



THE SLEEPING GIANT

HOW MEDICAL DEVICE RISKS THREATEN PATIENT SAFETY AND SECURITY

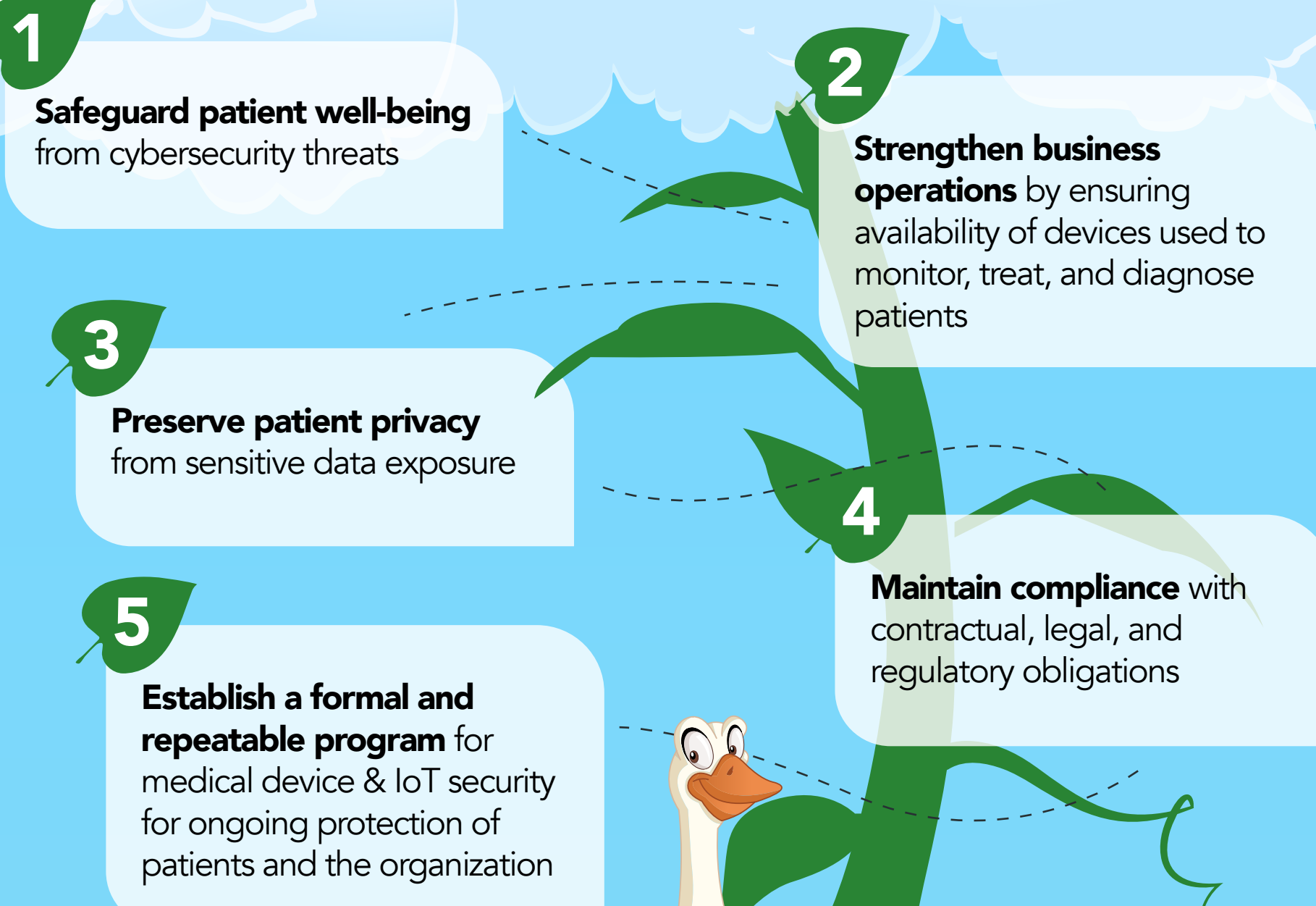
Improperly secured medical devices present a quiet but giant threat to patient safety and security.

The colossal risks associated with medical device security loom large over healthcare organizations as they struggle to identify legacy medical and IoT devices, prioritize risks, and coordinate vendors and internal stakeholders for remediation of known vulnerabilities.

CORL has experience collaborating with the nation's leading health systems, standards bodies, and medical device manufacturers to drive measurable risk reduction for medical devices.

Follow our guidance to avoid waking this sleeping giant.

Objectives for Medical Device VRM Programs

- 
- Safeguard patient well-being** from cybersecurity threats
 - Strengthen business operations** by ensuring availability of devices used to monitor, treat, and diagnose patients
 - Preserve patient privacy** from sensitive data exposure
 - Maintain compliance** with contractual, legal, and regulatory obligations
 - Establish a formal and repeatable program** for medical device & IoT security for ongoing protection of patients and the organization

Medical Device Vendor Risk Program Strategy

- Create medical device security-specific risk assessment models and questionnaires
- Define and document a medical device security program strategy and associated procedures
- Align with industry standards including UL-2900, MDS2, AAMI / ANSI, NIST, MDISS, NCCOE, and H-ISAC
- Monitor federal guidance and regulations updates, including recent White House executive orders on supply chain risks

Medical Device Vendor Risk Assessment Approaches

- **Conduct medical device inventory and risk assessments** on a routine basis for both new and legacy devices
- **Conduct targeted assessments** of medical device manufacturers, as well as the specific devices and products in scope for your organization
- **Assess risks** associated with the specific implementation of devices on your network rather than evaluating the device in a vacuum
- **Include the assessment of middleware** including servers, network devices, and workstations in scope for medical device risk assessments
- **Conduct penetration testing** of medical devices in a safe and offline manner to identify potential security exposures

Remediation & Risk Mitigation

- **Assign project management resources** to assist with coordination of patching and upgrades to vulnerable devices
- **Incorporate medical device breaches and outages** into your disaster recovery planning and testing initiatives
- **Invest in compensating controls** including network segmentation to protect vulnerable legacy medical devices
- **Consider engaging third-party managed services support** to conduct medical device assessments and coordinate remediation and patching with device manufacturers

CORL's Medical Device Risk Assessment Toolkit

CORL is committed to driving and delivering measurable risk reduction introduced by third-party vendors, including medical device manufacturers.

CORL's Medical Device Risk Assessment Toolkit incorporates CORL's experience collaborating with the nation's leading health systems, standards bodies, and medical device manufacturers.

CORL's medical device assessment model and technology includes the assessment of devices and products across a range of security domains including:



Governance and Risk Management



Network and Services



Physical Security



Authentication



Secure Development Lifecycle

The new toolkit has been deployed and is available for immediate use for all CORL customers and subscribers. CORL also delivers medical device security remediation managed services for many of the nation's leading healthcare organizations.

Contact our team here at CORL to learn more about how we can support your medical device vendor risk management program.

[Contact our team](#)

CORL is a leading provider of tech-enabled managed services for risk management and compliance for healthcare organizations. CORL's solution gets results by scaling organizational and vendor risk programs through our healthcare vendor clearinghouse, dashboard reporting that business owners can understand, and proven workflows that drive the organization to measurable risk reduction.