Black Book Insights

HEALTHCARE CYBERSECURITY STUDY

Europe Hospital Cyber Exposure & Clinical Continuity Index 2026

Where ransomware, state-linked intrusion, supplier failure and clinical downtime risk are converging

Independent healthcare cybersecurity intelligence for boards and buyers who need proof that care can continue after compromise.

2026

Black Book Research

August 2026

Table of Contents

A Black Book Research market assessment of threat exposure, clinical dependency and tested continuity across Europe

The report separates external attack pressure from comparative readiness. Country scores are evidence-weighted market intelligence measures rather than predictions that a particular provider will be breached. Ukraine is excluded from the index because active-war cyber conditions would overwhelm comparison with other European markets. The United Kingdom, Switzerland, Norway and Iceland are included.

2026 Europe-Wide Hospital Cyber Risk Reveal Table

Category leaders from the Black Book evidence-weighted index

Europe-wide category	Highest-priority market	Second priority	Black Book interpretation
Highest Overall Residual Clinical Cyber Risk	Poland (77)	Germany (71)	Destructive infrastructure exposure places Poland first; Germany follows on criminal scale and complexity.
Highest External Threat Exposure	Poland (96)	Germany (92)	This score measures attack pressure and dependency, not institutional weakness.
Highest Criminal Ransomware Pressure	Germany	Italy	ENISA claim references concentrate in the largest high-value markets.
Broadest Threat Convergence	France	Belgium	Criminal, state-linked, public-sector and supplier pathways overlap.
Highest Supplier-Contagion Concern	United Kingdom	Netherlands	Shared pathology, cloud, identity, device and logistics dependencies can affect multiple providers.
Highest Destructive / Hybrid Exposure	Poland	Finland	Healthcare consequence may originate in energy, communications, transport or public infrastructure.
Strongest Comparative Readiness	Norway / Denmark / Iceland	Sweden / Finland	Higher readiness reduces but does not eliminate digital-dependency risk.
Highest National Shared-Service Blast Radius	United Kingdom	Ireland	A single supplier or shared platform can produce multi-organisation clinical consequences.

Black Book market judgment

The decisive European healthcare cybersecurity question is no longer which country reports the most attacks. It is which health systems can preserve safe identity, diagnostics, medication, records and patient flow when the attack succeeds.

Black Book Insights

01

Executive Thesis and Black Book Market Judgment

Europe does not lack cyber controls. Europe lacks enough health systems that can prove care will continue when controls fail.

Europe does not lack cybersecurity programmes. Europe lacks enough health systems that can prove care will continue when those programmes fail.

European healthcare has entered a continuity reckoning. For more than a decade, cybersecurity programmes were judged primarily by privacy protection, regulatory compliance, perimeter controls, vulnerability management and the number of incidents detected or blocked. Those measures still matter, but they no longer define resilience.

The new competitive and governance threshold is whether a hospital can maintain clinically safe operation after a material compromise of identity, EHR/EPR, laboratory, imaging, pharmacy, cloud, medical-device, network or supplier infrastructure. That distinction changes the market question from prevention alone to prevention plus endurance.

A hospital may detect malicious activity within minutes and still require hours to remove every supplier credential, machine identity, token, certificate, session and network route. It may restore a server and still remain unable to authenticate clinicians, reconnect interfaces, validate results or reconcile paper records. The interval between technical detection and clinically safe recovery is now the decisive risk window.

309

significant EU health-sector cyber incidents reported for 2023

54%

of health-sector cyberattacks in the European Commission evidence involve ransomware

44/100

Black Book European Cyber Resilience Continuity Index baseline

Sources: European Commission healthcare cybersecurity action plan [3]; Black Book Research European hospital cybersecurity survey, n=284 [32].

82%	74%	59%	32%	14%
very high or extreme concern	expect a major cyber event	confident at 24 hours	confident at 48 hours	confident at 72 hours

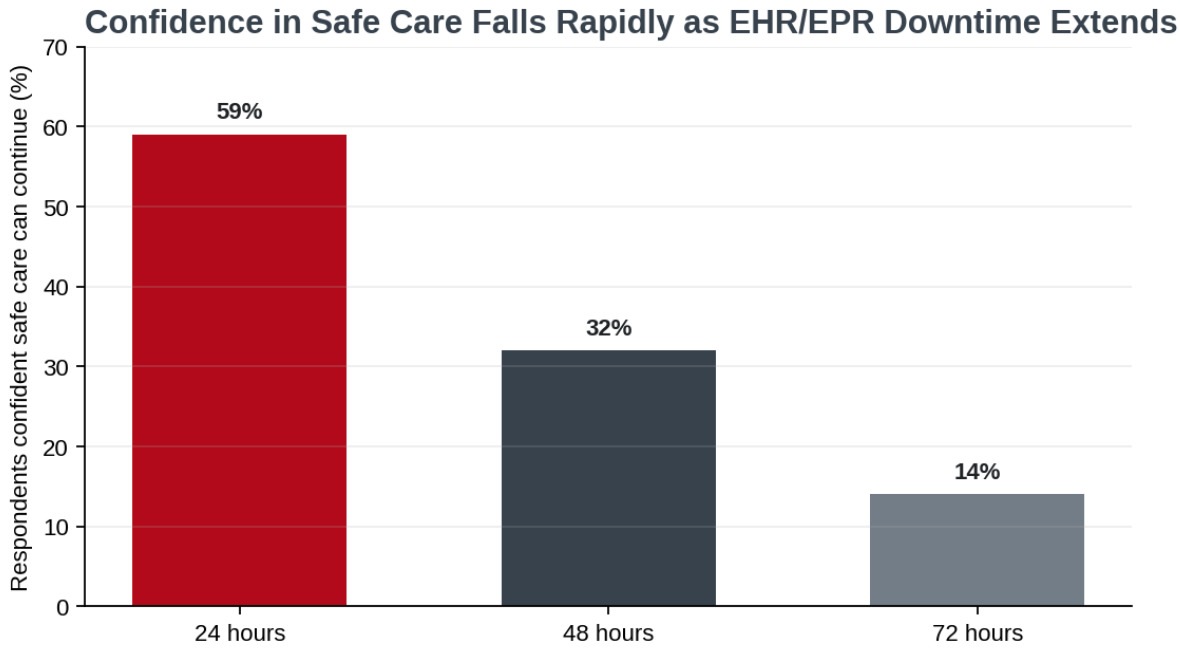

Figure 1. Confidence in safe care falls 45 percentage points between the first and third day without the core EHR/EPR.

Source: Black Book Research European hospital cybersecurity survey, May 2026, n=284 [32].

The market has moved from data theft to care disruption

The European Commission now describes healthcare cyberattacks in operational terms: delayed medical procedures, emergency-room gridlock and disruption to vital services. Its evidence base records 309 significant health-sector incidents in 2023, more than in any other critical sector, and identifies ransomware in 54% of health-sector attacks.[3] The implication is direct. A privacy event can become a patient-safety event when clinicians cannot obtain the information, products or services required to diagnose and treat.

That shift does not make confidentiality less important. Healthcare data remains extraordinarily sensitive, durable and useful for extortion. It means that confidentiality, integrity and availability must be managed as one clinical risk. An attacker who steals data can create legal and reputational pressure. An attacker who also disables identity, laboratory or medication workflows can create immediate care pressure. The combined event gives the adversary more leverage and gives the hospital less time.

ENISA analysed 4,875 incidents from July 2024 through June 2025. DDoS dominated the incident count, largely because of hacktivist activity, yet ransomware remained the most impactful threat. Phishing represented approximately 60% of observed initial access and vulnerability exploitation another 21.3%.[1][2] The figures show why health systems cannot treat this as a single-control problem: the human identity, the exposed edge device and the trusted supplier all remain credible paths to the same clinical outcome.

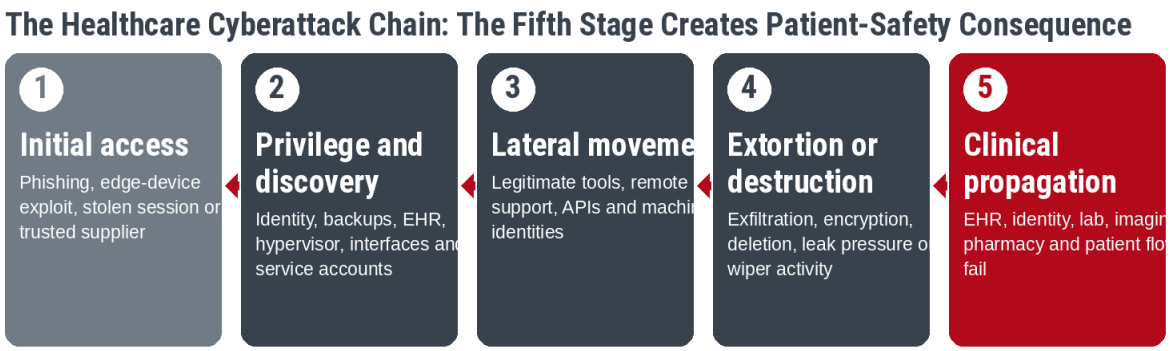

Figure 2. The healthcare cyberattack chain becomes clinically consequential at the fifth stage, when technical compromise propagates into care delivery.

Black Book Research synthesis of ENISA, ANSSI, CERT Polska, NHS and national cyber authority evidence [1][9][11][13].

What separates resilient health systems from compliant incumbents

A resilient health system is not the organisation with the longest control catalogue. It is the organisation that can answer, with current evidence, how long it can operate safely without core digital services; how quickly it can isolate a compromised supplier; which clinical workflows will fail first; and how it will restore, validate and reconcile the full care environment. The top-performing operating model looks less like a conventional disaster-recovery plan and more like a clinical command system: each technical action is connected to a patient-safety consequence, an accountable owner and a verified fallback.

Market claim	Black Book test	Why it matters
"We have backups."	Has a complete Tier-1 clinical service been rebuilt from trusted recovery assets, including identity, interfaces and clinical validation?	Backup completion is not proof of recoverability.
"We use multifactor authentication."	Is authentication phishing-resistant for privileged roles, and can sessions, tokens and non-human identities be revoked rapidly?	Ordinary MFA does not eliminate adversary-in-the-middle or session theft.
"We assess suppliers."	Can every human and machine access path used by a Tier-1 supplier be identified and disabled in less than ninety minutes?	Questionnaires do not contain an active compromise.
"We have downtime procedures."	Have clinical teams sustained EHR, identity, laboratory, imaging and medication workflows for twenty-four, forty-eight and seventy-two hours?	A paper binder is not a tested operating model.
"The board sees cyber metrics."	Do metrics express hours of safe care, services at risk, restore success and supplier blast radius?	Technical activity counts do not reveal patient consequence.
"Our national platform is resilient."	Can the organisation continue when the national or regional service is the component that must be isolated?	Centralisation can improve capability and magnify failure.

Black Book conclusion

European cyber maturity is increasingly defined by evidence of clinical endurance: proven restore, proven isolation, proven fallback and proven reconciliation. Policy without rehearsal remains an untested assumption.

Four markets define the current European front line

No single country is “the most vulnerable” in every dimension. The evidence identifies four different front lines. Poland represents destructive and infrastructure-dependent risk. Germany represents criminal ransomware scale and complex availability exposure. France represents the broadest convergence of criminal, public-sector and state-linked pressure. The United Kingdom represents supplier contagion and the possibility of prolonged multi-provider disruption.

Italy and Spain form the next criminal-pressure tier; Belgium, the Netherlands and Ireland carry distinctive institutional or shared-service dependencies; and the Baltic-Nordic corridor combines high digital reliance with geopolitical exposure. These are not rankings of competence. Several high-exposure countries possess strong national cyber institutions. Their risk is elevated because they are highly digital, strategically important, economically valuable and interconnected.

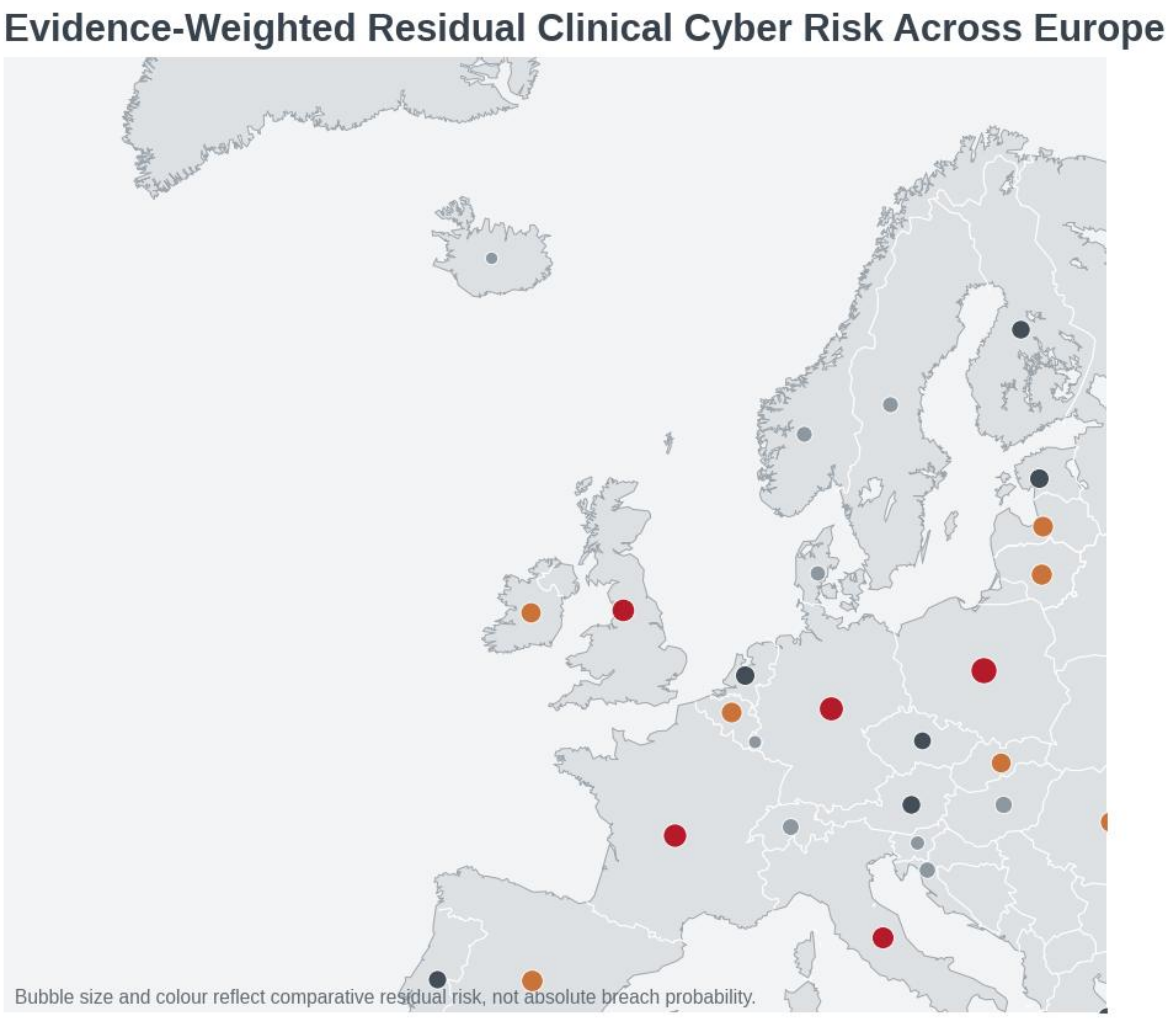

Figure 3. Residual clinical cyber risk reflects both external pressure and the readiness gap that determines how far an incident can propagate.

Black Book Research evidence-weighted index. Ukraine excluded. Scores are comparative analytical measures, not absolute breach probabilities.

The central thesis

Europe will not eliminate healthcare cyberattacks. The strategic objective is to prevent a successful intrusion from becoming a prolonged loss of clinical capacity.

Black Book Insights

02

Evidence Base and Black Book Methodology

A standardised framework that separates attack pressure, digital dependency and tested clinical continuity.

Evidence base and study scope

Two Black Book healthcare panels, official national reporting and a transparent evidence-weighted country index

This report integrates three evidence layers. The first is Black Book Research survey evidence from European hospital buyers and stakeholders. The second is a separate European executive and healthcare IT study focused on supplier isolation and cross-domain kill-switch capability. The third is an official-source review of European and national cyber authorities, regulators, ministries, health services and incident investigations through 1 August 2026.

The design intentionally avoids treating incompatible national incident counts as a single league table. Reporting rules, detection capability, sector definitions and public disclosure vary substantially. A large country with mature reporting may appear more exposed than a smaller country with limited visibility. Black Book therefore scores the evidence in separate dimensions and applies whole-number ratings to avoid implying false precision.

Evidence layer	Population or scope	Principal contribution	Interpretive limit
Black Book European hospital cybersecurity panel	284 healthcare cybersecurity buyers and stakeholders	Concern, event expectation, 24/48/72-hour continuity, supplier tiering, downtime exercise and board metrics	Europe-wide baseline; not designed as a definitive country ranking.
Black Book European supplier isolation study	561 executives, CISOs and healthcare IT leaders	Kill-switch testing, time-to-revoke, supplier runbooks, board reporting and AI/API supplier classification	Measures organisational practice; respondent roles and countries vary.
Official European evidence	ENISA, European Commission, Council of the EU and allied advisories	Threat vectors, policy, cross-border mechanisms, attribution and sector context	Incident taxonomies and time periods differ.
Official national evidence	National cyber agencies, health services, regulators and incident reports	Country-specific pressure, cases, response capability and clinical consequence	Public visibility varies; absence of reporting is not absence of risk.
Black Book analytical index	31 European countries; Ukraine excluded	Comparative exposure, readiness and residual clinical risk	A market intelligence index, not a forecast or insurance model.

Black Book survey baseline: clinical confidence decays faster than governance improves

The 284-respondent panel found very high concern but limited evidence of multi-day endurance. Eighty-two percent reported very high or extreme concern about a 2026 cyberattack, and 74% considered a major event likely or highly likely. Yet only 26% had conducted a full clinical downtime simulation in the preceding year, 25% had fully tiered critical suppliers by clinical impact, and 31% reported that their boards receive continuity-linked cyber metrics.[32]

The most consequential result was the confidence curve. Fifty-nine percent believed safe care could continue for twenty-four hours without the core EHR/EPR. The proportion fell to 32% at forty-eight hours and 14% at seventy-two hours. This is not simply a measure of whether paper forms exist. It reflects the accumulation of diagnostic backlog, missing histories, medication uncertainty, incomplete handoffs, staffing fatigue and reconciliation burden.

Black Book continuity measure	Positive response
Very high or extreme concern about a 2026 cyberattack	82%
Major cyber event considered likely or highly likely	74%
Confident of safe operation without core EHR/EPR at 24 hours	59%
Confident at 48 hours	32%
Confident at 72 hours	14%
Completed a full clinical downtime simulation in prior year	26%
Critical suppliers fully tiered by clinical impact	25%
Boards receive continuity-linked cyber metrics	31%

Why the seventy-two-hour threshold matters

Short outages can often be absorbed through prioritisation and manual work. After the first day, workarounds become the operating environment. The risk moves from inconvenience to cumulative clinical error and lost capacity.

Supplier isolation baseline: the organisation may detect the attacker before it can remove the attacker

The 561-respondent study exposed an operational gap that conventional third-party risk programmes rarely measure. Only 13% had tested a cross-domain kill switch for their highest-impact suppliers and AI platforms. Fifty-one percent had a written policy or diagram that had never been rehearsed end to end; 36% had no formal kill switch. The estimated median time required to revoke a compromised supplier across identity, network and integrations was approximately ten hours, and fewer than one-third believed they could isolate a Tier-1 supplier within ninety minutes.[33]

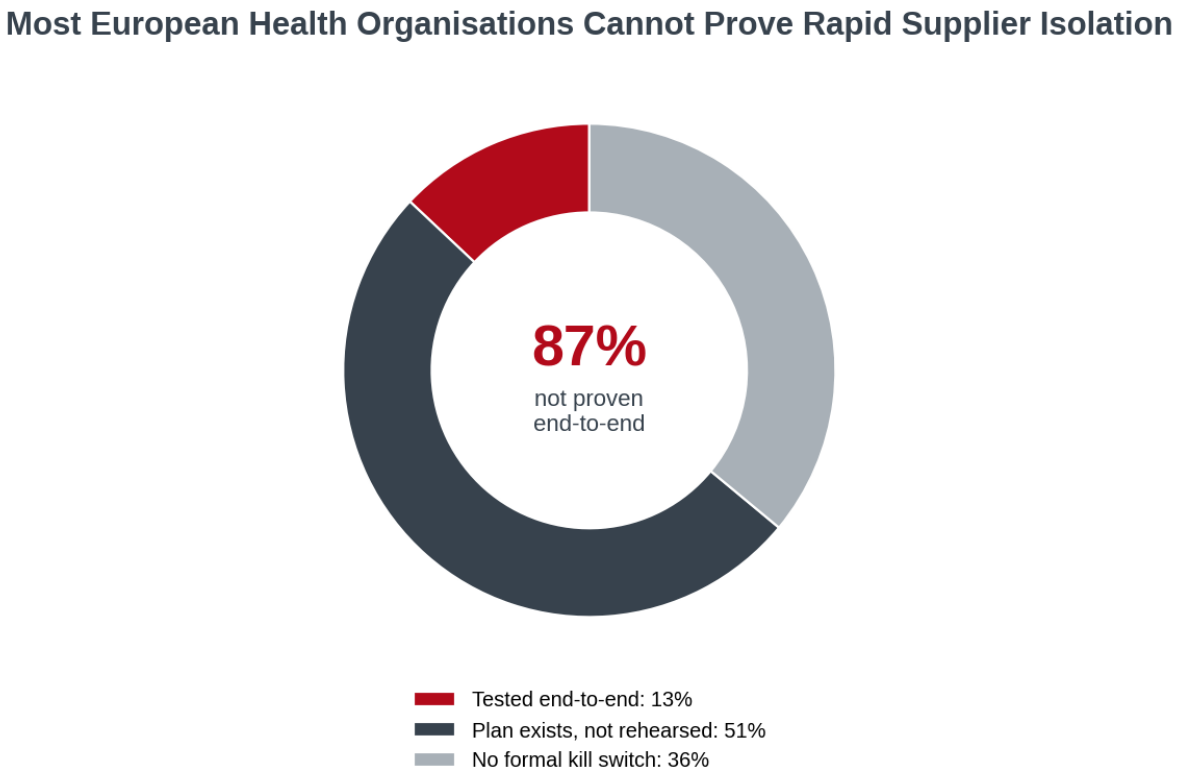

Figure 4. Written third-party controls are common; proven, cross-domain supplier isolation is rare.

Source: Black Book Research European supplier isolation study, n=561 [33].

Time-to-revoke is the hidden interval in European hospital cyber risk. During that interval, the organisation may disable an employee account while a service credential remains active, terminate a VPN while an API token still works, or block one network path while a remote-management tool continues to provide access. A supplier inventory that lists companies but not identities, certificates, endpoints and integrations cannot support rapid containment.

Supplier isolation measure	Reported capability
Tested cross-domain kill switch for highest-impact suppliers	13%
Written kill-switch plan never rehearsed end-to-end	51%
No formal kill switch	36%
Tested isolation runbooks for top ten suppliers	26%
Report time-to-revoke or kill-switch coverage to boards	19%
Automatically classify production AI/API suppliers as Tier 1	23%

Country index architecture

The country index is built in three stages. The Healthcare Cyber Exposure Index measures external pressure and dependency. The Clinical Continuity Readiness Index measures comparative response and endurance evidence. The Residual Clinical Cyber Risk score combines 65% exposure with 35% of the readiness gap. The weighting reflects a market reality: hospitals cannot control the entire external threat environment, but verified internal capability can materially reduce the clinical consequence.

Index	Weighted components	Interpretation
Healthcare Cyber Exposure Index	Attack pressure and incident evidence 25%; ransomware/extortion 20%; state/hybrid activity 20%; healthcare/critical-service disruption 15%; supplier concentration 10%; digital dependency 10%	How much relevant pressure and dependency surrounds the health system.
Clinical Continuity Readiness Index	National response 20%; restore and continuity evidence 20%; sector coordination 15%; identity and supplier control 15%; regulation and assurance 15%; exercise and reporting maturity 15%	How much evidence indicates that essential care can be sustained and recovered.
Residual Clinical Cyber Risk	65% Exposure Index + 35% inverse Readiness Index	The comparative risk that external pressure will become clinical disruption.

Whole-number scoring is deliberate. National reports are not sufficiently comparable to justify decimal-level precision. A two- or three-point difference should be interpreted as the same broad risk band unless supported by materially different evidence. The index is designed to prioritise research, exercises and investment - not to label a country as secure or insecure.

Scoring discipline

High reported attack volume can reflect economic scale, digital maturity, stronger detection and better disclosure. Low reported volume can reflect lower exposure, weaker visibility or underreporting. The index never treats raw counts as a standalone measure.

Definitions used throughout the report

Term	Black Book definition
Material cyber event	An event that materially affects confidentiality, integrity, availability, clinical operations, supplier performance or public trust.
Clinical continuity	The ability to sustain safe diagnosis, treatment, medication, monitoring, transfer and documentation under degraded digital conditions.
Tier-1 clinical supplier	A supplier whose compromise or unavailability can affect essential care, patient identity, diagnostics, medication, critical products or a large provider population.
Kill switch	A rehearsed process that removes all human and machine access paths used by a supplier across identity, sessions, networks, applications, APIs and integrations.
Validated restore	A timed restoration of a production-equivalent clinical service from trusted assets, followed by technical and clinical verification.
Residual clinical cyber risk	The exposure remaining after comparative readiness and continuity capability are considered.
Shared-service blast radius	The number and criticality of organisations, care pathways or patients affected by failure of one platform, supplier or infrastructure service.
Clinical reconciliation	The validated incorporation of orders, results, medications, notes, identifiers and operational changes created during downtime back into the system of record.

These definitions create the bridge to the next section. European policy increasingly requires risk management, continuity, supplier security and management accountability. The operational question is whether those requirements are producing the evidence described above.

Black Book Insights

03

European Threat, Policy and Operating Context

Ransomware remains the most impactful threat while state, criminal and supplier pathways converge.

The European threat environment is diverse in volume but convergent in consequence

ENISA's 2025 threat landscape analysed 4,875 incidents across the twelve months ending 30 June 2025. DDoS represented 77% of reported incidents and hacktivism almost 80%, but only about 2% of hacktivist incidents produced service disruption. Ransomware remained the most impactful threat in the European Union. The distinction between volume and consequence is fundamental to healthcare: thousands of low-impact website disruptions can generate more incident records than one supplier compromise that postpones surgery or disables pathology.[1][2]

The same evidence describes convergence. State-aligned groups intensified operations against European organisations; cybercriminals exploited shared dependencies; phishing-as-a-service lowered the barrier to social engineering; and different actors increasingly used the same tools, access brokers and hosting infrastructure. For hospital defenders, attribution may remain uncertain during the critical first hours. The continuity response must work whether the actor seeks money, intelligence, political effect or destruction.

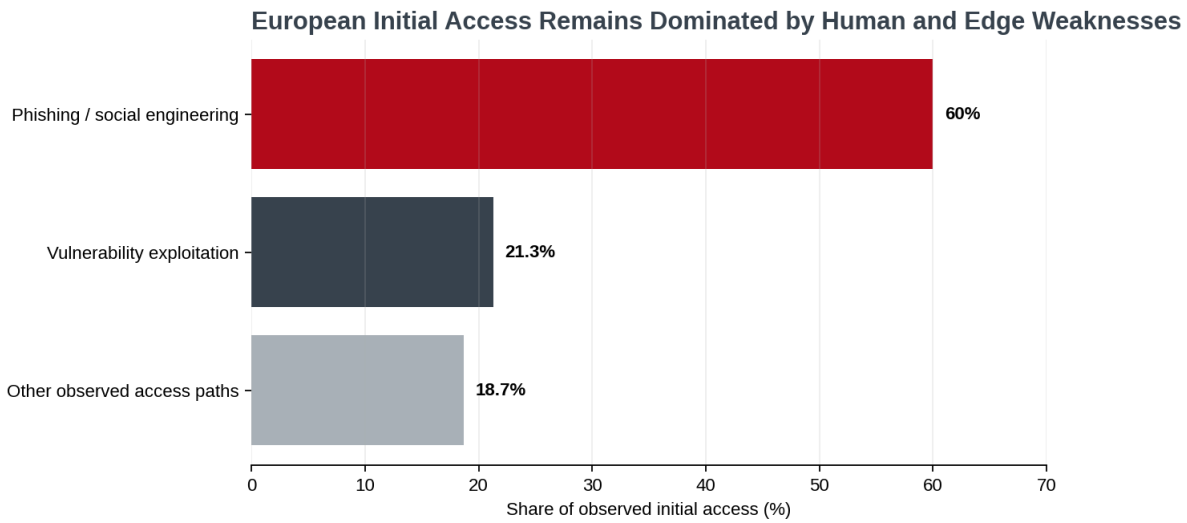

Figure 5. Phishing and vulnerability exploitation account for more than four-fifths of observed initial access in the ENISA evidence.

Source: ENISA Threat Landscape 2025 [1][2].

Market implication

European health systems need identity-first and edge-first controls, but they must assume those controls can be bypassed. Continuity architecture begins where preventive confidence ends.

Ransomware remains the most operationally consequential criminal model

The ransomware economy is resilient because it is modular. Initial-access brokers sell credentials or sessions. Affiliates conduct intrusion and exfiltration. Hosting providers, proxy services and malware infrastructure reduce the cost of operating. Negotiators and leak sites convert technical access into pressure. The July 2026 Council of the EU sanctions against actors including Media Land LLC, ML.Cloud and Z-Pentest illustrate the enabling ecosystem surrounding ransomware, phishing and critical-infrastructure attacks.[8]

Healthcare remains attractive for three reasons. First, clinical operations cannot remain offline indefinitely. Second, health data creates durable privacy and reputational leverage. Third, providers depend on suppliers that may offer access to several customers at once. The most effective defence therefore combines prevention with the ability to reduce leverage: trusted restoration, continued care, fast isolation, precise data-impact assessment and predetermined ransom governance.

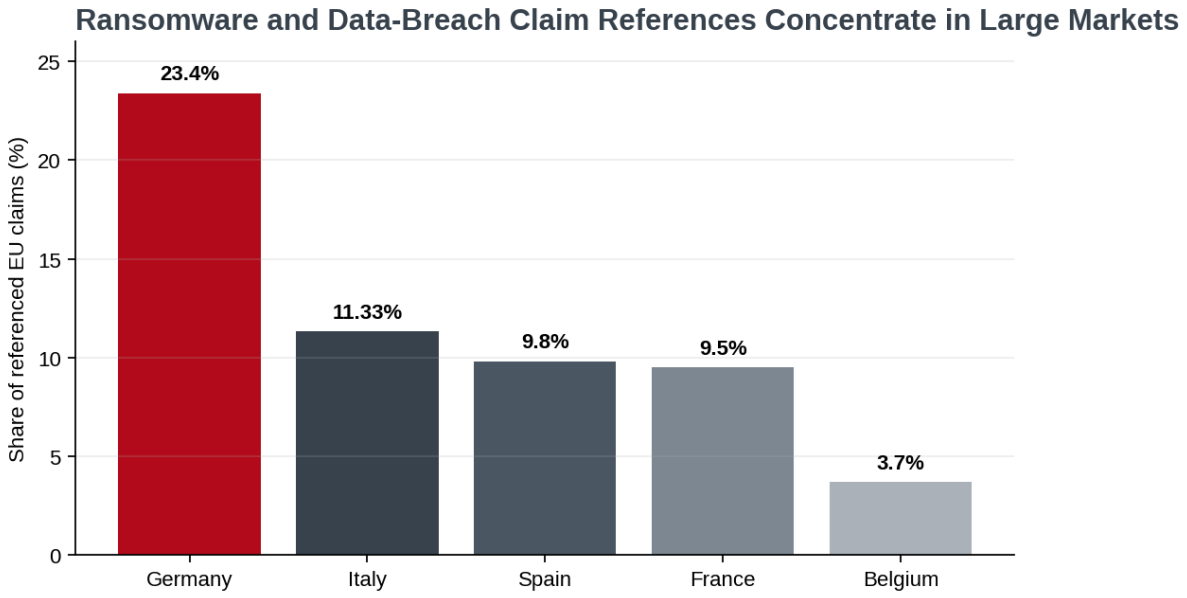

Figure 6. ENISA claim references concentrate in Germany, Italy, Spain and France, reflecting economic value, target volume and reporting visibility.

Source: ENISA Threat Landscape 2025 underlying country breakout [1]. Claim references are not verified national breach rates.

Germany's 23.4% share in the referenced claims does not mean that German healthcare is Europe’s least secure. It means that the German market is large, valuable and repeatedly visible in the available criminal evidence. Similar caution applies to every country comparison in this report.

State-linked and hybrid risk is no longer confined to espionage

On 13 July 2026, the European Union publicly denounced a Russian cyber ecosystem spanning intelligence services, cybercriminal groups, hacktivists and private companies. It identified FSB Centre 16 as controlling groups including Turla and described targeting of France, Germany, Poland, Cyprus, the Netherlands, Austria, Slovakia, Romania and Finland. The statement specifically referenced espionage against strategic French entities, targeting of German government organisations and disruptive sabotage against Polish critical infrastructure, including combined heat and power plants.[7]

Healthcare relevance is both direct and dependency-based. A state actor may target health ministries, research institutions, pharmaceutical supply, public communications or national identity systems. It may also target energy, telecommunications, logistics or cloud infrastructure that hospitals require. Poland's December 2025 energy incidents show how destructive intent can move from network compromise into industrial-device damage. The fact that defensive controls prevented service interruption should be treated as proof that resilience works - and proof that the scenario is real.[9]

Threat objective	Typical operating behaviour	Healthcare consequence
Financial extortion	Credential theft, exfiltration, encryption, leak pressure and negotiation	Care disruption, privacy exposure, recovery cost and ransom governance pressure.
Espionage	Long dwell time, stealth, strategic data collection and persistence	Research, policy, clinical, workforce and supplier intelligence loss; compromised trust.
Pre-positioning	Access to routers, edge devices, identity or critical infrastructure before activation	Latent ability to disrupt during geopolitical crisis or another emergency.
Destructive sabotage	Wiper deployment, firmware damage, deletion and industrial-device targeting	Loss of power, heating, communications, data or physical operational control.
Hacktivist disruption	DDoS, public claims and opportunistic probing	Public-facing portal outage, communications pressure and distraction during other incidents.
Supply-chain compromise	Abuse of trusted access, hosted services, updates or shared platforms	Multi-provider blast radius and difficult containment trade-offs.

NIS2, the healthcare action plan and the Cyber Solidarity Act are shifting the standard of proof

European policy is moving from general security expectations toward evidence of resilience. NIS2 requires covered entities to address risk management, incident handling, business continuity, disaster recovery, crisis management, supply-chain security, vulnerability management and appropriate authentication. Management bodies must approve and oversee the measures, creating direct executive accountability.[4]

The European Commission's healthcare cybersecurity action plan adds sector-specific prevention, early warning, ransomware response, rapid assistance and maturity support. The EU Cyber Solidarity Act, in force since February 2025, provides cross-border cyber hubs, preparedness testing, an emergency mechanism and a European Cybersecurity Reserve. Healthcare is among the sectors eligible for preparedness testing, and ENISA is operating the reserve under a three-year agreement valued at EUR 36 million.[3][5][6]

These mechanisms matter because the next severe European healthcare event may not respect organisational or national boundaries. A diagnostic supplier can serve several health systems; a cloud service can support multiple countries; and a state-linked campaign can target the same vulnerable product across Europe. The policy architecture is increasingly capable of cross-border response. Hospital evidence must catch up.

Market claim	Black Book test	Why it matters
“We are NIS2-compliant.”	Can the organisation show current evidence of restore, continuity, supplier isolation and management oversight?	Regulatory scope does not prove operational performance.
“The supplier is certified.”	Has the supplier demonstrated access inventories, rapid notification, recovery objectives and joint exercise performance?	Certification is not a substitute for customer-specific dependency evidence.
“The national CSIRT will assist.”	Can the hospital maintain safe care while specialist assistance is mobilised and containment decisions are made?	External support does not remove the first-hour operating burden.
“The Cybersecurity Reserve is available.”	Are internal decision rights, logs, system inventories and clinical priorities ready for external responders?	Emergency capacity is effective only when the organisation can use it rapidly.

The internet-facing edge has become the European front door

ANSSI, ENISA, the Finnish national cyber centre and allied security agencies continue to emphasise internet-facing edge devices. VPNs, firewalls, routers, email gateways and remote-management appliances are attractive because they provide privileged network position and may receive less monitoring than standard endpoints. Vulnerabilities can be exploited within minutes or hours of disclosure, compressing the patching window beyond conventional monthly change cycles.[1][12][30]

In July 2026, the UK National Cyber Security Centre and allied agencies warned that FSB Centre 16 was scanning for and compromising poorly configured routers and network devices. Communications, defence, energy, financial services, government and healthcare were among the sectors advised to act. The guidance connects the European geopolitical context directly to hospital infrastructure.[10]

Edge control	Minimum evidence	Failure mode if absent
Asset ownership	Complete inventory, internet exposure, owner, support status and clinical dependency	Unknown devices remain unpatched or unmonitored.
Rapid patch decision	Documented emergency change path and compensating controls	The exploit window closes before normal governance acts.
Configuration assurance	No default credentials; administrative interfaces restricted; secure management plane	Attackers gain privileged footholds through preventable exposure.
Detection and logging	Centralised telemetry, time synchronisation, anomaly detection and retained logs	Intrusion remains invisible or evidence is lost.
Recovery and replacement	Known rebuild configuration, spare capacity and tested failover	Containment disables connectivity for longer than planned.

Black Book conclusion

A health system cannot patch at healthcare speed when adversaries exploit at internet speed. Emergency edge-device governance must be a distinct operating process.

AI changes the economics of social engineering before it changes the fundamentals of intrusion

Generative AI improves language quality, localisation, impersonation and the speed at which attackers can prepare convincing messages. ANSSI observed growing interest in advanced AI tools while cautioning that this had not yet produced a complete paradigm shift.[12] The core vulnerabilities remain familiar: trust, urgency, authority, compromised accounts and weak verification outside the normal communication channel.

Healthcare is especially exposed because workflows involve referrals, locums, contractors, vendors, urgent clinical requests and high volumes of external communication. Voice and video synthesis can increase the credibility of requests to reset access, release data or bypass normal process. The defence is not an “AI detector.” It is a control design in which high-risk actions require verified identity, separate-channel confirmation, least privilege and immediate revocation capability.

AI-enabled pressure	Healthcare scenario	Control that remains decisive
Highly localised phishing	Messages imitate a regional health authority, supplier or clinical leader	Phishing-resistant authentication and verified sender context.
Voice impersonation	Urgent request to reset a privileged account or release records	Call-back to a known number and dual approval.
Synthetic document fraud	Fake invoice, procurement change, clinical attachment or legal notice	Out-of-band validation and content isolation.
Automated reconnaissance	Rapid tailoring using public leadership, supplier and project information	Reduced public exposure, monitored identity signals and least privilege.
Scaled credential testing	Stolen sessions and passwords tested across cloud and supplier portals	Session controls, conditional access and rapid revocation.

With the threat and policy context established, the next section converts the evidence into the market findings that boards, governments and buyers can act on.

Black Book Insights

04

Executive Findings and Market Scorecard

Eight findings that define the 2026 European healthcare cybersecurity market.

Executive findings

The market is moving from preventive assurance to clinically tested resilience

01	**The most consequential European hospital cyber metric is hours of safe care, not alerts blocked.** The Black Book confidence curve falls from 59% at twenty-four hours to 14% at seventy-two hours. This collapse reveals that many organisations have initial workarounds but not a sustainable degraded operating model.
02	**Supplier compromise is becoming a clinical operating event.** Synnovis demonstrated multi-trust pathology disruption; Stryker demonstrated physical supply interruption without onward hospital compromise. Supplier cyber risk now reaches diagnostics, blood products, devices, consumables and logistics.
03	**Identity is the common control plane for humans, suppliers and machines.** Phishing remains the leading access vector, while service accounts, API tokens, certificates and sessions can preserve access after an employee password is reset. Identity resilience must cover every actor and integration.
04	**The most acute EU hybrid-risk signal is in Poland.** Destructive attacks against energy and industrial systems demonstrate a pathway to healthcare disruption through power, heating, communications and transport, even when hospitals are not the original target.
05	**Germany, France and the United Kingdom lead different risk categories.** Germany represents ransomware scale; France represents threat convergence; the United Kingdom represents shared-supplier and prolonged-continuity exposure. One undifferentiated ranking would conceal the reason each market matters.
06	**Highly digital health systems can be both more resilient and more dependent.** The Netherlands and Nordic countries often show strong institutional capability, yet national platforms, cloud services and shared identity can create large blast radii. The decisive design principle is graceful degradation.
07	**Regulatory accountability is rising faster than tested readiness.** NIS2, the healthcare action plan and national board guidance are strengthening governance. Only a minority of Black Book respondents, however, had exercised full downtime or supplier isolation.
08	**Recovery is not complete until the clinical record is reconciled.** Restoring servers or applications does not resolve paper orders, temporary identifiers, results, medication activity, deferred procedures and interface queues created during the outage.

Europe-wide market scorecard

Country	Exposure	Readiness	Residual risk	Priority band
Poland	96	58	77	Extreme
Germany	92	69	71	Very high
France	90	70	69	Very high
United Kingdom	88	72	67	Very high
Italy	82	67	65	Very high
Spain	80	66	64	High
Lithuania	79	66	63	High
Belgium	78	68	62	High
Latvia	77	65	62	High
Romania	74	61	62	High
Ireland	76	67	61	High
Slovakia	72	63	60	High
Netherlands	79	78	59	High
Estonia	78	76	59	High
Cyprus	71	62	59	High
Finland	77	80	57	Elevated
Austria	72	70	57	Elevated
Portugal	65	62	56	Elevated

Poland is the only country in the Extreme residual-risk band because destructive infrastructure evidence combines with a lower comparative continuity score. Germany, France, the United Kingdom, Italy and Spain form the first large-market tier. Lithuania and Latvia rise because geopolitical exposure and smaller-system concentration create a meaningful readiness penalty, while the Netherlands and Nordic markets rank lower on residual risk despite high exposure because comparative readiness is stronger.

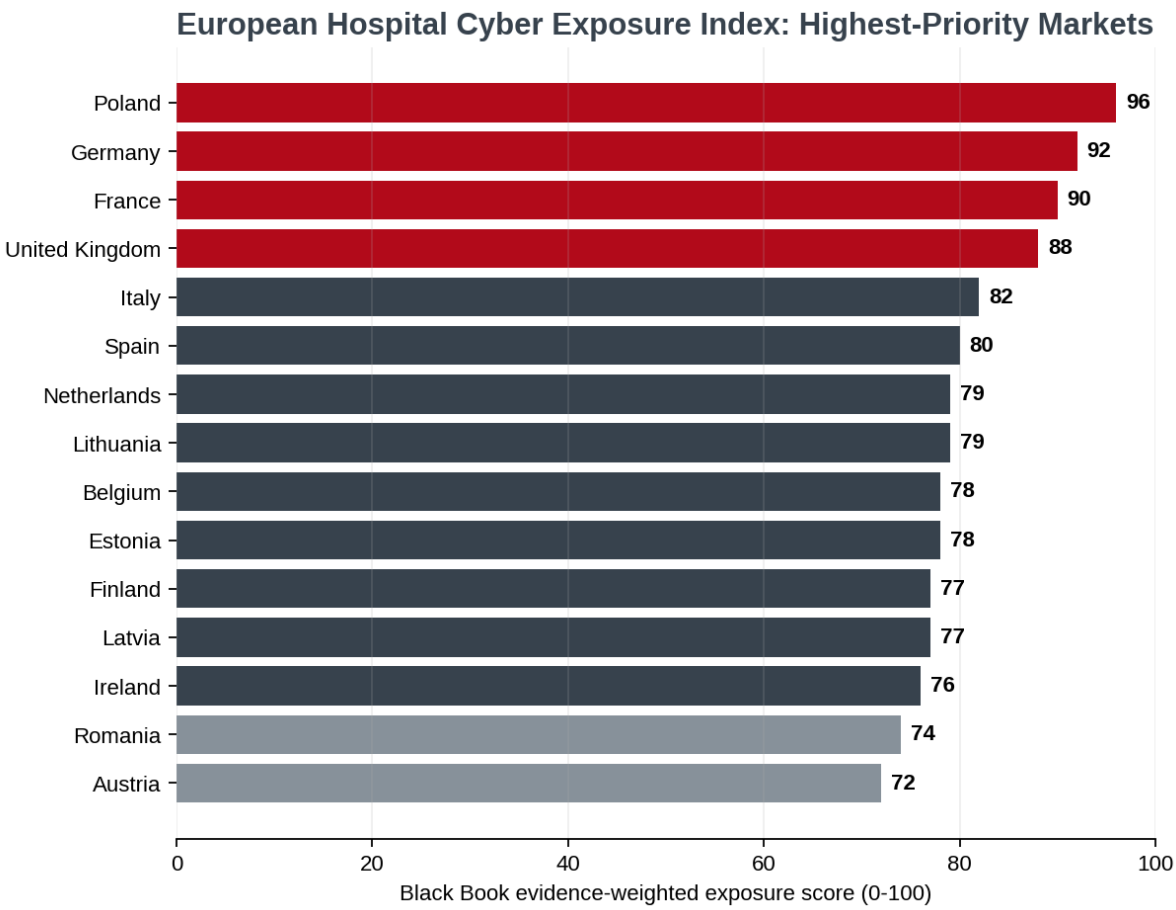

Figure 7. The Exposure Index isolates external pressure from national readiness.

Source: Black Book Research evidence-weighted index, official evidence through 1 August 2026.

Governance is moving in the right direction - but exercises remain the missing proof

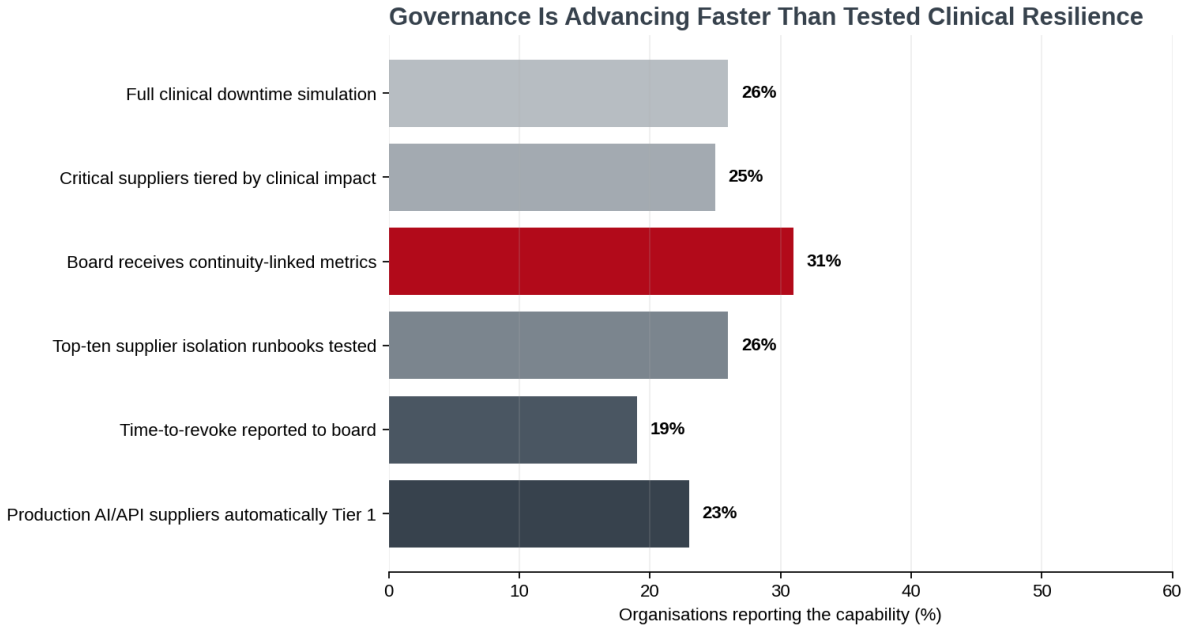

Figure 8. The lowest Black Book response rates concern the activities that must work under live incident pressure.

Sources: Black Book Research hospital panel, n=284, and supplier isolation study, n=561 [32][33].

The chart shows a consistent pattern. Organisations are increasingly discussing cyber risk at executive level, but fewer have tested the operating capabilities that determine clinical consequence. The weakest measures are board reporting of time-to-revoke, automatic Tier-1 classification of production AI/API suppliers, full supplier tiering and multidisciplinary clinical downtime exercises.

This is the evidence gap that the European market will increasingly price. Insurers, regulators, ministries, boards and buyers will ask not only whether a policy exists, but when the process was last exercised, what failed, who accepted the residual risk and whether the next test closed the finding.

Buyer implication

The winning healthcare cybersecurity platform or service will not be the one with the largest feature list. It will be the one that reduces time to safe containment, preserves clinical function and produces evidence that boards and regulators can trust.

Board-level scorecard: the metrics that should replace generic cyber activity counts

Board metric	What it reveals	Target direction
Hours of safe EHR/EPR downtime	How long care can continue before information and workflow gaps create unacceptable risk	Increase through tested read-only access, paper workflow and alternative services.
Tier-1 supplier time-to-revoke	How long a trusted third party can remain connected after compromise	Reduce toward less than sixty to ninety minutes.
Validated restore success	Whether critical clinical production can be rebuilt from trusted assets	One or more full restores per Tier-1 service each year.
Critical supplier exercise coverage	Whether the most consequential dependencies have been rehearsed jointly	Increase to all top-ten suppliers and every national/shared platform.
Non-human identity ownership	Whether tokens, certificates and service accounts have accountable owners and expiry	Move toward complete inventory and automated rotation.
Clinical workflow fallback coverage	Which diagnostic, medication, identity and patient-flow processes have safe degraded modes	Close all high-harm gaps; retest after workflow or platform change.
Backlog and reconciliation time	How long care delivery remains impaired after technical restoration	Reduce through predesigned reconciliation tooling and staffing.
Regional mutual-aid dependency	Whether diversion plans assume unaffected neighbours that share the same supplier	Identify and remove common-mode assumptions.

These measures create a transition into the clinical core of the report. The next section examines the seven outcomes that determine whether a cyber event remains technical or becomes a patient-safety crisis.

Black Book Insights

05

Seven Clinical Continuity Outcomes

The operating capabilities that determine whether a cyber event becomes a patient-safety event.

Seven clinical continuity outcomes

The report evaluates resilience through care delivery, not through technology controls in isolation

The seven outcomes below translate cybersecurity into the functions a hospital must preserve. They are deliberately clinical. Identity, records, diagnostics, medication, devices, suppliers and recovery are not separate risk silos; they form a chain. Failure in one domain can remove the information or authority required to operate another. A laboratory may remain technically available while clinicians cannot authenticate. An EHR may be restored while interfaces remain disconnected. A pharmacy may dispense urgent medication while the administration record and allergy history are incomplete.

This structure also changes procurement. Buyers should not ask only whether a product detects ransomware, protects endpoints or stores immutable backups. They should ask which clinical failure point the product reduces, how quickly that reduction can be demonstrated, and what dependency the product introduces in return. The strongest evidence connects a technical function to a measurable improvement in safe downtime, time-to-revoke, restore time or reconciliation burden.

Outcome	Primary resilience question	Evidence that matters
1. Patient identity and longitudinal record integrity	Can the right clinician access the right patient record when primary identity or record services fail?	Independent read-only data, break-glass access, identity proofing, temporary-identifier control and reconciliation tests.
2. EHR/EPR and clinical workflow continuity	Can essential orders, documentation, handoffs and patient-flow decisions continue safely?	24/48/72-hour exercise, workflow-specific paper process, interface backlog plan and clinical sign-off.
3. Laboratory, pathology and blood-service continuity	Can specimens, results, transfusion and critical alerts operate during supplier or network failure?	Patient matching, manual worklists, result acknowledgement, alternative capacity and blood-product contingency.
4. Imaging and diagnostic continuity	Can images be acquired, interpreted and distributed without normal PACS/RIS or identity services?	Local acquisition, downtime worklists, prior-image access, reporting fallback and cross-site transfer.
5. Medication and pharmacy continuity	Can prescribing, verification, dispensing and administration remain safe without full digital support?	Downtime medication history, allergy access, controlled-substance governance and post-outage reconciliation.
6. Devices, facilities, cloud and supplier containment	Can compromised dependencies be isolated without removing essential care capability?	Segmentation, access inventory, kill switch, alternative products and tested service substitution.
7. Recovery, reconciliation and crisis governance	Can the organisation restore trust, resolve the backlog and return to normal operation safely?	Trusted rebuild, phased reconnect, clinical verification, record reconciliation and accountable decision rights.

Black Book operating principle

Every continuity control should answer two questions: which clinical function does it preserve, and for how long has that preservation been proven?

Outcome 1: Patient identity and longitudinal record integrity

Identity is the control plane of the modern hospital. It determines who can see a record, who can place an order, which supplier can maintain a system, and whether a machine or application can exchange data. A hospital can therefore lose clinical access without losing the application itself. Directory failure, SSO outage, compromised privileged accounts or disabled multifactor authentication can make otherwise healthy systems unusable.

The continuity requirement is broader than a break-glass username. Emergency access must confirm that the user is authorised, restrict the scope of privilege, preserve an audit trail and remain available when the primary identity provider is isolated. The organisation must also manage temporary patient identifiers, duplicate registration, merged records and delayed demographic updates. These are patient-safety controls, not administrative details.

Non-human identities create the second layer. Service accounts, API tokens, certificates, integration users, robotic-process accounts and AI platform credentials often have broad access and weak ownership. They can preserve an attacker's pathway after visible user accounts have been disabled. Black Book's supplier-isolation findings show why an inventory of companies is insufficient; containment requires an inventory of every identity and trust relationship used by those companies.[33]

Identity evidence test	Minimum acceptable evidence	Red flag
Phishing-resistant privileged access	FIDO2 or equivalent for high-risk roles, with tested recovery and no weaker bypass path	Ordinary push MFA remains the only barrier for administrators and remote suppliers.
Independent emergency access	Break-glass identities work when directory, SSO and network segments are unavailable	Emergency accounts depend on the same service being contained.
Session and token revocation	Cloud sessions, refresh tokens and machine credentials can be disabled centrally and rapidly	Password reset is treated as complete containment.
Supplier identity ownership	Every supplier user, service account, certificate and API token has an owner and expiry	Accounts remain active after projects, staff changes or contract termination.
Patient identity downtime	Temporary identifiers, duplicate checks and later merge processes are exercised	Paper registration has no tested reconciliation path.

Outcome judgment

The best identity programme is not the one that makes normal access easiest. It is the one that can preserve controlled clinical access while the normal identity plane is untrusted.

Outcome 2: EHR/EPR and clinical workflow continuity

The core record is the hospital's operational memory. It holds allergies, medications, orders, results, notes, care plans and the sequence of decisions that make treatment safe. During a cyber event, the EHR/EPR may be encrypted, intentionally disconnected, unavailable because identity is down, or reachable but untrusted because the organisation cannot confirm data integrity.

A credible continuity model therefore has three modes. The first is independent read-only access to a recent, clinically useful record. The second is a safe degraded workflow for new orders, documentation, handoffs and patient movement. The third is a controlled re-entry process that reconciles all actions performed during the outage. Most plans concentrate on the second mode and underestimate the first and third.

The Black Book confidence curve shows that many organisations can manage the opening phase but not the cumulative burden. At twenty-four hours, paper forms and local workarounds may preserve urgent services. At forty-eight hours, missing longitudinal context, duplicated work and growing queues begin to affect capacity. At seventy-two hours, staff fatigue and reconciliation volume become material patient-safety hazards.[32]

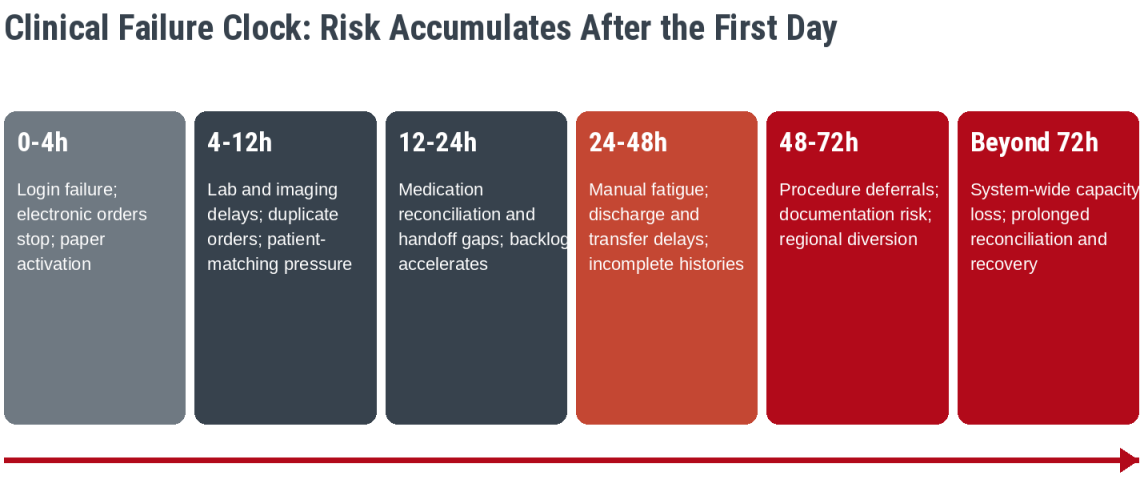

Figure 9. The clinical failure clock shows why safe downtime must be measured as an endurance curve rather than a binary capability.

Source: Black Book Research continuity framework, informed by European hospital incidents and the 284-respondent panel [13][19][22][32].

EHR/EPR continuity checkpoint	Board evidence
0-4 hours	Downtime activation time; availability of paper packs and read-only record; emergency identity functioning.
4-12 hours	Order and result routing; patient-matching controls; prioritisation of emergency and surgical activity.
12-24 hours	Medication reconciliation; handoff integrity; bed, transfer and discharge visibility.
24-48 hours	Backlog control; staff rotation; alternative diagnostics; regional diversion and mutual aid.
48-72 hours	Procedure deferrals; reconciliation capacity; clinical risk acceptance and executive decision rights.
Return to service	Trusted restore, interface sequencing, data-integrity validation and complete downtime reconciliation.

Outcome 3: Laboratory, pathology and blood-service continuity

Laboratory and pathology services are among the most consequential shared dependencies in healthcare. They support emergency assessment, surgery, maternity, oncology, infection management, chronic disease, primary care and transfusion. A supplier compromise can therefore affect several clinical pathways and several organisations at the same time.

The Synnovis incident demonstrates the scale of that propagation. A ransomware attack against one pathology provider significantly reduced processing capacity, delayed more than 11,000 outpatient and elective appointments and affected five NHS trusts and local providers. The loss of normal blood cross-matching also contributed to pressure on universal-donor blood supplies. The incident later became a national reference point because it contributed to the death of a patient.[13][14]

Laboratory downtime is not solved by printing a list of tests. Specimens require verified patient identity, priority, location, collection time, chain of custody and result acknowledgement. Critical results must reach the right clinician and be documented. Blood services require compatibility, inventory and emergency release controls. When systems return, every specimen, result and clinical decision must be reconciled.

Laboratory continuity domain	Required capability	Failure consequence
Specimen identity	Barcoded or manually controlled fallback with duplicate and mismatch checks	Wrong-patient result or untraceable specimen.
Critical-result communication	Named receiver, read-back and documented acknowledgement	Life-threatening result is delayed or lost.
Blood bank	Emergency release, cross-match alternatives, stock visibility and regional coordination	Transfusion delay or avoidable use of scarce universal donor stock.
Alternative capacity	Pre-agreed neighbouring or commercial laboratory support with transport plan	Mutual aid fails because all providers share the same supplier.
Interface backlog	Sequenced replay, duplicate suppression and result validation	Restored interfaces flood the record with duplicates or omissions.
Clinical prioritisation	Explicit test and procedure hierarchy for constrained capacity	Elective backlog competes with emergency demand without transparent rules.

Outcome judgment

Pathology supplier risk should be measured in diagnostic capacity lost, blood-service impact and appointments deferred - not only systems unavailable.

Outcome 4: Imaging and diagnostic continuity

Imaging continuity is often overestimated because scanners can remain physically operational. In practice, diagnostic imaging depends on modality worklists, patient identity, protocol information, PACS, RIS, reporting, prior studies, voice recognition and result distribution. Loss of any one component can slow or stop the pathway even when the equipment still produces images.

The resilience objective is graceful degradation. Modalities should support controlled local operation; emergency worklists should be available; images should be retrievable or transferable through a trusted alternative; and radiologists should have a documented reporting fallback. The plan must distinguish between acquisition, interpretation and distribution because each may fail independently.

Regional imaging networks and cloud archives create both protection and concentration. They can provide alternative access and specialist coverage, but they can also create a shared blast radius. The buyer's evidence standard should therefore include a test in which the shared platform itself is unavailable or intentionally isolated.

Imaging failure point	Degraded-mode requirement	Evidence standard
Patient and worklist identity	Verified manual or local worklist with later reconciliation	Exercise demonstrates zero unresolved wrong-patient or duplicate-study events.
Image acquisition	Local modality operation with secure temporary storage	Capacity and retention are sufficient for the planned outage duration.
PACS/RIS access	Independent emergency viewer or alternate archive path	Viewer does not depend on the same identity or network domain.
Prior comparison	Documented risk process when prior images are unavailable	Clinicians understand which studies cannot proceed safely.
Reporting	Dictation or structured manual reporting with signed delivery	Critical findings reach the responsible clinician with acknowledgement.
Cross-site support	Secure transfer and credentialing for external readers	Regional mutual aid has been tested under common-platform failure.

Outcome judgment

The imaging continuity test is not whether the scanner turns on. It is whether the complete diagnostic chain remains clinically accountable.

Outcome 5: Medication and pharmacy continuity

Medication safety is one of the first domains in which missing information becomes dangerous. Prescribing depends on current medication history, allergies, renal and hepatic function, interactions, formulary and patient context. Verification depends on pharmacy access and communication. Administration depends on the correct patient, product, dose, route and time. A cyber outage can weaken every control in the chain simultaneously.

Paper medication administration is possible, but the process must be designed for sustained use. Staff need an authoritative medication history, a method to record administrations and omissions, access to allergy information, controlled-substance governance, and a mechanism for communicating changes across shifts and locations. The longer the outage, the greater the risk that the paper record diverges from reality.

The return to service is equally hazardous. Bulk re-entry without verification can duplicate orders, miss discontinuations or create an inaccurate administration history. Pharmacy, nursing and medical teams need a shared reconciliation sequence and clear ownership of discrepancies.

Medication continuity control	Question for the exercise	Evidence of readiness
Medication history	What source remains available when the EHR and national record are unavailable?	Independent, recent and clinically legible history with known limitations.
Allergy and interaction safety	How are high-risk alerts replaced during downtime?	Manual high-risk checks and pharmacist review for defined cohorts.
Dispensing	Can labels, stock, controlled drugs and urgent supply operate offline?	Downtime process tested across inpatient, emergency and discharge scenarios.
Administration	How are doses recorded, witnessed and handed over?	Standard forms, patient verification and shift reconciliation.
Changes during outage	How are new, stopped and modified therapies communicated?	Single accountable paper record and cross-disciplinary review.
System return	Who reconciles orders and administrations before normal workflow resumes?	Phased restart with clinical validation and discrepancy tracking.

Outcome judgment

Medication downtime is safe only when the temporary record is treated as a clinical system of record - with ownership, controls and reconciliation.

Outcome 6: Devices, facilities, cloud and supplier containment

The hospital's attack surface now extends beyond conventional IT. Connected medical devices, building-management systems, refrigeration, sterile services, pneumatic tubes, access control, nurse call, communications, cloud platforms and remote suppliers all contribute to care. Many cannot be patched or disconnected on the same timetable as ordinary endpoints. Some require vendor access to remain safe and supported.

That creates a containment dilemma. The technically safest action may be to sever connectivity broadly; the clinically safest action may require preserving a limited path for essential devices or services. The only credible resolution is predesigned segmentation, known dependencies and tested isolation. An incident is the wrong time to discover that several clinical services share one unmanaged vendor account or one flat network segment.

The Stryker incident shows that supplier cyber risk also affects physical availability. Production, shipping, distribution and ordering were disrupted, and the NHS shifted to an interim allocation process while assessing stock and alternatives. No onward hospital compromise was required for the event to create patient-safety concern.[16]

Dependency category	Containment requirement	Continuity requirement
Connected medical devices	Network segmentation, monitored vendor access and documented compensating controls	Safe local mode, alternative device or clinical procedure when connectivity is removed.
Facilities and operational technology	Separation from enterprise identity and controlled remote administration	Manual operation, local safety controls and facilities-engineering response.
Cloud clinical platforms	Tenant, session, token and API revocation with independent logging	Exported critical data, alternate workflow and tested regional failover.
Medical product suppliers	Account and ordering isolation, fraud controls and incident communication	Stock visibility, substitution, allocation and clinical prioritisation.
Managed service providers	Full access inventory and customer-controlled kill switch	Internal or alternate support for critical functions during isolation.
AI and automation platforms	Tier-1 classification when production care or revenue depends on them	Manual process and secure removal of model/API connections without workflow collapse.

Outcome judgment

Third-party risk is no longer a procurement questionnaire. It is the ability to disconnect trust without disconnecting care.

Outcome 7: Recovery, reconciliation and crisis governance

Recovery is a controlled restoration of trust, not a race to reconnect. The organisation must determine whether the attacker retains access, whether recovery assets are clean, which identities can be trusted and in what sequence applications and interfaces should return. Reconnecting too quickly can reintroduce compromise or overwhelm dependent systems with queued transactions.

Clinical verification must accompany technical verification. Laboratory, pharmacy, imaging, identity and EHR teams should confirm that data are current, interfaces are complete, alerts work, worklists are correct and downtime activity has been reconciled. Executive pressure to declare recovery should not override unresolved patient-safety risks.

Governance is the structure that protects those decisions under pressure. The organisation should determine in advance who can disconnect a supplier, who accepts clinical risk, who engages law enforcement and regulators, who considers a ransom demand, who authorises public statements and who decides that normal operations can resume. NHS England's 2026 board assurance guidance reinforces the expectation that cyber responsibility sits explicitly at executive and board level.[17]

Recovery phase	Technical decision	Clinical decision	Executive evidence
Containment	Which domains, suppliers, sessions and integrations are isolated?	Which services must divert or move to degraded operation?	Named authority and documented rationale.
Eradication	How is persistence removed and identity trust re-established?	Which data and workflows remain unreliable?	Independent challenge and evidence retention.
Restore	What is rebuilt first and from which trusted assets?	What minimum clinical service is safe to reopen?	Recovery objectives and sign-off criteria.
Reconnect	In what sequence are interfaces, suppliers and network paths restored?	Can receiving systems handle queues without duplicate or missing data?	Change control adapted for crisis speed.
Reconcile	How are paper and disconnected records incorporated?	Who validates orders, results, medications and identifiers?	Backlog, harm and unresolved-risk reporting.
Return to normal	When does crisis command stand down?	Have deferred patients and clinical backlogs been addressed?	Post-incident review and funded corrective actions.

Section conclusion

The seven outcomes form one operating system. A hospital is only as resilient as the weakest clinical dependency that can no longer be safely substituted, isolated or restored.

Black Book Insights

06

Exposure, Readiness and Residual Risk Indexes

A comparative European market view that avoids confusing attack visibility with institutional weakness.

European Hospital Cyber Exposure Index

External pressure and digital dependency, separated from comparative readiness

The Exposure Index measures the evidence surrounding a country's health system: criminal pressure, state-linked targeting, critical-infrastructure dependency, supplier concentration and digital reliance. It does not measure the quality of every hospital's controls. A high score indicates that the market contains more pathways through which a cyber event could become clinically consequential.

Poland leads because destructive infrastructure targeting, geopolitical position and strategic logistics create a distinctive risk profile. Germany follows because of ransomware visibility, economic value and healthcare complexity. France and the United Kingdom occupy the next positions for different reasons: France for multi-vector pressure and the United Kingdom for supplier concentration and nationally interconnected care.

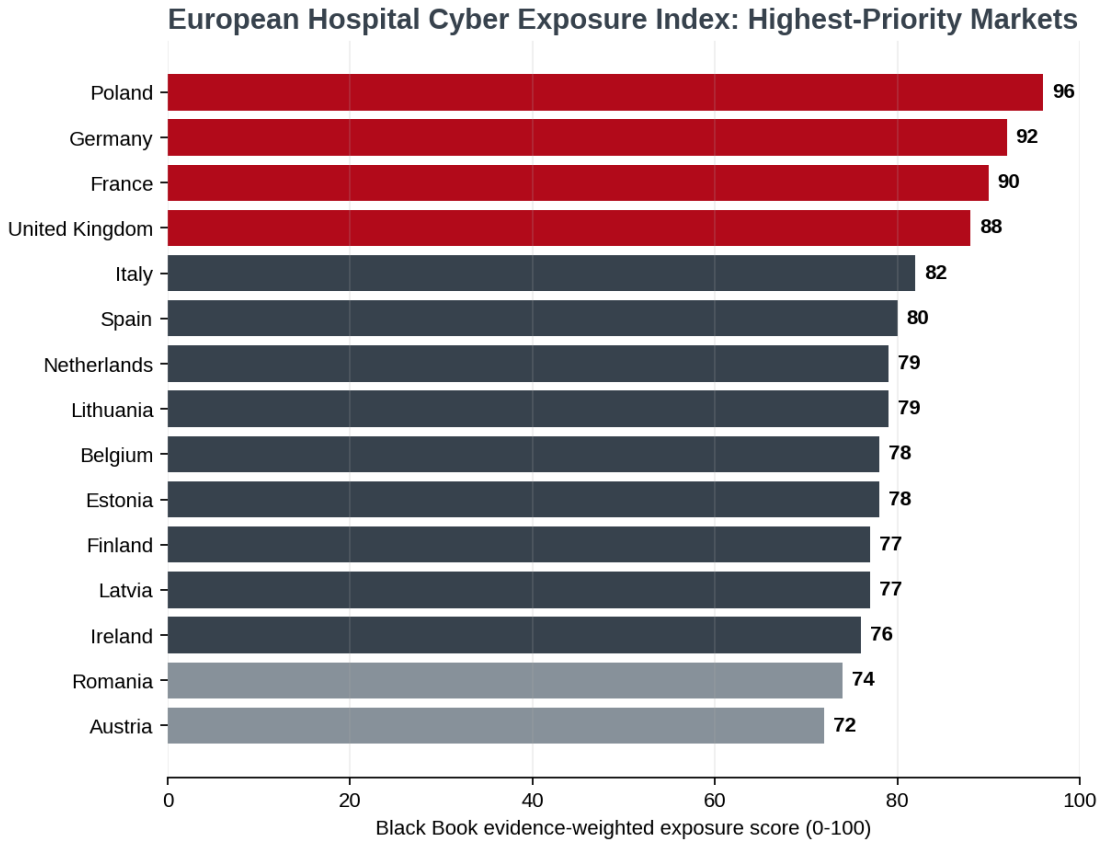

Figure 10. Fifteen highest country exposure scores, excluding Ukraine.

Source: Black Book Research evidence-weighted index using official evidence through 1 August 2026.

Exposure band guide

Extreme 90-100; Very high 80-89; High 70-79; Elevated 60-69; Watch below 60. Bands express comparative evidence and dependency, not a prediction that a specific organisation will be breached.

Clinical Continuity Readiness Index

The Readiness Index evaluates comparative evidence of national response capacity, sector coordination, continuity and restore expectations, supplier and identity controls, regulation, exercises and reporting. It is deliberately conservative. Strong national institutions can improve coordination and expertise, but the score does not assume that every provider has the same capability.

Norway, Denmark and Iceland lead the comparative readiness group, followed by Sweden, Finland, Switzerland and the Netherlands. These countries benefit from strong public institutions, mature digital services and coordinated national capability. Their challenge is not a lack of expertise; it is the concentration created by shared platforms and highly digital workflows. Readiness must therefore include local fallback and the ability to operate when the national service itself is unavailable.

Country	Readiness score	Primary strength	Remaining concentration risk
Norway	82	National security capability and systematic resilience emphasis	Energy, maritime, cloud and specialist-supplier dependencies.
Denmark	82	Coordinated digital public services and shared capability	National and regional platform blast radius.
Iceland	82	Small-system coordination and high institutional visibility	Limited specialist and alternative-provider capacity.
Sweden	81	Strong public institutions and digital health infrastructure	Shared services and highly connected care pathways.
Finland	80	National threat monitoring and explicit edge/supply-chain focus	Frontline geopolitical and critical-infrastructure exposure.
Switzerland	79	Strong national capability and high-value sector awareness	Cross-border health, research and life-sciences suppliers.
Netherlands	78	Identity-first and shared-service maturity	Cloud and platform concentration across providers.
Estonia	76	Deep digital-government and cyber defence experience	Small-system concentration and local provider variance.

Readiness caution

National strength reduces response friction; it does not guarantee that a small hospital, community provider or supplier can sustain seventy-two hours of degraded care.

Residual Clinical Cyber Risk

Residual risk combines exposure with the inverse of readiness. This is the index that most directly supports prioritisation. A high-exposure, high-readiness country may still rank below a lower-exposure market with substantial continuity gaps. That outcome is intentional: the model asks where external pressure is most likely to become clinical disruption, not where the most attacks are counted.

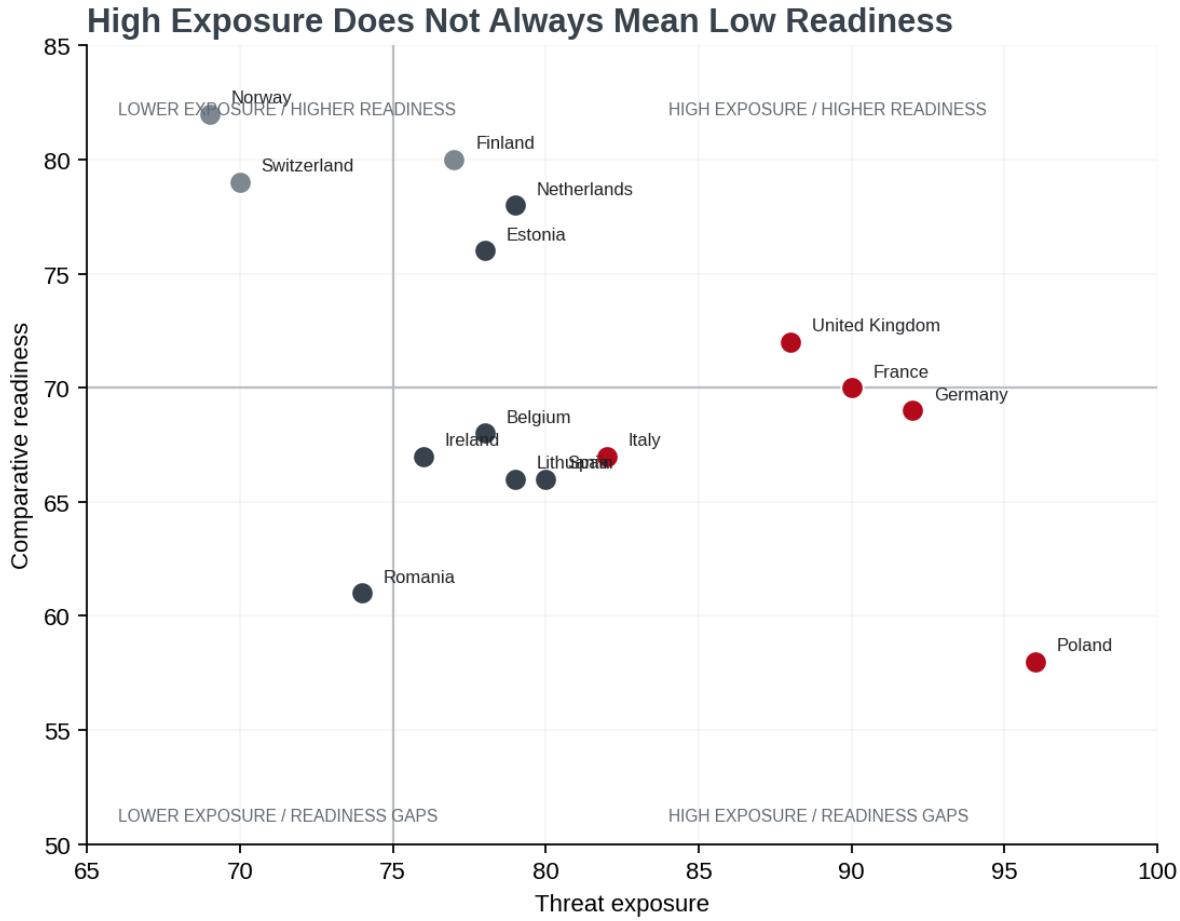

Figure 11. The matrix distinguishes frequently targeted but comparatively prepared markets from those where readiness gaps amplify lower external pressure.

Source: Black Book Research evidence-weighted index. Country positions are comparative and should be read by quadrant, not as exact distances.

Poland occupies the high-exposure/readiness-gap quadrant. Germany, France and the United Kingdom remain high exposure but benefit from stronger national capability. The Netherlands, Finland, Estonia, Norway and Switzerland illustrate the digital maturity paradox: readiness is stronger, yet dependency remains significant. Romania and parts of southern and eastern Europe warrant attention because a smaller public evidence base can coexist with larger operational gaps.

Interpretation rule

Use the score to decide where to validate continuity, not to decide where cyberattacks “will happen.” The index prioritises evidence collection, investment and exercise.

Full country index - first half

Rank	Country	Exposure	Readiness	Residual	Band
1	Poland	96	58	77	Extreme
2	Germany	92	69	71	Very high
3	France	90	70	69	Very high
4	United Kingdom	88	72	67	Very high
5	Italy	82	67	65	Very high
6	Spain	80	66	64	High
7	Lithuania	79	66	63	High
8	Belgium	78	68	62	High
9	Latvia	77	65	62	High
10	Romania	74	61	62	High
11	Ireland	76	67	61	High
12	Slovakia	72	63	60	High
13	Netherlands	79	78	59	High
14	Estonia	78	76	59	High
15	Cyprus	71	62	59	High
16	Finland	77	80	57	Elevated

The ranking should be interpreted in bands. Poland's 77 is materially different from the 60s; the countries clustered between 58 and 65 should be treated as one intensified-priority group unless country-specific evidence indicates otherwise. Small changes in reporting or one severe incident can move a country several positions.

Full country index - second half

Rank	Country	Exposure	Readiness	Residual	Band
17	Austria	72	70	57	Elevated
18	Portugal	65	62	56	Elevated
19	Czechia	67	68	55	Elevated
20	Greece	64	63	55	Elevated
21	Bulgaria	62	58	55	Elevated
22	Hungary	63	62	54	Elevated
23	Switzerland	70	79	53	Elevated
24	Croatia	60	63	52	Elevated
25	Norway	69	82	51	Elevated
26	Sweden	68	81	51	Elevated
27	Denmark	67	82	50	Elevated
28	Malta	55	61	49	Watch
29	Slovenia	58	70	48	Watch
30	Luxembourg	58	77	46	Watch
31	Iceland	54	82	41	Watch

Lower ranking does not mean low local risk. A single vulnerable supplier, exposed edge device, under-tested hospital or regional dependency can produce a severe incident in any country. The index is a national comparative lens; every organisation still requires its own dependency and continuity assessment.

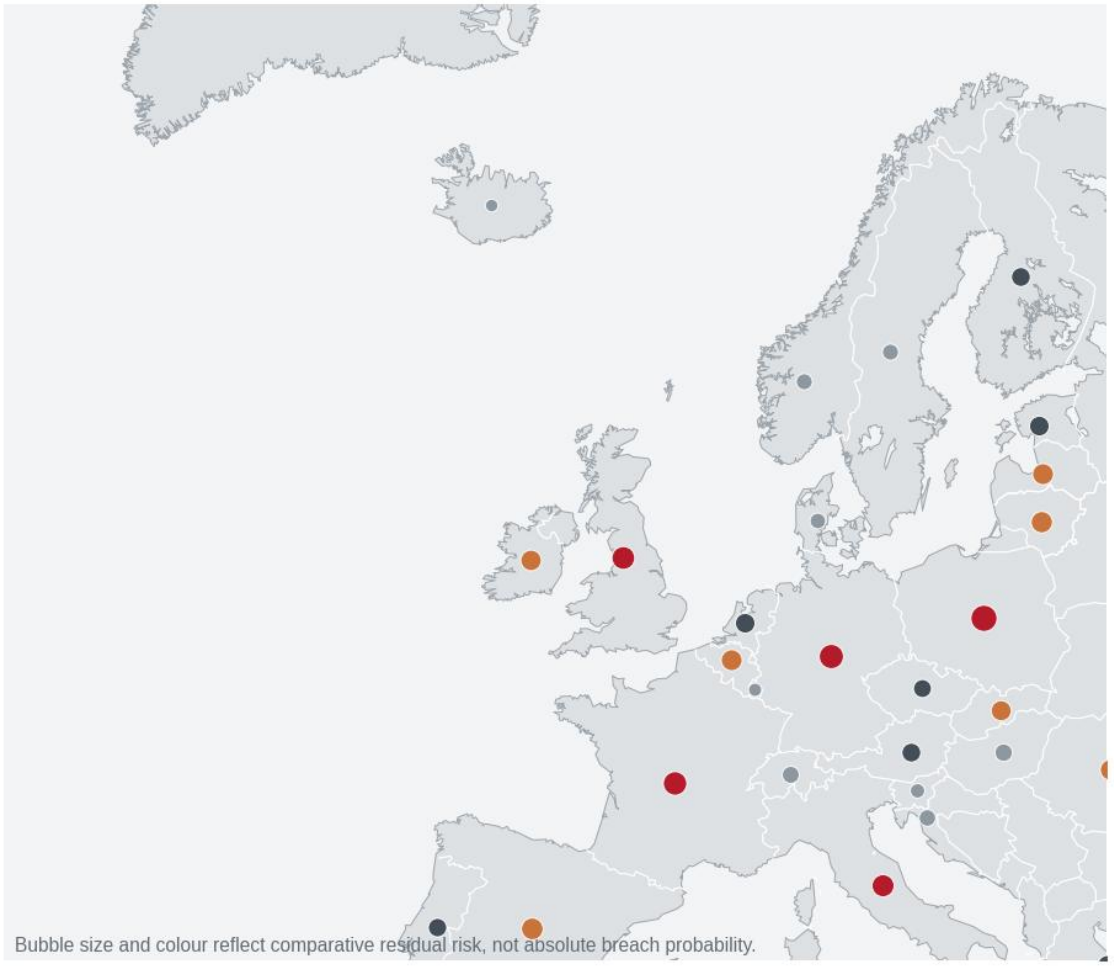

Figure 12. Residual risk distribution across Europe.

Source: Black Book Research evidence-weighted index. Natural Earth/Basemap geography; Ukraine excluded from scoring.

Black Book Insights

07

Attack Pathways, Red Flags and Evidence Standards

How attackers enter, how clinical risk propagates, and what buyers should require as proof.

2026 Europe Hospital Cyber Exposure & Clinical Continuity Index

Attack pathways that most often create healthcare consequence

Different actors converge on the same identities, edge devices and trusted dependencies

The attack pathway matters because it determines which controls can still be trusted. A phishing compromise begins with a user or session. An edge-device exploit may bypass endpoint controls entirely. A supplier compromise enters through an authorised relationship. A destructive campaign may target industrial devices and recovery assets. Yet the pathways converge once the attacker gains privilege, maps dependencies and reaches the systems that support clinical care.

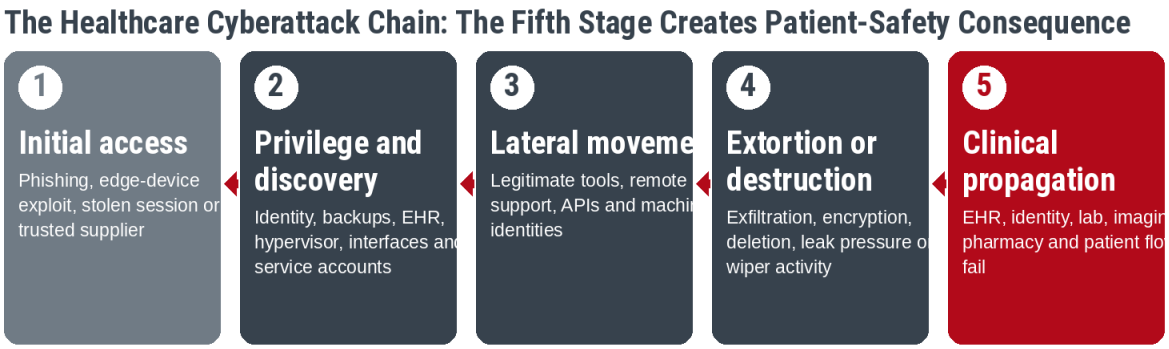

Figure 13. Five stages from access to clinical propagation.

Black Book Research synthesis of European threat and incident evidence [1][7][9][11][13].

Pathway	Early warning	Containment priority
Phishing and session theft	Impossible travel, unusual token use, new mailbox rules, MFA fatigue or help-desk manipulation	Revoke sessions and refresh tokens, not only passwords; verify related cloud and supplier identities.
Edge-device exploitation	Unexpected configuration change, new admin account, anomalous tunnel or outbound traffic	Remove internet exposure, preserve logs, rebuild from known configuration and search downstream.
Supplier compromise	Unusual support activity, off-hours access, unexplained API calls or supplier incident notice	Activate customer-controlled kill switch across all identities, routes and integrations.
Ransomware / exfiltration	Large staging, archiving, unusual cloud transfer, backup access or security-tool disablement	Protect recovery assets, segment clinical services, preserve evidence and activate clinical downtime.
Destructive / hybrid activity	Long-term infrastructure access, OT reconnaissance, coordinated disruption or wiper indicators	Protect life safety, isolate IT/OT, activate facility and regional contingency.

Red flags that a healthcare organisation is overestimating readiness

1	Backups are reported, but no complete clinical production restore has been timed in the last year.
2	The supplier inventory names companies but not accounts, certificates, tokens, endpoints, routes and integrations.
3	Downtime exercises end after four hours and do not include night shift, weekend staffing or regional diversion.
4	Read-only EHR access depends on the same identity provider, network or cloud tenant being contained.
5	Clinical departments own paper procedures, but no one owns post-outage reconciliation.
6	The board receives vulnerability and phishing statistics but not hours of safe care, time-to-revoke or restore success.
7	A national platform or neighbouring hospital is assumed to remain available without testing common suppliers.
8	AI, automation and low-code integrations operate in production but are not classified as critical suppliers.
9	Medical-device remote access is enabled by shared or persistent vendor credentials.
10	The organisation cannot identify who has authority to isolate a supplier or reject a ransom demand.

Diagnostic rule

If the evidence cannot be produced during an exercise, it will not become easier to produce during an attack.

Evidence standards for hospital buyers

Healthcare cybersecurity procurement should move beyond product demonstrations and security questionnaires. Buyers need evidence that the supplier can operate within the hospital's clinical continuity model. The contract should support customer control, rapid notification, joint exercise and restoration - not create delay when containment is urgent.

Supplier claim	Evidence the buyer should require	Contractual protection
"We provide rapid incident response."	Named severity criteria, notification clock, contact path and recent customer exercise	Mandatory notification within defined hours; 24/7 escalation and evidence sharing.
"Access is secure."	Complete human and machine access inventory; phishing-resistant admin access; session logs	Customer right to revoke, rotate and disable all access immediately.
"The platform is resilient."	Recent restore test, RTO/RPO evidence, dependency map and failure-mode exercise	Defined recovery objectives, service credits and joint recovery obligations.
"We use subcontractors."	Current list of hosting, support, data, model and integration subcontractors	Prior notice, flow-down security duties and customer termination rights.
"Data can be exported."	Tested bulk and incremental export with semantics, provenance and audit history	Exit assistance, documented format and no punitive restriction during incident.
"We support healthcare continuity."	Clinical workflow runbook, read-only/offline mode and post-outage reconciliation support	Participation in hospital exercises and incident command.

ENISA's hospital procurement guidance reinforces the need for explicit supplier responsibility, timely vulnerability and incident notification, security documentation and enforceable obligations across the relationship.[34] The Black Book addition is operational: those clauses should be exercised before renewal, not merely reviewed by legal counsel.

Evidence hierarchy: from assertion to proven resilience

Evidence level	Description	Black Book rating
Level 1 - Assertion	Policy, questionnaire response, architecture claim or certification without customer-specific operating evidence	Insufficient for Tier-1 clinical dependency.
Level 2 - Documented design	Current runbook, dependency map, recovery objective and named owner	Necessary but unproven.
Level 3 - Component test	Backup restore, account revocation, network block or tabletop exercise performed separately	Partial evidence; integration and clinical impact remain uncertain.
Level 4 - End-to-end exercise	Supplier, technology, clinical and executive teams perform the complete containment or downtime workflow	Strong evidence if findings are closed.
Level 5 - Production-equivalent proof	Timed restore, isolation or failover using production-equivalent data, identities, interfaces and clinical validation	Highest evidence standard.
Level 6 - Incident-proven performance	Capability performed successfully during a material real-world incident and independently reviewed	Strongest evidence, but must still be retested after change.

Black Book evidence standard

Tier-1 suppliers should reach Level 4 or Level 5 for isolation and recovery. Level 1 evidence may satisfy procurement administration; it does not protect care delivery.

The clinical failure clock should drive exercise design

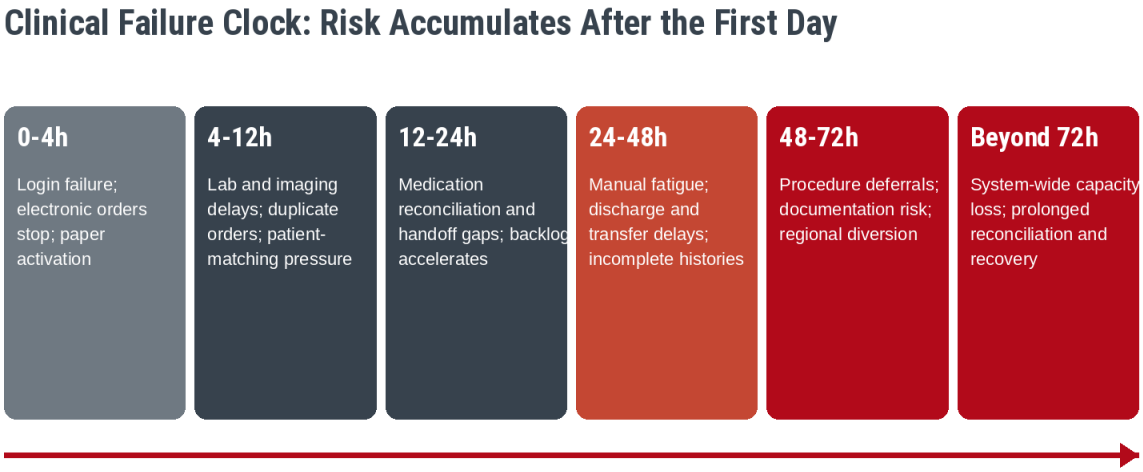

Figure 14. Exercise objectives should change as the outage extends.

Source: Black Book Research clinical continuity framework.

A four-hour tabletop tests activation, communication and first decisions. It does not test whether the hospital can operate through a second medication round, a night shift, a surgical list, accumulated critical results, weekend staffing or regional diversion. Every Tier-1 continuity programme should therefore contain nested scenarios: rapid containment, twenty-four-hour operation, forty-eight-hour capacity management and seventy-two-hour recovery plus reconciliation.

Exercise duration	What must be tested	Common false confidence
0-4 hours	Incident command, isolation authority, downtime activation, emergency communication and initial prioritisation	A successful tabletop is treated as proof of operational continuity.
4-12 hours	Shift handover, diagnostics, medication, patient identity and critical-result communication	Day-shift experts remain available throughout the scenario.
12-24 hours	Backlog management, elective deferral, staff fatigue, read-only data and regional coordination	Manual workload is assumed to remain stable.
24-48 hours	Supply, blood, discharge, transfer, alternative services and executive risk acceptance	Neighbouring providers are assumed to have capacity and different suppliers.
48-72 hours	Sustained degraded care, public communication, reconciliation staffing and phased restore	Technical restoration is assumed to end clinical impact.

Ransom governance: decision architecture before the demand arrives

A predetermined ransom governance process does not imply willingness to pay. It prevents the organisation from inventing decision rights during a crisis. The process should integrate law enforcement, national cyber authorities, legal counsel, sanctions screening, insurance, clinical safety, evidence preservation and public communication. It should also recognise that payment does not guarantee deletion, non-publication, decryption quality or absence of future targeting.

Decision domain	Pre-incident requirement	Why delay is dangerous
Authority	Named executive, board and clinical roles; documented escalation thresholds	Conflicting instructions waste the period when containment and care decisions are most urgent.
Law and sanctions	Jurisdiction, notification and sanctions-screening process	Payment or engagement may be prohibited or create legal exposure.
Clinical safety	Assessment of care capacity, time to restore and diversion options	Technical or financial decisions may underestimate patient harm.
Insurance	Current coverage, notification requirements and approved specialist contacts	Late notification can impair support or coverage.
Evidence	Forensic preservation and chain-of-custody expectations	Premature rebuilding destroys information needed for containment and attribution.
Communications	Patient, staff, regulator, supplier and media templates with approval path	Inconsistent messaging damages trust and creates operational confusion.

Section conclusion

The strongest controls reduce attacker leverage before a demand is made: safe care can continue, recovery assets are trusted, supplier access can be removed, and decision rights are already clear.

Black Book Insights

08

Country and Regional Risk Profiles

Where European healthcare cyber pressure, dependency and continuity risk are converging now.

2026 Europe Hospital Cyber Exposure & Clinical Continuity Index

Country and regional risk profiles

The same cyber event produces different consequences in different health-system structures

National comparisons are most useful when they explain the mechanism of risk. Germany's challenge is not Poland's challenge; the United Kingdom's supplier concentration is not the same as France's threat convergence; and the Baltic states should not be evaluated using the same assumptions as large decentralised markets. Each profile therefore identifies the dominant signal, the healthcare pathway through which the risk propagates and the question boards should be able to answer now.

Locations and ecosystems requiring the most immediate attention

Priority location or ecosystem	Why attention is elevated	Healthcare consequence to test
Polish energy, heating, transport and Ukraine-support corridor	Recent destructive infrastructure activity and current EU attribution context	Simultaneous loss of power, communications, cloud, transport and EHR/EPR access.
Brussels institutional and supplier ecosystem	Government, EU, diplomatic, consultancy, telecom and cloud concentration	Indirect hospital access through shared suppliers, identity and communications infrastructure.
United Kingdom pathology and shared supplier networks	Demonstrated multi-trust clinical disruption and prolonged recovery	Loss of diagnostics, blood services, products and regional elective capacity.
German municipal, industrial and hospital networks	High ransomware visibility and extensive technology interconnection	Availability failure across EHR, diagnostics, municipal services and specialised suppliers.
French public-sector, telecom and major hospital environments	Criminal, state-linked, exfiltration and edge-device pressure	Concurrent operational recovery and data-impact investigation.
Baltic-Nordic digital public-service corridor	Geopolitical targeting, edge exploitation and national platform dependence	National identity, communications or cloud failure with limited local substitute capacity.
Internet-facing hospital edge across Europe	Fast exploitation of routers, VPNs, gateways and remote-management systems	Privileged access that bypasses endpoint controls and accelerates lateral movement.

Current watch condition

The highest-risk “location” may be a shared dependency rather than a place: an identity provider, pathology network, cloud tenant, managed service, router fleet or medical-product supplier used across many hospitals.

Poland: Destructive escalation and critical-infrastructure dependency

The sharpest evidence of attempted destructive cyber sabotage within the EU's current operating environment.

96	58	77	Extreme
Exposure	Readiness	Residual risk	Priority band

Poland occupies the first position in the exposure index because its healthcare risk cannot be separated from the country's role as a strategic logistics corridor, its proximity to Russia and Belarus, and the demonstrated targeting of energy infrastructure. On 29 December 2025, coordinated attacks struck more than thirty wind and photovoltaic facilities, a manufacturing company, and a combined heat and power plant serving almost half a million customers. The attackers damaged or attempted to damage industrial devices, delete system data, and deploy wiper malware. Defensive controls prevented the intended heat and electricity disruption, but the campaign established both intent and capability.[9]

The healthcare implication is indirect but immediate. A hospital does not need to be penetrated for care to fail. Extended loss of electricity, district heating, telecommunications, transport or cloud connectivity can disable imaging, laboratory analyzers, pharmacy refrigeration, sterile services, patient transfer and emergency communications. The July 2026 EU statement that FSB Centre 16 had conducted disruptive sabotage operations against Polish critical infrastructure further elevates this from a theoretical contingency to a current planning requirement.[7]

Black Book's market judgment is that Polish providers should treat combined infrastructure and cyber failure as the defining exercise scenario. Plans that test an EHR outage while assuming stable power, mobile networks and regional transport are not sufficient for the threat profile Poland now faces.

Profile dimension	Black Book assessment
Dominant risk mechanism	Destructive escalation and critical-infrastructure dependency
Most likely first clinical failure	Telecommunications, identity, power-dependent diagnostics and regional patient transfer.
Board-level question	Can the organisation sustain critical care when EHR, power, communications and transport are degraded simultaneously?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Can the organisation sustain critical care when EHR, power, communications and transport are degraded simultaneously?

Germany: Ransomware scale, decentralisation and availability risk

The strongest criminal-volume signal among the large European healthcare markets.

92	69	71	Very high
Exposure	Readiness	Residual risk	Priority band

Germany's position is driven by scale, value and complexity rather than a conclusion that German cyber institutions are weak. ENISA's underlying ransomware and data-breach claims most frequently referenced Germany, at 23.4% of the EU claims in that analysis - more than twice the share of the next country. The country's hospital, ambulatory, insurance, industrial, pharmaceutical and digital-service ecosystems offer attackers many high-value entry points and extensive opportunities for supplier-mediated compromise.[1]

The clinical risk is availability. German health services span university hospitals, municipal providers, private groups, ambulatory practices, laboratories and national digital-health components. A technically local compromise can propagate through interfaces, shared identity, regional diagnostics or vendor support. Public evidence has linked ransomware incidents to postponed procedures, demonstrating that the effect is no longer confined to data protection.[1]

Germany therefore becomes the primary market for measuring whether large, heterogeneous organisations can restore complete clinical production environments rather than isolated servers. The decisive benchmark is the elapsed time from containment to verified identity, interface and workflow restoration.

Profile dimension	Black Book assessment
Dominant risk mechanism	Ransomware scale, decentralisation and availability risk
Most likely first clinical failure	Identity, EHR interfaces, imaging and municipal or regional service coordination.
Board-level question	How many Tier-1 clinical services have been restored from trusted recovery assets in the last twelve months?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

How many Tier-1 clinical services have been restored from trusted recovery assets in the last twelve months?

France: The broadest convergence of criminal and state-linked pressure

A national threat environment in which ransomware, exfiltration, espionage and infrastructure pre-positioning overlap.

90	70	69	Very high
Exposure	Readiness	Residual risk	Priority band

France recorded 3,586 security events handled by ANSSI in 2025, including 2,209 reports and 1,366 confirmed incidents. Healthcare represented 10% of the incidents brought to the agency's attention. At the same time, ANSSI described increasing data exfiltration, persistent interest in edge devices, and continued state-linked activity associated with Russian and Chinese services.[11][12]

This breadth matters because health systems must prepare for different attacker objectives. A ransomware affiliate seeks leverage and payment. An espionage actor may remain hidden, collect strategic information and preserve access. A disruptive actor may attempt to damage services or create public uncertainty. The same vulnerable VPN, router, privileged identity or supplier connection can support any of those objectives.

French healthcare organisations therefore need response plans that separate operational recovery from information recovery. Restoring an application does not answer which data were accessed, whether the attacker retains another path, or how long patient and workforce notifications will take. France is the clearest market for testing that dual-track capability.

Profile dimension	Black Book assessment
Dominant risk mechanism	The broadest convergence of criminal and state-linked pressure
Most likely first clinical failure	Edge-device trust, identity, regional hospital coordination and data-exfiltration investigation.
Board-level question	Can the organisation restore care while preserving evidence and determining what information was stolen?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Can the organisation restore care while preserving evidence and determining what information was stolen?

United Kingdom: Supplier contagion and prolonged operational recovery

The clearest European demonstration that one supplier compromise can disrupt several trusts and clinical pathways.

88	72	67	Very high
Exposure	Readiness	Residual risk	Priority band

The United Kingdom's defining risk is systemic concentration. The June 2024 ransomware attack on pathology supplier Synnovis significantly reduced testing capacity, disrupted five NHS trusts and associated providers, delayed more than 11,000 outpatient and elective appointments, and was later reported by Parliament to have contributed to the death of a patient. The direct financial impact on Synnovis was estimated at GBP 32.7 million.[13][14]

The episode demonstrated that pathology is not a back-office service. It is a clinical dependency for emergency care, surgery, maternity, oncology, transfusion and primary care. The attack also contributed to pressure on O-type blood supplies because affected trusts temporarily lost normal cross-matching capability. Recovery required the rebuilding or restoration of dozens of laboratory systems and extended well beyond the first technical containment actions.[13]

The March 2026 Stryker incident expanded the lesson. A supplier network attack disrupted production, shipping, distribution and ordering, creating concern about the physical availability of medical equipment and consumables even though there was no known onward compromise of NHS systems. NHS England's requirement that specific trusts prepare for cyber-related outages lasting up to six months confirms that continuity planning is now a long-duration operating discipline, not a short IT exercise.[15][16]

Profile dimension	Black Book assessment
Dominant risk mechanism	Supplier contagion and prolonged operational recovery
Most likely first clinical failure	Pathology, blood products, shared suppliers, medical logistics and regional elective capacity.
Board-level question	Which services fail if the supplier remains unavailable for weeks while the hospital network itself remains intact?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Which services fail if the supplier remains unavailable for weeks while the hospital network itself remains intact?

Italy: Persistent ransomware pressure and uneven regional resilience

A high-volume environment in which organisational and regional variation can determine clinical consequence.

82	67	65	Very high
Exposure	Readiness	Residual risk	Priority band

Italy held the second-largest share of ransomware and data-breach claims in ENISA's cited country breakout, at 11.33%. National reporting for the first nine months of 2025 also indicated a substantial increase in health-sector cyber events compared with the same period of 2024, while ransomware remained the highest-impact category even when its event count declined.[1]

The important Italian issue is not a single national score. It is variance. Regional health authorities, local providers, private groups and specialist facilities operate with different technology estates, supplier arrangements and staffing levels. A supplier compromise can create many downstream incidents, while a well-resourced regional centre may recover differently from a smaller local provider.

Black Book's study design therefore treats Italy as a test of consistency. The market question is whether national and regional policy is translating into uniform clinical downtime capability, or whether patient impact still depends too heavily on local staffing, architecture and supplier support.

Profile dimension	Black Book assessment
Dominant risk mechanism	Persistent ransomware pressure and uneven regional resilience
Most likely first clinical failure	Regional coordination, local identity, smaller-provider staffing and shared supplier services.
Board-level question	Would the same incident produce materially different patient consequences in another region or facility?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Would the same incident produce materially different patient consequences in another region or facility?

Spain: High national incident pressure and documented hospital disruption

A mature example of how ransomware creates both immediate care interruption and a long reconciliation tail.

80	66	64	High
Exposure	Readiness	Residual risk	Priority band

Spain reported 122,223 cybersecurity incidents handled by INCIBE in 2025, 26% more than in 2024. The national total included 55,411 malware incidents, 392 ransomware incidents, 25,133 phishing cases and 3,849 incidents involving information theft or unauthorised access. These are cross-sector figures, but they define the pressure surrounding health organisations.[18]

Hospital Clinic Barcelona remains one of Europe's most instructive healthcare cases. The March 2023 ransomware attack affected normal care activity, led to cancelled procedures and outpatient visits, and required manual operating procedures while essential services were prioritised. The case demonstrates that a hospital can recover infrastructure while still carrying a backlog of deferred tests, treatments, documentation and billing.[19]

Spain's defining research question is therefore reconciliation. Continuity plans often describe how to move to paper; fewer describe how thousands of paper orders, results, medication records and temporary identifiers will be re-entered and validated after the systems return.

Profile dimension	Black Book assessment
Dominant risk mechanism	High national incident pressure and documented hospital disruption
Most likely first clinical failure	Laboratory, elective schedules, outpatient throughput and post-restoration reconciliation.
Board-level question	How long will it take to reconcile every clinical action taken during a seventy-two-hour outage?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

How long will it take to reconcile every clinical action taken during a seventy-two-hour outage?

Belgium: Institutional concentration, account compromise and cross-sector dependency

A high-value ecosystem around Brussels in which government, international institutions, suppliers and healthcare share infrastructure and talent.

78	68	62	High
Exposure	Readiness	Residual risk	Priority band

Belgium's national cyber authority reported 635 incident notifications in 2025, including 556 cyber incidents, with account compromise identified as the largest threat category. Public administration and healthcare were among the most frequently targeted sectors. Belgium also moved quickly on NIS2 implementation and national crisis coordination, strengthening the response environment while increasing reporting visibility.[24][25]

The Brussels ecosystem creates a distinctive concentration of diplomatic, governmental, consultancy, cloud, telecommunications and managed-service relationships. A campaign aimed at institutions may not target a hospital directly, yet suppliers and identity providers can create shared pathways. This makes third-party privilege and cross-sector segmentation the central healthcare issue.

Belgium should not be treated simply as a ransomware market. It is an institutional-dependency market in which espionage, account compromise and criminal activity can intersect.

Profile dimension	Black Book assessment
Dominant risk mechanism	Institutional concentration, account compromise and cross-sector dependency
Most likely first clinical failure	Supplier identity, communications, cloud dependencies and regional coordination.
Board-level question	Which suppliers serve both healthcare and high-value government or institutional customers using the same access infrastructure?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Which suppliers serve both healthcare and high-value government or institutional customers using the same access infrastructure?

Netherlands: High digital maturity with concentrated platform dependency

Strong comparative capability paired with the possibility of a large shared-service blast radius.

79	78	59	High
Exposure	Readiness	Residual risk	Priority band

The Netherlands demonstrates the digital resilience paradox. The country combines sophisticated cyber institutions, shared services and identity-first architectures with extensive cloud, platform and supplier connectivity. Dutch authorities recorded 65 police ransomware reports in 2025 while incident-response companies assisted in 40 cases; the national cyber centre cautioned that the true total was higher because reporting and provider participation were incomplete.[20]

Centralisation can reduce response time, standardise controls and improve expertise. It can also magnify failure. The same regional exchange, cloud tenant, managed identity platform or diagnostic network may support many providers. The key issue is whether these platforms can be segmented rapidly without eliminating the clinical benefits they were designed to create.

The Netherlands therefore scores strongly on readiness but remains a high-dependency watch market. Its most valuable evidence will be tested isolation and graceful degradation rather than policy maturity alone.

Profile dimension	Black Book assessment
Dominant risk mechanism	High digital maturity with concentrated platform dependency
Most likely first clinical failure	Cloud identity, shared data exchange, managed services and regional digital dependencies.
Board-level question	Can a national or regional shared service be isolated while preserving minimum safe clinical functionality?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Can a national or regional shared service be isolated while preserving minimum safe clinical functionality?

Ireland: National shared-service concentration and recovery memory

A country with direct experience of national-scale ransomware consequences and substantial post-incident investment.

76	67	61	High
Exposure	Readiness	Residual risk	Priority band

Ireland's 2021 HSE ransomware attack remains a defining European event. The compromise followed a phishing attachment, triggered extensive system shutdowns and rebuilding, and required notification of approximately 90,000 people. The HSE did not pay a ransom. By November 2024, the estimated service-remediation cost was EUR 102 million, while dedicated cyber investment rose across successive budgets.[22][23]

Ireland's national cyber risk assessment identifies geopolitical pressure, evolving technology and supply-chain security as systemic risks, with the possibility of cascading impact across energy, transport, healthcare and financial services. That framing is important: the country's health resilience cannot be evaluated separately from national identity, telecommunications, cloud and public-service dependencies.[21]

The current research question is how consistently the post-2021 improvements have reached hospitals, voluntary providers, community services and suppliers. A national programme can be strategically strong while local readiness remains uneven.

Profile dimension	Black Book assessment
Dominant risk mechanism	National shared-service concentration and recovery memory
Most likely first clinical failure	National shared services, community-provider connectivity, identity and local supplier readiness.
Board-level question	What evidence shows that post-incident investment has produced repeatable recovery capability at every care setting?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

What evidence shows that post-incident investment has produced repeatable recovery capability at every care setting?

Baltic corridor: High digital dependence under persistent geopolitical pressure

Estonia, Latvia and Lithuania combine strong national cyber awareness with small-system concentration and frontline exposure.

77-79	65-76	59-63	High
Exposure range	Readiness range	Residual range	Priority band

The Baltic states should not be described as weak. Estonia in particular has deep national experience in digital government and cyber defence. Yet digital concentration means that a failure in identity, communications or a national service can affect a large share of the population quickly. Estonia recorded 10,185 cyber incidents in 2025 and 756 DDoS attacks, although fewer than one hundred DDoS incidents materially affected the targeted services. A ransomware incident at a family medicine centre demonstrated how stale accounts, excessive privilege and compromised backups can halt patient operations.[27][28]

Lithuania adds a healthcare-specific warning. In June 2026, the data protection authority imposed a EUR 450,000 fine on a healthcare company after investigations of personal-data breaches and security controls. National reporting has also emphasised social engineering and the persistence of vulnerable systems.[29]

The regional risk is the combination of geopolitical targeting, highly digital services, specialist workforce constraints and cross-border infrastructure. The appropriate benchmark is not whether national cyber centres are capable; it is whether every hospital can translate that capability into seventy-two-hour clinical endurance.

Profile dimension	Black Book assessment
Dominant risk mechanism	High digital dependence under persistent geopolitical pressure
Most likely first clinical failure	National identity, communications, primary-care systems and limited specialist recovery capacity.
Board-level question	Which nationally shared function has no clinically safe local fallback?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Which nationally shared function has no clinically safe local fallback?

Nordic corridor: Strong response capacity facing fast exploitation and supplier risk

Finland, Norway, Sweden and Denmark generally score well on readiness but remain exposed through edge devices, critical infrastructure and shared services.

67-77	80-82	46-57	Elevated
Exposure range	Readiness range	Residual range	Priority band

Nordic countries benefit from comparatively mature public institutions, coordinated response and extensive digital infrastructure. Those strengths do not eliminate risk. Finland's national cyber centre reported that the 2025 threat level remained elevated, serious cases stayed high, and critical vulnerabilities could be exploited within minutes or hours. It also highlighted phishing, internet-facing edge devices and supply-chain dependencies.[30]

Norway's Risk 2026 assessment describes a serious security environment in which actors take greater risks and use more sophisticated methods. Similar concerns apply across the region because healthcare depends on energy, maritime logistics, telecommunications, cloud infrastructure and national platforms.[31]

The Nordic challenge is graceful degradation. Highly digital workflows produce efficiency and clinical visibility, but they can leave little manual capacity when national or regional platforms fail. The strongest organisations will prove that centralisation improves resilience without creating an unmanageable blast radius.

Profile dimension	Black Book assessment
Dominant risk mechanism	Strong response capacity facing fast exploitation and supplier risk
Most likely first clinical failure	Shared identity, cloud, telecommunications, remote care and regional logistics.
Board-level question	Does high digital maturity include tested offline operation, or only strong normal-state performance?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Does high digital maturity include tested offline operation, or only strong normal-state performance?

Switzerland: High-value health and life-sciences ecosystem with cross-border dependencies

Strong capability and economic attractiveness, with incident counts that reflect a broad national attack surface.

70	79	53	Elevated
Exposure	Readiness	Residual risk	Priority band

Switzerland's national cyber centre received 35,727 incident reports in the first half of 2025, with fraud dominating the total and ransomware reports increasing to 57 from 44 in the same prior-year period. These national figures are not healthcare-specific, but they show the intensity of the environment surrounding hospitals, insurers, laboratories, pharmaceutical companies and research institutions.[26]

The healthcare risk is compounded by high-value intellectual property, cross-border care, multinational suppliers and a dense life-sciences ecosystem. A compromise may seek patient information, research data, manufacturing intelligence or access through a trusted partner.

Switzerland scores comparatively well on readiness. Its remaining priority is end-to-end supplier assurance across national borders and organisational boundaries, particularly where clinical, research and manufacturing systems share identities or service providers.

Profile dimension	Black Book assessment
Dominant risk mechanism	High-value health and life-sciences ecosystem with cross-border dependencies
Most likely first clinical failure	Cross-border suppliers, research-clinical boundaries, cloud services and specialised diagnostics.
Board-level question	Can the organisation isolate a multinational supplier without interrupting specialised clinical or research services?
Priority evidence	Timed supplier isolation, 24/48/72-hour continuity, complete restore and post-outage reconciliation.

Black Book profile judgment

Can the organisation isolate a multinational supplier without interrupting specialised clinical or research services?

Black Book Insights

09

Conclusion: The Clinical Continuity Reckoning

The next phase of European healthcare cybersecurity will be decided after the attacker gets in.

The clinical continuity reckoning

European healthcare cannot prevent every intrusion, but it can decide how much care is lost after compromise

The evidence does not support naming one European nation as universally the most vulnerable. It supports a more useful conclusion: several countries occupy different front lines of the same expanding risk. Poland carries the sharpest destructive and infrastructure-dependent signal. Germany carries exceptional criminal scale. France faces the broadest convergence of criminal, public-sector and state-linked activity. The United Kingdom demonstrates how supplier concentration can convert one compromise into multi-provider clinical disruption.

Italy and Spain remain high-priority ransomware and operational markets. Belgium combines institutional concentration with account and supplier risk. Ireland continues to convert the lessons of national-scale ransomware into stronger resilience. The Netherlands and Nordic countries illustrate the digital maturity paradox: strong capability can coexist with high dependence on shared platforms. The Baltic states show why a small, highly digital system on the geopolitical front line requires both national strength and local clinical fallback.

Across every market, the operating questions are the same. Can the attacker be contained before trusted access becomes clinical propagation? Can clinicians authenticate when the normal identity plane is unavailable? Can the hospital access a recent, trustworthy patient record? Can laboratory, imaging and pharmacy continue? Can suppliers be isolated without disabling care? Can the organisation restore from trusted assets and reconcile everything that occurred during downtime?

Black Book final judgment

The next major European healthcare cyber failure will not be defined only by the sophistication of the attacker. It will be defined by the length of time the health system needs to regain clinically trusted operation.

A twelve-month board roadmap

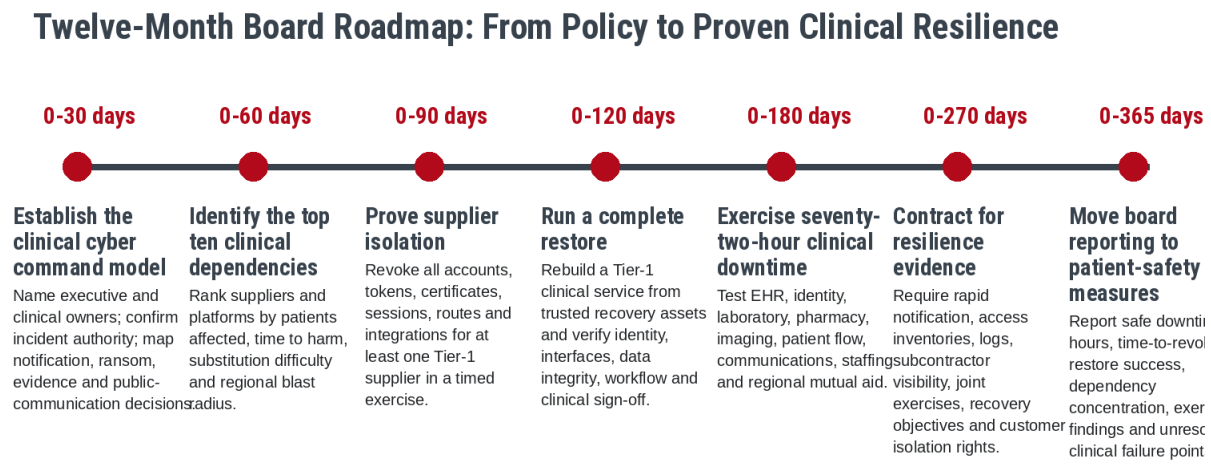

Figure 15. The sequence moves governance from named ownership to proven clinical resilience.

Source: Black Book Research board action framework.

Time horizon	Board action	Required output
0-30 days	Establish the clinical cyber command model	Name executive and clinical owners; confirm incident authority; map notification, ransom, evidence and public-communication decisions.
0-60 days	Identify the top ten clinical dependencies	Rank suppliers and platforms by patients affected, time to harm, substitution difficulty and regional blast radius.
0-90 days	Prove supplier isolation	Revoke all accounts, tokens, certificates, sessions, routes and integrations for at least one Tier-1 supplier in a timed exercise.
0-120 days	Run a complete restore	Rebuild a Tier-1 clinical service from trusted recovery assets and verify identity, interfaces, data integrity, workflow and clinical sign-off.
0-180 days	Exercise seventy-two-hour clinical downtime	Test EHR, identity, laboratory, pharmacy, imaging, patient flow, communications, staffing and regional mutual aid.
0-270 days	Contract for resilience evidence	Require rapid notification, access inventories, logs, subcontractor visibility, joint exercises, recovery objectives and customer isolation rights.
0-365 days	Move board reporting to patient-safety measures	Report safe downtime hours, time-to-revoke, restore success, dependency concentration, exercise findings and unresolved clinical failure points.

The roadmap is cumulative. A hospital should not wait until month ten to test a supplier that can interrupt pathology tomorrow. The sequencing indicates how the evidence base should mature: authority first, dependency clarity second, isolation and restore proof next, sustained downtime exercise after that, and board reporting that makes the results visible.

Recommendations for hospital and health-system leaders

Priority	Required change	Evidence due to the board
Make cyber a clinical safety discipline	Place clinical leadership inside incident command, exercise design, recovery sign-off and supplier prioritisation	Named clinical safety owner; approved risk thresholds; documented decisions from exercises.
Measure endurance, not only recovery time	Set safe-operation objectives at 24, 48 and 72 hours for EHR, identity, laboratory, imaging and pharmacy	Service-specific endurance score and unresolved failure points.
Prove the supplier kill switch	Inventory and revoke every supplier account, session, route, token, certificate and integration	Timed exercise result; residual access exceptions; corrective plan.
Restore complete clinical services	Rebuild identity, application, interface, data and user access from trusted assets	Production-equivalent restore record with technical and clinical sign-off.
Protect non-human identities	Assign owners, rotate credentials and monitor machine behaviour	Coverage and expiry metrics for service accounts, APIs, bots and certificates.
Design reconciliation before downtime	Define how paper and disconnected actions will enter the system of record	Reconciliation staffing model, priority sequence and validation controls.
Remove common-mode mutual aid assumptions	Identify suppliers, networks and platforms shared with diversion partners	Regional dependency map and alternate capacity test.
Report patient impact	Translate cyber findings into diagnostics lost, procedures deferred, safe hours remaining and patients diverted	Quarterly clinical cyber dashboard with trend and accepted risk.

Recommendations for governments, ministries and regional authorities

Hospital resilience is insufficient when essential services are nationally or regionally concentrated. Authorities should identify suppliers and platforms whose failure could affect multiple providers, including national identity, prescribing, shared records, pathology, blood, imaging, emergency communications, medical products, cloud and health-data exchange.

Government priority	Action	Strategic result
Map systemic health dependencies	Create and maintain a confidential national register of Tier-1 health suppliers, platforms and common infrastructure	Makes shared blast radius visible before an incident.
Exercise cross-sector failure	Test health, energy, telecommunications, transport, cloud and civil-protection scenarios together	Reflects the hybrid and infrastructure-dependent risk demonstrated in Poland.
Establish sector mutual aid	Define diagnostic, blood, clinical, cyber and logistics support across regions and borders	Reduces reliance on improvisation during multi-provider events.
Use the EU Cybersecurity Reserve	Pre-arrange evidence, access, contracts and decision routes for external response teams	Accelerates effective use of European emergency capacity.
Standardise clinical cyber metrics	Require safe downtime, restore proof, supplier isolation and reconciliation reporting	Enables comparable assurance across providers.
Protect smaller providers	Provide shared expertise, managed controls, exercises and recovery capability to community and specialist organisations	Prevents national strength from masking local weakness.
Coordinate public communication	Prepare messages that distinguish service availability, data impact and patient action	Maintains trust and reduces pressure on emergency services.

Recommendations for cybersecurity, cloud and health-technology suppliers

European hospital buyers are moving from feature-based procurement toward operational evidence. Suppliers will be expected to participate in the customer's continuity model, not simply protect their own environment. This changes product design, contracting and support.

Supplier requirement	What good looks like	Market differentiator
Customer-controlled isolation	All access paths can be revoked by the customer without waiting for supplier approval	Sub-hour containment with clear clinical degradation options.
Transparent dependency map	Hosting, subcontractors, remote support, APIs, models and identity paths are current and customer-visible	Blast radius is understood before change or incident.
Clinically safe degraded mode	Read-only, local, manual or alternate operation is documented and exercised	Product remains useful or safely removable during crisis.
Production-equivalent recovery proof	Full restore includes data, identity, interfaces, audit, user access and customer validation	Recovery evidence is stronger than generic availability claims.
Rapid evidence sharing	Logs, indicators, scope and access records are available immediately	Customer investigation is not delayed by commercial or legal friction.
Joint exercise participation	Supplier technical and executive teams join realistic hospital scenarios	The relationship is tested under the conditions in which it matters.
Exit and portability	Critical data, configuration and workflow information can be exported and used during incident or transition	Reduces lock-in as a source of clinical risk.

Supplier market conclusion

The European healthcare cybersecurity winner will be the supplier that can prove it contains risk without becoming the next critical dependency.

Executive statement

> *"Europe does not face one hospital cyber threat. Germany carries exceptional ransomware scale, Poland faces destructive geopolitical escalation, France confronts overlapping criminal and state-linked pressure, and the United Kingdom carries profound supplier and continuity dependencies. The common danger is that a digital incident becomes a patient-safety event before the hospital can restore identity, EPR, laboratory, imaging, pharmacy or essential supply operations."*
>
> **Douglas Brown, Founder, Black Book Research**

The market's most valuable finding is therefore not which nation reports the greatest number of attacks. It is which health systems can still deliver safe care when the attack succeeds. That is the standard against which cybersecurity investment, supplier performance and board assurance should now be judged.

Black Book Insights

10

Appendices

Country tables, KPI ballot architecture, incident chronology, threat directory, buyer checklist, methodology and sources.

Appendix A: Complete country index table

Rank	Country	Exposure	Readiness	Residual	Band
1	Poland	96	58	77	Extreme
2	Germany	92	69	71	Very high
3	France	90	70	69	Very high
4	United Kingdom	88	72	67	Very high
5	Italy	82	67	65	Very high
6	Spain	80	66	64	High
7	Lithuania	79	66	63	High
8	Belgium	78	68	62	High
9	Latvia	77	65	62	High
10	Romania	74	61	62	High
11	Ireland	76	67	61	High
12	Slovakia	72	63	60	High
13	Netherlands	79	78	59	High
14	Estonia	78	76	59	High
15	Cyprus	71	62	59	High
16	Finland	77	80	57	Elevated
17	Austria	72	70	57	Elevated
18	Portugal	65	62	56	Elevated
19	Czechia	67	68	55	Elevated
20	Greece	64	63	55	Elevated
21	Bulgaria	62	58	55	Elevated
22	Hungary	63	62	54	Elevated
23	Switzerland	70	79	53	Elevated
24	Croatia	60	63	52	Elevated
25	Norway	69	82	51	Elevated
26	Sweden	68	81	51	Elevated
27	Denmark	67	82	50	Elevated
28	Malta	55	61	49	Watch
29	Slovenia	58	70	48	Watch
30	Luxembourg	58	77	46	Watch
31	Iceland	54	82	41	Watch

Formula: Residual Clinical Cyber Risk = 65% Healthcare Cyber Exposure Index + 35% inverse Clinical Continuity Readiness Index. Scores are evidence-weighted comparative judgments based on public official evidence and Black Book research; they are not absolute breach probabilities or actuarial loss forecasts.

Appendix B: Black Book 18-KPI ballot architecture

No.	KPI domain	Measurement definition
1	Material cyber-event expectation	Expected probability of an event that materially affects confidentiality, integrity, availability, or care delivery within twelve months.
2	Ransomware and data-extortion pressure	Observed and expected exposure to encryption, exfiltration, leak-site pressure, and coercive communications.
3	State-linked and hybrid exposure	Evidence of espionage, pre-positioning, sabotage, hacktivism, or infrastructure targeting that could affect health services.
4	Supplier concentration and blast radius	Clinical dependence on a small number of EHR, pathology, cloud, identity, device, logistics, or managed-service suppliers.
5	Shared-platform dependence	Reliance on national, regional, or cross-provider platforms whose failure would affect multiple organisations.
6	Human identity resilience	Phishing-resistant authentication, rapid session revocation, break-glass access, and workforce identity assurance.
7	Non-human identity control	Inventory, ownership, rotation, and revocation of service accounts, API tokens, certificates, bots, and machine identities.
8	Internet-facing edge exposure	Visibility, patch speed, configuration assurance, and compromise detection for VPNs, firewalls, routers, gateways, and remote-management tools.
9	EHR/EPR continuity	Safe access to essential records, orders, documentation, allergies, and medication histories when the primary platform is unavailable.
10	Laboratory and pathology continuity	Specimen identification, result delivery, blood-bank operation, critical-result acknowledgement, and backlog recovery.
11	Imaging and diagnostic continuity	PACS/RIS availability, worklist integrity, acquisition, reporting, image exchange, and comparison with prior studies.
12	Medication and pharmacy continuity	Prescribing, verification, dispensing, administration, reconciliation, and allergy/interaction controls during downtime.
13	Medical device and IoMT containment	Asset visibility, network segmentation, compensating controls, safe isolation, and vendor remote-access management.
14	Validated restore capability	Recent, complete, timed restoration of Tier-1 clinical production services from trusted recovery assets.
15	24-, 48-, and 72-hour clinical endurance	Ability to sustain safe clinical operations as manual workload, backlog, fatigue, and information latency accumulate.
16	Supplier time-to-revoke	Minutes or hours required to eliminate every human and machine access path used by a compromised supplier.
17	Multidisciplinary exercise maturity	Frequency and realism of exercises involving clinical, technical, executive, legal, communications, procurement, and regional partners.
18	Board and crisis governance	Decision rights, clinical safety oversight, ransom governance, regulatory notification, evidence preservation, and executive assurance.

The 18 domains support an organisation-level assessment as well as country and regional benchmarking. For provider scoring, each domain should be supported by behaviour-based questions, documentary evidence and a recent test result. Supplier responses should be reported separately from provider scores.

Appendix C: Selected European healthcare and dependency incident chronology

Date	Country	Entity or dependency	Event type	Clinical or strategic significance
May 2021	Ireland	Health Service Executive	Ransomware following phishing	National-scale service disruption; extensive rebuilding; no ransom paid; approximately 90,000 people notified.
March 2023	Spain	Hospital Clinic Barcelona	Ransomware and data theft	Emergency, laboratory, pharmacy and elective activity disrupted; manual processes and regional coordination required.
June 2024	United Kingdom	Synnovis pathology services	Supplier ransomware	More than 11,000 outpatient and elective appointments delayed; five NHS trusts and local providers affected; incident contributed to a patient death.
2024-2025	Germany	Healthcare providers	Ransomware and availability incidents	Published European evidence linked ransomware events to postponed medical procedures and reinforced availability as a patient-safety issue.
2025	France	Hospitals, clinics and care providers	Ransomware and exfiltration	Healthcare represented 10% of incidents reported to ANSSI; data-exfiltration pressure increased across sectors.
2025	Italy	Healthcare organisations	Ransomware, compromise and supply-chain effects	Health-sector events increased in the first nine months; one prior supplier event demonstrated how a single upstream compromise can create many downstream incidents.
December 2025	Poland	Energy and industrial infrastructure	Destructive sabotage	More than 30 renewable facilities and a CHP plant were targeted; attackers attempted firmware damage, deletion and wiper deployment.
2025	Estonia	Family medicine centre	Ransomware	Patient records, appointments and backups were affected; weak account closure and privilege practices amplified the impact.
2025-2026	Lithuania	Healthcare group	Encryption, ransom demand and access-control failures	Regulator imposed a substantial fine following investigations into security controls and healthcare data breaches.
March 2026	United Kingdom / Europe	Stryker Medical	Supplier network disruption	Production, shipping, distribution and ordering were affected, demonstrating that a cyber event can interrupt physical medical supply without compromising hospital networks.
July 2026	Multiple EU states	Government and critical infrastructure	State-linked campaigns and enabling ecosystem	The EU named targeted member states, identified FSB Centre 16 activity and sanctioned actors enabling ransomware, phishing and critical-infrastructure attacks.

The chronology is selective and evidence-led. It is designed to show recurring failure mechanisms - supplier contagion, national shared-service disruption, destructive infrastructure targeting, ransomware and identity weakness - rather than to catalogue every publicly reported incident.

Appendix D: Threat actor and enabling-ecosystem directory

Actor or ecosystem	Category	Observed operating model	Healthcare relevance	Current evidence note
FSB Centre 16 / Turla ecosystem	Russian state-linked	Long-term espionage, strategic network access, infrastructure targeting and sabotage support.	EU institutions, national government, defence, telecommunications and critical infrastructure; healthcare risk is direct or dependency-based.	Current EU attribution and sanctions context.
Static Tundra / Berserk Bear / Ghost Blizzard / Dragonfly cluster	State-linked activity cluster	Long-term infiltration, privileged access, industrial-device targeting and destructive execution.	Polish energy infrastructure; relevant to hospitals through power, heating and telecommunications dependency.	CERT Polska found strong infrastructure overlap in the December 2025 incidents.
APT28 / GRU-linked router operations	Russian military intelligence-linked	Compromise of vulnerable routers and DNS/network infrastructure to support espionage and follow-on operations.	Government, defence, logistics and critical sectors; hospital edge devices and third-party networks are exposed.	Allied advisories stress configuration, patching and monitoring of network edge devices.
UNC1151 / Ghostwriter	State-aligned information and credential-theft activity	Phishing, account compromise and influence-supporting operations.	Polish public officials, organisations and email users; healthcare leaders remain susceptible to credential campaigns.	Campaign methods continue to evolve across mail platforms.
Z-Pentest and affiliated pro-Russia hacktivist activity	Hacktivist / state-aligned	Critical-infrastructure probing, disruption claims and attacks against energy and water sectors.	Public services and infrastructure on which hospitals depend.	Sanctioned by the Council of the EU in July 2026.
Bulletproof-hosting and malware-enablement ecosystem	Criminal infrastructure	Hosting, proxying and infrastructure that supports malware, phishing, credential theft and ransomware.	Enables attacks against critical infrastructure and essential services across Europe.	Media Land LLC and ML.Cloud were sanctioned by the EU in July 2026.
Ransomware-as-a-service affiliates	Financially motivated criminal	Initial access, privilege escalation, exfiltration, encryption, leak-site pressure and negotiation.	Hospitals, suppliers, diagnostics, managed services, municipalities and smaller providers.	Group names change rapidly; defensive planning should focus on the repeatable operating model.
Initial-access brokers and infostealer operators	Financially motivated criminal	Sale of credentials, sessions, VPN access and cloud tokens to downstream extortion actors.	Healthcare workforce identities, contractors, service accounts and browser sessions.	The brokered-access model reduces the time between credential theft and enterprise compromise.
DDoS hacktivist collectives	Ideological / geopolitical	High-volume denial-of-service and public claims designed to disrupt or signal political support.	Public-facing health portals, appointment sites, government health services and communications.	Most incidents are low impact, but timing and coordination can magnify operational pressure.

Actor names and aliases change, and attribution may remain uncertain. The directory prioritises operating models and officially described activity. It should not be used as a substitute for current threat intelligence, indicators of compromise or national authority guidance.

Appendix E: Tier-1 supplier procurement and renewal checklist

No.	Control area	Buyer evidence question	Verified
1	Criticality	Has the supplier been tiered by patients affected, time to harm, substitution difficulty and shared blast radius?	□
2	Access inventory	Are all users, service accounts, API tokens, certificates, endpoints, remote tools and network paths documented?	□
3	Customer kill switch	Can the provider revoke all supplier access immediately and independently?	□
4	Notification	Does the contract require rapid vulnerability and incident notification with defined severity thresholds?	□
5	Logging	Can the supplier provide complete, time-synchronised customer logs and indicators without delay?	□
6	Recovery evidence	Has a full production-equivalent restore been completed within the contracted objectives?	□
7	Clinical degraded mode	Is there a safe read-only, local, manual or substitute workflow when the service is unavailable?	□
8	Subcontractors	Are hosting, support, model, data and infrastructure subcontractors disclosed and controlled?	□
9	Exercise	Has the supplier participated in a joint containment and continuity exercise during the contract period?	□
10	Portability	Can critical data, configuration and audit history be exported in a usable form during incident or exit?	□
11	Insurance and liability	Are cyber insurance, liability allocation and recovery obligations aligned to clinical consequence?	□
12	Termination	Are all credentials, data, integrations and remote access removed and verified at contract end?	□

Appendix F: Core survey instrument

Domain	Survey question
Exposure	How likely is a material cyber event to affect your organisation in the next twelve months?
Exposure	Which event is most likely: ransomware, exfiltration, identity compromise, supplier compromise, destructive attack, DDoS or accidental supplier outage?
Dependency	Which external dependency would produce the largest clinical impact if unavailable?
Dependency	What share of essential clinical services depends on the top five suppliers or shared platforms?
Identity	Can emergency clinical access be issued when directory, SSO or MFA services are unavailable?
Identity	How long would it take to revoke all human and machine access used by the most critical supplier?
EHR/EPR	For how long can the organisation maintain safe care without the core record?
Diagnostics	Can laboratory, blood, imaging and pathology continue with verified patient matching?
Medication	Can prescribing, verification, dispensing and administration operate safely for seventy-two hours?
Restore	When was the last complete production restore of a Tier-1 clinical service?
Exercise	When was the last multidisciplinary clinical downtime exercise, and how long did it run?
Reconciliation	How long would it take to reconcile paper and disconnected activity after restoration?
Regional	Would neighbouring providers remain available if they share the same supplier or platform?
Governance	Who can isolate a supplier, accept clinical risk, engage authorities and decide ransom policy?
Board	Does the board receive cyber metrics expressed in clinical capacity and safe downtime?

Appendix G: Methodological limitations and interpretation controls

- National disclosure rules and incident definitions differ.
- Larger economies contain more potential targets and generally produce more public reporting.
- Ransomware leak-site claims are not equivalent to verified breaches.
- Strong reporting can increase apparent exposure; underreporting can reduce it.
- Official national evidence is not always healthcare-specific.
- Country readiness scores reflect comparative evidence and cannot represent every provider.
- Black Book survey panels measure informed respondent experience and expectations, not every European healthcare organisation.
- State attribution can evolve as new technical and intelligence evidence becomes available.
- One severe incident can materially change a small country's score or a specific supplier's risk.
- The index should be refreshed when material incidents, official reports or national policy changes occur.

Interpretive safeguard

Country scores are most reliable as risk bands and explanatory profiles. They should not be used to infer that every organisation within one country is stronger or weaker than every organisation in another.

Appendix H: Source notes

[1] ENISA. ENISA Threat Landscape 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[2] ENISA. EU consistently targeted by diverse yet convergent threat groups. https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups

[3] European Commission. Cybersecurity of hospitals and healthcare providers. https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_en

[4] European Commission. NIS2 Directive policy overview. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[5] European Commission. EU Cyber Solidarity Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

[6] European Commission. ENISA to operate the EU Cybersecurity Reserve. https://digital-strategy.ec.europa.eu/en/news/enisa-operate-eu-cybersecurity-reserve

[7] Council of the European Union. EU statement denouncing Russia's malicious cyber ecosystem. https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/

[8] Council of the European Union. Council sanctions nine individuals and four entities. https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/russian-cyber-attacks-and-destabilising-activities-council-sanctions-nine-individuals-and-four-entities/

[9] CERT Polska. Energy Sector Incident Report - 29 December 2025. https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[10] UK National Cyber Security Centre. Critical sectors urged to improve defences against Russian intelligence targeting. https://www.ncsc.gov.uk/news/uk-and-allies-urge-critical-sectors-to-improve-defences-against-russian-intelligence-targeting

[11] ANSSI. Panorama de la cybermenace 2025. https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025/

[12] CERT-FR. Cyber Threat Overview 2025. https://cert.ssi.gouv.fr/cti/CERTFR-2026-CTI-003/

[13] NHS England. Synnovis cyber incident. https://www.england.nhs.uk/synnovis-cyber-incident/

[14] UK Parliament. Written ministerial statement on the Synnovis ransomware attack. https://questions-statements.parliament.uk/written-statements/detail/2025-11-13/hlws1054

[15] NHS England. Emergency Preparedness, Resilience and Response annual report and assurance update. https://www.england.nhs.uk/long-read/emergency-preparedness-resilience-and-response-eprr-annual-report-and-assurance-update/

[16] NHS England. Stryker Medical cyber-attack and supply disruption. https://www.england.nhs.uk/long-read/stryker-medical-cyber-attack-disruption-supply-medical-equipment-consumables/

[17] NHS England. Board and executive assurance: cyber security risk. https://www.england.nhs.uk/long-read/board-and-executive-assurance-cyber-security-risk/

[18] INCIBE. INCIBE detected more than 122,000 cybersecurity incidents in 2025. https://www.incibe.es/incibe/sala-de-prensa/incibe-detecto-mas-de-122000-incidentes-de-ciberseguridad-en-2025

[19] Government of Catalonia. Cyberattack on Hospital Clinic affects normal care activity. https://govern.cat/salapremsa/notes-premsa/488382/ciberatac-al-clinic-afecta-seva-activitat-assistencial-habitual

[20] Netherlands NCSC. Ransomware Yearbook 2025. https://www.ncsc.nl/nieuws/jaarbeeld-ransomware-2025

[21] Ireland NCSC. National Cyber Risk Assessment 2025. https://www.ncsc.gov.ie/ncra/

[22] Health Service Executive Ireland. HSE cyberattack: what happened. https://www2.hse.ie/services/cyber-attack/what-happened/

[23] Oireachtas. HSE cyber remediation cost and dedicated cyber funding. https://www.oireachtas.ie/en/debates/question/2025-03-27/381/

[24] Belgium Centre for Cybersecurity. The cyber reality in Belgium 2025. https://ccb.belgium.be/nl/news/meer-aanvallen-meer-meldingen-de-cyberrealiteit-belgie-2025

[25] Belgium Centre for Cybersecurity. Belgium adopts new national cyber crisis response plan. https://ccb.belgium.be/news/belgium-adopts-new-national-cyber-crisis-response-plan

[26] Switzerland NCSC. Semiannual report 2025/1. https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2025-1.html

[27] Estonia Information System Authority. Cyber security in Estonia: new records, old mistakes. https://www.ria.ee/en/news/cyber-security-estonia-new-records-old-mistakes

[28] Estonia Information System Authority. Ransomware: new attacks, familiar mistakes. https://www.ria.ee/en/ransomware-new-attacks-familiar-mistakes

[29] Lithuanian State Data Protection Inspectorate. Company fined for personal data breaches. https://vdai.lrv.lt/en/news/company-fined-for-personal-data-breaches-hJA/

[30] Finland National Cyber Security Centre. Cybersecurity year 2025. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuden-vuosi-2025-uhkataso-pysyi-kohonneena-vakavien-tapausten-maarat-korkealla-tasolla

[31] Norwegian National Security Authority. Risk 2026. https://nsm.no/aktuelt/risiko-2026

[32] Black Book Research. Europe's hospital cyber risk has moved from data theft to care disruption. https://www.accessnewswire.com/newsroom/en/healthcare-and-pharmaceutical/europes-hospital-cyber-risk-has-moved-from-data-theft-to-care-disrupt-1167612

[33] Black Book Research. Europe's hospitals cannot cut off hacked vendors fast enough. https://www.accessnewswire.com/newsroom/en/healthcare-and-pharmaceutical/europes-hospitals-cant-cut-off-hacked-vendors-fast-enough-new-cyber-r-1114998

[34] ENISA. Procurement guidelines for the cybersecurity of hospitals and healthcare providers. https://www.enisa.europa.eu/publications/procurement-guidelines-for-the-cybersecurity-of-hospitals-and-healthcare-providers

Source review current through 1 August 2026. Black Book Research sources [32] and [33] contain the European survey baselines used in this report.

About Black Book Research

Black Book Research provides independent healthcare technology, services and market intelligence for provider, payer, government, investor and supplier decision-makers. Its research programmes use validated user and executive input, qualitative performance indicators and market-specific evidence to evaluate technology performance, operational readiness and buyer priorities.

Black Book's healthcare cybersecurity work focuses on the connection between cyber controls and clinical operations: identity, supplier concentration, downtime, restore, medical technology, board governance and the ability to sustain safe care under degraded conditions. The firm maintains vendor-agnostic research standards and separates provider evidence from supplier perspective.

Report attribute	Publication information
Title	Europe Hospital Cyber Exposure & Clinical Continuity Index 2026
Edition	August 2026
Geographic scope	Europe excluding Ukraine; includes the United Kingdom, Switzerland, Norway and Iceland.
Primary audience	Hospital boards, ministries, health-system executives, CIOs, CISOs, clinical leaders, risk officers, procurement teams, insurers and technology suppliers.
Research position	Independent, vendor-agnostic healthcare cybersecurity market intelligence.
Website	www.blackbookmarketresearch.com
Research contact	research@blackbookmarketresearch.com

Publication statement

This report is designed to help European healthcare leaders convert cyber exposure into measurable clinical continuity priorities, investment decisions and procurement evidence.

Black Book Insights

BLACK BOOK RESEARCH

Clinical continuity is the new cybersecurity benchmark.

The defining question is not whether a hospital will be attacked. It is whether the hospital can continue delivering safe care when the attack succeeds.

Independent healthcare cybersecurity intelligence for boards and buyers who need proof that care can continue after compromise.

BBR

Black Book Research
August 2026