

One day Seminar at Institution of Engineers,
UP State Centre, Lucknow
on
“Digital Wellbeing and Cyber Security”

Technical Talk
Cyber Security Awareness & Its Importance in
Industrial Internet of Things

Prof.(Dr) Neelam Srivastava
Department Of Electronics and Communication
Institute of Engineering and Technology Lucknow
Dean, Training and Placement, AKTU Lucknow
Member ET,IEI,UP State Centre Lucknow



Evolution of Industries
Industry 1.0 (Late 18th Century – Mechanization)

- Introduction of Steam Engines and Water power.
- Mechanization of Textile, Agriculture, and Manufacturing.
- Shift from hand production to Machine-based production.
- Example: Steam locomotives, mechanized weaving.

Industry 2.0 (Late 19th – Early 20th Century – Mass Production)

- Adoption of **Electricity** and **Assembly lines**.
- Start of **Mass production** and **Economies of scale**.
- Introduction of **telegraph** and **telephone** for communication.
- Example: Henry Ford's moving assembly line for cars.



Industry 3.0 (Mid-20th Century – Automation & IT)

- Rise of **Electronics, IT systems, and Automation.**
- Use of **Computers, Robotics, and Programmable Logic Controllers (PLCs).**
- Digital revolution: faster production, less manual intervention.
- Key example: Automated manufacturing and early robotics in factories.

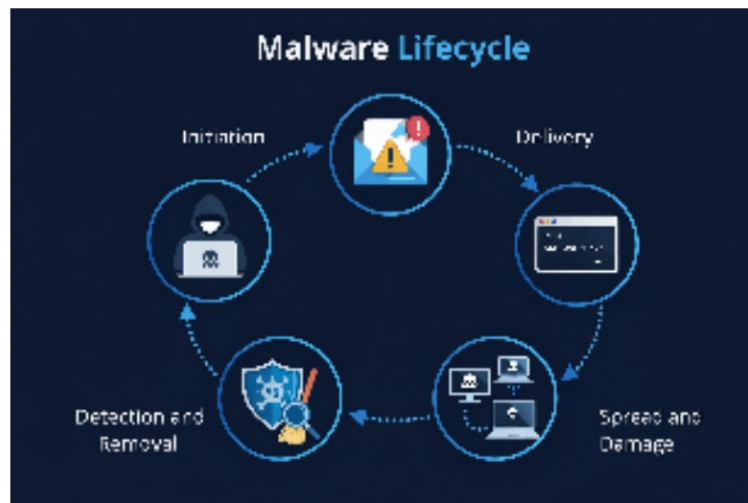
Industry 4.0 (21st Century – Cyber-Physical Systems & Smart Manufacturing)

- Integration of IoT, AI, Big Data, Cloud Computing, and Cybersecurity.
- Development of **smart factories** with real-time monitoring.
- Use of **digital twins**, predictive maintenance, and advanced robotics.
- Focus on **connectivity**, efficiency, flexibility, and personalization.
- Example: Smart factories, autonomous production lines, 3D printing.

Cyber Security and its Importance

- Cyber Security is the practice of protecting digital devices, networks, and sensitive data from cyber threats such as hacking, malware, and phishing attacks.
- It involves a range of strategies, technologies, and best practices designed to safeguard computers, networks, and data from cyber attacks.

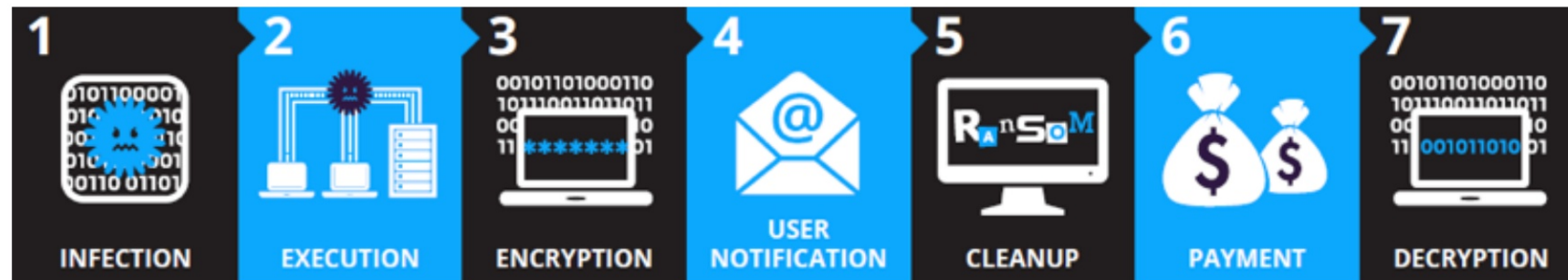
Cyber Threats in Society



Ransomware is a type of malware attack in which the attacker locks and encrypts the victim's data, important files and then demands a payment to unlock and decrypt the data.

Identity theft occurs when a cybercriminal uses another person's personal data like credit card numbers or personal pictures without their permission to commit a fraud or a crime.

Ransom ware Cyber threat



1. **Infection**—Ransomware is covertly downloaded and installed on the device.

2. **Execution**—Ransomware scans and maps locations for targeted file types, including locally stored files, and mapped and unmapped network-accessible systems. Some ransomware attacks also delete or encrypt any backup files and folders.

3. **Encryption**—Ransomware performs a key exchange with the Command and Control Server, using the encryption key to scramble all files discovered during the Execution step. It also locks access to the data.

4. **User Notification**—Ransomware adds instruction files detailing the pay-for-decryption process, then uses those files to display a

ransom note to the user.

5. **Cleanup**—Ransomware usually terminates and deletes itself, leaving only the payment instruction files.

6. **Payment**—Victim clicks a link in the payment instructions, which takes the victim to a web page with additional information on how to make the required ransom payment. Hidden TOR services are often used to encapsulate and obfuscate these communications to avoid detection by network traffic monitoring.

7. **Decryption**—After the victim pays the ransom, usually via the attacker's Bitcoin address, the victim may receive the decryption key. However, there is no guarantee the decryption key will be delivered as promise.

Cyber threats Impact on Individuals and Organization

- Financial loss,
- Privacy breach,
- Mental stress

- Data breaches,
- Operational disruption,
- Reputation damage.

Need of Cyber Security in Industrial Operations

- Protects sensitive industrial and customer data
- Ensures safety of critical infrastructure and operations
- Prevents costly production downtime and financial loss
- Safeguards intellectual property and trade secrets
- Builds trust among customers, partners, and stakeholders
- Reduces risks from cyberattacks, malware, and insider threats
- Supports regulatory compliance and avoids legal penalties
- Enables secure adoption of Industry 4.0 technologies (IoT, AI, Cloud)



Case Study 1: WannaCry Ransomware (2017)

- Affected 150+ countries
- UK NHS impacted
- Lesson: Update systems regularly

Case Study 2: AIIMS Cyber Attack (India, 2022)

- Hospital data breach
- Services disrupted
- Lesson: Critical infra needs strong security

Case Study 3: Colonial Pipeline Attack (USA)

- Fuel supply disruption
- Ransom paid
- Lesson: Protect critical infrastructure

Case Study 4: Facebook Data Leak

- Millions of users data exposed
- Lesson: Privacy & data protection

Human Factor in Cyber Security

- 90% attacks involve human error
- Awareness is key defense

Best Practices for Students

- Avoid unknown links
- Strong passwords
- Privacy settings
- Secure devices

Best Practices for Professionals

- Use VPN
- Regular updates
- Data encryption
- Access control

Zero Trust Model (Diagram)

- Never Trust → Always Verify
- User → Authentication → Authorization → Access

Feature	Traditional Security	Zero Trust Security
Access Control	Based on network perimeter	Based on user identity & behavior
User Verification	Assumed trusted inside network	Continuous authentication
Lateral Movement	Attackers can move inside network	Microsegmentation prevents movement
Device Security	Limited visibility into devices	Only compliant devices are allowed
Cloud Security	Less focus on cloud environments	Designed for cloud and hybrid work

Cyber Hygiene

- Regular updates
- Antivirus
- Backup data
- Secure Wi-Fi

Role of AI in Cyber Security

- Threat detection
- Anomaly detection
- Automated response

Future Threats

- AI-powered attacks
- IoT vulnerabilities
- Deepfakes



Key Elements of Cybersecurity

01

Confidentiality, Integrity, and Availability (CIA) Triad

Significance of CIA triad in cybersecurity. Interaction between confidentiality, integrity, and availability. Measures ensuring each element of the triad.

02

Role of Risk Management in Cybersecurity

Definition and importance of risk management in cybersecurity.
Identifying, assessing, and mitigating risks.
Role of risk management frameworks and methodologies.

03

Importance of Security Policies and Procedures

Role of security policies in guiding behavior and decisions.
Creating clear and comprehensive security procedures.
Regular updates and enforcement of security policies.

Understanding Cybersecurity Threats

Definition and Types of Cybersecurity Threats

Various types of cybersecurity threats
malware, phishing, etc. ☒
Cyberattacks, data breaches, and their
distinctions. ☒
Evolution of cyber threats due to
technological advancements.

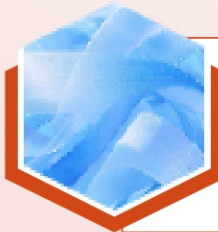
Importance of Cybersecurity in the Digital Age

Growing reliance on digital
technology and vulnerabilities. ☒
Role of cybersecurity in
safeguarding personal and
sensitive data. ☒
Consequences of neglecting
cybersecurity in personal and
organizational contexts.

Impact of Cybersecurity Breaches on Organizations

Financial, reputational,
and operational
damages from
cyberattacks. ☒
Real- world examples of
significant cybersecurity
breaches. ☒
Necessity of robust
cybersecurity measures
for organizational
protection.

Overview of Cybersecurity Solutions



Preventive, Detective, and Corrective Measures

Distinctions between preventive, detective, and corrective measures. ☒

Examples: firewalls, access controls, authentication. ☒

How detective and corrective measures address threats.



Role of Security Technologies (Firewalls, Intrusion Detection Systems)

Firewalls' role in monitoring and controlling network traffic. ☒

Intrusion detection and prevention systems for threat detection. ☒

Other security technologies i.e. antivirus, encryption.



Human Factors in Cybersecurity (Training, Awareness)

Significance of cyber security training for employees. ☒

Employee awareness against social Engineering attacks. ☒

Examples: phishing simulations, awareness campaigns.

Cyber Security Challenges in Industry 4.0



Increased Attack Surface

More connected devices lead to higher vulnerability points.

Legacy Systems

Older infrastructure presents significant risks and integration difficulties.

Data Sensitivity

Exposure of critical operational data risks industrial espionage and disruption.

Defining IIoT



What is IIoT?

The Industrial Internet of Things (IIoT) connects industrial devices into smart networks.

Core Features

It enables seamless connectivity, extensive data exchange, and robust machine-to-machine communication.

Purpose

The primary goal is to boost operational efficiency and enable real-time decision-making in industrial settings.

Key Enablers of Industry 4.0



Artificial Intelligence (AI)

- Drives predictive analytics
- Enables smart decision-making at scale



Big Data

- Facilitates real-time processing of vast datasets
- Generates critical insights for optimization



Cloud Computing

- Provides scalable infrastructure for IIoT
- Ensures secure data storage and seamless sharing

Industrial Internet of thing

The **industrial internet of things (IIoT)** refers to interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management. This connectivity allows for data collection, exchange, and analysis, potentially facilitating improvements in productivity and efficiency as well as other economic benefits.

The IIoT is an evolution of a distributed control system (DCS) that allows for a higher degree of automation by using cloud computing to refine and optimize the process controls.

The IIoT is enabled by technologies such as cyber security, cloud computing, edge computing, mobile technologies, machine-to-machine, 3D printing, advanced robotics, big data, Internet of things, RFID technology, and cognitive computing.

Layered Modular Architecture In IIoT

Content layer: User interface devices (e.g. computer screens, PoS stations, tablets, smart glasses, smart surfaces)

Service layer: Applications, software to analyze data and transform it into actionable information

Network layer Communications protocols, Wi-Fi , Bluetooth , LoRa, cellular

Device layer: Hardware, CPS, machines, sensors

Common Cyber Threats in IIoT

Malware & Ransomware

These attacks disrupt operations and lead to severe financial losses for industrial firms.

Phishing & Social Engineering

Cybercriminals target employees to breach credentials, gaining unauthorized access to critical systems.

DDoS Attacks

Distributed Denial of Service attacks overload networks, causing service disruption and operational downtime.

Data Breaches and Identity Theft

Protecting Personal and Sensitive Information

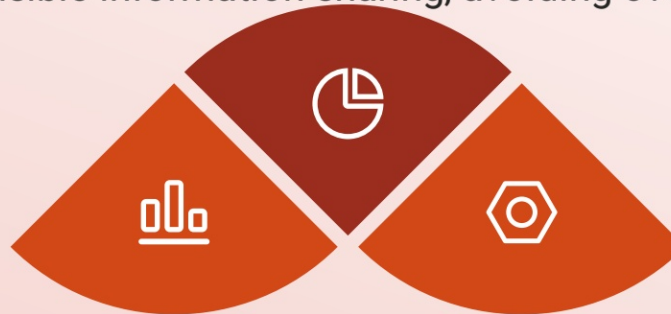
Best practices for personal information protection. ☒
Secure password practices, multi- factor authentication, encryption. ☒

Causes and Responsible information sharing, avoiding overs

Consequences of Data Breaches

- Common data breach causes :weak passwords, insider threats. ☒

Consequences for individuals and organizations:
Reputational and legal impact of data breaches.



Legal and Regulatory Implications of Data Breaches

GDPR, CCPA data protection regulations. ☒
Organization obligations post-data breach. ☒
Fines, penalties for non-compliance.

Impact on the Workforce

Skill Transformation

There's a growing demand for digital skills, leading to new roles, particularly in cybersecurity.

Workplace Automation

Automation fosters human-machine collaboration, significantly increasing overall productivity.

Training Needs

Continuous upskilling and cyber awareness programs are crucial for the evolving workforce.



Artificial Intelligence and Machine Learning in Cybersecurity

Application of AI/ML in Threat Detection and Analysis

Role of AI, ML in identifying threats. ☒
Automation in threat detection. ☒
Real-time analysis using AI/ML.

Challenges and Limitations of AI-powered Security

Challenges of AI/ML in cybersecurity. ☒
Limitations, potential biases. ☒
Human- AI collaboration for effective security.

Ensuring Ethical and Responsible Use of AI in Cybersecurity

Ethical considerations of AI in security. ☒
Transparency, accountability in AI use. ☒
Guidelines for ethical AI deployment.

Successful Cybersecurity Implementations

Energy and Utilities Industry

- AI-driven monitoring in smart grids reduces cyberattacks by 40%.¹
- Enhances energy distribution security.²
- Ensures uninterrupted utility services.

Industrial Manufacturing Sector

- Real-time threat detection and AI-driven anomaly monitoring.³
- Reduces downtime and protects IIoT assets.⁴
- Safeguards critical infrastructure from cyber threats.

Transportation and Logistics

- Real-time tracking and predictive maintenance.⁵
- Strong cybersecurity prevents data breaches.⁶
- Ensures safe and efficient logistics management.

Case Study Stuxnet Attack



1 Overview

Stuxnet specifically targeted nuclear facilities, exploiting vulnerabilities in their industrial control systems.

2 Lessons Learned

The attack highlighted the critical vulnerability of IIoT systems, emphasizing the urgent need for proactive, robust security measures.

3 Impact

Stuxnet created global awareness of cyber risks to critical infrastructure, prompting a significant shift in cybersecurity priorities worldwide.

Lessons Learned from Cyber Incidents

Case of Ransomware Attacks

Ransomware attacks highlight the critical need for robust backup systems, employee training, and timely software updates to minimize disruption and financial loss in IIoT-driven industrial environments.

Recovery and Mitigation Strategies

Effective recovery involves rapid incident response, system isolation, and data backups, while mitigation requires continuous monitoring, employee training, and updating security to prevent future IIoT cyber threats.

Supply Chain Vulnerabilities

Supply chain cyber incidents reveal risks from interconnected vendors, emphasizing the need for comprehensive security audits, real-time monitoring, and strict access controls to prevent widespread operational disruptions.

IIoT's Societal Benefits



Smart Cities

IoT-enabled infrastructure leads to improved public services, from traffic management to waste collection, creating more livable urban environments.



Healthcare Innovation

Remote monitoring devices enhance patient care, enabling timely interventions and significantly better health outcomes, especially for chronic conditions.



Environmental Sustainability

IIoT fosters eco-friendly industrial practices, optimizing resource use and reducing waste, contributing to a substantial cut in carbon footprint.

Benefits of IIoT for Industries



Operational Efficiency

IIoT optimizes production processes, significantly reducing operational downtime and bottlenecks.



Predictive Maintenance

It enables early fault detection in machinery, leading to substantial cost savings and prolonged asset life.



Smart Resource Use

IIoT implementation enhances energy efficiency and minimizes waste across industrial operations.

IIoT in the Healthcare Industry

Smart Devices & Remote Monitoring

- Connected wearables for continuous patient data
- Remote monitoring of vital signs and chronic conditions

Critical Cyber Threats

- Sensitive patient data leaks leading to privacy breaches
- Device manipulation risking patient safety and treatment integrity

Robust Security Solutions

- Implementing strong, multi-factor authentication for all devices
- Mandating end-to-end encrypted communication for all data transfers

The integration of IIoT in healthcare promises revolutionary advancements but demands stringent security measures to protect patient lives and confidential data.

IIoT in Smart Agriculture



Key Benefits

- Significantly higher crop yields and quality
- More efficient use of scarce resources like water and fertilizer
- Reduced labor costs and environmental impact

Emerging Challenges

- Vulnerability of connected agricultural devices to cyberattacks
- Gaps in rural connectivity hindering widespread adoption & security updates

Revolutionizing the Farm

- Precision farming techniques for optimized yields
- Automated smart irrigation systems conserve water
- Real-time soil and crop monitoring for healthier produce

IIoT in Transportation



Connected Vehicles

Autonomous driving systems and real-time data exchange for traffic management.



Critical Risks

Potential for hacking vehicle controls, leading to accidents or traffic disruption.



Security Solutions

Implementing robust secure communication protocols and mandatory regular software updates.

The future of transportation is interconnected, making robust IIoT security paramount for public safety and infrastructure integrity.

Ethical & Legal Issues in IIoT

Data Ownership Dilemmas

The vast data generated by IIoT raises complex legal ambiguities: who owns the data—the device manufacturer, the facility owner, or the data generator? This has significant implications for monetization and privacy.

Navigating Global Regulations

Compliance with diverse and evolving regulations like GDPR or industry-specific IT laws is paramount. Non-compliance can lead to severe penalties, necessitating continuous legal vigilance.

Ensuring Ethical AI Use

Beyond legalities, ethical considerations around responsible data use, avoiding algorithmic bias in AI, and safeguarding human autonomy are crucial for maintaining societal trust and preventing harm.

Industrial Best Practices for IIoT Security

01

Regular Security Audits

Conducting periodic penetration testing and vulnerability assessments to identify weaknesses.

02

Comprehensive Employee Training

Educating personnel on cyber hygiene practices and incident response awareness.

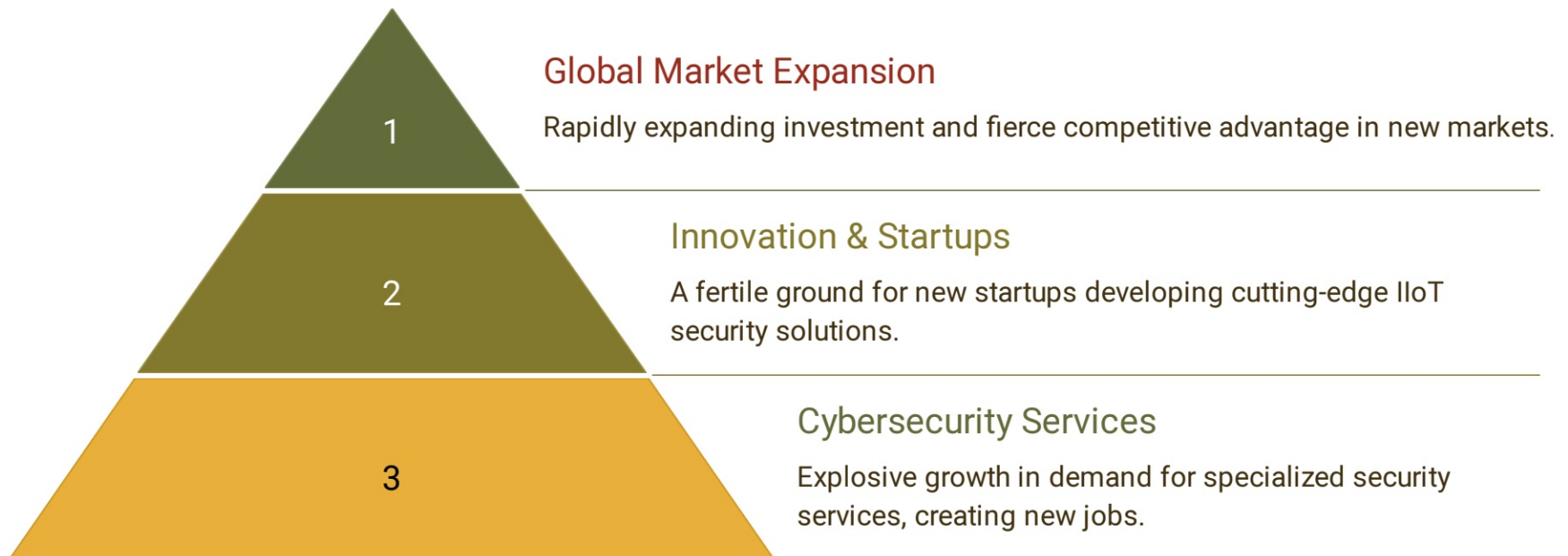
03

Implementing Layered Defense

Deploying multi-faceted security controls including firewalls, intrusion detection systems, and robust backup solutions.

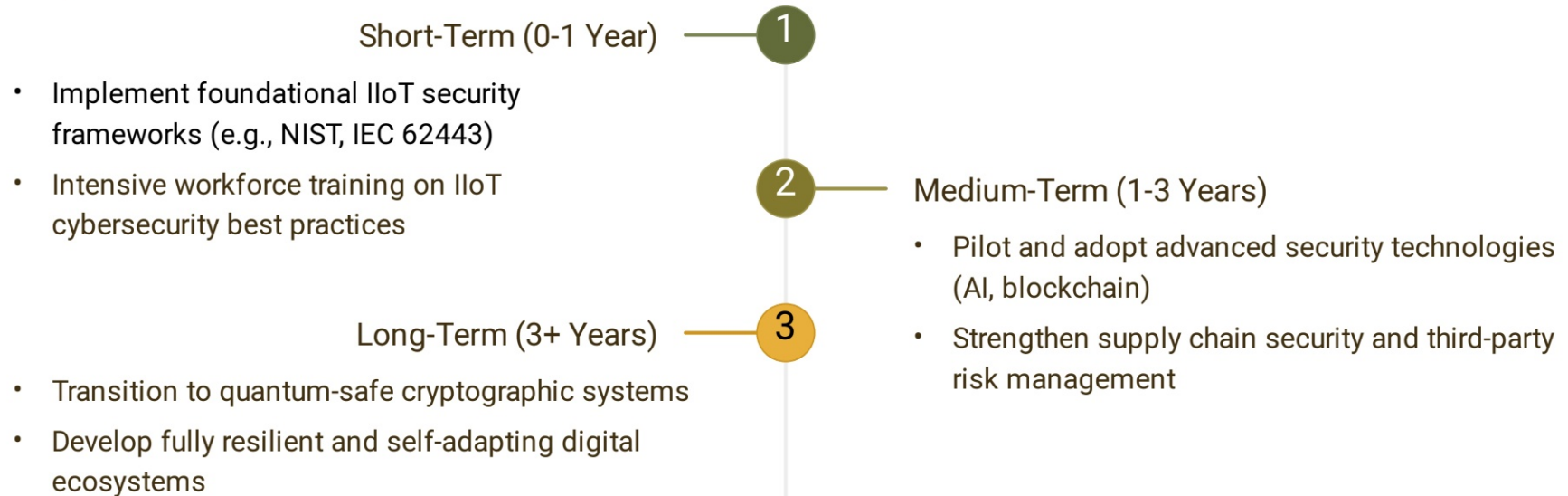
Proactive and multi-layered security strategies are essential for protecting industrial operations from evolving cyber threats.

Business Opportunities in IIoT Security



The imperative for IIoT security is not just a challenge, but a burgeoning sector for innovation, investment, and job creation worldwide.

Roadmap for Secure Industry 4.0



Industry 4.0 and IIoT are transforming our world, bringing unprecedented efficiency and innovation. Yet, with great power comes great responsibility: cybersecurity is the essential backbone for safe digital adoption.

Future Outlook

- XAI in cybersecurity.
- Quantum-safe cryptography.
- Digital twins for societal planning.
- Stronger collaboration between industry, academia, and government.

Conclusion

- Industry 4.0 depends on secure IIoT ecosystems.
- Cybersecurity is vital for trust and resilience.
- IIoT has transformative effects on society.
- Balanced approach needed: innovation + security.



THANK YOU