SATORI CONSULTING

CYBERSECURITY FOR HEALTHCARE

Data breaches and ransomware are facts of life in today's business environment, but organizations that care for our health are entrusted with our most intimate information and are the worst places for these to happen. Protect your patients' data and your reputation by implementing a cybersecurity regime without delay.

THE CYBERTHREAT IS REAL

Why healthcare is especially sensitive

Hardly a day goes by without a new data breach or ransomware attack in Healthcare. This isn't an accident: along with government and education, healthcare is one of the top targets for cybercriminals. There are several factors that make Healthcare an attractive target:

1. Healthcare organizations must handle large amounts of Protected Health Information (PHI), Personally Identifiable Information (PII), and Personal Financial Information (PFI) in order to function
2. Many Healthcare organizations, especially providers, don't invest heavily in Information Technology in general, and cybersecurity in particular
3. Organization feel obliged, through a duty of care, to respond quickly in order to reduce disruption to service – in particular, this increases the likelihood of paying ransoms for ransomware.

The implications of cybersecurity incidents are too great to be ignored. Even if an organization has cyber insurance, the cost of recovery is often high compared to income and profitability. Several organizations have also incurred punitive fines by regulators. Under-funded Information Technology may struggle to recover at all from attacks that result in significant data loss. In fact, several smaller providers that faced ransomware attacks have subsequently been forced to close.

On the other hand, implementing a robust cybersecurity program appears daunting. There is a myriad of technology products on the market claiming to solve everyone's cybersecurity woes, but whose claims should be believed, and do they even work in all circumstances? Meanwhile, it is easy to be sucked down the rabbit hole of compliance with regulations, steering organizations into a warren of paper-based policies, procedures, and controls.

Regardless of the complexity, doing nothing isn't a viable option. Obtaining short-term external help is often the only means to get the cybersecurity program on a secure footing. Once the program is up and running, it is easier to maintain, using part-time external assistance.

A Heavily Regulated Industry

Due to the nature of its work, healthcare is subject to numerous regulations aimed at:

- Delivering services to patients with the minimal risk of harm
- Administering safe drugs in the ways that were intended
- Providing government mandated healthcare to certain groups
- Avoiding fraud, waste, and abuse
- Ensuring that healthcare data is only collected and used in a meaningful way.

The industry is regulated by a complex mesh of regulators, including:

- State Departments of Health (DOH), which license healthcare providers
- The Food and Drugs Administration (FDA), which oversees the development of new drugs and safe use of approved drugs
- The federal Center for Medicare and Medicaid Services (CMS), which funds programs to serve elderly and low-income patients
- Federal Health and Human Services (HHS), which works to reduce fraud, waste and abuse, and oversees compliance with the Health Insurance Portability and Accountability Act (HIPAA).

While HHS's HIPAA tends to be to most influential industry regulation on Information Security, all these regulators may have an impact where it has a bearing on their domain.

KICKSTARTING THE CYBERSECURITY PROGRAM

The first step to a solid cybersecurity program is a risk analysis, which identifies the hot spots that require the most attention. This allows you to focus your efforts most effectively, saving time and money, and regulators will appreciate a risk-based approach that concentrates effort on the reducing the highest risks. While many "best practices" in cybersecurity appear to be designed for huge organizations employing thousands of people, a risk analysis can provide the guidance needed to scale down best practices to smaller organizations with only a few dedicated IT staff and limited resources.

The federal government also provides guidance for cybersecurity in the healthcare industry in Section 405(d) of the 2015 Cybersecurity Act and an HHS Task Force subsequently built out practical guidance for implementing cybersecurity in different sizes of organizations. 405(d) provides a good start for a risk-based approach to cybersecurity, including recommendations for technical implementation in small, medium, and large practitioners.

The 405(d) Task Force identified the following five threats as being currently most relevant to the Healthcare industry (the list is specific to 2019 and may change in future as the IT landscape changes and attackers adapt their response):

1. Email Phishing Attacks
2. Ransomware Attacks
3. Loss or Theft of Equipment or Data
4. Insider, Accidental or Intentional Data Loss
5. Attacks Against Connected Medical Devices That May Affect Patient Safety.

In order to address these threats, the 405(d) Task Force prioritized the following security practices:

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies.

While this is a good start, each area must be evaluated to understand how it relates to the specific organization and what protections need to be applied. Protections need not be particularly resource intensive or expensive – there are often good cloud-based and "as a Service" solutions that avoid upfront costs and dedicated resources. These solutions should also be considered in the context of broader Information Technology strategy, such as whether entire business functions can be bought "as a Service" instead of in-house. In this case there is an element of risk transfer, because in-house implementation risk is replaced by third-party risk, which needs to be addressed through periodic reviews and audits.

RISK ANALYSIS AND ROADMAP

Satori's approach to risk analysis is to perform an onsite assessment lasting from three to six weeks, depending on the scope and size of the organization. The project aims to cover three aspects:

- **Cybersecurity Risk Assessment**– Assess current cybersecurity controls against applicable regulatory standards (e.g. HIPAA, NIST) and leading practices
- **Perform Gap Analysis**– Identify cybersecurity gaps and develop priorities for remediation.
- **Develop Roadmap** -- Define the roadmap needed to close the gaps and align with cybersecurity controls with the business.

The project usually comprises of several stages, as described below.

Initiation & Discovery

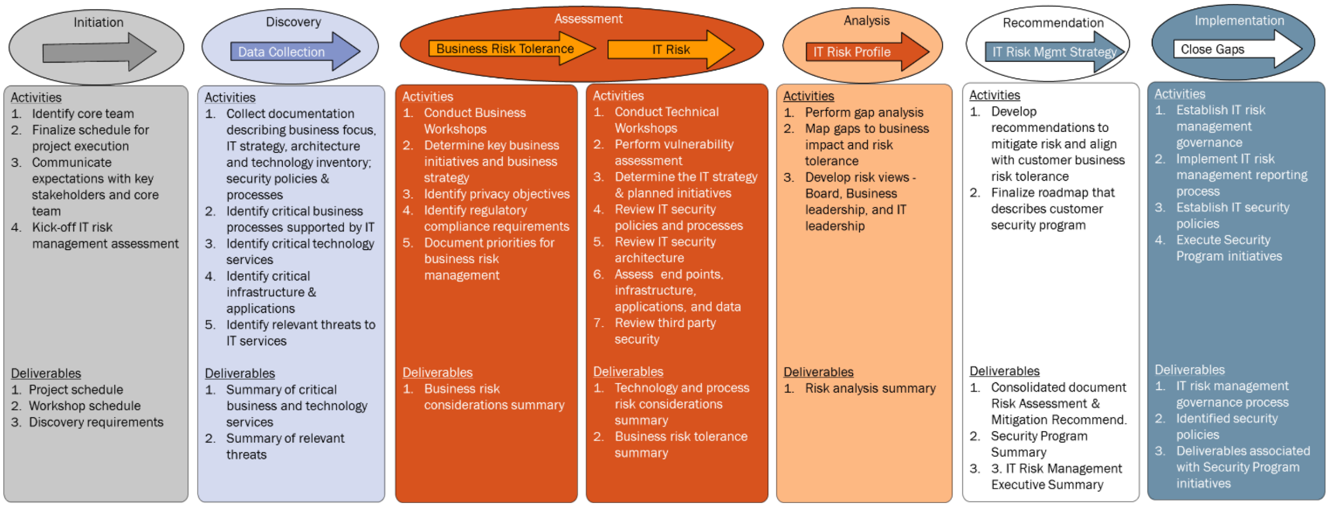
The assessment team meets with core team members individually prior to kick-off meeting to communicate what we are trying to accomplish, the methodology used to achieve our goal and their role in the effort.

Scope of Activities:

- Confirm stakeholders and client team
- Conduct kick-off meeting
- Document services and business risk tolerance
- Initiate data discovery

Example Data Review:

- Network and infrastructure diagrams
- Application and hardware inventories
- Master Service Agreements with third-party suppliers



Initiation

Activities
1. Identify core team
2. Finalize schedule for project execution
3. Communicate expectations with key stakeholders and core team
4. Kick-off IT risk management assessment

Deliverables
1. Project schedule
2. Workshop schedule
3. Discovery requirements

Discovery – Data Collection

Activities
1. Collect documentation describing business focus, IT strategy, architecture and technology inventory; security policies & processes
2. Identify critical business processes supported by IT
3. Identify critical technology services
4. Identify critical infrastructure & applications
5. Identify relevant threats to IT services

Deliverables
1. Summary of critical business and technology services
2. Summary of relevant threats

Assessment – Business Risk Tolerance

Activities
1. Conduct Business Workshops
2. Determine key business initiatives and business strategy
3. Identify privacy objectives
4. Identify regulatory compliance requirements
5. Document priorities for business risk management

Deliverables
1. Business risk considerations summary

Assessment – IT Risk

Activities
1. Conduct Technical Workshops
2. Perform vulnerability assessment
3. Determine the IT strategy & planned initiatives
4. Review IT security policies and processes
5. Review IT security architecture
6. Assess end points, infrastructure, applications, and data
7. Review third party security

Deliverables
1. Technology and process risk considerations summary
2. Business risk tolerance summary

Analysis – IT Risk Profile

Activities
1. Perform gap analysis
2. Map gaps to business impact and risk tolerance
3. Develop risk views - Board, Business leadership, and IT leadership

Deliverables
1. Risk analysis summary

Recommendation – IT Risk Mgmt Strategy

Activities
1. Develop recommendations to mitigate risk and align with customer business risk tolerance
2. Finalize roadmap that describes customer security program

Deliverables
1. Consolidated document Risk Assessment & Mitigation Recommend.
2. Security Program Summary
3. 3. IT Risk Management Executive Summary

Implementation – Close Gaps

Activities
1. Establish IT risk management governance
2. Implement IT risk management reporting process
3. Establish IT security policies
4. Execute Security Program initiatives

Deliverables
1. IT risk management governance process
2. Identified security policies
3. Deliverables associated with Security Program initiatives

Assessment

We will conduct workshops to understand the cybersecurity and compliance requirements (organization, policies, and controls). We will use the information collected during the Initiation & Discovery phases as input to the workshops.

In parallel, we will perform an initial triage to identify urgent gaps that must be addressed. This triage analysis will be provided to the project sponsor two weeks after the project starts, to form the basis of a rapid response plan and expedite remediation activities.

The items we will address during the workshops include:

- *Business Risk Workshop*
  - Identify/review key business services and underlying processes, systems and assets
  - Identify privacy policy and objectives
  - Identify regulatory compliance requirements – GDPR, HIPAA, and CCPA
  - Identify relevant control frameworks and standards, such as NIST, HITRUST, COBIT, and ISO27002
  - Identify sensitive data assets and critical technologies
- *Technical Risk Workshop*
  - Review governance structure including policies and standards
  - Identify relevant threats to IT assets and develop threat model
  - Identify existing cybersecurity controls deployed to protect data and technology assets

Scope of Activities:

- Conduct business risk workshops
- Conduct technical risk workshops
- Identify components of rapid response plan

Analysis

We review and analyze the requirements obtained during the Assessment phase to develop a practical, actionable approach to manage data and technology risk. We leverage the agreed relevant frameworks to guide analysis.

Scope of Activities:

- Perform detailed analysis using the agreed framework(s)
- Establish a risk register
- Document the gap analysis considering leading practices and compliance requirements

Recommendation Development

We will leverage the approach developed during the Analysis phase and construct a detailed roadmap to effectively manage data and technology risk. The roadmap will consider dependencies needed to execute and achieve the outcomes.

In addition, we will provide recommendations on how to structure and manage the program of risk remediation.

Scope of Activities:

- Identify high-priority, short-term activities to support the admission and treatment of patients
- Develop IT risk mitigation strategy
- Document detailed and actionable recommendations to close cybersecurity gaps
- Develop IT cybersecurity roadmap.

IN CONCLUSION

Every Healthcare organization must avoid data leakage, disruption, cost, and reputational risk by planning and executing information security activities. Satori has helped organizations avoid information security challenges by working with them to develop:

1. High-level organization design for information security and governance
2. Risk-based Information Security Risk Management Systems
3. Priority remediation projects to be implemented.

Only by implementing an Information Security Risk Management System can you signal to patients, partners, and regulators that you are serious about patient privacy and data protection.

HOW SATORI CAN HELP

Satori is a leading international management consulting firm with offices in New York, Chicago, Boston, Washington DC, and London. We have a dedicated cybersecurity practice that assesses, designs, and implements cybersecurity programs for many types of businesses across multiple industries. We deliver:

1. A proven methodology for assessing current cybersecurity capabilities and recommending improvements
2. A comprehensive set of cybersecurity policies and procedures, which can be adapted by program maturity, alternative business sizes, and industries
3. Seasoned practitioners with real-life experience of cybersecurity programs in a variety of contexts
4. Strong understanding of standards such as NIST and ISO, and how to apply them to ensure effective risk management and compliance with regulations (e.g., GDPR and HIPAA)
5. A collaborative working style and an emphasis on developing strong long-term working relationships.

Satori's assessment and roadmap development approach generates detailed recommendations that are customized to the size and type of organization, rapidly reducing the real cybersecurity risk in a way that fits with regulatory requirements.

The implementation roadmap will drive remediation activities to further reduce risk and put the cybersecurity program on a firm footing.

Satori offers a follow-on part-time Virtual CISO service to provide cybersecurity assistance for medium sized businesses in the longer term without the need for investment in full-time employees.

At Satori Consulting, our mission is simple—to work side-by-side with clients to discover opportunities and solve problems. We strive to provide both comprehensive and expert service, mindful of every client's unique needs. Our team of highly skilled management consultants brings a wealth of industry and functional experience to provide wide-ranging services in project and program management, risk management, change management, organizational effectiveness, strategy and advisory, business process engineering, performance management, and infrastructure and technology.

Satori
CONSULTING

48 Wall Street
Suite 1100
New York, NY 10005

Phone 212.918.4560
Email info@satoriconsulting.com

www.satoriconsulting.com