STRATEGY BRIEF

Simplify & Strengthen: Effective Cybersecurity for Critical Infrastructure

How a Holistic Approach is Key to Protecting Your IT-OT Environment

inflexion point

> Attackers are increasingly choosing to deploy attacks on cyber-physical systems (CPS).
>
> It's not surprising, then, that governments worldwide are mandating more security controls for mission-critical CPS.
>
> **Gartner**

https://www.gartner.com/en/topics/cybersecurity

Want to Strengthen Your Cybersecurity? Simplify.

You don't need a government mandate to tell you what you already know. Hackers are getting smarter and you need to strengthen your cyber defenses. But in a complex, converged IT-OT environment that is easier said than done.

We understand. We help critical infrastructure companies in diverse industries to design, implement, and manage converged IT-OT systems with extensive cybersecurity capabilities.

Along the way we have encountered all sorts of challenges and learned that a simple, holistic approach works best.

This guide is the product of our learnings and a summary of the strategies we rely upon in our work. We hope you find it useful.

Kevin Hannigan
CEO
InflexionPoint

Massive Increase in Cyberattacks Targeting Cyber-Physical Systems.

Cost: $22 Billion and Growing.

According to Gartner, cyber-physical systems are engineered to orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). Connecting the digital and physical worlds presents a unique and growing area of vulnerability.

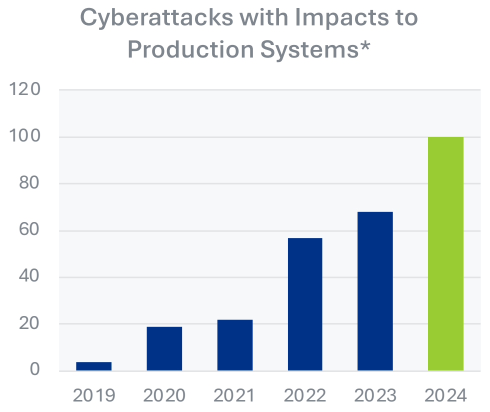
Remember when OT systems were air-gapped? Those days are over.

The promise of Digital Transformation to help operators run more efficiently and effectively is real, and we are enthusiastic supporters of these transformative technologies.

But hackers appear to have discovered that internet-connected OT systems are lucrative targets — and often not adqeuately protected.

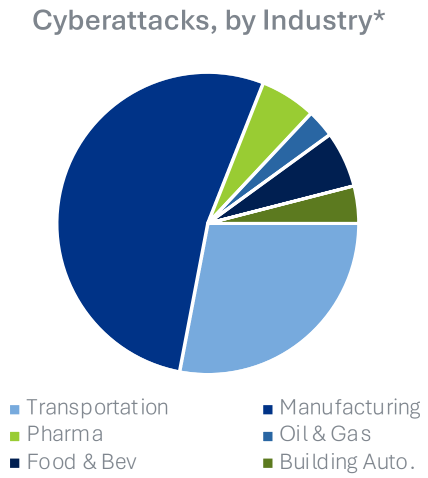
How do we know this? Because the number (and cost) of cyberattacks on critical infrastructure operators has been growing rapidly in recent years.

So what can you do? In the coming pages we share our strategies for simplifying and strengthening your cybersecurity.



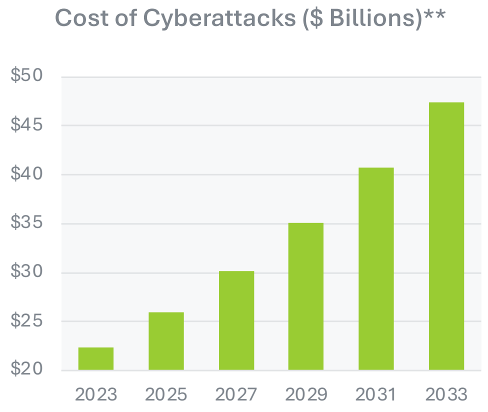
Rapid Rise in Incidents

- In 2023 there were 68 attacks with physical consequences (OT), affecting over 500 sites
- Projected 100 OT cyberattacks in 2024



Key Industries Targeted

- Over 50% of cyberattacks impacted manufacturing
- Effects included production shutdowns, work stoppages, and/or shipping delays



Mounting Losses

- The cost of cyber breaches in the OT space projected to grow grow from $22.36 Billion in 2023 to $47 Billion in 2033 (7.8% CAGR)

*Source: 2024 Threat Report of Cyberattacks with Physical Consequences, ICS STRIVE. **Source: McKinsey & Company

Types of Cyberattacks

From unsophisticated hackers to intruders using state-of-the-art techniques, cyber attacks seemingly can come from anywhere. In all cases, hackers want to steal information and disrupt, deny access to, degrade, or destroy critical information systems. What should you be watching out for? Here are brief descriptions of the most common types of cyberattacks.

Phishing and Social-Engineering

Attackers trick legitimate users with proper access credentials into taking action that opens the door for unauthorized users.

Internet-Facing Services

These threats relate to the failure of enterprises, partners and vendors to adequately secure cloud services or other internet-facing services.

Password Compromises

Unauthorized users deploy software or other hacking techniques to identify passwords they can exploit to gain access to systems or assets.

Network-Related, Man-in-the-Middle

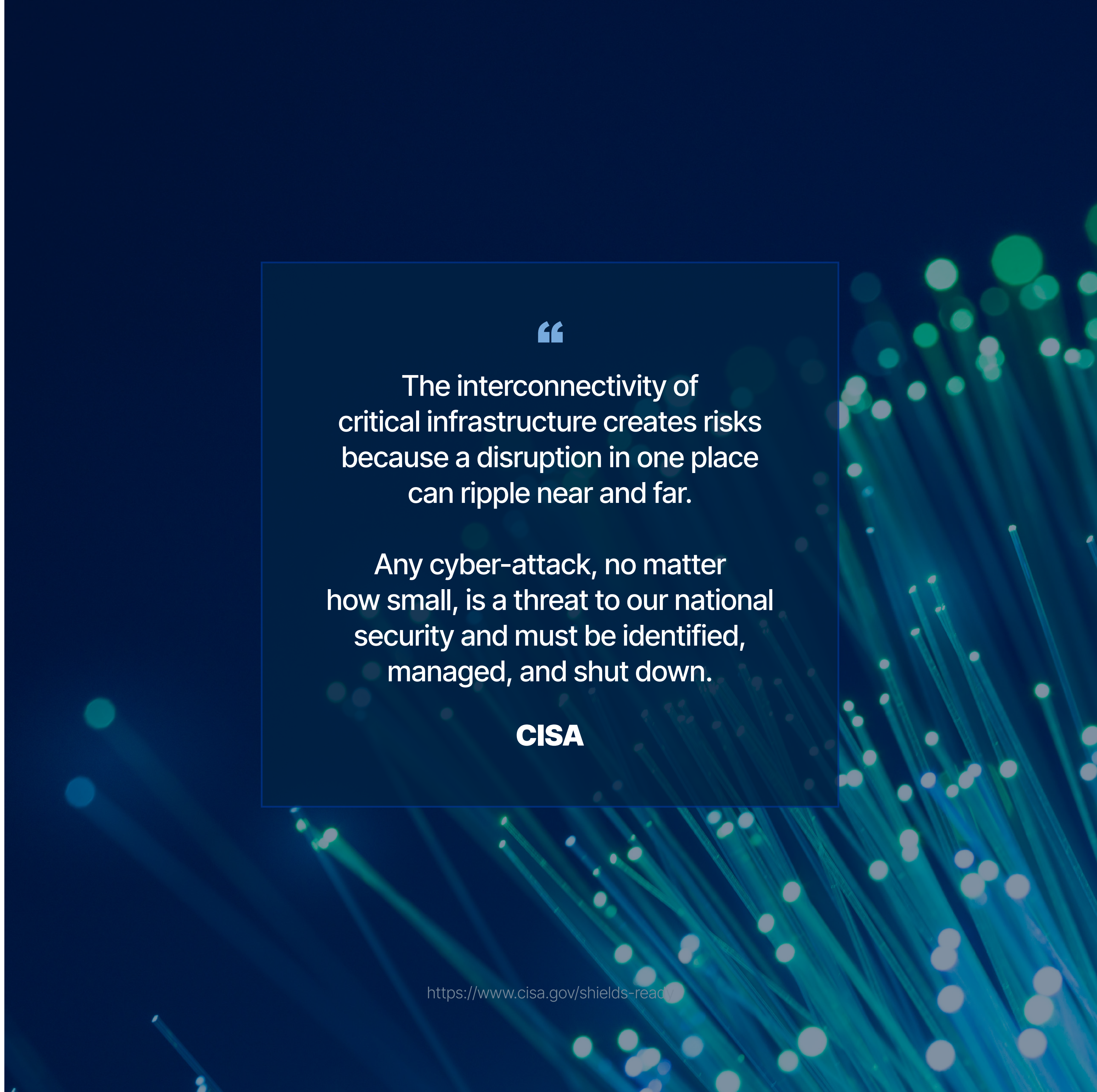
Failure to encrypt messages within and outside an organization's firewall can give attackers the ability to eavesdrop on or even redirect traffic.

Supply Chain

Partners, vendors or other third-party assets or systems (or code) become compromised, creating a vector to attack enterprise systems.

Denial-of-Service (DoS)

Attackers overwhelm enterprise systems and cause a temporary shutdown or slowdown.



> “
>
> The interconnectivity of critical infrastructure creates risks because a disruption in one place can ripple near and far.
>
> Any cyber-attack, no matter how small, is a threat to our national security and must be identified, managed, and shut down.
>
> **CISA**

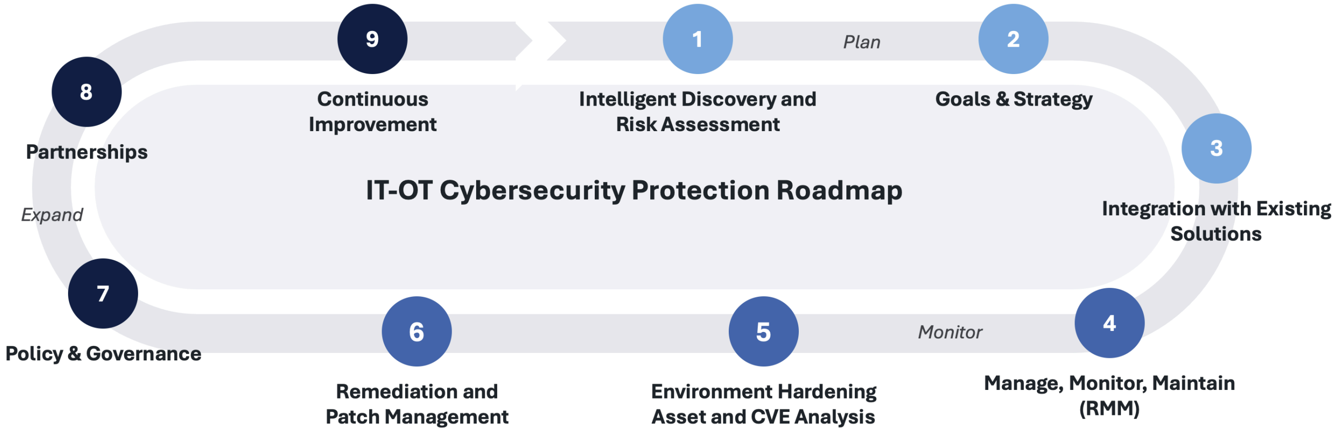
https://www.cisa.gov/shields-ready/

> To help organizations manage and reduce their cybersecurity risks NIST has identified six functions: Govern; Identify; Protect; Detect; Respond; and, Recover.
>
> Together, these functions provide a comprehensive view for managing cybersecurity risk.
>
> **NIST**

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf

Strengthen: A Roadmap for Effective Cybersecurity

According to the Cybersecurity & Infrastructure Security Agency (CISA) critical infrastructure entities and other organizations can be more resilient by following a few key practices. We agree. Here is our roadmap for effective cybersecurity.



IT-OT Cybersecurity Protection Roadmap
Plan
1 Intelligent Discovery and Risk Assessment
2 Goals & Strategy
3 Integration with Existing Solutions
Monitor
4 Manage, Monitor, Maintain (RMM)
5 Environment Hardening Asset and CVE Analysis
6 Remediation and Patch Management
7 Policy & Governance
Expand
8 Partnerships
9 Continuous Improvement

A Neverending Journey

When it comes to cybersecurity, the job is never really done. Your strategy must include continuous monitoring, assessments, and mitigation across various interrelated components, including servers, the cloud, Internet of Things (IoT), internet connections and the many physical assets used to access networks.

We follow a proven roadmap to create an integrated, resilient, and responsive cybersecurity posture that protects critical infrastructure from emerging threats while supporting operational efficiency and regulatory compliance.

Simplify:
A Three-Phase Cybersecurity Program

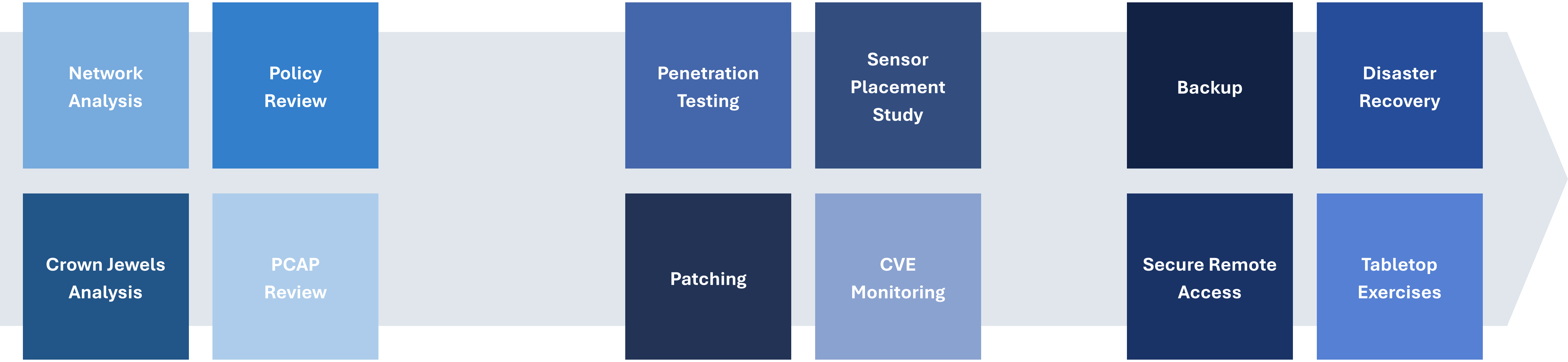
How do you climb a mountain?
One step at a time.

As the roadmap on the previous page shows, we approach cybersecurity as a journey of continuous improvement, with processes, services, and solutions designed to address the intricacies of IT-OT systems and enhance your digital defenses at every level.

To keep things simple, we recommend you break down your journey into three distinct phases:

1. Planning
2. Monitoring
3. Expanding

Within each phase you will perform several key actvities; and each phase builds upon the one before it.



Network Analysis

Policy Review

Crown Jewels Analysis

PCAP Review

Penetration Testing

Sensor Placement Study

Patching

CVE Monitoring

Backup

Disaster Recovery

Secure Remote Access

Tabletop Exercises

1. Planning

- Develop robust and functional network infrastructure and policies
- Implement meticulous design and review processes
- Comprehensive analysis of your environment and systems
- Assess current compliance with industry standards and regulations

2. Monitoring

- Persistence in upkeep to your systems is paramount in both IT and OT
- Patching and maintenance help you minimize your attack surfaces
- Advanced monitoring tools for real-time threat detection and response
- Utilize AI and ML for predictive threat analysis and anomaly detection

3. Expanding

- Data backup and protection solutions that can scale — on-site, off-site, cloud, hybrid
- Interactive simulations of emergency situations, to test strategies, processes, and teams
- Blockchain technologies for secure and transparent supply chain management

Looking for a Cybersecurity Partner?

Look No Further.

It's one thing to talk about cybersecurity strategy. It's quite another to execute on a cybersecurity plan, day in, day out. We have the skills and experience to help you achieve your cybersecurity goals — allowing you to focus on what you do best.

- Cybersecurity-as-a-Service (CSaaS) shifts the burden of protection while reducing costs
- Ongoing services help ensure your security systems achieve maximum effectiveness
- Reduce your headcount and budget (we offer plans at a fraction of the cost of one FTE)

inflexion point

🌐 www.inflexionpoint.ai ✉ cyber@inflexionpoint.ai