

CYBER SECURITY RESILIENCE IN HEALTHCARE

THREAT READY



A blurred person in a blue shirt is working in a server room. The background shows rows of server racks with glowing lights and cables. The image has a dark, blue-toned aesthetic with some teal geometric shapes on the right side.

In the modern health and medical ecosystem, cybersecurity is no longer just a technical concern. It is a critical business risk. For hospitals, medical device and equipment manufacturers, and healthcare technology providers, the stakes are especially high. A single breach can result in the loss of patient data, damage to organizational reputation, and disruption to essential care.

With cyber threats growing in scale and sophistication, healthcare institutions must take a proactive, risk-based approach to cybersecurity. From identifying vulnerabilities and meeting regulatory requirements to responding quickly to incidents and strengthening resilience, cybersecurity should be embedded across operations and governance. mitigating cyber risk and combating threats in the always evolving cyber landscape.

HOW WE PARTNER WITH YOU, WHEREVER YOU ARE ON YOUR CYBER MATURITY JOURNEY



Don't assume you can stop attacks – validate your security controls across your attack surface

CYBER RISK MANAGEMENT

The challenges organizations like yours can face

- High-value targets for cybercrime and nation-state actors
- Complex, distributed IT environments
- Verifying the effectiveness of the organization's cybersecurity posture
- Preventing and withstanding a cyber attack against credible threat actors
- Complying with regulatory framework requirement
- Benchmarking cybersecurity controls against HIPAA, HITRUST CSF, NIST CSF, PCI DSS, ISO 27001
- Complying with requirements from the organization's customers or supply chain
- Identifying the weaknesses in the organization's infrastructure, networks, apps, people and processes
- Having a plan of action for vulnerability and incident remediation

LRQA solutions

- Penetration Testing
- Red / Purple Teaming
- IoT Medical Device Testing
- Third Party Risk Management
- Compliance Benchmarking (ISO, HIPAA, NIST, Etc.)
- PCI DSS Consultancy and Assessments
- CMMC Advisory Services
- Ransomware Readiness & Response
- Regulated Testing (HIPAA)
- Cloud Security Assessments
- Pen Testing-as-a-Service (PTaaS)
- Managed Security Services
- Supply Chain Security
- AI Security Testing
- Virtual CISO

LRQA supports the healthcare industry with embedding cyber risk management at every level, from executive reporting to board-level cyber risk committees. By integrating proactive cybersecurity with clear oversight, institutions can reduce risk exposure, protect patient data and strengthen market and stakeholder trust.



RED TEAMING

Expose the gaps, test the response, build the resilience

For the healthcare industry, red teaming isn't about ticking a box, it's about building resilience against adversaries already targeting you. We help you find the cracks before someone else does by focusing on seven key areas:

- 1 Realistic threat simulation
- 2 End-to-end risk exposure
- 3 Defensive layers test
- 4 Strategic risk insight for boards and executives
- 5 Crisis simulation and response hardening
- 6 Regulatory readiness
- 7 Elevating security culture

PROCESS

Our tried and tested approach

Using our experience to partner with you to deliver a successful



OUR TESTING EXPERIENCE

50+

regulatory assessments delivered

300+

systems listed in scope of completed assessments

150+

scenarios designed and tested

Multiple

engagements testing regional differences and interactions between SOCs globally

PENETRATION TESTING

Designed to uncover what matters most, first

At LRQA, we view penetration testing as more than just a checkbox exercise – it's about finding out how real your risks are, how attackers can move through your environment and what you can do about it before they do.

- ✓ Penetration testing uncovers real, exploitable weaknesses in your systems, applications and infrastructure. It's not just theoretical – it shows how attackers can chain those issues together to reach something valuable
- ✓ We don't just give you CVEs and severity scores. We show how those vulnerabilities could lead to patient data exposure, ransomware or operational disruption – putting risk into a business context your stakeholders can act on
- ✓ A good penetration test filters the noise. It tells you not just what's vulnerable, but what's exploitable and how deep the issue goes. That helps you focus your remediation efforts where they'll have the biggest impact
- ✓ Whether it's PCI-DSS, ISO 27001, or internal governance requirements, regular penetration testing helps demonstrate that you're not just compliant – you're secure by design
- ✓ Build a Culture of Continuous Assurance by feeding findings into a larger cycle of hardening, testing and improving. Done right, it becomes a core part of your offensive security strategy – not just an annual task.

PROCESS

Our tried and tested approach

Using our experience to partner with you to deliver a successful engagement

- Kick-off
- Recon/Enumeration
- Vulnerability analysis
- Exploitation
- Post exploitation
- Reporting
- Debrief



WHY LRQA?

We understand that every organization has slightly different requirements in how they manage their security testing program. Our experience shows that these are often large-scale programs involving high volumes of processes and project management. A key challenge is managing the output effectively so it can be used to reduce risk through timely remediation.

Our expertise can help with this and reduce the mean time to remediate (MTTR), by providing a platform that allows your organization to gain:

- ✓ A single view of vulnerabilities across an organization's estate
- ✓ Holistic analysis to make decisions
- ✓ Data visualization
- ✓ Real time collaboration with consultants and program team
- ✓ Access to findings and remediation advice
- ✓ Reduced scheduling time
- ✓ Continuous penetration testing

More importantly, we understand the nuances of your operations. We can operate in more traditional project management methods and offer integrations to commonly known and unique ticketing systems too.

WHAT MAKES LRQA UNIQUE?

- **Dedicated research and innovation team** focused on developing and exploring ideas that add value to our capabilities. Including core tooling, honey traps, zero-day exploits, blockchain and SOC maturity
- **Strong portfolio** of professional and managed services adaptable to customer needs
- The only organization in the world with a **full suite of CREST accreditations**
- Through the use of proprietary tooling we're able to automate parts of our testing to allow our security professionals to focus on more obscure threats
- We find zero-day vulnerabilities in mainstream applications and systems, all of which are awarded unique CVE numbers
- LRQA is certified by a range of governing bodies for work in the healthcare sector and payment card industry. We're approved as a Qualified Security Assessor (QSA), PCI 3DS, PCI ASV and have consultants who are ISO 27001 lead auditors
- We are an accredited supplier of CBEST, GBEST/GCASE, CAA ASSURE and other xBEST assurance services as an approved CREST STAR testing services provider
- ISO 27001 (Information Security), ISO 9001 (Quality), ISO 14001 (Environmental) and PCI DSS underpin our rigorous quality practices and procedures



500+
clients globally

100+
Penetration Testers and Red
Team consultants on staff

50+
Regulatory driven
tests completed

4,500
Penetration tests
conducted

“LRQA are always on hand to offer a solution and work with us as we encounter internal challenges. They also provide experience and technical expertise in everything they do for us.”

ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit [LRQA.com](https://www.lrqa.com) for more information or email cybersolutions@lrqa.com



LRQA
810 Seventh Avenue
Suite 1110
New York 10019

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management
Advantage