Whitepaper

Securing the Internet of Healthcare Things

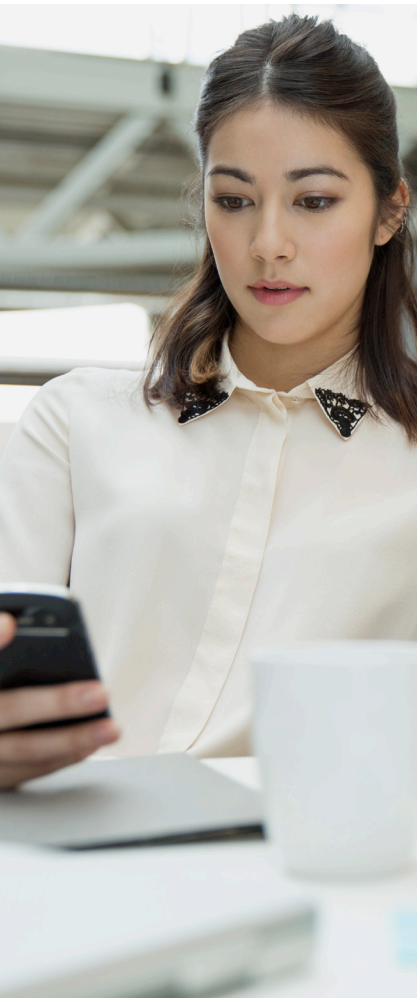
How to Safeguard Patients and their Data Against the Growing Threats

BlackBerry Cybersecurity Consulting

The Internet of Things (IoT) is emerging as one of the most significant developments of our era. This growing network of physical devices, vehicles and other items with Internet connectivity can collect and exchange rich data.

The IoT is transforming how organizations of all sizes, in almost all industries, operate: in short, the Enterprise of Things (EoT) has arrived. Gartner forecasts that more than 20 billion connected things will be in use worldwide by 2020.[1] KPMG says the projected value of IoT technology will be up to $6.2 trillion by 2025, while the McKinsey Global Institute predicts the IoT's total potential economic impact could reach $11.1 trillion by 2025.[2, 3]

The EoT holds great promise, but it also exponentially accelerates the vulnerability of organizations to data breaches and cybersecurity threats. Connected devices can be a competitive edge for organizations (supporting innovation, new use cases and more efficient workflows) or a liability (introducing vulnerability to hacks and data breaches). For healthcare organizations to realize the full potential of the EoT, they must be able to confidentially and reliably transmit highly sensitive data between connected devices.



The current threat landscape for the EoT

Many organizations are not even aware of all the connected devices in their environment, and bad actors are increasingly targeting this security vulnerability. The growing number of Distributed Denial of Service (DDoS) attacks launched using IoT devices, for example, points to the need to improve device security. In 2016, several massive DDoS attacks delivered by botnets made up of hijacked IoT devices caused major disruptions at various organizations and events (including the Rio Olympics).[4, 5]

Network World magazine predicts that new network security challenges will push security experts to their limits in 2018.[6] But it is not just private organizations reacting to the growing number of IoT cybersecurity incidents; the U.S. government recently introduced legislation to force vendors to ensure basic security within IoT devices sold to the government market.[7]

The challenge for organizations

The IoT allows billions of smart devices to communicate and share data, and millions of new devices are connected to the Internet every day.[8] This creates a complex challenge for organizations: determining who governs permission to see and use all this data.

The state of IoT cybersecurity remains fragmented. Even where IoT security standards are emerging, they might not always keep pace with the expanding variety of IoT devices and applications.

Organizations may lack clear knowledge of where data from IoT devices resides, where it flows and how to control it. This wide dispersion of data creates a broad attack surface for cybercriminals.

Considering all these factors, robust data security is critical within any environment where IoT devices and applications operate.

Security for the IoT era

There are three main components of information security, which are captured in the CIA Triad.[9]

Confidentiality: limits access to the information in IoT devices
Integrity: ensures that information in IoT devices is trustworthy and accurate
Availability: guarantees reliable access to the information in IoT devices by authorized people

Healthcare organizations have proven to be eminently capable of ensuring the integrity and availability of information within their connected devices. Yet as cybersecurity threats intensify, ensuring confidentiality has become increasingly difficult. To strengthen this third point in the triad, healthcare organizations can partner with outside cybersecurity experts.

In the IoT era, there is a need for security solutions that protect the confidentiality of data in IoT devices, no matter where the data originates or where it travels. To reduce the risk of data breaches in the healthcare industry, data should be protected both at the device level and the hospital network level.

The Internet of Healthcare Things

The market for IoT devices in healthcare is growing rapidly, fueled by factors that include:

- Technological advancements
- Growing demand for cost-effective treatment and disease management
- Better accessibility of high-speed internet
- Collaboration of top IT companies with healthcare organizations
- Decreased price of sensor technology

Currently, 60% of healthcare organizations have introduced the IoT into their infrastructure, and by 2019, 87% will have, according to a report in the HIPAA Journal.[10] A report by Allied Market Research on the IoT healthcare market found it was worth $60 billion in 2014 and is estimated to reach a net worth of $136 billion by 2021.[11] McKinsey Global Institute makes an even bolder prediction: by 2025 healthcare will comprise nearly one-third of the $11.1 trillion market for distributed devices, second only to manufacturing.[12]

Hospitals in the U.S. now have an average of 10 to 15 connected devices per bed, according to a study reported on Wired.[13] These devices have the potential to improve patient care, fuel innovative medical research and enhance healthcare system efficiency. At the same time, however, the cybersecurity risks are real and growing.

The benefits of IoT devices in healthcare

The following are just some of the myriad applications of IoT devices in healthcare:

- Patient monitoring and communication
- Patient drug supply (infusion pumps)
- Electronic health implants
- Hospital and building management
- Patient engagement
- Data collection

This last benefit is one of the main drivers of IoT devices in healthcare organizations. Compared to traditional paper-based methods, connected devices deliver better healthcare data, faster. They gather a vast amount of critical data that is valuable not only to patients and healthcare professionals, but to hackers.

The risks of IoT devices in healthcare

Connected devices in healthcare are appealing targets for hackers for multiple reasons:

- Healthcare organizations have many devices connected to their network and there can be gaps in their security
- Hospital security systems can overlook personal IoT devices brought in and out by patients, families and staff
- IoT devices for healthcare contain valuable Personally Identifiable Information (PII) and Personal Health Information (PHI), which can be exploited for profit

In a survey published by HIPAA Journal, 89% of healthcare executives said they have suffered a security breach resulting from adopting IoT, while 49% said malware is an issue.[14] One recent study sponsored by several major universities found poor information security practices among doctors, nurses and hospital IT staff, while another report published in Threat Post found many hospitals are failing to protect critical computer systems that can be manipulated by hackers.[15, 16]

Healthcare organizations confront a unique challenge when it comes to information security. They are "systems of systems" with huge arrays of connected devices, including those that are sanctioned (purchased for patient care) and unsanctioned (personal devices with varying levels of security). This situation creates multiple entry points to the network, making central management difficult and creating a wide attack surface for cybercriminals.

The growing threats and the potential repercussions

Managing IoT security may be a challenge and a headache in other industries, but in healthcare the stakes are far higher: security vulnerabilities could potentially affect people's safety, and even have life-and-death implications. Though there is currently no proof that a patient has suffered direct harm because of a hacked medical device, the possibility of a hijacked infusion pump, pacemaker or other critical device exists.

Students at the University of Alabama showed they could hack the pacemaker in a robotic dummy patient and theoretically kill it, according to Wired magazine.[17] The FDA has issued multiple security alerts about cybersecurity vulnerabilities in medical devices, including infusion pumps and implantable cardiac devices.[18]

By October 2016, 14 hospitals reported ransomware attacks that used medical devices as a gateway.[19] While a hospital's network may not control a medical device's safety functions, any cybersecurity threat to the network will cause outages, which have multiple negative effects, including delayed patient care and increased resource needs.

Beyond the potential immediate risk to patients, connected devices can also be hacked to steal valuable data. According to a NetDiligence Cyber Claim Study, up to 80% of damages from cyberattacks involve breaches of privacy-related information (Personally Identifiable Information 41%, personal health information 21% and payment card information 19%).[20] Some healthcare organizations may hold Personally Identifiable Information (PII) covered by the European Union's new General Data Protection Regulation (GDPR), set to come into effect in May 2018, and could face massive fines for any data breach involving PII.[21]

The growing threats outlined above are shaping public opinion about data protection and influencing the regulatory climate in several ways:

- The GDPR model of data protection is expected to influence other jurisdictions worldwide, resulting in greater financial penalties for data breaches
- Awareness of the growing number of cyberattacks is causing consumers to exert pressure on lawmakers for stricter regulations
- Organizations are increasingly facing liability claims when they report a data breach

Apart from the direct financial losses that organizations could face because of data breaches, there are significant indirect losses from reputational and brand damage. While all healthcare organizations have security measures in place, these systems are only useful if they cannot be compromised by cybersecurity threats. Determining the vulnerability of existing safeguards often requires the expertise of cybersecurity professionals, who are trained to think like hackers.

Policies and regulations for the Internet of Healthcare Things

The Health Insurance Portability and Accountability Act (HIPAA) covers data privacy and security provisions for safeguarding health information, but does not specifically govern IoT devices.

The U.S. Food and Drug Administration (FDA) works closely with the U.S. Department of Homeland Security (DHS), private sector organizations, medical device manufacturers, health care delivery organizations, security researchers and end users to improve the cybersecurity of medical devices.

10 ways healthcare organizations can protect themselves against the influx of insecure IoT devices

All forecasts point to major growth for the Internet of Healthcare Things in the coming years, which will create even more opportunities for cybercriminals. Healthcare organizations must take concrete steps now to protect patients, data and the healthcare system.

BlackBerry® has the experience,expertise and tools to mitigate the risk of cybersecurity attacks and data breaches. The BlackBerry Cybersecurity offerings leverage extensive research and development in two key domains:

- Security consulting practice (BlackBerry Cybersecurity Consulting)
- Security software

Together, BlackBerry Cybersecurity Consulting and software provide a complete solution to help defend the growing number of connected things within organizations against data breaches. BlackBerry Cybersecurity offerings can ensure the confidentiality and integrity of data, wherever it resides.

BlackBerry Cybersecurity Consulting partners with organizations to:

1. Adopt a risk-based approach to secure system design
2. Conduct security testing
3. Create a robust incident response strategy
4. Heighten security awareness across the organization through training programs

BlackBerry software enables organizations to:

5. Take inventory of devices and get a single view through unified endpoint management (BlackBerry® UEM)
6. Ensure complete visibility and control of data across the IoT chain (BlackBerry® Workspaces)
7. Authenticate all network users and allow single sign-on (BlackBerry® 2FA and BlackBerry® Enterprise Identity)
8. Develop custom mobile apps and workflows while protecting sensitive information (BlackBerry® Dynamics)
9. Enable secure collaboration involving personal data (BlackBerry® Work)
10. Balance security and productivity (all BlackBerry enterprise software)

BlackBerry — A global leader in security

Many of the world's most security-conscious organizations, as well as national government agencies, rely on BlackBerry products and services to secure their mission-critical operations. Built on more than two decades of security research and development, **BlackBerry® Cybersecurity Consulting** has the in-depth knowledge and investigative experience to help organizations identify and mitigate today's increasingly sophisticated threats, including the new and growing threats to IoT devices.

BlackBerry Secure

Our integrated security solution helps companies manage and secure their desktops, laptops, mobile devices and connected things in a manner that secures communications for all messaging and file types. BlackBerry Secure is a comprehensive approach to security that addresses the entire enterprise from endpoint to endpoint. Being BlackBerry Secure means enterprise-wide solutions that are informed by deep security expertise and experience, continuous technical innovation, industry partnerships and academic collaborations, on-demand cybersecurity expert services and a point of view that recognizes vulnerability wherever it lies.

External recognition for BlackBerry as a security leader

- BlackBerry is the only vendor to have achieved the highest score in 6 of 6 use cases of the Gartner Critical Capabilities for High-Security Mobility Management[22]
- BlackBerry was a leader in the 2017 Gartner Magic Quadrant for EMM[23]
- BlackBerry Workspaces achieved 2 of the 5 highest scores in Workforce Productivity and Centralized Content Protection in the Gartner Critical Capabilities for Content Collaboration Platforms[24]
- BlackBerry ranks in the top 10% of all global cybersecurity organizations in the Cybersecurity 500 ranking published by Cybersecurity Ventures[25]
- BlackBerry has 80+ Security Certificates, more than any other mobile vendor
- BlackBerry has thousands of security-related patents
- BlackBerry is deployed with all 7 of the G7 governments and 15 of the G20 governments

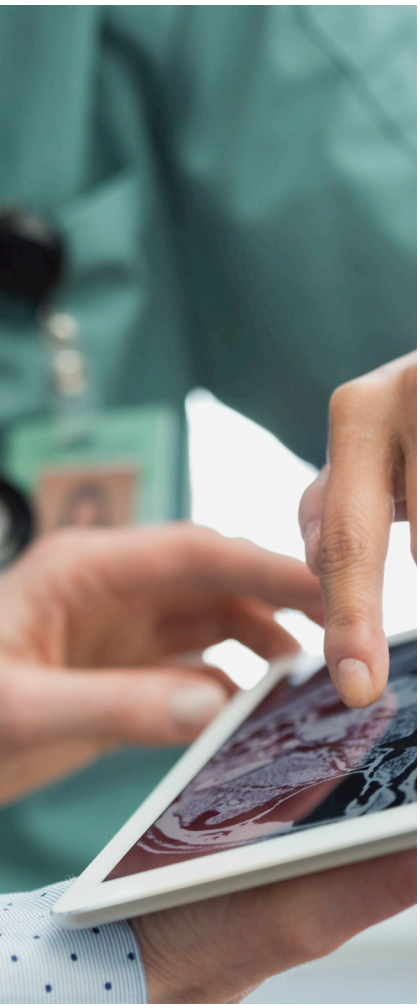
BlackBerry Core IoT Platform

The BlackBerry® IoT Platform is a trusted foundation for the Internet of Things, providing intelligent, end-to-end vertical solutions for complex user problems. It is designed to simplify and solve the complexity of data ownership and control. Built on years of technology investment, it can accelerate the development and deployment of secure, scalable and intelligent connected IoT solutions. The core design principles are:

- **Security**: Delivers authentication, authorization and data security through patented BlackBerry cryptography, certificate and key management technologies
- **Scalability**: Ensures scalability at every layer of the architecture
- **Efficiency**: Enables highly efficient communication between devices and applications, enabling advanced use cases

BlackBerry QNX: A trusted OS platform and technology partner for safety-critical medical devices

For more than 30 years, QNX® by BlackBerry has provided a multi-core development platform for manufacturers that exceeds the most demanding requirements for reliability, performance, data safety and security. This experience uniquely positions BlackBerry to address the challenge of securing connected devices already within healthcare environments, where we can strengthen the information security triad (see above) by ensuring confidentiality.



BlackBerry Cybersecurity: Integrated services and software

1. BlackBerry Cybersecurity Consulting

BlackBerry Cybersecurity Consulting works to analyze and mitigate the increasingly complex cybersecurity risks in individual organizations. We are a trusted security partner, helping organizations identify, respond to and prepare for ongoing cybersecurity threats. While most security consultants test to find holes in a security system and then leave when the real work of repairing those holes begins, BlackBerry Cybersecurity Consulting supports organizations every step of the way. Our tailored approach gives clients a detailed understanding of their unique security posture, then advises on the appropriate level of risk reduction within their budget.

Services available:

Security/Vulnerability Assessments
Highly accredited consultants assess vulnerabilities in connected devices, including penetration testing services, then provide recommendations for remediation.

Governance, Risk and Compliance
Consultants with in-depth knowledge of the regulated healthcare industry guide and support compliance and/or accreditation for numerous certifications, including HIPAA, PHIPA, GDPR and IEC 62304.

Threat intelligence
An extended assessment that considers the real-life threats to any organization, based on industry and strategy.

Event Handling/Response
Supports development of enhanced incident monitoring and response capabilities, and digital forensic services in the event of an attempted breach.

Wireless Penetration Testing
Tests the reliability of an organization's wireless network to reduce the risk of an attack.

Social Engineering & Physical Security
Identifies any vulnerabilities in an organization's staff and physical access to the organization's building.

Training & Certification
Provides internal and on-premises security courses covering general staff security awareness and social engineering.

Security Engineering
Includes gap analysis, threat modeling and secure implementation review.

2. BlackBerry security software

BlackBerry software provides the embedded intelligence to secure the EoT, so that the IoT can thrive. These are just a few of the capabilities of BlackBerry software:

- **BlackBerry® UEM** manages your diverse and growing set of devices from a single console.
- **BlackBerry® Workspaces** enables secure collaboration on any device.
- **BlackBerry® SecuSUITE** for Enterprise empowers employees with secure and reliable voice and text.
- **BlackBerry® Dynamics** provides the foundation for secure enterprise mobility by offering an advanced, mature and tested container for mobile apps.
- **BlackBerry® AtHoc** is a complementary offering that unifies crisis communications within and between organizations (including triggering organization-wide alerts in the event of cybersecurity attacks or breaches).

There is no stopping the flood of IoT devices – authorized and otherwise – entering healthcare organizations. They are improving patient care, medical research and healthcare systems efficiencies, and with the proper security in place they will transform healthcare for the better.

The best strategy is to get in front of the IoT wave with cybersecurity practices and tools designed to secure what is already in place – as well as what is coming. But any security approach is useless if it creates a frustrating, negative user experience, because people will find ways to work around it. BlackBerry balances security and productivity to deliver innovative solutions for a connected world, providing solutions to help secure sensitive data across all endpoints – including the growing number and variety of IoT devices in healthcare. BlackBerry seeks to ensure connected devices work for organizations, not against them.

Sources

[1] https://www.gartner.com/newsroom/id/3165317

[2] https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/10/internet-of-things-factsheet-au-2016.pdf

[3] https://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact

[4] https://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html

[5] http://www.securityweek.com/iot-botnet-targets-olympics-540gbps-ddos-attacks

[6] https://www.networkworld.com/article/3217750/internet-of-things/5-iot-trends-that-will-define-2018.html

[7] http://www.securityweek.com/new-legislation-could-force-security-iot

[8] https://www.gartner.com/newsroom/id/3165317

[9] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[10] https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/

[11] https://www.alliedmarketresearch.com/iot-healthcare-market

[12] http://www.healthcareitnews.com/sponsored-content/iot-healthcare-really-internet-patients-iop

[13] https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

[14] https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/

[15] https://threatpost.com/medical-study-blasts-hospitals-security-practices/118913/

[16] https://threatpost.com/hospital-security-fail-report-outlines-dangerous-shortcomings/116519/

[17] https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/

[18] https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm

[19] http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1

[20] http://www.litmos.com/wp-content/uploads/2016/06/webinar-IoT.pdf

[21] https://eugdprportal.godaddysites.com/

[22] https://www.gartner.com/doc/3791263/critical-capabilities-highsecurity-mobility-management

[23] https://www.gartner.com/doc/reprints?id=1-42A6Q84&ct=170607&st=sb

[24] https://www.gartner.com/doc/3799963/critical-capabilities-content-collaboration-platforms

[25] https://cybersecurityventures.com/cybersecurity-500-list/