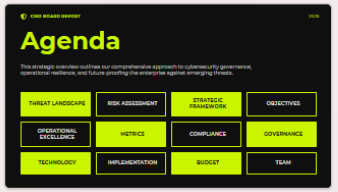
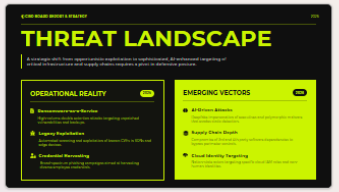
1

2

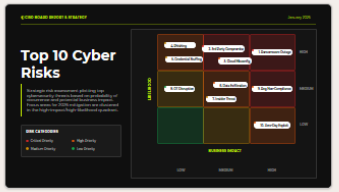


3

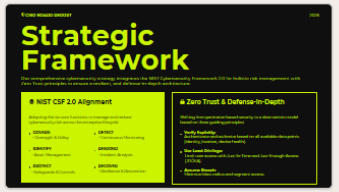


4

5



6



7

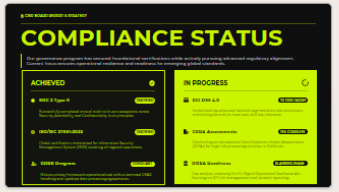
8

9

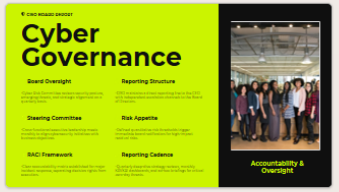
10

11

12

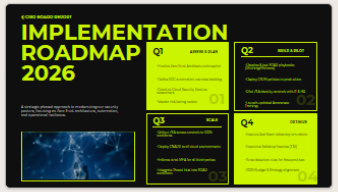


13



14

15



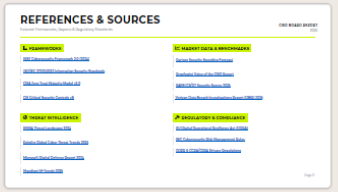
16

17

18

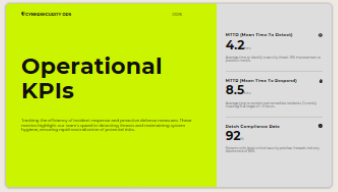
19

20

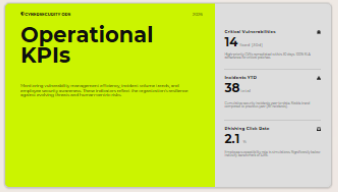


21

22

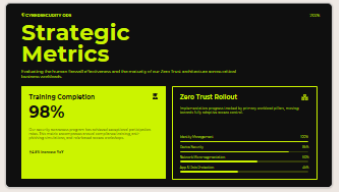


23

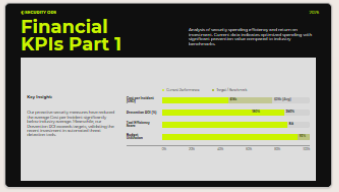


24

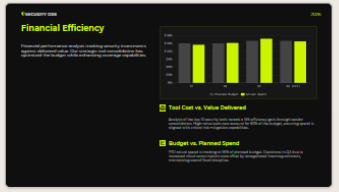
25



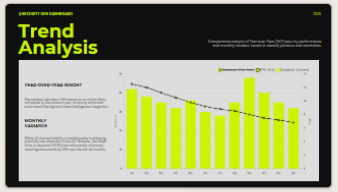
26



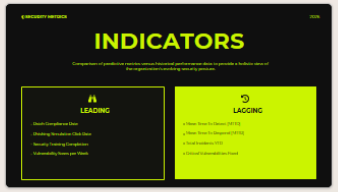
27



28



29

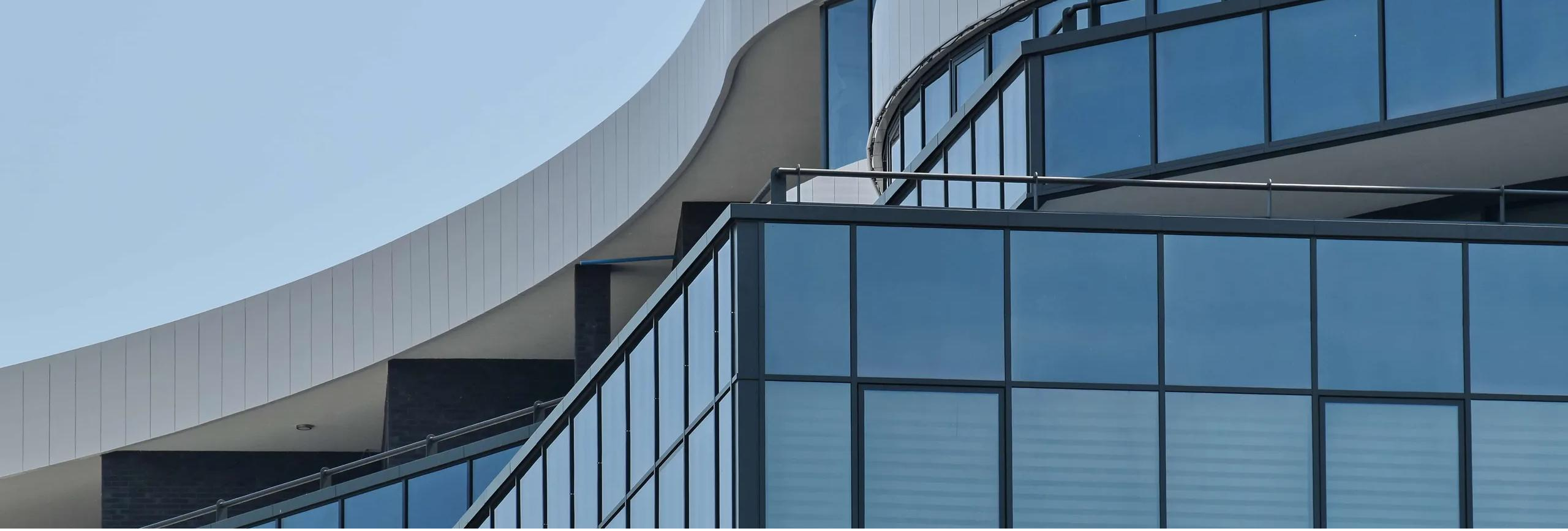


30

31

32

33



Top 20 Cybersecurity Risks 2026

Executive Brief for CISO

01

Prioritizing resilience against threat automation, software supply chain complexity, and critical infrastructure fragility.

[Your Company].

March 2026

Security Team

Table of Contents

Structured Overview of the 2026 Threat Landscape

Executive Overview

Strategic Threat Landscape & 2026 Priorities

KEY TRENDS 2026

- Shift from human-in-the-loop to **autonomous Agentic AI** attacks executing at machine speed.
- Explosion of unmanaged **Non-Human Identities (NHI)** as a primary cloud attack vector.
- Supply chain attacks targeting **transitive dependencies** deep within the software stack.
- State-sponsored **pre-positioning** in critical physical infrastructure (OT).

BUSINESS IMPACT

- **Velocity:** Defensive response times must shrink from minutes to seconds.
- **Cost:** Regulatory fragmentation drives up compliance overhead & breach penalties.
- **Safety:** Cyber-physical attacks now threaten patient lives & public safety.

5 Strategic Priorities

Focus areas to build resilience against 2026 threats.

1. **AI Governance & Policy Enforcement**
2. **Machine Identity Control (NHI)**
3. **Software Supply Chain Security**
4. **OT & Physical Infrastructure Preparedness**
5. **AI-Augmented SOC Operations**

Critical Metrics

MTTR (Mean Time To Respond)

< 15 Minutes (Target)

Sensitive Data Exposure

0% in Shadow AI Tools

NHI Control Coverage

100% Automated Rotation

OSS Dependencies Verified

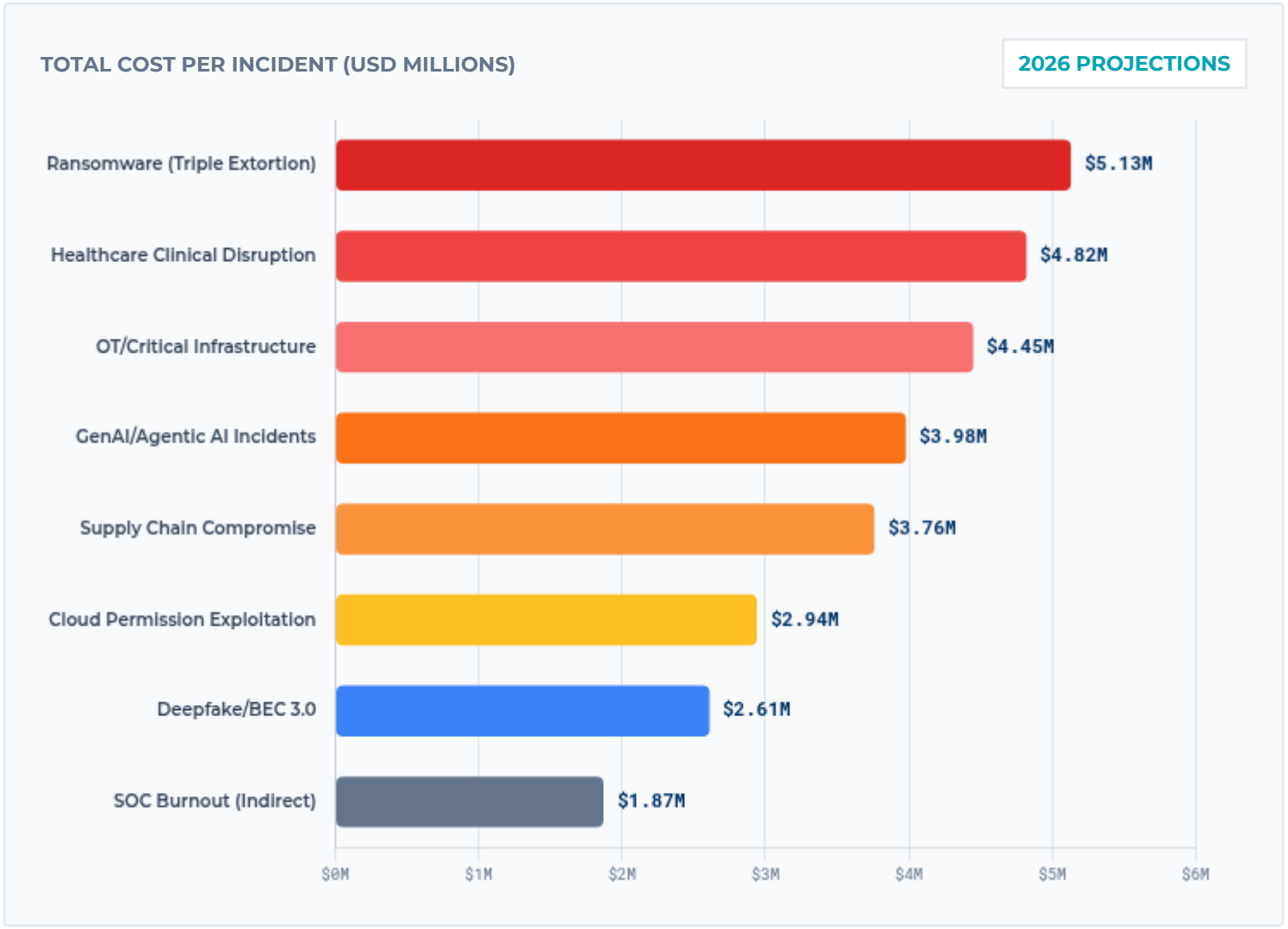
> 95% Signed/Attested

Critical Patch Time

< 24 Hours (Internet Facing)

Average Incident Cost by Risk Category

Financial Impact Analysis 2026



STRATEGIC INSIGHTS

Ransomware remains costliest at **$5.13M** due to triple extortion tactics. **GenAI incidents** are rapidly emerging as a top tier cost driver ($3.98M). Recovery times vary significantly, from 45 days (Ransomware) to 180+ days (Supply Chain).

COST BREAKDOWN (TOP 3 CATEGORIES)

CATEGORY	DIRECT COST	REGULATORY	RECOVERY
Ransomware	$2.5M	$1.4M	45 Days
Healthcare Disruption	$2.1M	$1.8M	90 Days
Supply Chain	$1.9M	$0.8M	180 Days
GenAI / Agentic AI	$1.5M	$1.2M	60 Days

PREVENTION ROI

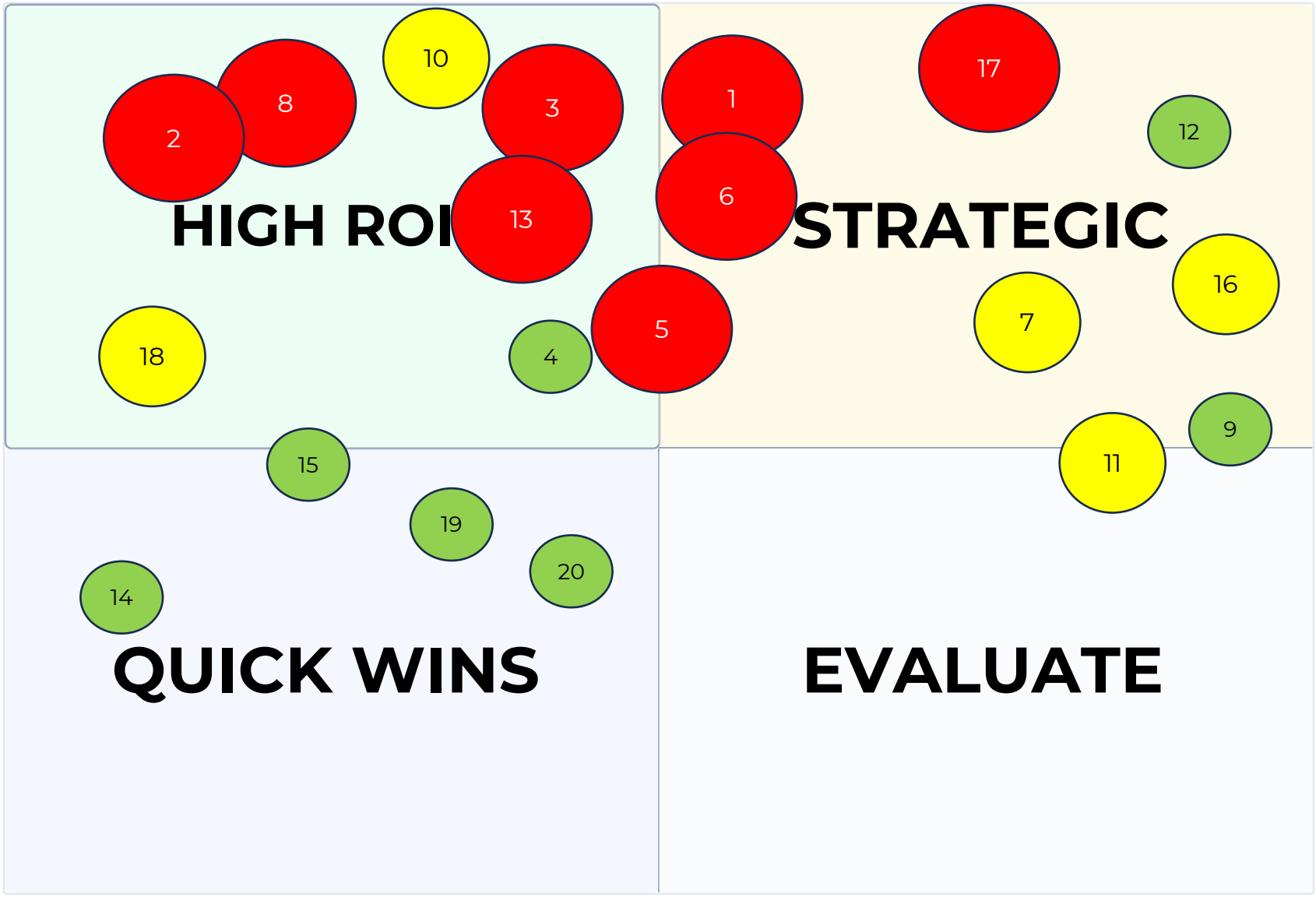
Every **$1** invested in prevention saves **$4-7** in response costs.

400-700%

SOURCES: IBM Cost of Data Breach 2025 Ponemon Institute Sophos Report

Cost vs. Impact Analysis

Strategic Investment Prioritization Matrix



INTERPRETATION LEGEND

- **Position:** Cost vs Impact
- **Size:** Urgency / Severity / Colour

#00 Corresponds to Risk ID

INVESTMENT ZONES

TOP LEFT: HIGH ROI (PRIORITY)
Low Cost / High Impact. Immediate action.

TOP RIGHT: STRATEGIC
High Cost / High Impact. Major CAPEX.

BOTTOM LEFT: OPERATIONAL
Low Cost / Quick wins.

METHODOLOGY & SOURCES

Cost est: **Gartner** 2025 Spending Guide & Bakerdonelson Cost of a data breach report 2025.

Impact: **IBM CODB 2025** ($4.88M avg), **WEF** Reports.

Bubble size: CVSS-style urgency scoring (exploit likelihood × business criticality).

RISK #08

Abuse of Non-Human Identities (NHI)

IMPACT SEVERITY

HIGH

DESCRIPTION

Non-human identities (service accounts, API keys, bots, tokens) now outnumber human users 10:1. These "machine identities" are often over-privileged and unmonitored. Attackers actively target these unguarded credentials to bypass MFA and gain silent, persistent access to cloud environments.

BUSINESS IMPACT

- **Persistence:** Silent backdoor access.
- **Escalation:** Rapid pivot to admin privileges.

PRIMARY ATTACK VECTORS

Hardcoded Secrets
Keys left in source code or public repositories.

Token Theft
Stealing session tokens from CI/CD logs.

Lateral Movement
Using service accounts to cross cloud boundaries.

NHI ATTACK LIFECYCLE

1. Discovery (Scan Repos)
2. Extraction (Steal Keys)
3. Lateral Movement
4. Privilege Escalation
5. Persistence (Backdoor)

STRATEGIC MITIGATION

- Deploy **Secret Scanning** in all CI/CD pipelines.
- Implement **ISPM** (Identity Posture Mgmt).
- Enforce short **TTL (Time-to-Live)** for tokens.
- Strict **Least Privilege** for service accounts.

SOURCES: · CyberArk Threat Research (NHI Trends) · The Ultimate Guide To Non-Human Identities

RISK #12

Smart Cities & IoT Vulnerabilities

IMPACT SEVERITY
HIGH

DESCRIPTION

The rapid proliferation of IoT devices in urban infrastructure (traffic, water, power) creates a massive, unpatched attack surface. With billions of connected sensors often lacking basic security, attackers can pivot from edge devices to critical control systems, threatening public safety and service continuity.

BUSINESS IMPACT

Public Safety: Disruption of emergency services and utilities.

Infrastructure: Compromise of OT/IT convergence points.

PRIMARY ATTACK VECTORS

Legacy Systems
Outdated firmware in critical infrastructure sensors with no update patch.

Interconnected Networks
Lateral movement from unsecured public IoT kiosks to core city networks.

Physical Impact (PDoS)
Permanent Denial of Service rendering smart hardware physically unusable.

STRATEGIC MITIGATION STRATEGIES

- Enforce strict **Network Segmentation** to isolate IoT/OT layers from corporate IT.
- Implement **Zero Trust** verification for every device interaction and data flow.
- Deploy automated **Firmware Auditing** & rapid patch management cycles.
- Mandate **"Secure by Design"** standards for all third-party city vendors.

Insight
IoT security protects billions of devices that cannot defend themselves. With 21.1 billion connected devices in 2025 and most unable to run endpoint agents, network-level visibility is the primary detection method. **Threats are escalating rapidly.**

SOURCES: · IoT Cyberattacks +41% (Check Point) · Smart City Cybersecurity (Kaspersky)

RISK #16

Undersea Cables & Space Assets

IMPACT SEVERITY
HIGH

DESCRIPTION

Critical global connectivity infrastructure-undersea cables carrying 99% of internet traffic and space assets like satellites are increasingly targeted by state actors. Physical sabotage and cyber-electronic jamming threaten to sever communications and disrupt GPS/GNSS services.

BUSINESS IMPACT

- **Connectivity:** Total loss of regional internet access.
- **Operational:** GPS failure impacting logistics/nav.

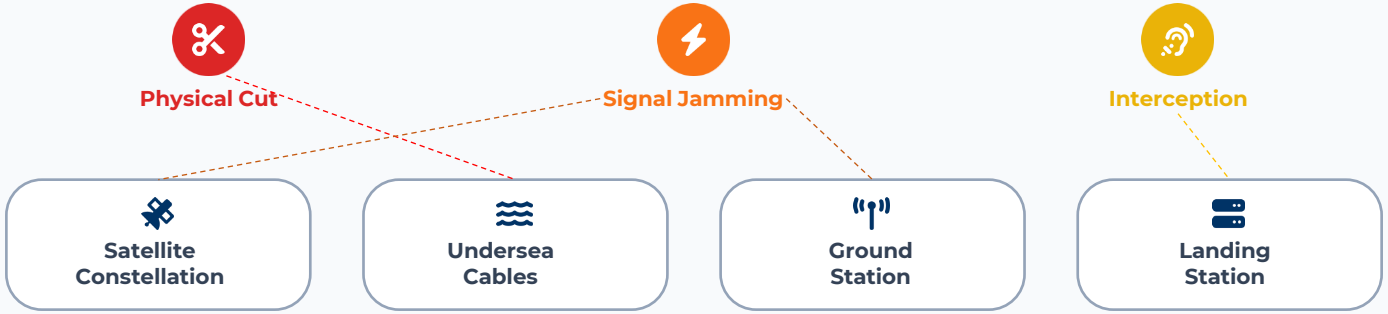
PRIMARY ATTACK VECTORS

Physical Sabotage
Cutting cables via "fishing vessels" or submersibles.

Signal Jamming
Disrupting satellite uplinks/downlinks.

Interception
Tapping data flows at landing stations.

INFRASTRUCTURE ATTACK SURFACE



STRATEGIC MITIGATION

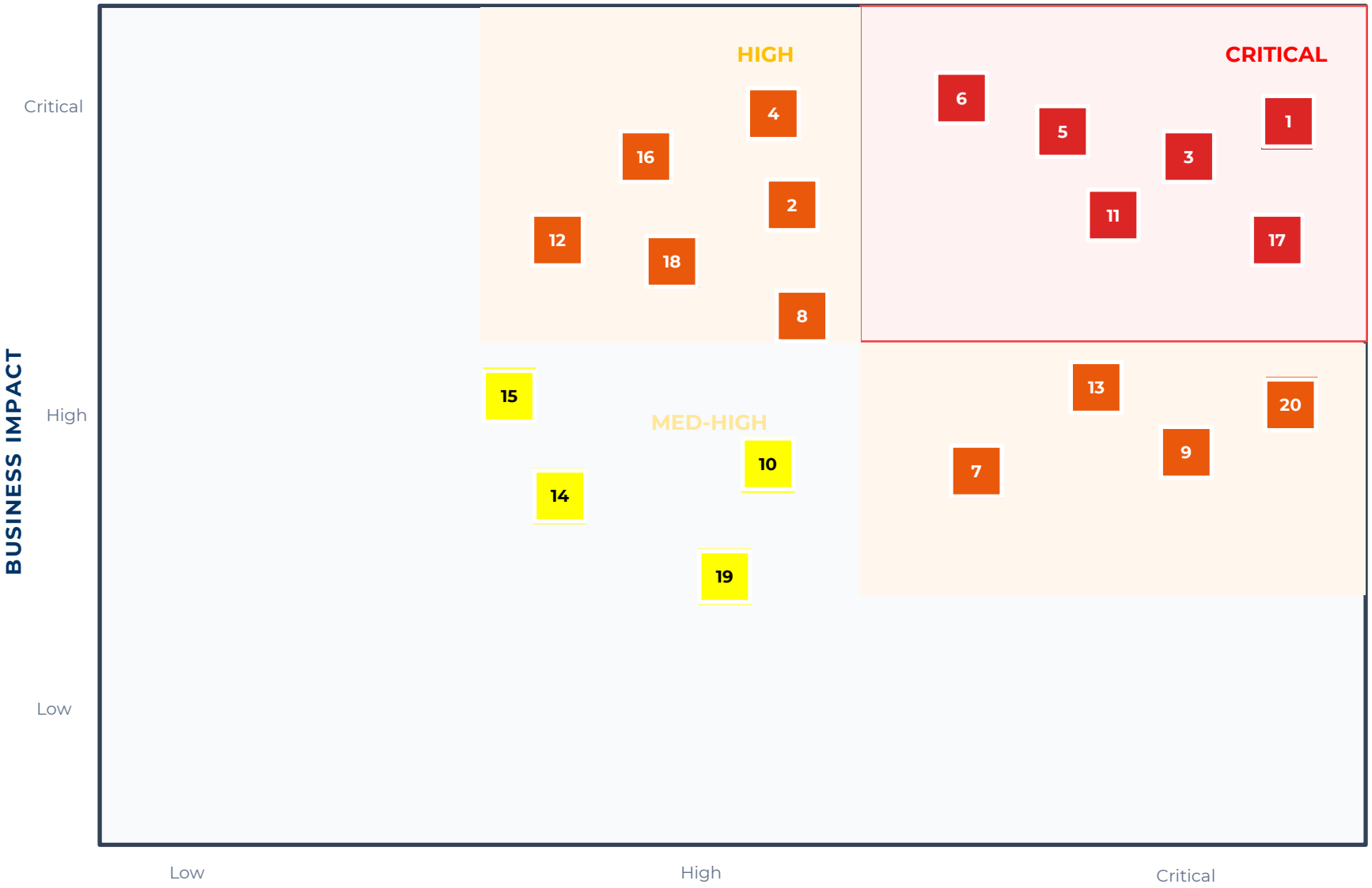
- Diversify **Network Routes** (terrestrial + satellite).
- Deploy **Out-of-Band** communications backup.
- Implement **Link-Layer Encryption** for all transit data.
- Monitor **Physical Proximity** alerts for cables.

SOURCES: · Atlantic Council: Submarine Cable Security · CSIS Space Threat Assessment 2025

Risk Prioritization Matrix

Strategic heatmap of top 20 risks based on business impact and probability.

2026 OUTLOOK



MATRIX LEGEND

- **Critical Priority**
- High Attention
- Systemic Risk

TOP 8 CRITICAL RISKS

#1 Agentic AI & Decision Hijacking
#3 Deepfake & Identity Fraud
#5 Triple Extortion Ransomware
#6 OT Pre-positioning
#11 Hybrid Warfare
#17 Clinical Risk in Healthcare

Action Plan

- Define Executive Risk Owners for all Quadrant 1 (Red) risks.
- Initiate 90-day mitigation sprints.
- Establish KPIs for exposure reduction in Cloud & Healthcare sectors.

Thank You

Let's Secure 2026.

> The 2026 landscape demands **AI-centric controls**, **NHI mastery**, and **supply chain/OT resilience**.
>
> **Next Steps:** Engage in our 4-week maturity assessment, define your 12-month roadmap, and implement CISO dashboards.

Email
security@company.com

Website
www. company.com

Location
Canada

Strategic Support
Maturity Assessments & Security Roadmaps

Acceptable Use Policy (AUP)

Information Technology Resources

This document is an illustrative example of an Acceptable Use Policy, based on generally recognized good practices. You are free to reuse and adapt it, in whole or in part, to align with your organization's context, branding, and existing policies. It does not constitute legal advice, and the author assumes no responsibility or control over how this content is implemented, interpreted, or modified within your environment.

#	Date	Modified by	Comments
0.1	04-05-2025	Synergie Consultation	
1.0	03-03-2026	Synergie Consultation	• New template version • Add section 8 • Add 2 references

Mettre à jour la table...

Table of contents

Executive Dashboard

2026 CYBERSECURITY RISK MANAGEMENT DASHBOARD

Date: January 2026

RISK SUMMARY

Total Risks Identified:	20	High Priority Risks:	8
Critical Priority Risks:	10	Medium Priority Risks:	2

TOP 5 HIGHEST RISK SCORES **

Risk ID	Risk Category	Risk Score	Priority
R05	Triple Extortion Ransomware	25	Critical
R01	Agentic AI and Decision Hijacking	20	Critical
R02	Shadow AI and Data Exfiltration	20	Critical
R08	Abuse of Non-Human Identities (NHI)	20	Critical
R11	Hybrid Warfare and Disinformation	20	Critical

IMPLEMENTATION STATUS TRACKER

Risk ID	Risk Category	Status	Timeline	Responsible Team	Budget Impact	Progress %	Notes
R01	Agentic AI and Decision Hijacking	Not Started	Q1-Q2 2026	AI Governance / SecOps	High		
R02	Shadow AI and Data Exfiltration	Not Started	Q1 2026	Data Security / Compliance	Medium		
R05	Triple Extortion Ransomware	Not Started	Q1 2026	Infrastructure / CISO	High		
R06	Cyber Pre-positioning in Critical Infrastructure	Not Started	Q1-Q3 2026	OT Security / Infrastructure	Very High		
R08	Abuse of Non-Human Identities (NHI)	Not Started	Q1-Q2 2026	Identity & Access / DevSecOps	Medium		

BUDGET IMPACT ANALYSIS

Budget Category	Number of Risks	Percentage	Notes
Very High	2	10,00%	
High	5	25,00%	
Medium	9	45,00%	
Low	4	20,00%	

RETURN ON INVESTMENT (ROI) CALCULATOR

SECTION A - Investment Cost Summary (from TCO Sheet)

Cost Category	Year 1	Year 2	Year 3	3-Year Total
Technology / Software Licensing	135 000,00 $	139 500,00 $	144 000,00 $	418 500,00 $
Implementation / Professional Services	80 000,00 $	40 000,00 $	35 000,00 $	155 000,00 $
Personnel (Internal FTE)	145 000,00 $	147 000,00 $	149 000,00 $	441 000,00 $
Training and Certification	18 000,00 $	14 000,00 $	14 000,00 $	46 000,00 $
TOTAL ANNUAL COST	378 000,00 $	340 500,00 $	342 000,00 $	1 060 500,00 $

SECTION B - Risk Reduction Benefits (from Risk Analysis Sheet)

Benefit Category	Year 1	Year 2	Year 3	3-Year Total
ALE Reduction — Breach Prevention	28 000,00 $	29 400,00 $	30 800,00 $	88 200,00 $
ALE Reduction — Ransomware	23 625,00 $	24 806,25 $	25 987,50 $	74 418,75 $
ALE Reduction — Downtime / BCP	10 500,00 $	11 025,00 $	11 550,00 $	33 075,00 $
Regulatory Fine Avoidance	12 000,00 $	12 600,00 $	13 200,00 $	37 800,00 $
Productivity Gains (FTE hours saved)	50000	52000	55000	157 000,00 $
TOTAL ANNUAL BENEFIT	74 125,00 $	77 831,25 $	81 537,50 $	233 493,75 $

SECTION C - ROI Summary

Metric	Year 1	Year 2	Year 3	3-Year Total
Total Cost (C)	378 000,00 $	340 500,00 $	342 000,00 $	1 060 500,00 $
Total Benefit (B)	74 125,00 $	77 831,25 $	81 537,50 $	233 493,75 $
Net Benefit (B - C)	(303 875,00) $	(262 668,75) $	(260 462,50) $	(827 006,25) $
ROI % [(B-C)/C]	**-80,4%**	**-77,1%**	**-76,2%**	**-78,0%**
Benefit-Cost Ratio	**0,20**	**0,23**	**0,24**	**0,22**

SECTION D - Payback Period

Payback Parameter	Value	Notes
Total 3-Year Investment	**$1 060 500**	*Sum of all costs over 3 years*
Total 3-Year Benefit	**$233 494**	*Sum of all quantified benefits over 3 years*
Average Monthly Net Benefit	**-$22 972,40**	*Based on linear distribution of benefits*
Estimated Payback (Months)	**13,6**	*Years until cumulative benefit covers total cost*

CYBERSECURITY RISK SCORING METHODOLOGY

RISK SCORE CALCULATION

Risk Score Formula:

Risk Score = Likelihood × Impact

Score Range: 1 (Minimum) to 25 (Maximum)

LIKELIHOOD SCALE (1-5)

Score	Level	Description	Probability
1	Very Low	Rare occurrence, highly unlikely	< 10%
2	Low	Unlikely to occur in normal circumstances	10-30%
3	Medium	Possible, may occur at some time	30-50%
4	High	Likely to occur in most circumstances	50-75%
5	Very High	Almost certain to occur	> 75%

IMPACT SCALE (1-5)

Score	Level	Business Impact	Financial Impact
1	Negligible	Minimal disruption, no data loss	< $10K
2	Minor	Limited disruption, minor data exposure	$10K-$100K
3	Moderate	Significant disruption, moderate data loss	$100K-$1M
4	Major	Severe disruption, major data breach	$1M-$10M
5	Critical	Business-critical systems down, catastrophic breach	> $10M

RISK PRIORITY MATRIX

Risk Level	Score Range	Priority	Action Required
High	13-25	Critical	Immediate action required, senior management involvement
Medium	7-12	Important	Action required within defined timeframe, regular monitoring
Low	1-6	Monitor	Accept risk or implement controls as resources permit