ISC INTERNATIONAL SECURITY CONFERENCE & EXPO

Securing the Unseen and the Seen:

BRIDGING THE GAP BETWEEN DIGITAL AND PHYSICAL SECURITY

A new ISC study finds that 51% of cybersecurity leaders say it's just blind luck that they haven't had a serious breach due to gaps in cyber and physical security.

Built by RX In the business of building businesses

Introduction

While digital defenses like firewalls and encryption dominate security conversations, vulnerabilities often lie in plain sight—within their physical infrastructure.

Cybersecurity leaders are increasingly realizing that true security demands an integrated approach, combining both digital and physical safeguards.

The ISC 2025 Security Survey exposes a critical divide.

While nearly all respondents acknowledge the importance of physical security systems in their overall defense strategy, only a small portion have successfully unified these with digital protections.

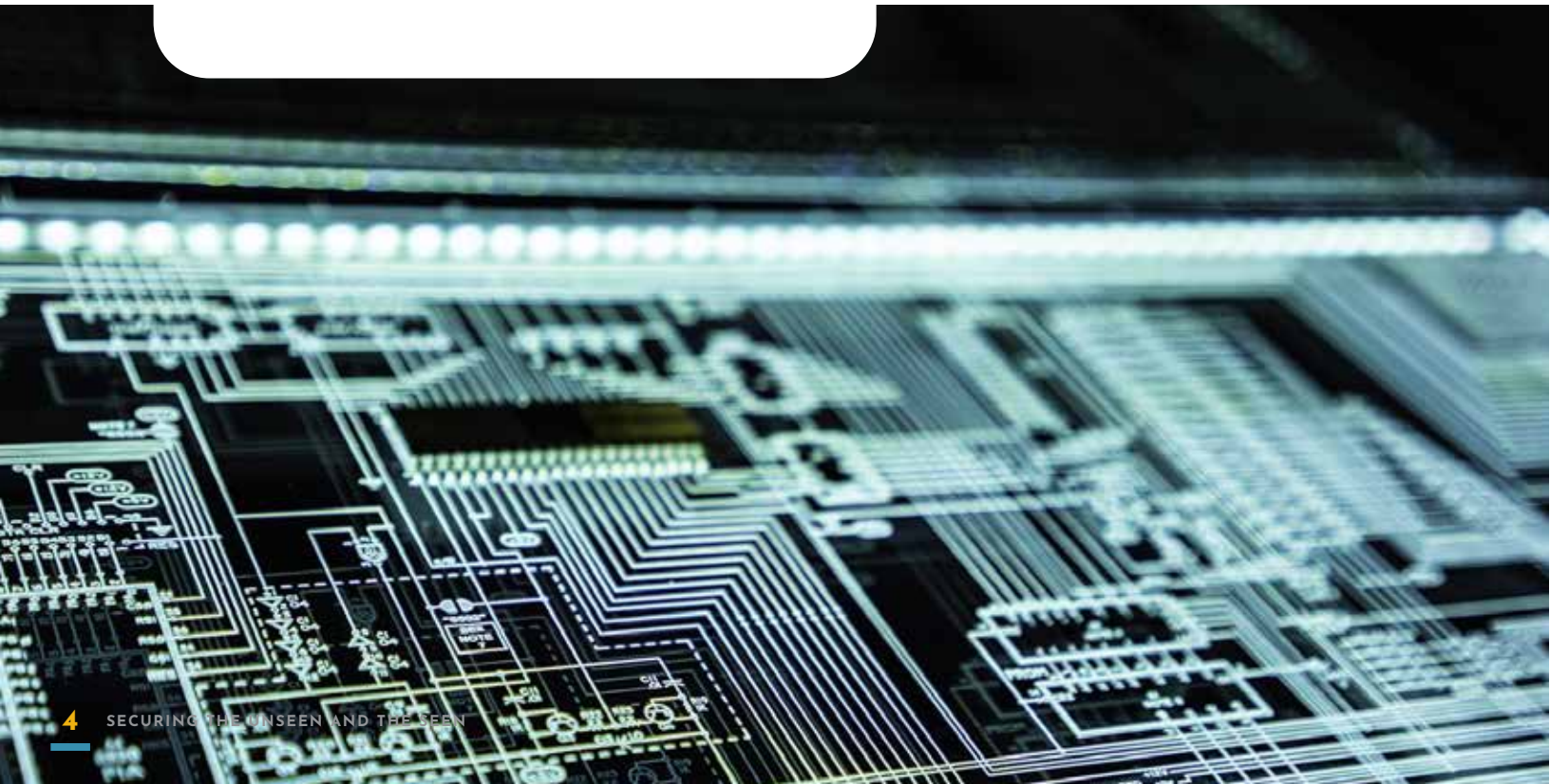
This eBook explores the growing convergence of physical and cyber risks, the technological and organizational hurdles faced by today's security professionals, and the solutions that can bridge the gap.

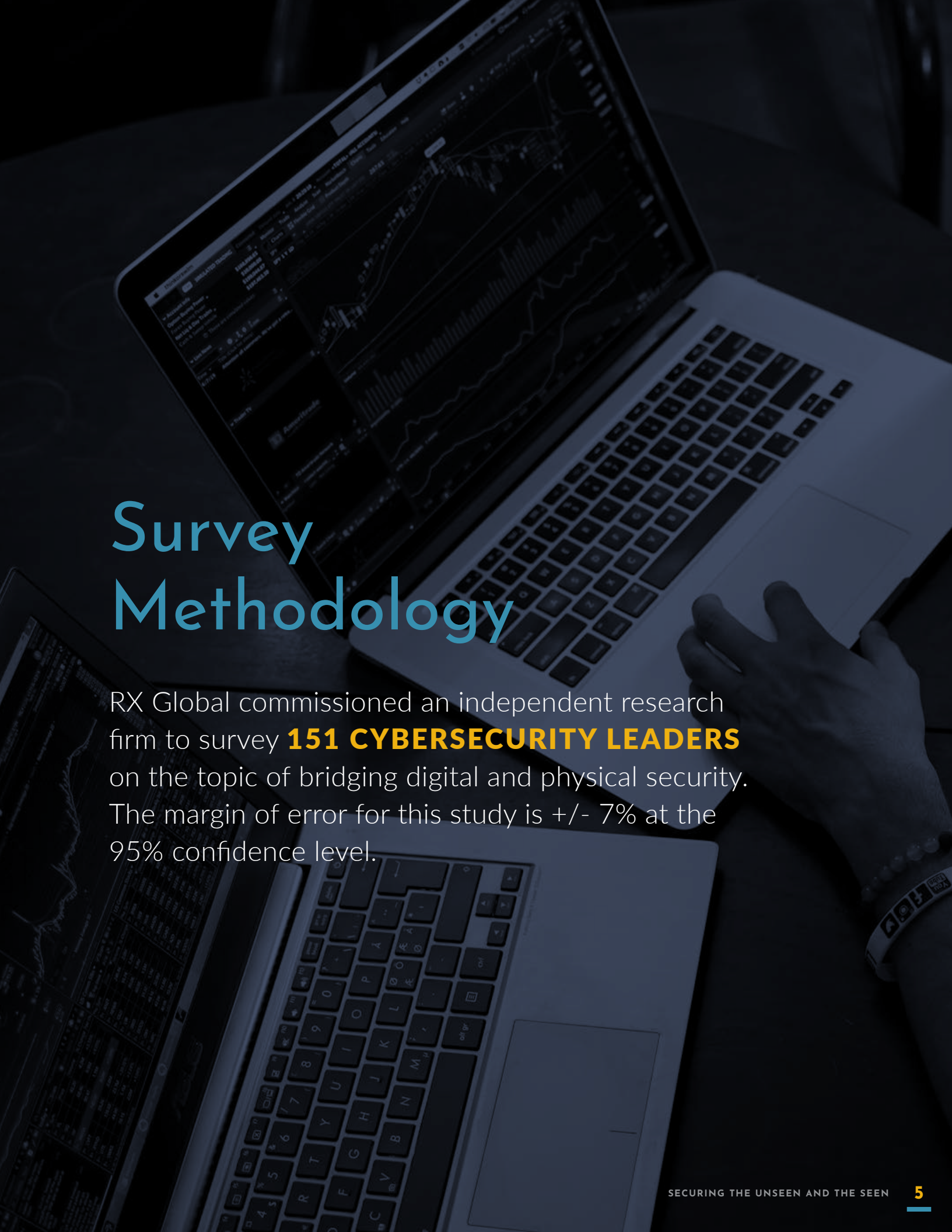
Abstract

Security leaders are grappling with a complex threat landscape, one where physical vulnerabilities can directly compromise digital security. The ISC 2025 survey reveals that while nearly all cybersecurity leaders recognize the need for integration between physical and digital security, gaps remain pervasive. Blind spots such as unpatched physical devices, unsecured IoT infrastructure, and insufficient employee awareness are commonplace.

To address these challenges, organizations are turning to hybrid solutions that combine physical and cyber threat monitoring. Technologies like AI-based analytics, centralized dashboards, and multi-layered defenses are gaining traction. But implementation is fraught with challenges—from skill gaps and internal resistance to budgetary constraints and legacy system limitations.

Despite these obstacles, the future holds promise. Leaders are prioritizing investments in AI, IoT security, and employee training to combat threats and streamline operations. By unifying teams and leveraging advanced technology, organizations can move toward a comprehensive security framework that bridges the digital and physical realms.





Survey Methodology

RX Global commissioned an independent research firm to survey **151 CYBERSECURITY LEADERS** on the topic of bridging digital and physical security. The margin of error for this study is +/- 7% at the 95% confidence level.

What You Will Learn in This eBook

The top blind spots that compromise both physical and digital security.

Key investments that leaders are making to secure physical infrastructure.

How hybrid security solutions are closing gaps between cyber and physical threats.

The role of AI in streamlining and strengthening security systems.

Strategies to overcome organizational challenges and unify security teams.

Who This eBook is For

CHIEF INFORMATION SECURITY OFFICERS (CISOS)

looking to modernize security strategies

IT AND CYBERSECURITY PROFESSIONALS

managing integrated security systems

PHYSICAL SECURITY MANAGERS

seeking to align with cyber operations

RISK AND COMPLIANCE OFFICERS

addressing regulatory requirements for security

FACILITIES MANAGERS

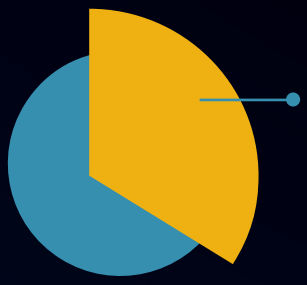
tasked with safeguarding physical infrastructure

Respondent Breakout

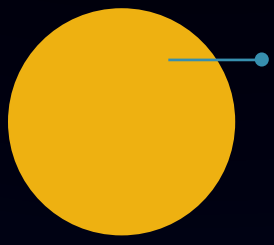
100%
IT leaders at organizations that manage both physical and digital security

THE KEY ROLES SURVEYED WERE

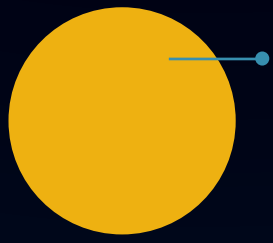
- Cybersecurity leaders
- Network Engineers
- Database Administrators



34%
of respondents were Executives or VPs



100%
were Managers or more senior with budget authority



100%
were at organizations with over 100 employees

Survey Insights

INTEGRATION WITH PHYSICAL INFRASTRUCTURE

1. **Physical security is a top priority for most organizations.**
   - 99% of cybersecurity leaders view physical security systems as critical to their broader network defense strategy.
     - ☑ *To Do: Audit your physical security systems to ensure they align with your network defense strategy.*

2. **Organizations are taking steps to integrate security efforts.**
   - 97% of organizations have formally integrated physical and digital plans company-wide.
     - ☑ *To Do: Develop and implement a formalized integration plan for physical and cyber security within your organization.*

3. **Industries leading the integration race.**
   - The industries best equipped to integrate digital and physical security are computer software, manufacturing, and telecommunications.
     - ☑ *To Do: Benchmark your security strategy against these industries to identify areas for improvement.*

4. **Cyber breaches concern leaders more than physical ones.**
   - 77% of cybersecurity leaders worry more about a digital break-in than a physical one (23%).
     - ☑ *To Do: Balance investments between digital and physical security to address both types of risks.*

5. **Hybrid solutions are becoming the norm, but gaps remain.**
   - 93% of organizations have implemented hybrid solutions for physical and cyber threat monitoring, but 77% suspect gaps exist.
     - ☑ *To Do: Conduct regular gap analyses to identify vulnerabilities in your hybrid security solutions.*

6. **Leaders admit to luck in avoiding breaches.**
   - 51% of cybersecurity leaders say it's just blind luck they haven't had a serious breach due to gaps in cyber and physical security.
     - ☑ *To Do: Implement robust risk assessment processes to move from reactive to proactive security.*

7. **Centralized dashboards are in demand.**
   - 96% of cybersecurity leaders want to deploy centralized dashboards for unified management of cyber and physical security by next year.
     - ☑ *To Do: Evaluate dashboard solutions that enable real-time integration of cyber and physical security data.*

8. **Confidence in managing integrated systems is low.**
    - Only 62% of leaders are highly confident they can manage both digital and physical security from one dashboard.
        - ☑ *To Do: Invest in training and technology that enhances unified security system management.*

GAPS AND BLIND SPOTS

9. **Unpatched physical devices remain a significant weakness.**
    - 91% of cybersecurity leaders identify unpatched vulnerabilities in physical devices, such as cameras and access control systems, as a primary blind spot.
        - ☑ *To Do: Implement a patch management program for physical security devices.*

10. **Real-time monitoring is key to avoiding blind spots.**
    - Lack of real-time monitoring is over 2x more likely than outdated legacy systems to be a blind spot for physical and digital security.
        - ☑ *To Do: Deploy real-time monitoring tools to reduce blind spots across systems.*

11. **IoT devices create unique vulnerabilities.**
    - 64% of cybersecurity leaders say insider threats, including disgruntled employees, remain the biggest risk to physical security.
        - ☑ *To Do: Enhance IoT security policies and enforce access controls on all connected devices.*

INVESTMENT TRENDS

12. **Organizations prioritize networked monitoring.**
    - The top ways business cybersecurity leaders are investing in securing physical infrastructure include networked security device monitoring, surveillance systems, access control, biometrics, and regular audits.
        - ☑ *To Do: Allocate budget for the top security investments, starting with networked monitoring tools.*

13. **AI reduces false alarms.**
    - 77% of cybersecurity leaders report that AI tools have helped reduce false alarms by automating threat prioritization.
        - ☑ *To Do: Adopt AI-driven tools to refine your threat prioritization processes.*

14. **Video analytics improve threat detection.**
    - 57% of cybersecurity leaders using AI-based video analytics have significantly improved their ability to detect suspicious activity.
        - ☑ *To Do: Leverage AI-powered video analytics to enhance your surveillance capabilities.*

15. AI adoption comes with cost-saving benefits.

- 86% of cybersecurity leaders expect AI to drive cost savings by reducing the need for manual monitoring.
  - ☑ *To Do: Perform a cost-benefit analysis for AI tools to streamline manual processes.*

SKILLS GAPS AND FUTURE CHALLENGES

16. IoT knowledge is insufficient among teams.

- 53% of organizations report that their teams lack sufficient knowledge of securing IoT devices used in physical security systems.
  - ☑ *To Do: Introduce targeted training programs focused on IoT security best practices.*

17. AI expertise is a growing need.

- 91% of cybersecurity leaders identify training in AI and machine learning applications as a top priority.
  - ☑ *To Do: Upskill your team with workshops and certifications in AI and machine learning applications.*

18. Hybrid threat expertise is in demand.

- **87% of cybersecurity leaders are planning to cross-train physical and cyber-**security teams to handle hybrid threats.
  - ☑ *To Do: Launch cross-training initiatives to build a team equipped to handle integrated security challenges.*

19. Threat modeling is the future.

- 96% of cybersecurity leaders believe proficiency in threat modeling is essential for future hires.
  - ☑ *To Do: Incorporate threat modeling exercises into hiring evaluations and team development.*

GAPS AND BLIND SPOTS

20. Vendor and contractor access is a blind spot.

- Vendor and contractor access is one of the top blind spots for cybersecurity leaders in securing physical infrastructure.
  - ☑ *To Do: Implement strict access control policies for third-party vendors and contractors, including time-limited credentials.*

21. Unsecured IoT devices are a recurring issue.

- Unsecured IoT devices remain a persistent blind spot for organizations.
  - ☑ *To Do: Conduct a security audit of all IoT devices and enforce encryption for data transmission.*

22. Employee awareness is lacking.

- Insufficient employee awareness is a significant blind spot for cybersecurity leaders.
  - ☑ *To Do: Regularly train employees on physical and digital security best practices, focusing on spotting suspicious behavior.*

23. Incident response planning is underdeveloped.

- Gaps in incident response planning rank among the top blind spots for physical and digital security.
  - ☑ *To Do: Update and test your incident response plans to include both physical and cyber scenarios.*

GOALS FOR THE FUTURE

24. AI is a major 2025 priority.

- Integrating AI in security systems is a top priority for 2025.
  - ☑ *To Do: Evaluate and select AI vendors to integrate into your security infrastructure roadmap.*

25. Remote access needs better protection.

- Securing remote access points is a critical goal for cybersecurity leaders.
  - ☑ *To Do: Deploy VPNs and multi-factor authentication (MFA) to secure remote access points.*

26. IoT device protection is a focus.

- Enhancing IoT device protection is a leading priority for 2025.
  - ☑ *To Do: Introduce automated patching and firmware updates for all IoT devices.*

27. Staff training is a cornerstone of progress.

- Training staff on security protocols is among the top 2025 goals for business leaders.
  - ☑ *To Do: Develop a security education program tailored to your organization's specific risks.*

CHALLENGES

28. Budget constraints hinder progress.

- 56% of cybersecurity leaders struggle to find affordable solutions that meet both physical and cyber security needs.
  - ☑ *To Do: Explore cost-sharing opportunities across departments to fund unified security solutions.*

29. Internal resistance slows innovation.

- 58% of cybersecurity leaders face resistance from internal stakeholders when proposing investments in unified solutions.
  - ☑ *To Do: Create a business case that demonstrates the ROI of unified security investments to key stakeholders.*

30. Fragmented teams create inefficiencies.

- 74% of cybersecurity leaders report that fragmented teams managing physical and cybersecurity create operational inefficiencies.
  - ☑ *To Do: Merge your physical and cyber security teams under a unified management structure.*

31. Legacy systems are difficult to integrate.

- Legacy system integration remains one of the top challenges in securing physical infrastructure.
  - ☑ *To Do: Prioritize upgrading legacy systems or integrating middleware to bridge gaps.*

AI'S ROLE

32. AI adoption is widespread but underperforming.

- 80% of organizations use AI to monitor physical and cyber systems, but 58% say it's not living up to full expectations.
  - ☑ *To Do: Partner with AI vendors to tailor solutions that meet your organization's specific needs.*

33. Predictive analytics hold promise.

- 91% of cybersecurity leaders believe predictive analytics from AI will prevent breaches in both cyber and physical domains.
  - ☑ *To Do: Implement predictive analytics tools to proactively address vulnerabilities.*

34. AI tools reduce manual monitoring needs.

- 86% of cybersecurity leaders expect AI to drive cost savings by reducing the need for manual system monitoring.
  - ☑ *To Do: Automate low-level monitoring tasks using AI to free up staff for strategic roles.*

EMERGING THREATS

35. Insider threats remain a top concern.

- 64% of cybersecurity leaders say insider threats, including disgruntled employees, remain the biggest risk to physical security.
  - ☑ *To Do: Introduce insider threat detection programs and enhance background checks for employees.*

36. DDoS attacks on IoT devices are rising.

- 58% of cybersecurity leaders report a rise in DDoS attacks targeting IoT-connected physical devices.
  - ☑ *To Do: Strengthen network segmentation to isolate IoT devices from the main network.*

37. Botnets are exploiting vulnerabilities.

- 77% of cybersecurity leaders are concerned about botnets exploiting vulnerabilities in physical systems to launch attacks.
  - ☑ *To Do: Deploy intrusion prevention systems (IPS) to detect and block botnet activity.*

38. Phishing attacks target physical systems.

- 58% of cybersecurity leaders say their physical security systems have been impacted by phishing attacks aimed at administrators.
  - ☑ *To Do: Train administrators to recognize and avoid phishing attempts targeting security system credentials.*

39. Unified dashboards could be a game-changer.

- 96% of cybersecurity leaders want to deploy centralized dashboards for unified management of cyber and physical security by next year.
  - ☑ *To Do: Prioritize selecting and implementing a centralized dashboard to streamline operations.*