Preemptive Cyber Defense for Critical Infrastructure

From Reaction to Denial-of-Opportunity

> The stronger question is:
> **'Can we remove the attacker's opportunity before the attack becomes possible?'**

Critical infrastructure is entering a new security era.

The question is no longer only: 'Can we recover after an attack?'

The stronger question is: 'Can we remove the attacker's opportunity before the attack becomes possible?'

That is the shift from reactive cybersecurity to denial-of-opportunity.

For power plants, water systems, oil and gas assets, transport networks, ports, telecoms, smart meters, industrial sites, and government-backed infrastructure programs, cyber defense is no longer an IT add-on. It is part of the asset itself.

A modern infrastructure project must be designed as: physically strong, digitally resilient, operationally recoverable, AI-aware, and safe under stress.

BG Titan Group sits at this intersection. BG Titan's public positioning spans infrastructure, natural resources, energy and power, financial services, technology, media and telecom, and water services. Its broader capabilities include EPC, PMC/PMT, procurement, project development, financing advisory, risk control, and customer-specific IT and cybersecurity solutions.

CRITICAL INFRASTRUCTURE CYBERSECURITY MARKET

USD 56.52B
in 2025

Projected to reach
USD 85.91B
by 2033

Source: Grand View Research

THE NEW INFRASTRUCTURE RULE

- **If it connects, it must be protected.**
- **If it controls, it must be segmented.**
- **If it learns with AI, it must be governed.**
- **If it fails, it must fail safely.**

The Threat Has Changed

Attackers Are No Longer Waiting Outside the Fence

Critical infrastructure used to be protected by distance. A plant had control rooms. A pipeline had field equipment. A substation had local controls. A water facility had isolated systems.

Now, infrastructure is connected through remote access, sensors, cloud dashboards, contractors, smart meters, edge devices, mobile apps, vendor portals, AI tools, and supply-chain software.

That connectivity creates efficiency. It also creates opportunity for attackers.

THE 6-STEP ATTACK FLOW

1. **Find exposure**
   internet-connected OT device, remote access point, supplier login, or unpatched system is discovered.
2. **Enter quietly**
   default passwords, stolen credentials, phishing, or vendor access.
3. **Move laterally**
   cross from IT into OT, or from one supplier into many customers.
4. **Wait, learn, and map**
   study operations, backups, shift patterns, and failure points.
5. **Disrupt at maximum pressure**
   ransomware, data theft, process disruption, payment fraud, or public embarrassment.
6. **Convert weakness into business damage**
   downtime, safety risk, regulatory pressure, lost revenue, and loss of trust.

Ransomware complaints affecting critical infrastructure remain among the highest reported cyber threats.

3,600+
ransomware complaints in 2025

USD 32M+
reported losses

Source: FBI IC3 2025

What authorities are telling operators to do now

- Remove OT from the public internet.
- Change default passwords.
- Secure remote access.
- Segment IT and OT.
- Maintain manual operation capability.

The Opportunity

Build Infrastructure That Gives Attackers Nothing Easy to Use

Preemptive cyber defense is becoming one of the most important business opportunities in infrastructure. Not because customers want more cybersecurity. Because customers need continuity. A hospital cannot pause care. A water utility cannot lose control. A port cannot stop moving goods. A power operator cannot guess whether a control signal is real. A government cannot tell citizens that the service failed because a default password was still active.

SIX FORWARD-LOOKING OPPORTUNITIES

1

OT Exposure Reduction Programs

Identify exposed assets, remove unnecessary access, close unsafe remote entry points.

2

Cyber-Resilient EPC and Procurement

Embed cyber into engineering, vendor selection, commissioning, and acceptance.

3

Secure Edge Infrastructure

Build secure edge connectivity, IoT integration, edge AI, and Zero Trust access from the beginning.

4

AI Threat Readiness

AI is making cyber intrusion faster, more effective, and more frequent.

5

AI Governance and Shadow-AI Control

Create AI inventories, access controls, data protection, monitoring, and vendor governance.

6

Manual Recovery and Operational Continuity

Ensure essential services continue under pressure, with tested manual fallback.

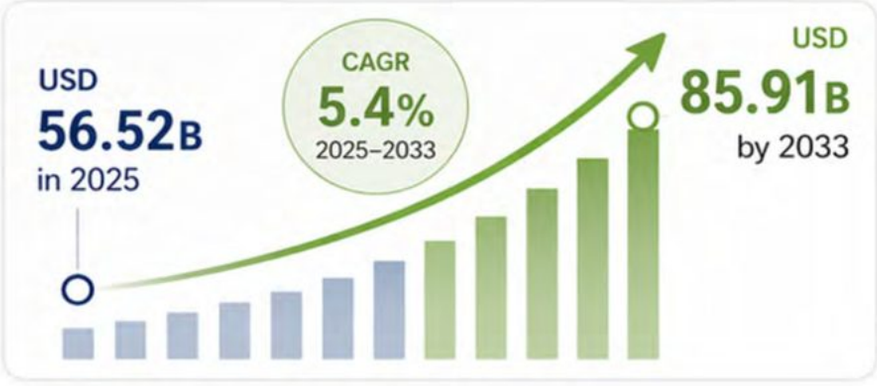
> **The winners will be the infrastructure owners, governments, developers, and operators that make attacks harder, slower, less profitable, easier to detect, and less damaging when attempted.**

BG Titan naturally works across infrastructure, project delivery, procurement, technology, and cybersecurity support to help turn these opportunities into operational results.

The Opportunity Radar

Where Demand Is Moving Now

Cyber defense for critical infrastructure is moving from response spending to resilience investment. The market is projected to grow from about USD 56.52B in 2025 to about USD 85.91B by 2033, shaped by supply-chain complexity, third-party vendors, cloud adoption, hybrid environments, IoT/IIoT expansion, and AI-powered threats.



Four Demand Pools Are Forming

1. Assess and expose

Know what is owned, exposed, obsolete, supplier-accessed, and operationally critical.

2. Design and build securely

Bake cyber into design, procurement, construction, commissioning, and handover.

3. Monitor and control access

Secure remote operations, field maintenance, sensors, dashboards, and AI analytics.

4. Rehearse and recover

Prepare manual operations, restore testing, offline backups, alternate communications, and leadership playbooks.

BG Titan's Natural Position

Cybersecurity belongs in every step.

Critical Infrastructure Is No Longer a Single Asset

It Is a Chain of Dependencies

A plant can be secure and still be exposed through a supplier. A water utility can have strong physical security and still be vulnerable through an old remote-access tool. A port can modernize its logistics platform and accidentally create new points of failure across shipping, customs, payments, and communications.

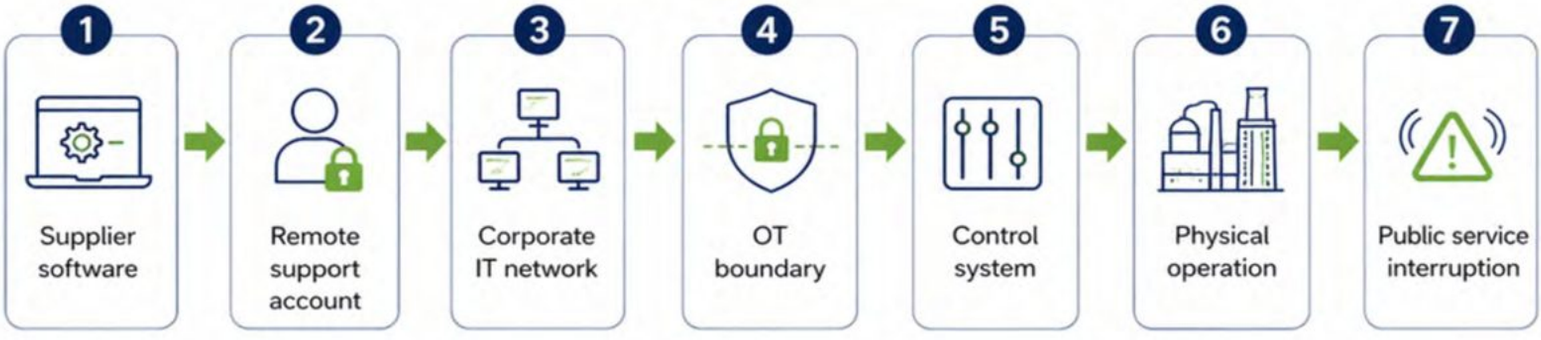
CRITICAL INFRASTRUCTURE PROTECTION MARKET

USD 151.00B in 2025

Projected to reach **USD 229.12B** by 2033

Source: Grand View Research.

THE DEPENDENCY CHAIN



> **The attacker does not care which department owns the weakness. The customer only experiences the outage.**

THE BUSINESS OPENING

The opportunity is not simply to protect systems. It is to secure the chain of dependencies that infrastructure now depends on: suppliers, access paths, contracts, backup assumptions, regulatory obligations, engineering choices, physical safety, and decision-making during an incident.

This is where **BG Titan's** cross-sector infrastructure model matters.

Opportunity 1

Cyber-Resilient EPC and PMC

> **Stop adding cybersecurity after the asset is already built.**

Cybersecurity should be visible before equipment is ordered, before vendors are selected, before remote access is granted, before commissioning begins, and before operators inherit the system.

What Changes in a Cyber-Resilient Project

1. **Design stage**
   define zones, conduits, remote access rules, data flows, backups, and manual operating assumptions.
2. **Procurement stage**
   require secure-by-default devices, update commitments, vulnerability disclosure, supplier access controls, and lifecycle support.
3. **Construction stage**
   control temporary access, contractor laptops, shared credentials, engineering workstations, portable media, and undocumented changes.
4. **Commissioning stage**
   test segmentation, backups, logging, fail-safe behavior, account ownership, password changes, and operator handover.
5. **Operational stage**
   maintain inventories, patch windows, supplier records, remote access logs, restore tests, and incident playbooks.

How BG Titan Can Assist

BG Titan can help infrastructure owners and developers bring cybersecurity into the same project discipline as safety, quality, cost, delivery, procurement, and commissioning.

Cybersecurity stops being a side document and becomes part of the project acceptance standard.

The Issue

Exposed OT Is an Open Door

Many industrial systems were designed for reliability, not internet exposure. That was acceptable when they were isolated. It is dangerous when they are searchable, remotely reachable, or connected through poorly controlled support paths. Authorities warn that internet-connected OT devices are easy targets and can be found using open-source search tools.

THE EXPOSURE FLOW

01 **Internet-facing HMI**
a human-machine interface is reachable from outside.

02 **Weak or default credential**
a password was never changed, reused, or shared.

03 **Unauthorized access**
the attacker can view or attempt to manipulate industrial activity.

04 **Operational confusion**
operators may not know whether readings, alarms, or commands are trustworthy.

05 **Safety and continuity pressure**
the site may need to shut down, isolate equipment, or revert to manual control.

WHY THIS IS A BUSINESS OPPORTUNITY

- Find what is visible.
- Remove what should not be visible.
- Control what must remain reachable.
- Prove the change with evidence.

Opportunity 2

OT Exposure Reduction Sprints

An OT exposure reduction sprint is a focused program designed to remove unnecessary attacker opportunity within weeks, not years. The goal is not to perfect everything. The goal is to reduce what is visible, reachable, weak, undocumented, or uncontrolled.

A PRACTICAL 30-60-90 PATH

FIRST 30 DAYS

VISIBILITY

- Identify internet-facing OT
- Map remote access paths
- Identify exposed engineering tools
- Find shared accounts
- Find default credentials
- Identify critical supplier connections

NEXT 60 DAYS

CONTAINMENT

- Remove public exposure
- Disable unnecessary services
- Enforce MFA where appropriate
- Close dormant accounts
- Place remote access behind controlled gateways
- Separate IT from OT pathways

NEXT 90 DAYS

PROOF

- Document the new access model
- Validate segmentation
- Confirm backup and manual operation plans
- Review supplier access logs
- Rehearse incident escalation

WHAT CUSTOMERS RECEIVE

- **A clear asset and exposure picture.**
- **A prioritized remediation list.**
- **Executive evidence.**
- **Operational continuity confidence.**

HOW BG TITAN CAN ASSIST

BG Titan can coordinate this work across engineering, operations, IT, suppliers, contractors, finance, and leadership, because exposure reduction is a change-control exercise inside a live operating environment.

The Issue

Remote Access Has Become the New Service Road

Every infrastructure operator needs maintenance. Vendors need to patch equipment. Engineers need to troubleshoot. Contractors need temporary access. Management wants dashboards. Field teams need mobility. Remote access is not the enemy.

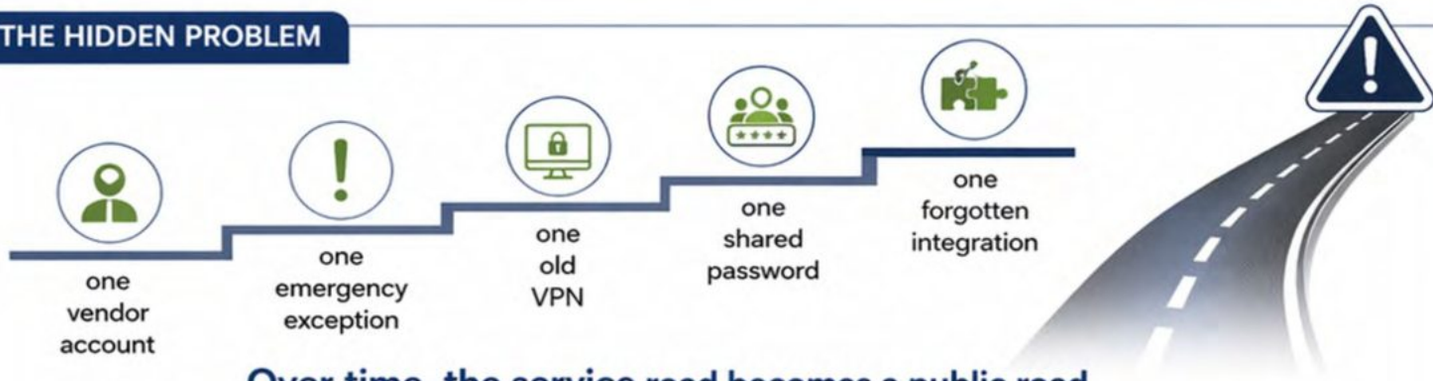
Uncontrolled remote access is.

60%
phishing remained the dominant intrusion vector

80%+
AI-supported phishing was reported in more than 80% of observed social engineering activity worldwide by early 2025

Source: ENISA Threat Landscape 2025.

THE HIDDEN PROBLEM



Over time, the service road becomes a public road.

WHAT MUST CHANGE

- approved before it starts
- limited to what is needed
- recorded while it happens
- revoked when it ends
- reviewed when risk changes

The opportunity is not to block remote work.
It is to make remote work safe enough for critical operations.

Opportunity 3

Controlled Remote Operations and Zero-Trust Edge Access

Critical infrastructure needs a modern access model: never assume trust simply because someone has a password or is on the network. A controlled remote operations model brings discipline to vendors, field teams, engineers, and command centers.

THE FLOW CUSTOMERS NEED

1. **Verify the person** – who is asking for access?
2. **Verify the device** – is the laptop or workstation approved, updated, and known?
3. **Verify the purpose** – what system is being accessed, for what task, and for how long?
4. **Broker the session** – access is granted through a controlled path, not an open tunnel.
5. **Record and monitor** – the session is logged, monitored, and available for review.
6. **Expire the privilege** – access ends automatically when the work ends.

TITAN | veea

BG Titan's partnership with Veea points toward secure edge infrastructure as a major *practical arena*, combining computing, communications, storage, security, IoT integration, edge AI, and Zero Trust Network Access at the edge.

Source: *Veea/BG Titan announcement.*

HOW BG TITAN CAN ASSIST

BG Titan can help infrastructure customers design controlled access into new and existing projects by aligning project requirements, edge connectivity, supplier access, operating practices, and cybersecurity partners. This is especially relevant for utilities, energy assets, distributed facilities, ports, remote communities, field operations, and industrial environments.

Connect more, expose less.

The AI Threat

Attackers Are Becoming Faster, Cheaper, and More Convincing

Artificial intelligence is changing the economics of cybercrime. It lowers barriers, removes friction, and multiplies an attacker's reach—making every organization a more likely target.

AI-ENABLED ATTACKER ADVANTAGES

1. Research faster
AI scans publicly available data to profile targets in minutes.

2. Write better phishing messages
AI crafts polished, context-aware messages that bypass suspicion.

3. Translate scams naturally
AI translates and localizes content with native accuracy.

4. Generate code faster
AI helps attackers build and adapt tools and malware in less time.

5. Impersonate voices and brands
AI voice cloning and brand replication increase believability.

6. Process stolen data at greater scale
AI summarizes, correlates, and extracts value from more data, faster.

THE UK NCSC POINT IS CLEAR

AI will almost certainly make cyber intrusion more effective and efficient, increasing the frequency and intensity of cyber threats.

AI's growing use in critical infrastructure also increases the attack surface.

Source: UK NCSC.

WHY THIS MATTERS TO INFRASTRUCTURE CUSTOMERS

Finance employee receives a perfect supplier-payment email.

Plant manager receives a convincing urgent safety message.

Contractor receives a fake login prompt.

Technician receives AI-assisted instructions from an attacker posing as support.

THE NEW RISK EQUATION

OLD MODEL: HIGH FRICTION

Attackers needed more:

- Time to research and craft attacks
- Specialized skills and tools
- Language ability
- Manual effort to scale

NEW MODEL: AI REDUCES FRICTION

AI lowers the bar:

- Faster research and targeting
- Higher-quality content and code
- Real-time translation and localization
- Automated scale and adaptability

THE TAKEAWAY

More attempts. More believable attempts. More pressure on organizations with outdated awareness training, weak verification, or informal approval processes.

For infrastructure operators, AI threat readiness is no longer optional. It is part of operational safety.

Opportunity 4

AI Threat Readiness and Shadow-AI Control

AI is not only a tool used by attackers; it is also being adopted inside organizations faster than security and compliance teams can govern it.

IBM FINDINGS

63%
of breached organizations studied lacked AI governance policies

20%
experienced breaches linked to shadow AI

USD 670,000
shadow AI incidents added up to USD 670,000 to the average breach cost

97%
among organizations reporting AI-related breaches, said they lacked proper access controls

WHAT CUSTOMERS NEED NOW

1. **AI inventory –** which tools, models, vendors, copilots, chatbots, and automation features are being used?
2. **Data boundaries –** what information can employees upload and what data must never leave controlled environments?
3. **Access controls –** who can use AI tools, connect them to company systems, or train them on operational data?
4. **Deepfake and fraud verification –** how are payment changes, executive instructions, vendor requests, and emergency actions verified?
5. **AI incident playbooks –** what happens if AI output is manipulated, sensitive data is uploaded, or an AI-enabled vendor tool behaves unexpectedly?

HOW BG TITAN CAN ASSIST

BG Titan can help customers turn AI from unmanaged risk into a governed capability. We bring structure, controls, and clarity to every stage of AI adoption, connecting leadership, legal, procurement, IT, OT, vendors, and operations.

> **AI governance must be practical. It cannot live only in policy. It must control what people actually do during procurement, maintenance, reporting, planning, analytics, and emergency response.**

The AI-in-OT Issue

When Smart Systems Touch Physical Operations

AI can improve infrastructure by helping predict maintenance needs, optimize energy use, detect abnormal behavior, analyze sensor streams, support operators, and identify early warning signs.

AI in operational technology is different from AI in office work. **In OT, a bad recommendation can lead to real-world consequences.**

AI IN OT INTRODUCES REAL RISKS

- **A bad recommendation** can affect physical systems.
- **A delayed decision** can affect safety.
- **A false reading** can affect operations.
- **An opaque vendor feature** can create hidden exposure.
- **An always-connected cloud tool** can become a new attack path.

JOINT INTERNATIONAL GUIDANCE

Joint international guidance states that AI can improve efficiency and decision-making in industrial control systems.

However, AI integration into OT introduces risks such as:

- OT process-model drift
- Safety-process bypasses

Source: *Secure AI in OT guidance.*

ADDITIONAL CHALLENGES

- Increased system complexity
- New vulnerabilities
- Cloud security risks
- Latency
- Compatibility problems
- Lack of vendor transparency

THE CUSTOMER CONCERN

Infrastructure owners want the benefits of AI, but do not want AI to:

- Create new attack paths
- Enable unapproved vendor connections
- Drive unsafe automation
- Blur accountability and responsibility
- Cause data leakage
- Drive operator overreliance

The opportunity is not anti-AI.
It is safe AI adoption for critical operations.

Opportunity 5

Safe AI-in-OT Integration

> The right question is not:
>
> **"Should critical infrastructure use AI?"**
>
> The right question is:
>
> **"Where can AI add value without taking unsafe control?"**

STRONG EARLY USE CASES

Predictive maintenance
identify equipment degradation before failure

Anomaly detection
spot unusual network, process, or sensor behavior

Energy optimization
support efficiency without overriding safety-critical controls

Operator assistance
summarize alarms, manuals, logs, and procedures

Document intelligence
search engineering records, supplier documents, compliance files, and maintenance histories

GUARDRAILS THAT MATTER

1. **Human-in-the-loop for safety-critical actions**
   AI may advise, but humans approve actions affecting physical systems
2. **Test before production**
   use non-production or simulated environments wherever possible
3. **Fail back to known-good operation**
   AI-enabled processes should revert to traditional automation or manual control
4. **Vendor transparency**
   operators need to know where models are hosted, what data is used, what external connections exist, and whether AI features can be disabled
5. **Logged decisions**
   inputs, outputs, overrides, and exceptions should be recorded for review

HOW BG TITAN CAN ASSIST

BG Titan can help customers evaluate AI opportunities in the context of engineering design, OT safety, vendor selection, procurement, project execution, operating requirements, and long-term maintainability.

The winning AI strategy is not the flashiest; it is the one operators can trust under pressure.

The Ransomware Reality

Criminals Target Organizations That Cannot Afford Downtime

Ransomware has become an industrial business model. Attackers do not need to physically damage a facility to create leverage. They can encrypt systems, steal data, threaten public disclosure, disrupt scheduling, interrupt payments, pressure executives, and exploit regulatory fears.

THE ATTACKER'S LEVERAGE

1. You cannot operate
2. You cannot invoice
3. You cannot trust your data
4. You cannot serve customers
5. You cannot explain the outage fast enough

KEY STATISTICS

FBI IC3 2025

3,600+

ransomware complaints in 2025

reported losses exceeded USD 32 million

NEW VARIANTS

63

new ransomware variants identified by IC3 in 2025

about 5.25 new variants per month

DRAGOS INDUSTRIAL TREND

742

industrial ransomware incidents in Q3 2025

Q1: 708 | Q2: 657 | Q3: 742

MANUFACTURING EXPOSURE

72%

of Q3 industrial incidents recorded by Dragos affected manufacturing

ENISA INSIGHT

Ransomware-as-a-service, access brokers, and aggressive extortion are lowering barriers to entry and increasing pressure on victims.

WHY THIS MATTERS FOR CRITICAL INFRASTRUCTURE

- Downtime becomes leverage
- Recovery delays become negotiation pressure
- Operational opacity increases business risk
- Public and regulatory scrutiny intensifies

Ransomware prevention alone is not enough.
Customers need architectures that deny ransomware its leverage.

Opportunity 6

Denial-of-Ransomware Architecture

The strongest ransomware strategy is not only to stop malware; it is to make ransomware less profitable. A denial-of-ransomware architecture reduces the attacker's ability to spread, encrypt, extort, and pressure the business.

WHAT THAT LOOKS LIKE

1. **Immutable and offline backups**
   Backups cannot be altered or deleted by an attacker.
2. **Restore testing**
   The organization knows how long recovery takes because it has tested it.
3. **IT/OT segmentation**
   A corporate compromise does not automatically become an operational crisis.
4. **Least privilege**
   No user or system has more access than needed.
5. **Phishing-resistant access where possible**
   Credentials alone are not enough to enter critical systems.
6. **Controlled vendor access**
   Third parties do not become permanent side doors.
7. **Manual operating procedures**
   Operators know how to maintain essential functions if digital systems are restricted.
8. **Executive decision playbooks**
   Leaders know when to isolate systems, notify authorities, communicate with customers, and activate recovery.

FBI RECOMMENDATIONS

- Maintain **off-site or offline** backups.
- Use **encrypted** and **immutable** backup data.
- **Eliminate default passwords.**
- **Disable unnecessary protocols** and services.
- **Audit privileged accounts.**
- Apply **least privilege** across all systems and users.

Source: FBI IC3 2025.

HOW BG TITAN CAN ASSIST

BG Titan can connect technical ransomware controls to operational continuity and infrastructure delivery across operations, engineering, suppliers, communications, procurement, finance, regulators, and executive leadership.

A ransomware event should never be the first time those groups learn how to work together.

The Supply-Chain Issue

Your Weakest Door May Belong to Someone Else

CRITICAL INFRASTRUCTURE RELIES ON MANY SUPPLIERS

- Equipment manufacturers
- System integrators
- Maintenance contractors
- Cloud platforms
- Telecom providers
- Software vendors
- Security vendors
- Specialist engineers

Every supplier can help you perform better—faster delivery, lower cost, stronger capabilities.
Every supplier can also introduce risk—new access paths, unknown settings, and hidden weaknesses.

DEMAND AND REGULATORY DRIVERS

1 Market demand is rising.

Grand View Research cites **growing supply-chain complexity** and **third-party vendor ecosystems** as a driver of cybersecurity demand in critical infrastructure protection.

2 Regulation is catching up.

The EU **Cyber Resilience Act** introduces mandatory cybersecurity requirements for products with digital elements.

Reporting obligations from **11 September 2026**

Main obligations from **11 December 2027**

THE UNCOMFORTABLE REALITY

Hidden supplier issues can create major exposure.

- Default passwords
- Unpatched firmware
- Unclear update commitments
- Uncontrolled vendor remote access
- Unknown embedded AI features
- Unsupported legacy devices
- Weak incident-notification terms

A BUSINESS OPPORTUNITY

Customers need procurement that treats cybersecurity as a **selection criterion**, not an afterthought.

THE OLD QUESTION

Can you deliver the equipment?

THE NEW QUESTION

Can you deliver equipment we can safely operate, update, monitor, and recover?

Opportunity 7

Supplier Trust and Secure Procurement

Cyber-resilient procurement is one of the highest-leverage opportunities in critical infrastructure because once weak equipment is purchased, installed, integrated, and commissioned, the cost of correction rises sharply.

WHAT SECURE PROCUREMENT SHOULD INCLUDE

1	**Supplier cyber qualification**	Evaluate vendor security practices before selection.
2	**Secure-by-default requirements**	No default credentials, unnecessary open services, or undocumented remote-access paths.
3	**Vulnerability and patch commitments**	Define how vendors disclose, prioritize, and support security updates.
4	**Remote access rules**	Specify who can connect, when, how, for how long, and under what monitoring.
5	**AI transparency**	Require disclosure of embedded AI features, data use, external connectivity, model hosting, and disablement options.
6	**Acceptance testing**	Cyber controls are tested before handover, not assumed.
7	**Lifecycle evidence**	The customer receives documentation needed for audits, insurers, regulators, and future operators.

HOW BG TITAN CAN ASSIST

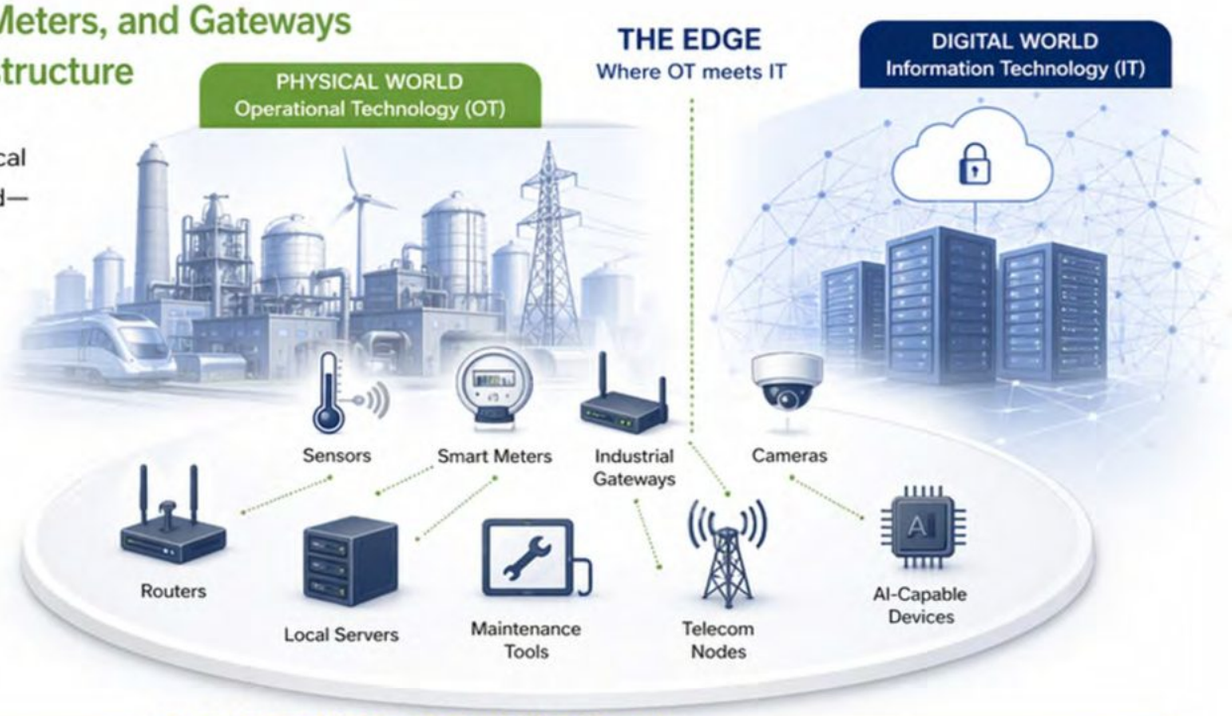
BG Titan can help turn cybersecurity into a procurement filter and help infrastructure owners avoid buying future risk in the name of short-term speed.

The best time to reject a weak cyber design is before it is bolted into the project.

The Edge Issue

Sensors, Cameras, Meters, and Gateways Are Becoming Infrastructure

The edge is where the physical world meets the digital world—near assets, people, and processes. It's where data is created, first decisions are made, and reliability is won or lost.



THE BENEFITS OF EDGE TECHNOLOGY

- Faster local decision-making
- Lower latency
- Better service reach
- Local analytics
- Less dependence on distant cloud systems
- More efficient field operations

THE CHALLENGE

The edge multiplies the number of devices that must be known, secured, updated, and monitored.

- Many locations
- Many devices
- Many updates
- Many configurations
- Many blind spots

More devices. More complexity. More to defend.

INSIGHT

Grand View Research reports that IoT and IIoT proliferation are accelerating cybersecurity demand. At the same time, cloud adoption and virtualization introduce risks such as:

- Shared-responsibility gaps
- Misconfiguration at scale
- Unauthorized access
- Insecure APIs

Source: Grand View Research.

THE EDGE RISK

Every edge device can become:

- A sensor for operations
- A bridge into the network
- A blind spot for security
- A data source for AI
- A dependency during an outage

THE CUSTOMER QUESTION

Not only "Can this device connect?" but "Can this device be trusted for years?"

- ☑ Secure identity
- ☑ Controlled access
- ☑ Update paths
- ☑ Local logging
- ☑ Segmentation
- ☑ Physical protection
- ☑ Supply-chain assurance
- ☑ Operating model for remote sites

Edge infrastructure is no longer peripheral; it is becoming **part of the critical asset.**

Opportunity 8

Secure Edge Infrastructure

The next generation of infrastructure will be more distributed, spanning power assets, water systems, transport corridors, ports, campuses, public safety networks, telecom expansions, and underserved communities. The business opportunity is to deploy this connectivity securely from the start.

WHAT SECURE EDGE INFRASTRUCTURE NEEDS

1. Identity for every device

Each device is known, approved, and accountable.

2. Segmentation by function

A camera network should not freely touch industrial controls; a meter should not open a path into corporate systems.

3. Secure update capability

Devices must be patched safely throughout their lifecycle.

4. Local resilience

Essential functions should continue when cloud connectivity is degraded.

5. Controlled data movement

Data should flow out safely without creating persistent inbound access to OT environments.

6. Zero-trust access

Users, vendors, and services are verified before access is granted.

TITAN | veea

BG Titan's strategic partnership with Veea is relevant because Veea describes its platform as edge computing with IoT integration, edge AI, security solutions, and Zero Trust Network Access for edge services.

HOW BG TITAN CAN ASSIST

BG Titan can help customers think beyond connectivity alone by combining connectivity, public-service delivery, cyber resilience, AI governance, supplier controls, and long-term operations. We bring the right partners, playbooks, and operating models to design and deliver secure edge infrastructure at scale—from planning and deployment to continuous improvement.

> **When a community or facility is connected for the first time, secure design should not arrive second.**

Regulation Is Becoming a Market Driver

Evidence Is Replacing Assurances

Governments and regulators are raising the bar. Organizations must demonstrate security through evidence—across assets, suppliers, and operations.

NIS2 COVERS 18 CRITICAL SECTORS

NIS2

NIS2 expands accountability, reporting, and oversight across 18 sectors vital to the EU economy and society.

THE EU CYBER RESILIENCE ACT RAISES THE BAR

Applies to products with digital elements across their entire lifecycle—planning, design, development, maintenance, and vulnerability handling.

WHAT CUSTOMERS ARE LEARNING

- Asset inventories
- Risk assessments
- Supplier due diligence
- Incident-response procedures
- Backup and restore tests
- Access-control records
- Training records
- Governance minutes
- Audit logs
- Business-continuity exercises

THE OPPORTUNITY

Make compliance a path to resilience—not just paperwork.

- Can we prove what we control?
- Can we prove who has access?
- Can we prove we can recover?
- Can we prove suppliers meet our standards?

In this market, documentation becomes part of the defense.

Opportunity 9

Compliance-to-Resilience Programs

Turn regulatory pressure into operational improvement. A well-designed program moves you from checking boxes to building resilience that stands up to real-world cyber pressure.

WHAT THE PROGRAM SHOULD PRODUCE

1. **A control map**
   Clear mapping of requirements to controls, systems, and owners.
2. **An evidence pack**
   Organized, audit-ready evidence that proves control effectiveness.
3. **A risk register**
   Living list of key risks, owners, mitigations, and residual risk.
4. **An executive dashboard**
   Real-time visibility into risk, compliance status, and resilience posture.
5. **An incident reporting path**
   Defined, tested path for fast and transparent incident reporting.
6. **A recovery proof point**
   Validated recovery procedures and tested results you can prove.

HOW BG TITAN CAN ASSIST

BG Titan helps align cyber resilience with how infrastructure gets built, financed, and operated.
We embed resilience across the full project lifecycle and bring stakeholders together around clear outcomes.

Legal
Owns rules
Translate laws and standards into clear contractual obligations.

IT
Owns systems
Design, secure, and operate technology with built-in controls.

Operations
Owns uptime
Run reliable operations and test resilience continuously.

Procurement
Owns suppliers
Select, manage, and monitor vendors for security and performance.

Finance
Owns funding
Protect investments and link resilience to value and risk management.

Executives
Own accountability
Set expectations, oversee performance, and ensure outcomes.

FROM
We have policies.
Reactive. Paper-based. Unproven.

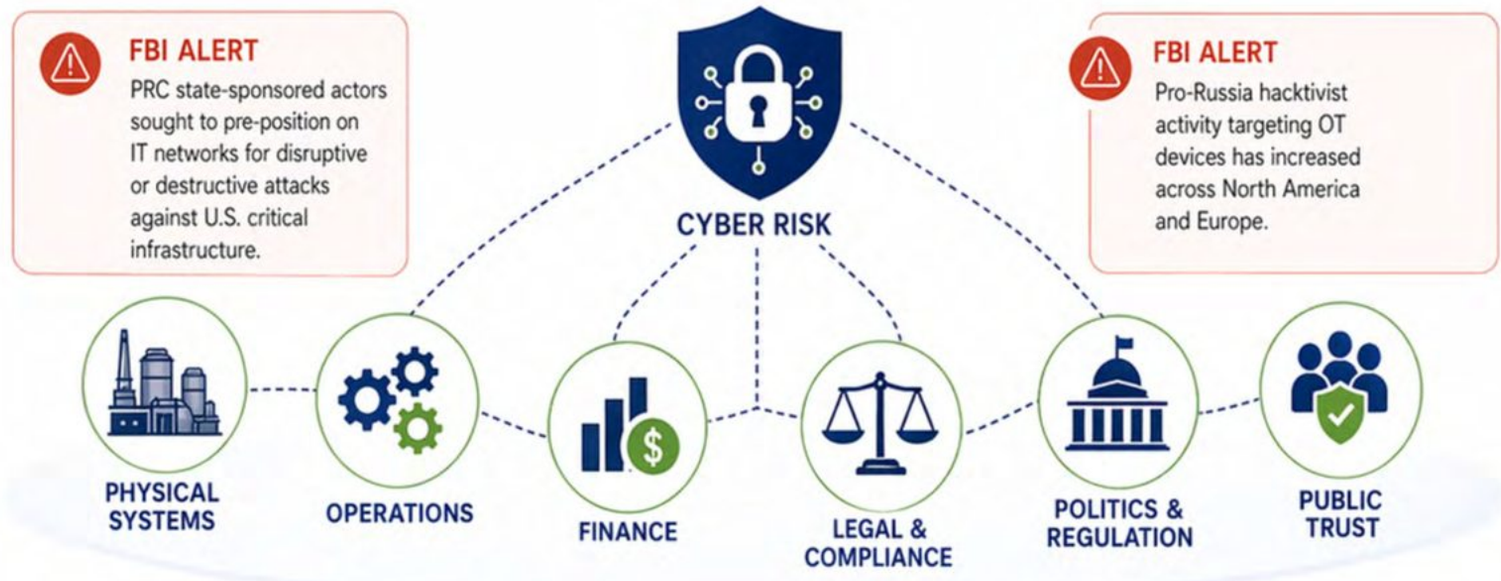
TO
We have proof that our infrastructure can withstand and recover from cyber pressure.
Resilient. Proven. Trusted.

Cyber, Physical, and Operational Risk Are Converging

The Control Room and the Boardroom Now Share the Same Risk

FBI ALERT
PRC state-sponsored actors sought to pre-position on IT networks for disruptive or destructive attacks against U.S. critical infrastructure.

FBI ALERT
Pro-Russia hacktivist activity targeting OT devices has increased across North America and Europe.



WHAT CONVERGENCE LOOKS LIKE

1. **Cyberattack on scheduling systems** leads to port delays and logistics disruption.
2. **Compromise of building systems** affects security, access, temperature, or safety.
3. **Water utility incident** forces operational caution and creates public trust pressure.
4. **Telecom disruption** cascades across emergency services, payments, transport, and operations.
5. **Ransomware event at a supplier** delays maintenance, makes parts unavailable, or erases operational visibility.

THE CUSTOMER NEED

FRAGMENTED REPORTING. FRAGMENTED RISK.

Cyber | Safety | Physical Security | Operations | Suppliers | Recovery

Siloed data. Different definitions. Limited visibility.
Gaps get missed. Decisions are slower.

ONE INTEGRATED RISK PICTURE.

Shared context. Real-time visibility. Faster, better decisions.
Resilience built into every decision.

That is the move from fragmented defense to resilient infrastructure.

Opportunity 10

Integrated Cyber-Physical Resilience Design

Resilient infrastructure projects connect cybersecuity, physical security, operational safety, business continuity, and executive governance—by design, not by chance.

CYBERSECURITY

- Identity
- Segmentation
- Monitoring
- Patching
- Logging
- Backups
- Secure remote access
- Supplier governance

PHYSICAL SECURITY

- Access control
- Site protection
- Cameras
- Perimeter monitoring
- Visitor processes
- Secure equipment rooms

EXECUTIVE GOVERNANCE

- Clear ownership
- Escalation paths
- Risk acceptance
- Investment decisions
- Incident authority

OPERATIONAL SAFETY

- Fail-safe mechanisms
- Human override
- Emergency stop logic
- Safe shutdown
- Tested procedures

BUSINESS CONTINUITY

- Manual operation
- Alternate sites
- Backup communications
- Spare equipment
- Recovery teams
- Customer communication

THE DESIGN PRINCIPLE

If digital control fails, operator should know what remains available.

If supplier connection is cut, operator should know what functions continue.

If cloud dashboard goes down, local site should still understand its state.

If AI gives an unsafe recommendation, the system should contain the impact.

HOW BG TITAN CAN ASSIST

BG Titan supports infrastructure customers by making resilience part of project development and delivery—designed for real-world conditions such as:

Contractors on site | Legacy equipment | Remote locations | Budget pressure | Regulatory scrutiny | Safety requirements | Long asset lifecycles

Critical infrastructure customers do not need theoretical security. They need operating resilience.

Capital, Insurance, and Cyber Diligence

Weak Cyber Posture Is Becoming a Transaction Risk

Cyber insurance adoption is accelerating, and boards are placing operational resilience at the top of enterprise risk agendas. These trends are driving growth in the critical infrastructure protection market.

The global critical infrastructure protection market is projected to reach **$338.3B by 2030,** driven by cyber insurance adoption, regulatory pressure, and investor demand for resilience.

THIS MATTERS BECAUSE CYBER WEAKNESS CAN BECOME A TRANSACTION ISSUE

1	Financing confidence	Lenders assess cyber risk before they commit.
2	Insurance terms	Underwriters set premiums based on real cyber exposure.
3	Project valuation	Weak controls reduce value and increase contingencies.
4	Government approvals	Regulators expect evidence of cyber readiness.
5	Supplier selection	Buyers exclude vendors that do not meet cyber standards.
6	Post-acquisition integration	Cyber gaps complicate integration and continuity.
7	Operational readiness	Cyber readiness is required for safe, reliable operations.

THE BUYER'S CONCERN

- Unsupported control systems
- Unknown remote access
- Missing network diagrams
- Unverified backups
- Untrained operators
- Supplier access with no contract controls
- AI tools using sensitive data
- Regulatory obligations not yet mapped

THE OPPORTUNITY

Cyber due diligence as a business service for infrastructure deals

1. What are we buying?
2. What could stop it?
3. What will remediation cost?
4. What must be fixed before close?
5. What must be funded after close?

In critical infrastructure, cyber diligence is no longer a technical appendix. It is part of investment protection.

Opportunity 11

Cyber Due Diligence for Infrastructure Deals

Cyber due diligence should become standard for investment, acquisition, concession, refinancing, and major modernization projects. The value is **turning risk into a clear investment plan.**

WHAT A CYBER DILIGENCE PACKAGE SHOULD INCLUDE

1	**Asset and architecture review**	Understand critical assets, systems, data flows, and external connections.
2	**Material risk assessment**	Identify, rate, and prioritize cyber risks that could impact operations, safety, or value.
3	**Supplier and contract review**	Evaluate suppliers, third-party access, SLAs, indemnities, and security obligations.
4	**Recovery capability review**	Assess backup, business continuity, incident response, and recovery time and point objectives.
5	**AI and data review**	Review AI use, data governance, data residency, model security, and privacy controls.
6	**Remediation budget**	Estimate cost to close gaps and align with risk appetite and transaction timelines.
7	**Insurer and lender pack**	Prepare evidence and documentation to support insurance, financing, and lender requirements.

HOW BG TITAN CAN ASSIST

BG Titan's advisory, financing, procurement, project development, engineering, risk-control, and cybersecurity positioning can help customers treat cyber diligence as part of the full transaction picture.

DECISION-MAKER VIEW

RISK | COST | PRIORITY | TIMELINE | ACCOUNTABILITY | BUSINESS IMPACT

That is what decision-makers need before they commit capital.

The People and Ownership Gap

OT Security Needs Clear Leadership

No single group sees everything.

OT security is a shared responsibility that requires aligned roles, clear decision rights, and executive oversight.

IT	OT	ENGINEERING	PROCUREMENT	EXECUTIVES
Protects data, networks, and identity.	Keeps assets safe, available, and reliable.	Designs and maintains systems.	Brings in vendors and manages contracts.	Sets direction, approves risk, owns outcomes.

Only together can they see the full picture and make the right decisions.

FORTINET: STATE OF OT SECURITY 2025

46% achieved Level 4 OT security maturity in 2025.

52% place OT security under the CISO, up from 16% in 2022.

80% are planning to follow.

THE CUSTOMER CHALLENGE

- Who approves OT changes?
- Who owns vendor access?
- Who validates backups?
- Who decides when to isolate systems?
- Who communicates with regulators?
- Who tells operations what changed?
- Who trains contractors?

WHY THIS IS AN OPPORTUNITY

Customers need operating models, not just more tools.

A strong OT cybersecurity program defines:

- Clear roles and accountability
- Decision rights and authority
- Escalation paths
- Training and competency
- Supplier responsibilities
- Executive reporting

The market is moving from "buy another security product" to "make the organization cyber-operationally ready."

Opportunity 12

OT Managed Resilience and Training

Resilience is built through structure, preparation, and practice. A managed operating model ensures people, processes, and technology work together to prevent, withstand, and recover.

THE MANAGED RESILIENCE MODEL

1. **OT security governance**
   Define roles, responsibilities, and decision rights for OT security.
2. **Asset and exposure monitoring**
   Maintain real-time visibility of assets, connections, and configurations.
3. **Incident readiness**
   Prepare people, processes, and tools to detect, respond to, and contain incidents.
4. **Supplier access control**
   Control and monitor third-party and remote access to OT environments.
5. **Training for real roles**
   Provide role-based training so teams know what to do and why it matters.
6. **Tabletop exercises**
   Practice realistic scenarios to strengthen coordination and decisions.
7. **After-action improvement**
   Capture lessons learned and turn them into clear improvements.

HOW BG TITAN CAN ASSIST

We help you build a practical operating rhythm with recurring activities that keep resilience strong.

- **Monthly risk reviews**
  Review risks and controls; track issues to closure.
- **Quarterly access audits**
  Validate user access and remote connections; remove unnecessary access.
- **Semiannual recovery exercises**
  Test backup, restore, and failover capabilities under realistic conditions.
- **Annual supplier reassessments**
  Reassess supplier security performance and risk.
- **Executive cyber-resilience briefings**
  Share status, priorities, and decisions with leadership.

Make cyber resilience a normal part of infrastructure operations, not a panic activity after an incident.

The Denial-of-Opportunity Model

Make Attacks Smaller, Slower, Louder, and Less Profitable

1	**Know the asset**	You cannot defend what you cannot see.
2	**Reduce exposure**	Remove internet-facing OT, default passwords, unnecessary services, weak remote access, and dormant accounts.
3	**Control identity**	Verify users, devices, vendors, and service accounts.
4	**Segment and contain**	Prevent one compromise from becoming an enterprise-wide or site-wide crisis.
5	**Watch behavior**	Detect unusual access, abnormal process behavior, suspicious data movement, and supplier anomalies.
6	**Rehearse recovery**	Test backups, manual operations, communications, and decision-making.
7	**Govern AI and suppliers**	Control new attack surfaces before they become embedded dependencies.

WHAT THIS DOES TO THE ATTACKER

Smaller
reaches fewer systems.

Slower
must work harder and take more time.

Louder
abnormal actions are more visible.

Less profitable
the organization can recover, communicate, and continue essential operations.

THE BG TITAN PERSPECTIVE

Denial-of-opportunity is a business and infrastructure strategy. It affects every project, modernization, procurement decision, connectivity rollout, AI deployment, and supplier relationship.

That is how cyber defense moves upstream.

Ten Questions Every Critical Infrastructure Customer Should Ask Now

1

What operational systems are reachable from the internet?

If the answer is unknown, exposure may already exist.

2

Which vendors can remotely access our environment?

Access should be approved, logged, limited, and revocable.

3

Can IT compromise reach OT?

Segmentation should prevent corporate incidents from becoming operational crises.

4

Are default credentials fully removed?

Default passwords remain one of the most preventable risks.

5

Can we operate manually if digital systems are degraded?

Manual capability must be realistic and tested.

6

Have we restored from backups recently?

A backup that has never been restored is an assumption, not a recovery capability.

7

Where are AI tools touching our data or operations?

Shadow AI, embedded AI features, and vendor AI tools must be governed.

8

Do suppliers meet our cyber requirements?

Procurement should verify security before equipment and software are accepted.

9

Do executives know who decides during a cyber incident?

Slow decision-making can deepen operational damage.

10

Can we prove our resilience to regulators, lenders, insurers, and customers?

Evidence is becoming part of the market.

The practical takeaway

A customer does not need to answer every question perfectly on day one.
But unanswered questions should become funded workstreams.
That is where resilience starts.

The Direction of Travel

Critical Infrastructure Will Be Resilient by Design or Exposed by Default

The future of critical infrastructure is connected. It will use more sensors, more edge computing, more AI, more remote operations, more cloud analytics, more supplier integration, more automation, and more regulatory reporting.

Done well, that future is powerful. Done poorly, it becomes fragile.

1 WHAT THE FUTURE WILL INCLUDE

- More sensors
- More edge computing
- More AI
- More remote operations
- More cloud analytics
- More supplier integration
- More automation
- More regulatory reporting

2 THE OPPORTUNITY AHEAD

The next wave of value will come from infrastructure that is resilient by design, not patched after the fact.

1. Securely designed
2. Carefully procured
3. Properly segmented
4. Supplier-aware
5. AI-governed
6. Edge-secured
7. Continuity-tested
8. Investment-ready

3 HOW BG TITAN GROUP CAN ASSIST

BG Titan Group helps customers bring cyber resilience into the broader infrastructure lifecycle.

Concept and feasibility › Project development › Financing and advisory › EPC and PMC/PMT › Procurement and supplier qualification › Technology and cybersecurity solutions › Commissioning and operational readiness › Risk management and continuity planning

The market is moving from reaction to denial-of-opportunity.

The organizations that move first will not simply reduce cyber risk.
They will protect uptime, safety, capital, reputation, compliance, and public trust.

The strongest cyber defense for critical infrastructure is not a single tool. It is a better-built infrastructure business.