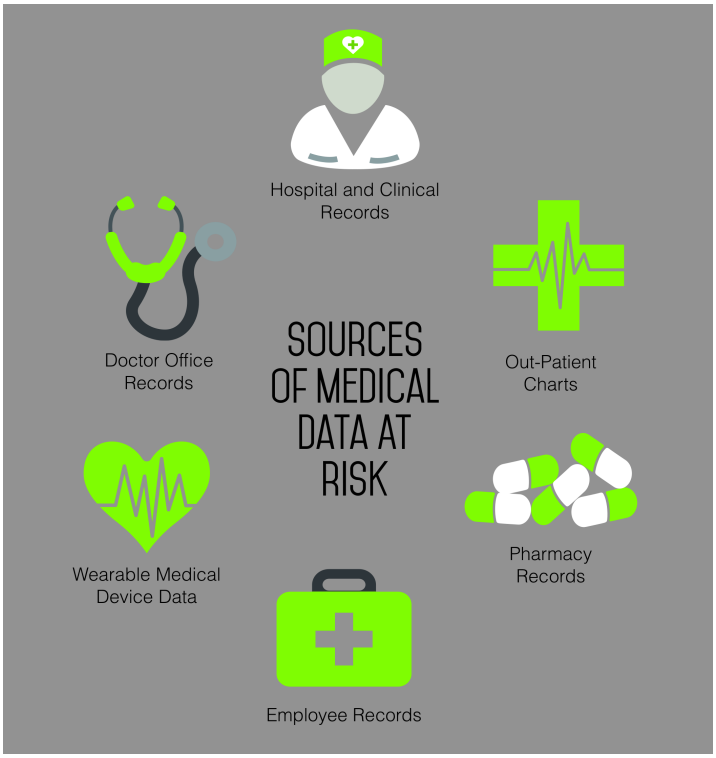
A Systematic Approach to Cyber Health

A TwelveDot White Paper

WWW.TWELVEDOT.COM

We can be reached at info@twelvedot.com

Healthcare, as with many sectors, has embraced technologies such as cloud computing and Internet of Things (IoT). While this has led to better productivity and better service levels, it has exposed data putting patient safety at risk. For example, new wearables haven't followed secure design practices and as a result are prone to compromise and data leaks. Currently there is a lack of widely adopted standards and compliance in the healthcare cybersecurity arena. As of December 2015, there was an estimated 111,022,154[1] Million medical records exposed in the United States alone. The combined top six breaches account for about 1 Million individuals.



Medical data exposure stems from the following:

1. Product and solution designers do not use Threat Modelling to determine how their products or solutions are vulnerable in the field
2. Security testing guidelines and standards are still in development and are not widely available
3. Privacy Impact Assessments (PIA)s are not being performed prior to product design or do not consider where all the data elements are stored
4. Infrastructure monitoring technologies that identify when devices are under attack are being overlooked as a vital step in deployments
5. Lack of security validation of electronic components and software libraries used in solutions presents many opportunities for intrusion at the component level
6. Failure to properly implement and maintain an Information Security Management System (ISMS)

As a result of these systemic issues, many solutions are prone to data theft as a result of data breaches. Many of these threats can be mitigated by using a security approach that builds upon the implementation of a proper Information Security Management System (ISMS).

So how can you mitigate this risk?

Using an assurance-based approach to security that considers each of the following:

1. Gap Analysis
2. Threat and Risk Assessment (TRA)
3. Information Security Management System (ISMS)
4. System Development Lifecycle (SDLC)
5. Objective Evaluation

Gap Analysis
Conduct a Gap Analysis that focuses on your data. Not only where you believe it is, but also where others might try to hide it unknowingly. Depending on your goals, you may wish to do a broad sweep of your current security controls, or to focus on specific areas such as your development or service processes. The information gathered will allow you to develop and propose options for developing a suitable approach to cyber security.

The Gap Analysis considers all cyber aspects of your business and the data. Focus on what is collected, processed and stored; then shift to who has access and why. It's equally important to look at the controls that are implemented to protect this data. Is it sufficient? Was it properly configured and maintained? All of this leads to recommendations for improvement.

Threat and Risk Assessments (TRA)
Using a formal ISO process, conduct an evaluation against targeted systems and processes. This is conducted at a greater depth than the Gap Analysis and attempts to peel back the layers of how a technology solution has been implemented in order to determine both cyber and business risk of the data stored in these systems. Threat and Risk Assessments are conducted prior to launching a project.These go hand in hand with an Action Plan (AP) that will guide the project management team through the implementation of new controls and/or correct current cyber implementation issues identified in the TRA.

Information Security Management System (ISMS)
The processes listed above aid in the creation and implementation of an Information Security Management System. An ISMS is an approach whereby the senior management of an organization aligns their business processes with the secure implementation of technology. Your ISMS drives both business decisions for all projects that implement technology solutions while ensuring that cyber security is considered when making business decisions. The ISMS guides a broad spectrum of business decisions to ensure that all the necessary controls are implemented and the proper risk management process has been implemented. This ensures that formal decision points are created, evaluated and recorded for future audit and assessment, should they be required. They can also be used in the event of a process or system failure to determine whether proper controls were implemented correctly. If you don't have a formal ISMS, you can start with security policy to drive how you determine cyber risk and mitigate it.

System Development Lifecycle (SDLC)
For those organizations that develop products and solutions, analyze how have they implemented a SDLC with a focus on where and when security and privacy are considered. The goal is to ensure that these elements are considered at the product concept stage and that they are mandatory considerations for design, testing and validation prior to production. This typically leads to lower production costs over the life of the product/solution. It also ensures that the users and buyers of these solutions are using a product that is considerably more secure while maintaining a positive user experience. This can be expanded to conduct threat profiling to ensure the in-field risks are known and mitigated.

Objective Evaluation

When considering formal evaluations or certifications there are several options involved but it comes down to company goals and objectives. If the hospital or HMO is looking to secure their operations they could target ISO 27000 for the ISMS. If a product or service organization is looking for certification there are several options including ISO 27000. This includes ISO 15408 on Common Criteria and FIPS 140-x for systems containing cryptographic modules. The goal at the provide customers, partners and patients the assurance that security has been considered and is important to the these organizations.

Regardless of the path chosen, thoroughly prepare your organization for the formal assessment and provide pre-assessment evaluation, documentation, training and evaluating certification providers. The focus to ensure that you meet and/or exceed the minimum requirements for these certifications.

For example, a solid Cyber Assurance Program can be leveraged to ensure compliance with current US requirements under the FDA for mitigation and managing of cybersecurity threats These are some high-level considerations to contemplate prior to evaluation:

A. Medical device manufacturers and health care facilities should take steps to ensure appropriate safeguards. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. They are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.
B. Hospitals and other health care facilities should evaluate their network security and ensure they protect their hospital systems against malware.
C. Encouraging health care public health stakeholders to develop innovative strategies to assess and mitigate cyber security vulnerabilities.
D. Building a foundation of trust within the public health sector that encourages the timely sharing of cybersecurity vulnerabilities that can have a negative effect on patient safety.

TwelveDot Cyber Assurance and Healthcare

With our hands on experience in the healthcare sector, we understand that this industry has some unique challenges in the cyber security arena. Because of the highly sensitive and personal data being collected, stored and reported on, the healthcare industry is held to extremely high moral and legal obligations, expectations and standards that other industries simply cannot relate to. Even when legal obligations are met and widely accepted standards are

followed, this may not be enough. As custodians of the very well-being of humans, the deep emotional connection patients have with highly sensitive personal data cannot be ignored.

Addressing cybersecurity threats to reduce information security risks is especially challenging in any application. Because cybersecurity threats cannot be completely eliminated, manufacturers, hospitals and facilities must work to manage them. At the same time, there is also a need to balance protecting patient safety with the promotion of the development of innovative technologies and improved device performance.

Using our cyber assurance program we can provide assistance to healthcare service providers, product and/or services companies, hospitals, HMOs, and pharmaceutical companies to implement the necessary safe guards for cyber security.

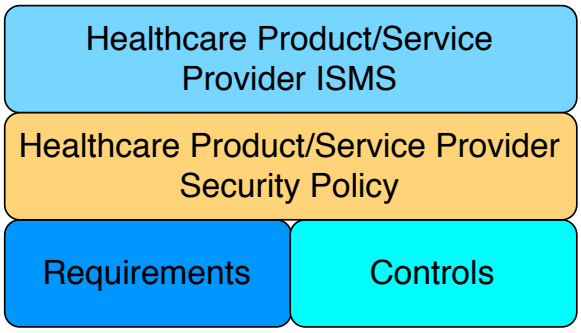
We provide the necessary recommendations and implementation guidance for technologies, procedures and processes to ensure that identified data at risk is protected. Of course, this is supported by a solid security awareness campaign which we can help to implement. Your staff plays a key role in your success and should be considered in any plan being created.

Our cyber assurance program assists with the identification and gathering of metrics that measure ongoing execution of controls, and managing security risks. Metrics and trend analyses are utilized to demonstrate assurance, proactively identify compliance and control failures relevant to your business.

Healthcare organizations need to build a strategic automated approach to vulnerability, risk management and compliance reporting. TwelveDot can provide the necessary expertise to complete the implementation of an efficient vulnerability management program and easily understandable reporting system so the entire organization understands the security and compliance status at any time.

We believe that implementing an ISMS is critical to success as it becomes the means to determine whether the approach to security aligns with the operational aspects of any healthcare institution. If not, those areas of improvement can be identified and addressed accordingly. It ensures that as the institution or service business grows and develops, so does its approach to security and risk.

APPROACH TO BUILDING A ISMS



The diagram above shows how a healthcare provider could approach implementing an ISMS. Once the ISMS aspects are implemented, the solution providers need to focus on ensuring that products and services being selected for usage are evaluated against the security requirements of the organization. Healthcare service providers and hospitals need to ensure that they are only selecting products and solutions that can provide the necessary controls. This includes conducting evaluation of 3rd party providers to ensure they too can meet these requirements.

Some of these considerations include:

1. What data is being collected by the device?
2. Where is this data being stored? On the device? In the cloud?
3. What protections are in place to protect this stored data?
4. What controls does the product/service have in place for data collection, breach notification, hiring and training security practices and policies.
5. What formal testing process and procedures are in place to ensure the software and hardware security risks are kept to an acceptable minimum.
6. Can the solution provider show evidence that all the security tasks mentioned are actually in practice and not just a policy document for marketing purposes?
7. For hardware and software technologies: are the vendors performing security design and testing into the solution and can they prove these claims?
8. Do you have an incident management process that includes handling of data breaches?

Conclusions

With the growing dependence on technology in healthcare, technology can provide better quality of care for both in and out patient care. However, ensuring that these technologies and the operational policy aspects are considered, evaluated and mitigated is going to greatly reduce the potential for a data breach. This will greatly improve patient reliability and trust in these systems.

In many countries there are regulatory requirements to ensure patient data is protected, but still breaches occur through negligence in institutions not doing enough to protect patient data. When this happens, administrators are often found liable and become personally accountable for the breaches.

Healthcare managers and administrators can greatly reduce their liability exposure by ensuring they can prove due diligence. This is easily accomplished by implementing an ISMS and showing a strong audit record of risk management of new technology solutions.

Call us today, TwelveDot has the experience and methodology to help secure healthcare product and service organizations determine their risk exposures and build a plan to ensure these issues are addressed now and as new projects and technologies are considered in the future.

References

[1] Forbes: Data Breaches In Healthcare Totalled Over 112 Million Records In 2015, Dec.31, 2015

Standards for Implementing an ISMS

ISO/IEC 27001:
2013-10-01 Information technology - Security techniques - Information security management system - Requirements
ISO/IEC 27002:
2013-10-01 Information technology - Security techniques - Code of practice for information security controls
ISO/IEC 27005:
2011-06-01 Information technology - Security techniques - Information security risk management
ISO/IEC 27007:
2011-11-15 Information technology - Security techniques - Guidelines for information security management systems auditing

TwelveDot Inc.
343 Preston Street 11th Floor
Ottawa, ON, CANADA
K1S 1N4
info@twelvedot.com