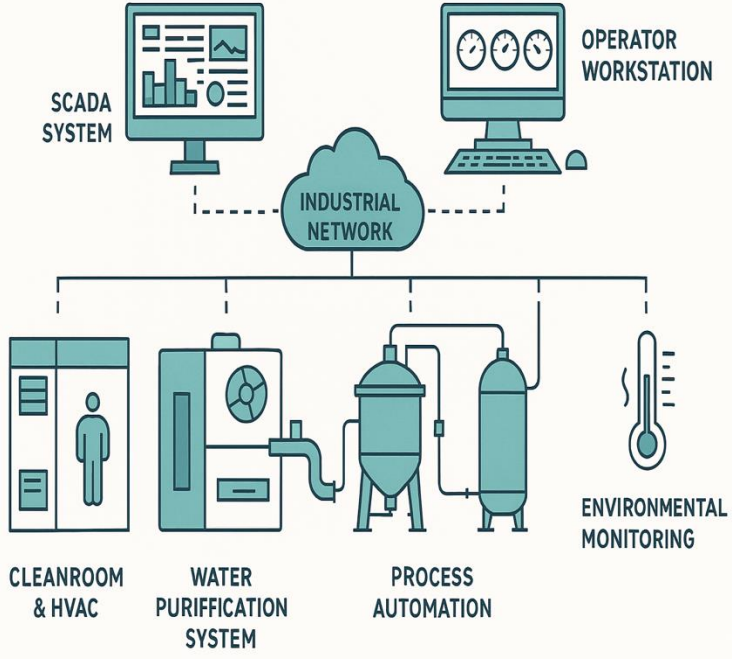


The Girl with the Dragon Tattoo

- **SCADA-Like Scene**: Hacker plants a physical device in a network cabinet to gain access.
- **Relevance to Pharma**: Demonstrates physical security risks in server rooms and control panels

The Bourne Legacy

- **SCADA Role**: Used by the CIA to monitor agents via GPS and biometric data.
- **Relevance to Pharma**: Highlights surveillance and control risks—similar to pharma's use of SCADA for environmental monitoring and compliance



Cybersecurity Risks in Biostatistics & RWE

Biostatistics involves analyzing clinical trial data (Data science) – often sensitive and regulated.

- **Data Integrity**
  - Risk of unauthorized changes to clinical trial datasets and Impact on statistical outcomes and regulatory submissions.
- **Access Control**
  - Unauthorized access to statistical tools and sensitive data.
- **Tools Security**
  - Risks from unpatched or misconfigured statistical software (e.g., SAS, R). Potential for malicious scripts or insecure libraries.

Real World Evidence (RWE) uses data from EHRs, claims, registries, and wearables — often from external sources.

- **Data Aggregation Risks**
  - Insecure APIs or data pipelines from hospitals, or 3rd parties. Risk of data poisoning or leakage.
  - Vendors and data providers may introduce vulnerabilities.
- **Patient Privacy**
  - Re-identification risks from de-identified datasets. And Compliance challenges with GDPR and HIPAA.
- **Cloud & AI Security**
  - Misconfigured cloud environments used for RWE analytics.
  - Risks in AI/ML models trained on sensitive health data

Cybersecurity Best Practices

- **Network & Infrastructure Security**
  - Segment networks to isolate critical systems.
  - Use encryption for data at rest and in transit.
  - Adopt ISA-99 / IEC 62443 standards for OT environments.
- **Access Control & Identity Management**
  - Implement Zero Trust architecture.
  - Enforce Multi-Factor Authentication (MFA).
  - Use Role-Based Access Control (RBAC).
- **Operational Technology (OT) Security**
  - Align with FDA's cybersecurity guidance for medical devices.
  - Use asset discovery and microsegmentation tools.
  - Design systems with security built-in from the start.
- **Data Integrity & Compliance**
  - Follow ALCOA+ principles for data governance.
  - Maintain audit trails and use digital signatures.
  - Consider blockchain storage for immutability.
- **Threat Detection & Incident Response**
  - Deploy real-time monitoring across IT and OT.
  - Establish and test incident response plans.
  - Validate backups and ensure business continuity.
- **Vendor & Supply Chain Risk Management**
  - Conduct cybersecurity assessments of 3rd party vendors.
  - Secure IT integration during mergers and acquisitions.
- **Employee Awareness & Training**
  - Provide regular anti-phishing and cybersecurity training.
  - Promote secure remote work practices (VPNs, endpoint protection).

Cybersecurity Dos & Don’ts

Dos

- **Use Strong Passwords & MFA**
  Combine complex passwords with multi-factor authentication to secure access.
- **Encrypt Sensitive Data**
  Protect patient records, clinical trial data, and IP with robust encryption.
- **Update Systems Regularly**
  Patch legacy systems and IoT devices to close known vulnerabilities.
- **Report Suspicious Activity**
  Notify IT immediately about phishing attempts or unusual system behavior.
- **Secure Remote Access**
  Use company-approved VPNs and avoid public Wi-Fi for work-related tasks.
- **Follow Access Controls**
  Access only the data and systems necessary for your role.

Don’ts

- **Don’t Share Credentials**
  Never share passwords or access tokens—even with trusted colleagues.
- **Don’t Click Unknown Links**
  Avoid clicking on links or downloading attachments from unsolicited emails.
- **Don’t Use Unauthorized Devices**
  Refrain from connecting personal USBs or external drives to company systems.
- **Don’t Ignore Security Alerts**
  Take all system warnings seriously and consult IT if unsure.
- **Don’t Store Data Locally**
  Use secure cloud or network storage—never save sensitive data on desktops.
- **Don’t Bypass Security Protocols**
  Always follow company-approved procedures, even if they seem time-consuming.

Real Cybersecurity advice from them…

Now you will listen- Real Cybersecurity advice

Sholay Meets Cybersecurity in Pharma

The CISO

Vision and leadership are key

Security Teams

Collaboration is essential

Cyber Threats

Always evolving, always dangerous

Village

Ensure resilient defenses

End Users

Train and protect your people

Poor Cyber Hygiene

Don't be careless with your data

Pharma Infrastructure

Ensure resilient defenses

New Avatar of Cybersecurity - AI vs AI

AI in Cybercrime

- **Weaponized AI Models: -** Insert harmful code into pre-trained AI/ML models to execute a ransomware attack.
- **AI Poisoning Attacks:** Attackers change the data that AI/ ML model learns from, which can either damage the model or even alter its output.
- **Data Security Breaches:** If AI models are not designed with enough privacy safeguards, attackers can expose the privileged information of the data used to train those models.
- **Sponge Attacks:** Modern type of Denial-of-Service attack called a sponge attack. aims to make an AI inaccessible.
- **Prompt Injection:** new avatar of SQL injection is a prompt injection. Attackers use harmful prompts to make generative AI produce wrong or malicious output**.**
- **AI-Created Phishing Traps:** Attackers use AI to enhance their phishing attacks by using generative AI.
- **Deepfake Threats:** Making it very simple to fake a CEO or other executive in order to trick workers into falling for business email compromise and other frauds.

AI in Cybersecurity

- Predictive Threat Intelligence
  - Predict and prevent attacks before they happen.
  - Protect clinical trial data and IP..
- Autonomous Response Systems
  - Automatically isolate infected devices, block malicious traffic, and alert teams in real-time.
- AI-Powered SOCs (Security Operations Center)
  - AI helps prioritize alerts, reduce false positives, and accelerate incident response.
- Secure AI Models
  - Pharma companies are investing in AI model security to prevent data poisoning and adversarial attacks.

Potential AI Fraud in Pharma

- AI enables fake drug distribution by manipulating supply chain data and packaging authenticity.
- AI hacker compromise 3D Printer & alters the pill & drug printing…without changing its appearance
- Cybercriminals could remotely hijack robotic arms used in isolators.
- AI systems using high-resolution cameras to detect defects can be tricked and bypass defect detection.
- IoT vulnerabilities in logistics systems are exploited to reroute or replace shipments.
- Attackers manipulate AI training data to twist clinical trial outcomes.
- Insider misuse of Gen AI tools (e.g., ChatGPT) can lead to data leaks to outside.
- Deepfakes used to spread false claims about drug safety or efficacy, damaging public trust and stock value.

AI vs AI will define the next era of cybersecurity.

AI vs AI will define the next era of cybersecurity.

- “AI vs. AI” isn’t just about technology battling itself. It’s a story of innovation, redemption, and digital integrity….

Always Vigilant – We’re going to survive.

The Global Healthcare Data Science Community

Contact Channels

UK +44 1843 609600
office@phuse.global
phuse.global

Social Media

@phusetwitta
/phusebook
/phusetube
/company/phuse