The Cybersecurity Lawyer and the Medical Industry

By: Graciela Roig, MS, JD.
President
General Computer Services Inc.
Smart Building Telecom Inc.
admin@becru.com

Citation: Copyright of Graciela Roig Santana-Allen, Created Date 4/15/2024, available at

https://ssrn.com/abstract=4801007

Contents

Introduction 1
I. First, it is essential to determine who are the users of the systems and data to protect 4
II. Second, it is essential to recognize and understand what a Cybersecurity Attack is. 4
III. Third, selecting the cybersecurity framework and complying with the law is essential. 5
i. Examples of Cybersecurity Frameworks and Laws: 6
IV. The New US Cybersecurity Framework created in 2023 by the NIST: 10
V. Cybersecurity Lawyer Specialty: 10
VI. HIPAA and the Electronic Protected Health Information (ePHI): 13
VII. International Cybersecurity Law and the Impact in the US : 13
VIII. The European Union Cyber Resilience Act and the impact on the economy and Cybersecurity Lawyers in the US and worldwide 14
IX. Essential cybersecurity requirements for products sold in the EU 15
X. What are the fundamental laws that the medical organization must comply with and that involve Cybersecurity? 16
XI. The Federal Healthcare Law, Regulations, and Framework in the US. 18
XII. Cybersecurity Attacks, Ransomware, and Policies to Prevent the Incidents 21
XIII. How can the Cybersecurity Lawyer help create the incident response plan based on Cybersecurity Policies and Laws? 23
V. Conclusion 29
References 30

Introduction

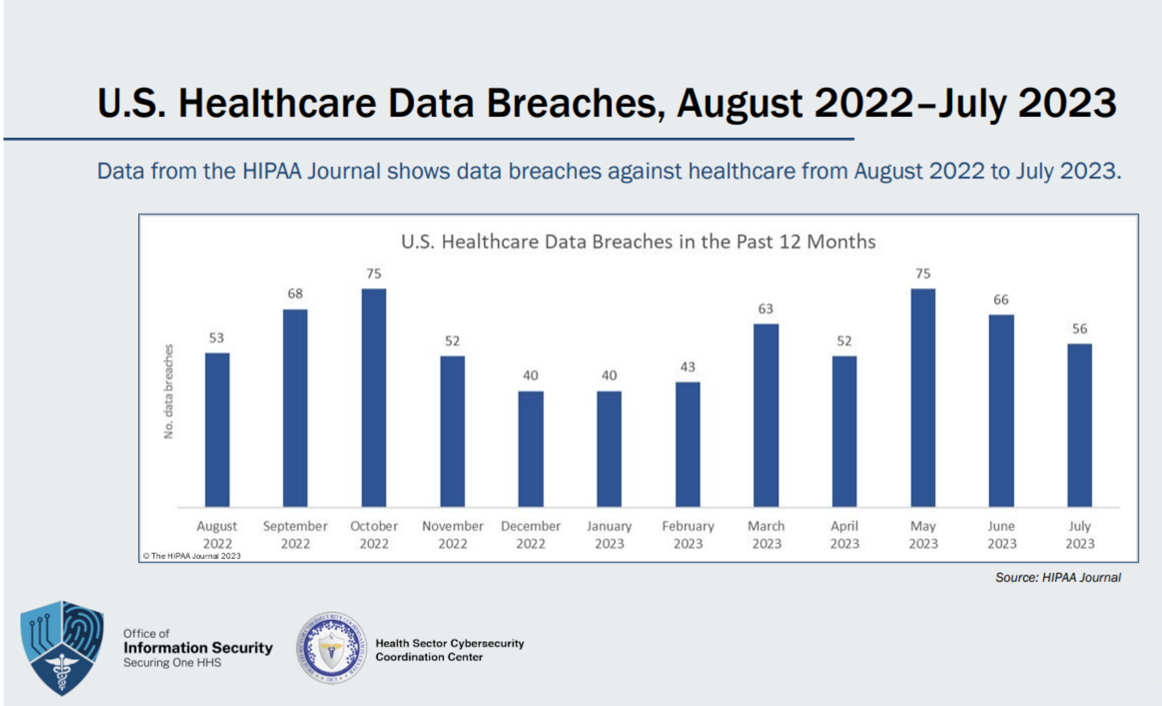
Welcome to the forefront of legal practice: cybersecurity law. This article explains Cybersecurity Lawyers' role and impact on the new digital landscape, focusing on the medical industry and how these lawyers are critical to modern economic organizations and States to protect their data from Cyberattacks under the umbrella of the national and international laws of Cybersecurity.

We highlight the indispensable function of cybersecurity lawyers in formulating policies that protect data and operations amidst the ongoing battle for privacy and security on both national and international fronts. This includes ensuring compliance with key legislations such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the European Union's newly enacted Cyber Resilience Act ("CRA").

The Cyber Resilience Act ("CRA"), passed by the European Parliament on March 12, 2024, affects all industries whose products and components will be sold in the EU and will be in full effect in the next 36 months. This Act will significantly impact the digital medical products industry, in which the United States of America is a worldwide leader. We address the role of Cybersecurity Lawyers in ensuring that all manufacturers' and subcontractors' contracts adhere to this new legislation.

Furthermore, we explore various cybersecurity frameworks and laws, illustrating how frameworks like HIPAA and the National Institute of Standards and Technology (NIST) cybersecurity guidelines are applied within the medical industry. Additionally, we analyze the profound impact of cybersecurity law on medical organizations, emphasizing cybersecurity lawyers' crucial role in safeguarding healthcare entities' security and compliance.

Moreover, we discuss the escalating threat of ransomware attacks and other cyber threats alongside the implementation of policies and contingency plans to mitigate such incidents. Through presenting statistics on cybersecurity attacks, we highlight the essential role of cybersecurity lawyers in the lifecycle of cybersecurity frameworks, particularly those developed by NIST, in preventing these attacks.



U.S. Healthcare Data Breaches, August 2022–July 2023

Data from the HIPAA Journal shows data breaches against healthcare from August 2022 to July 2023.

Source: HIPAA Journal

(*15)

In recognizing the legal obligations imposed by Federal, State, and international laws, we spotlight prominent US laws such as HIPAA and HITECH and regulations by governmental agencies like the Centers for Medicare and Medicaid Services (CMS). Additionally, we provide insights into state legislation, exemplified by Florida's stringent laws protecting personal and financial data, which necessitate prompt breach disclosure. Throughout this article, we aim to elucidate the intricate landscape of cybersecurity law, emphasizing the critical role of cybersecurity lawyers in navigating legal complexities, safeguarding organizations, and ensuring compliance with evolving regulations.

To comprehend the necessity of cybersecurity lawyers, we begin by defining the users of systems and data, clarifying the concept of a cybersecurity attack, and stressing the importance of adapting cybersecurity frameworks to organizational needs, best practices, and the laws that apply to the industry like HIPAA in the medical industry.

I. First, it is essential to determine who are the users of the systems and data to protect

The user is any person, including employees of the organization or representatives of corporations, who are authorized users of the organization's systems, including but not limited to temporary or permanent employees or subcontractors.

The data encompasses all information within your electronic systems, for example, a list of clients, patients, or vendors, and all economically sensitive data such as bank accounts, reports, documents, pictures, videos, backup data, and passwords.

II. Second, it is essential to recognize and understand what a Cybersecurity Attack is.

It is well known that a cybersecurity attack must be identified and understood to overcome the enemy. The US National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. It is one of the oldest physical science laboratories in the United States. Its definition of a cybersecurity attack is accepted by professionals and institutions worldwide. According to the NIST, a cybersecurity attack is: "any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself." It is also_"an attack, via cyberspace, targeting an enterprise's use of cyberspace to disrupt, disable, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." (* 1).

Both legal and technical components are essential in the battle to maintain the national security of data and the integrity of systems operating nationwide. To succeed, they must work together, as legal cybersecurity policies must guide the creation of technical policies. Simultaneously, technical expertise aids in the development and implementation of cybersecurity policies. It's a symbiotic relationship between law and Technology.

III. Third, selecting the cybersecurity framework and complying with the law is essential.

A solid plan that includes legal and technical policies following a cybersecurity framework is fundamental. The framework has to be the best option for the data of that specific industry, and in some cases, it is mandatory by law.

There are multiple Frameworks of Cybersecurity and different industries that use it. For example, ISO27001/ ISO 27002, SOC, PCI, COBIT, COSO, FedRAMP, GDPR, FISMA, HIPAA, and NIST.

These cybersecurity frameworks are not limited to the United States, and some are recognized and accepted internationally, with many organizations worldwide adopting them to enhance their cybersecurity posture and ensure compliance with regulatory requirements.

i. Examples of Cybersecurity Frameworks and Laws:

We will explore some of the most important and explain in which industry or part of the world it is used and for what purpose.

ISO/IEC 27001 and ISO/IEC 27002: ISO/IEC 27001 is an international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). ISO/IEC 27002 guides on implementing controls for information security management. These standards are used across various industries globally to protect sensitive information and ensure compliance with regulatory requirements.

SOC (Service Organization Control) Frameworks: SOC frameworks, developed by the American Institute of Certified Public

Accountants (AICPA), are used to assess and report on the controls of service organizations. They include SOC 1 for internal controls over financial reporting, SOC 2 for security, availability, processing integrity, confidentiality, and privacy, and SOC 3 for general use reports on controls at a service organization. While SOC reports are commonly associated with U.S.-based organizations, the principles and criteria outlined in SOC frameworks are applicable internationally. Many multinational companies and service providers undergo SOC audits to demonstrate their commitment to security and compliance.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS is a set of security standards designed to ensure the secure handling of credit card information by organizations that process, store, or transmit cardholder data. Major credit card companies mandate it, which is crucial for the retail, hospitality, and e-commerce industries.

COBIT (Control Objectives for Information and Related Technologies): COBIT is a framework developed by ISACA for the governance and management of enterprise IT. It provides a comprehensive framework for aligning IT objectives with business goals and ensuring effective governance and control over information and technology resources.

COSO (Committee of Sponsoring Organizations of the Treadway Commission): COSO is a framework for internal control. Organizations use it to assess and enhance their risk management, control, and governance processes. It focuses on principles-based control environments, risk assessment, control activities, information and communication, and monitoring activities.

FedRAMP (Federal Risk and Authorization Management Program): FedRAMP is a US government program that standardizes the security assessment, authorization, and continuous monitoring of cloud products and services. Federal agencies use it to ensure the security of cloud solutions and protect sensitive government data.

General Data Protection Regulation (GDPR): GDPR is a regulation in the European Union (EU) that governs the protection of the personal data of EU citizens. It imposes requirements on organizations regarding data protection, privacy rights, consent, and data breach notification. GDPR compliance is essential for organizations handling the personal data of EU residents.

Federal Information Security Management Act (FISMA): FISMA is a US federal law that establishes cybersecurity requirements for federal agencies and their contractors. It mandates developing and implementing risk-based cybersecurity programs to protect federal information and systems.

<u>Health Insurance Portability and Accountability Act (HIPAA):</u> The US federal law sets standards for protecting sensitive **patient health information** (PHI). It applies to healthcare providers, health plans, healthcare clearinghouses, and business associates handling PHI. HIPAA mandates safeguards for the confidentiality, integrity, and availability of PHI, and organizations must comply with its requirements to ensure patient privacy and security.

These frameworks provide organizations with guidance and standards to effectively manage cybersecurity risks, ensure compliance with regulatory requirements, and protect sensitive information across various industries and sectors.

<u>NIST Cybersecurity Framework (CSF):</u> Developed by the National Institute of Standards and Technology (NIST), the NIST CSF provides a flexible framework for managing and improving cybersecurity posture. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover. The framework is widely adopted across industries, including government, finance, **healthcare**, and critical infrastructure.

While developed by the National Institute of Standards and Technology (NIST) in the United States, the NIST CSF has gained global recognition and adoption. Many organizations outside the US use it as a comprehensive framework to manage cybersecurity risks effectively.

IV. The New US Cybersecurity Framework created in 2023 by the NIST:

The NIST Cybersecurity Framework (NIST CSF), introduced in 2023, is a voluntary set of guidelines designed by the National Institute of Standards and Technology to bolster organizations' cybersecurity resilience. While mandatory for government contractors and agencies, it offers valuable insights for all organizations. Initially structured around five core functions—Identify, Protect, Detect, Respond, and Recover—the framework aids in asset understanding, vulnerability reduction, swift incident detection, effective response, and efficient recovery. In 2023, the framework expanded with the addition of the "Govern" function, emphasizing establishing robust cybersecurity governance structures. This addition highlights the importance of aligning Cybersecurity with organizational objectives and risk appetite, fostering a proactive approach, and enabling customization to specific industry needs. Organizations adhering to the NIST CSF strengthen their defenses, promote continuous improvement, and fortify their long-term cybersecurity resilience.

V. Cybersecurity Lawyer Specialty:

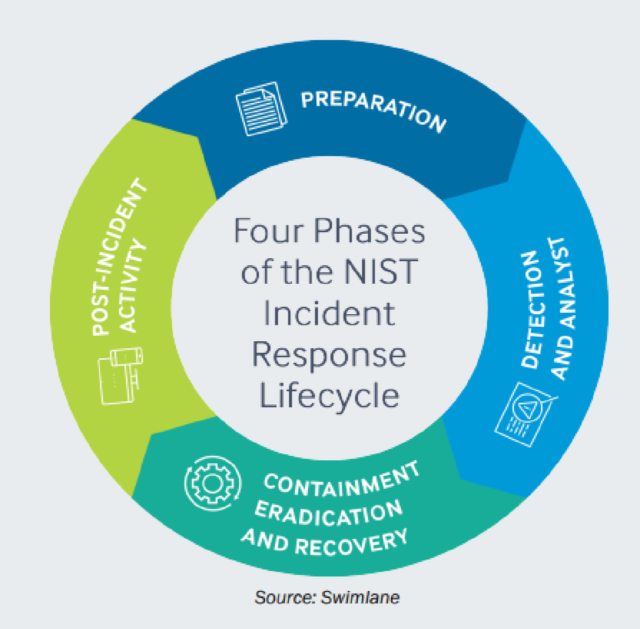
It's a new specialty for lawyers and a vital component for every organization and State to lead the framework adaptation, implementation, and monitoring across industries and states.

In today's digital age, safeguarding sensitive data and mitigating cyber threats is paramount for businesses across all industries. It is reflected in international law and specific laws of the US, EU, and other countries. The Privacy & Cybersecurity Layer is a vital component that has emerged as a cornerstone for organizational resilience. The Internet and economy work together as a global enterprise that involves almost all human activity. Cybersecurity lawyers play a pivotal role in making the states and organizations comply with national and international laws, preventing and managing risks, crafting robust cybersecurity policies, overseeing their implementation, and orchestrating damage control and recovery efforts.

At the forefront of this defense are cybersecurity lawyers, whose expertise bridges the realms of law and Technology. Tasked with navigating the intricate landscape of cybersecurity law, they are instrumental in ensuring compliance with state, federal, and international regulations. From advising on strategic implementations to representing clients before regulatory bodies, these legal experts serve as the linchpin during incidents, orchestrating crisis management to mitigate losses and uphold legal compliance.

As highlighted by the American Bar Association, cybersecurity lawyers are licensed Juris Doctors with specialized knowledge in cybersecurity law. Whether serving as consultants or in-house counsel, they are indispensable assets for any organization or law firm. With Technology and cybersecurity law evolving rapidly, these professionals are poised to play a pivotal role in shaping the future of Cybersecurity across all industries by creating incident report plans and policies. (*10). NIST Special Publication (SP) 800-61 Revision 2 "Computer Security Incident Handling Guide" outlines the principles and steps for developing an Incident Response Plan. Preparation and Planning; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activities.(*11)

In the healthcare sector, cybersecurity lawyers take a tailored approach, adapting policies to adhere to regulations such as **HIPAA** while aligning with each organization's unique needs. By leveraging their expertise, they ensure that medical institutions remain compliant and resilient in the face of evolving cyber threats.


Four Phases of the NIST Incident Response Lifecycle
PREPARATION
DETECTION AND ANALYST
CONTAINMENT ERADICATION AND RECOVERY
POST-INCIDENT ACTIVITY

Source: Swimlane

In conclusion, the role of a Privacy & Cybersecurity Lawyer is indispensable in safeguarding organizations against cyber risks and complying with the national and international laws that apply in each industry and State. As Technology advances with a global economy, the Privacy & Cybersecurity lawyer's expertise will be essential in creating the cybersecurity policies and contingency plans crucial for national security to fortify defenses, mitigate threats, and ensure the integrity of sensitive data. It is a new world that many lawyers have to discover.

VI. HIPAA and the Electronic Protected Health Information (ePHI):

The Health Insurance Portability and Accountability Act (HIPAA) mandates that entities under its regulation must establish robust authentication measures to safeguard the **electronic Protected Health Information** (ePHI) they handle. It entails ensuring the confidentiality, integrity, and availability of ePHI. Entities subject to HIPAA are advised to conduct thorough risk analyses to inform their choice of authentication solutions, guaranteeing adequate ePHI protection. Furthermore, adopting multi-factor authentication (MFA) is recommended as a best practice, especially solutions resistant to phishing attacks, to enhance ePHI security and fortify defense against cyber threats targeting their information systems.

VII. International Cybersecurity Law and the Impact in the US :

International cybersecurity laws and agreements provide a framework for cooperation and address cyber threats across borders. Key instruments include the United Nations Charter and Group of Governmental Experts reports, establishing norms for responsible state behavior in cyberspace. The Budapest Convention and Council of Europe Convention on Cybercrime harmonize national laws and promote international cooperation in combating cybercrime. Additionally, the

Tallinn Manual offers guidance on interpreting international law in cyberspace, while regional agreements, such as the EU's NIS Directive and ASEAN's Cybersecurity Cooperation Strategy, address Cybersecurity within specific regions. These instruments aim to enhance Cybersecurity, promote stability, and facilitate cooperation at the global level, though their effectiveness relies on state compliance and meaningful engagement.

VIII. The European Union Cyber Resilience Act and the impact on the economy and Cybersecurity Lawyers in the US and worldwide

The Cyber Resilience Act ("CRA") was passed as a law by the European Parliament on March 12, 2024. This law means that in approximately 36 months, the products sold in the EU must be complied with, and information technology contracts and multiple component contracts will have to be updated in the US and all countries that do business with the EU.

The CRA proposes stringent cybersecurity regulations for products with digital components to address escalating risks and inadequacies in current laws. It aims to "bolster cybersecurity rules to ensure more secure hardware and software products, " bolster security standards, increase transparency, and empower users to make informed decisions. The Act rules about the compliance requirements, the reporting process of issues to the European Union Agency for Cybersecurity (ENISA), a manufacturers' single point of contact (human, not automatic) for reporting vulnerabilities and providing information to users, the Monitoring and Enforcing process in a timeline. **(* 8)**

In the case of violating the Cyber Resilience Act, for example, it can cost up to 15 million euros or 2,5% of the organization's total worldwide annual turnover in the preceding financial year. The EU Member States have specific rules. Although the CRA won't be fully enforceable for about 36 months, companies with lengthy development cycles and contracts must consider its implications early. **(* 9)**

The Act introduces multiple security requirements for manufacturers, importers, and distributors of hardware and software products that want to enter into the European Union market. For example, key objectives include enhancing manufacturer accountability, establishing a comprehensive cybersecurity framework, increasing transparency of security attributes, and promoting secure product usage. The Act seeks to create a safer digital landscape and foster resilience in the digital economy through these measures.

IX. Essential cybersecurity requirements for products sold in the EU

It includes a thorough assessment and documentation of cybersecurity risks throughout the product's lifecycle, from planning to production and expected lifetime. This assessment informs the need for the product to be free from known exploitable vulnerabilities, configured securely by default, and capable of receiving automatic security updates. Additionally, products must safeguard against unauthorized access, uphold the confidentiality and integrity of data, minimize data processing, and maintain core functionality even during disruptions.

The Cyber Resilience Act (CRA) mandates businesses to prioritize cybersecurity measures impacting their operations across the European Union (EU). While this entails significant extra efforts, it also offers legal clarity as the CRA is universally applicable within the EU, ensuring that products meeting its standards can be sold across member states without facing varying cybersecurity requirements that could impede trade.

In conclusion, the international laws of Cybersecurity of the EU opened a new world for lawyers specializing in Cybersecurity. From a legal standpoint, to comply alongside mandatory disclosures, negotiating IT contracts and related contracts that involve technology components will now include new elements, such as ensuring that components sourced from third parties comply with the CRA, adding an extra layer of accountability in the supply chain. So, it is an open world for legal work and a new specialty.

.

X. What are the fundamental laws that the medical organization must comply with and that involve Cybersecurity?

A Cybersecurity lawyer is crucial within the medical industry to ensure organizations remain informed and compliant with industry laws and regulations.

In the United States, federal and State laws and industry-specific standards require that individuals be notified in case of a data breach that compromises their personal information. Compliance with federal industry-specific requirements may satisfy state breach notification requirements, which vary from State to State. It is important to note that breach notification laws are generally based on the State of residence of the individual whose data was compromised rather than the company's location that suffered the breach. As a result, companies must be aware of the notification requirements for each State where they do business and ensure they comply with all relevant laws and regulations. (* 3).

State Legislation: We can provide an updated list on the National Conference of State Legislators' website where the legislation per State is on the internet link: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (* 3).

Example of Florida State Legislation:

In Florida, stringent laws are in place to safeguard personal and financial data, mandating prompt disclosure of any breaches. For the private sector, compliance is required under Fla. Stat. § 501.171, while the governmental sector falls under the purview of Fla. Stat. § 501.171 (* 3). These statutes outline the legal obligations of organizations operating in Florida, emphasizing the importance of transparency and accountability in handling data breaches. By enforcing these laws, Florida aims to enhance data security and protect individuals' sensitive information from unauthorized access or misuse. Compliance with these regulations is essential for private and governmental entities to uphold consumer trust and mitigate the impact of data breaches on individuals and organizations. (* 3).

In conclusion, cybersecurity frameworks and laws are a world to explore, and it can depend on which industry the lawyer works in. We can predict that the lawyers will specialize in each sector and framework and will have to lead the battle for the security and reliability of the data.

XI. The Federal Healthcare Law, Regulations, and Framework in the US.

Like other sectors, the medical industry is subject to various laws and regulations governing Cybersecurity to protect patient data and ensure the integrity of healthcare systems. Some of the critical rules and regulations related to Cybersecurity in the medical industry include:

1) **Health Insurance Portability and Accountability Act** (HIPAA): HIPAA is perhaps the most well-known regulation governing healthcare data security in the United States. It sets standards for protecting sensitive patient health information, known as protected

health information (PHI). HIPAA includes the Security Rule, which outlines specific safeguards that covered entities and their business associates must implement to ensure the confidentiality, integrity, and availability of electronic PHI (ePHI).

HIPAA is a law that aims to improve access to health insurance and ensure the security and privacy of electronic health-related data. It requires covered entities to implement policies and procedures to protect electronic health information from unauthorized access, use, or disclosure and to mitigate any harmful effects of security incidents. These policies and procedures include national standards for electronic transmission, unique health identifiers, security standards, and privacy standards. **Covered entities must also be prepared to identify, document, and respond to suspected or known security incidents. Compliance with HIPAA's security standards is required for most covered entities as of April 21, 2005, with a later deadline for small health plans. (* 10 and * 4).** As a result, HIPAA requires all healthcare organizations to implement policies and procedures to address security Incidents.

2) **Health Information Technology for Economic and Clinical Health Act (HITECH)** was enacted as part of the American Recovery and Reinvestment Act (ARRA) 2009. It aims to promote

the adoption and meaningful use of electronic health records (EHRs) and includes provisions to strengthen HIPAA's privacy and security requirements. HITECH introduced breach notification requirements for covered entities and business associates in case of a breach involving unsecured PHI. By implementing these policies and procedures according to each organization's characteristics, needs, and size, healthcare organizations can better protect their electronic health information from potential cyber threats and comply with HIPAA regulations.

3) **General Data Protection Regulation (GDPR)**: While GDPR is a European Union regulation, it has implications for healthcare organizations worldwide if they process data of EU residents. GDPR imposes strict requirements for the processing and protection personal data, including healthcare data. Healthcare organizations must ensure compliance with GDPR when handling patient data, mainly if patients are in the EU.
4) **The Health Information Trust Alliance (HITRUST):** While not a law or regulation, HITRUST provides a **comprehensive framework** for healthcare organizations to effectively manage their cybersecurity and compliance efforts. It incorporates industry

standards and regulatory requirements, including HIPAA, into a unified framework to streamline compliance and mitigate cybersecurity risks.

5) **Medical Device Regulation (MDR):** MDR applies specifically to medical devices and aims to ensure their safety and effectiveness. While primarily focused on product safety, MDR also includes provisions related to Cybersecurity, requiring medical device manufacturers to implement appropriate cybersecurity measures to protect against potential threats to patient safety and data security.

These are just a few examples of the laws and regulations healthcare organizations must navigate to ensure compliance and safeguard patient data in an increasingly digitized healthcare landscape. Healthcare organizations must stay informed about evolving cybersecurity regulations and best practices to protect patient information and mitigate cybersecurity risks.

The role of the Cybersecurity lawyer in the medical industry is essential to keep the organizations informed and in compliance with all laws and regulations of the industry.

XII. Cybersecurity Attacks, Ransomware, and Policies to Prevent the Incidents

Ransomware Attacks are malicious software, also known as malware, that can infect computers and networks — spying on users, disrupting operations, or stealing data. Ransomware is one of the most common types of malware. It locks the target's data or device, holding it ransom unless the target pays off the cyber attacker. (*16)

In 2023, IBM estimated that ransomware attacks cost victims $30 billion, covering ransom payments and broader disruptions. Ransomware encrypts data, making it inaccessible until a ransom is paid. Attack methods have evolved, with phishing emails being a common vector, causing 45% of ransomware attacks in 2021. Other methods include exploiting system vulnerabilities and credential theft. Interestingly, the percentage of victims paying ransoms dropped from 85% in early 2019 to 37% by late 2022, indicating a shift in response strategies, likely due to increased awareness and alternative mitigation techniques. However, ransomware remains a persistent threat, demanding ongoing vigilance and proactive defenses. (*16)

The role of the Cybersecurity lawyer in creating the Cybersecurity policy mentioned above is pivotal. As legal experts specializing in cybersecurity law, they bring valuable insights and expertise to developing and implementing policies to mitigate cyber threats, particularly ransomware attacks.

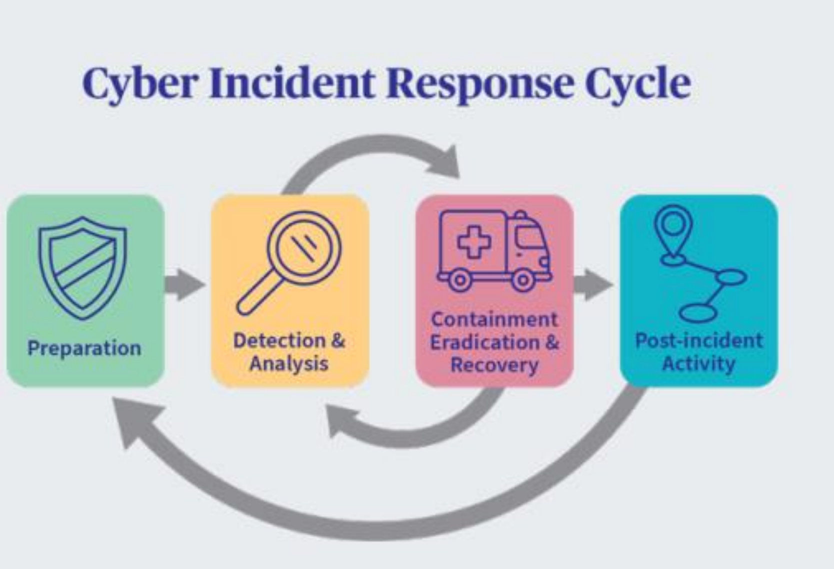
Cybersecurity lawyers ensure the policy aligns with relevant laws, regulations, and industry best practices, reducing legal risks and ensuring compliance. They may also guide liability issues, contractual obligations, and incident response procedures within the policy framework. Additionally, Cybersecurity lawyers play a crucial role in assessing the legal implications of ransomware incidents and advising on strategies to address them effectively. Their involvement ensures the policy is comprehensive, legally sound, and tailored to the organization's needs and regulatory requirements.

Policies and cybersecurity attacks, particularly ransomware attacks, are of paramount concern in today's digital landscape. Cyber threats, such as malware, phishing, denial of service, man-in-the-middle attacks, and ransomware, pose significant risks to organizations. Ransomware, in particular, is malicious software that can deny access to files or data, often demanding electronic currency payment for their release. In response to this threat, implementing a ransomware policy is crucial. This policy, overseen by the Chief Security Officer, encompasses a range of activities to minimize risk and enhance recovery capabilities in the event of a ransomware attack. These activities include risk assessment, analysis, and treatment, antivirus installations, establishing policies and procedures for risk management, backup policies and procedures, and training initiatives to mitigate social engineering threats.

XIII. How can the Cybersecurity Lawyer help create the incident response plan based on Cybersecurity

Policies?

A Cybersecurity lawyer is crucial within the medical industry to ensure organizations respond to the attacks according to each organization's characteristics and the industry laws and regulations. We will explore how the Cybersecurity lawyer can be an asset in the NIST's Cyber Incident Response Cycle.


Cyber Incident Response Cycle
Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-incident Activity

(*15 p28)

In response to a cybersecurity attack, an organization must have a comprehensive strategy in place.

1) Preparation:

First, it includes having a Cybersecurity Plan outlining protocols and procedures to mitigate and respond to threats effectively. It has to be tailored to each organization and in compliance with the applicable laws of the industry :

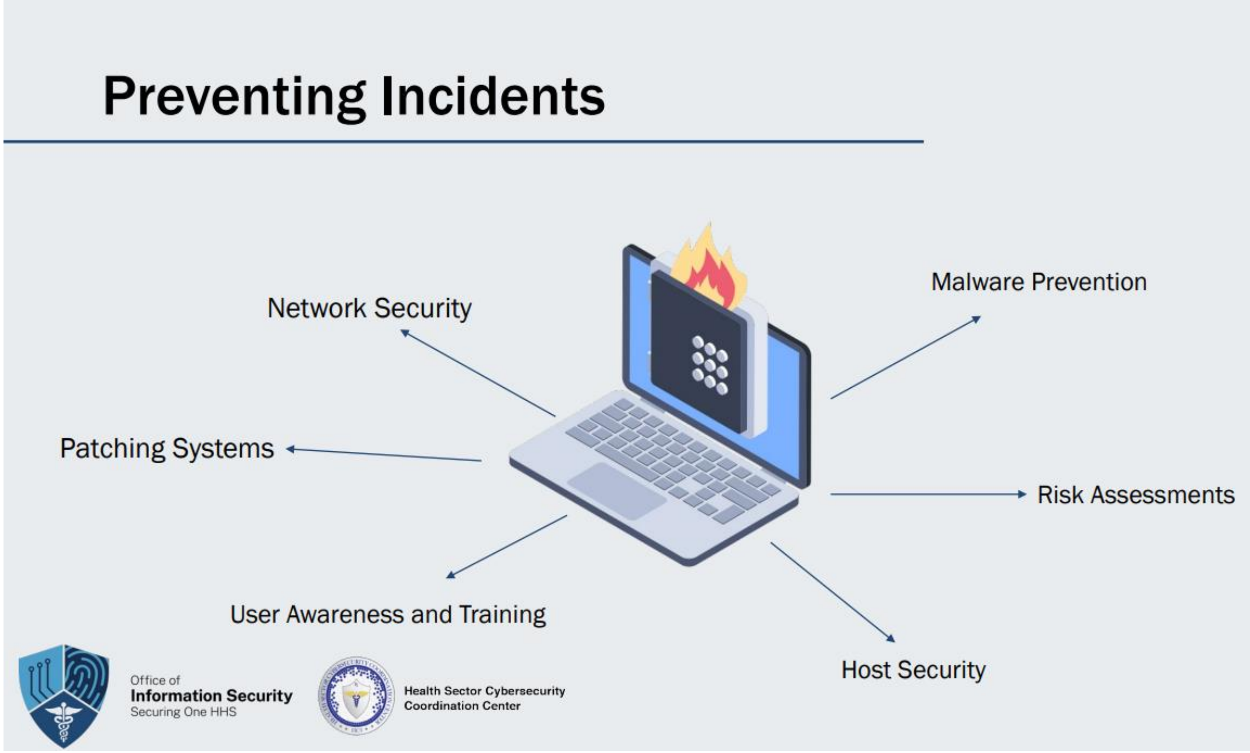
"• Identifying Assets and Risks: Can include hardware, software, networks, and personnel

• Creating specialized response teams

• Identifying tools and resources needed

• NIST recommends classifying incidents based on severity and impact.

• Organizations can tailor response strategies to be more effective." (*15 p28)



Preventing Incidents

Network Security

Malware Prevention

Patching Systems

Risk Assessments

User Awareness and Training

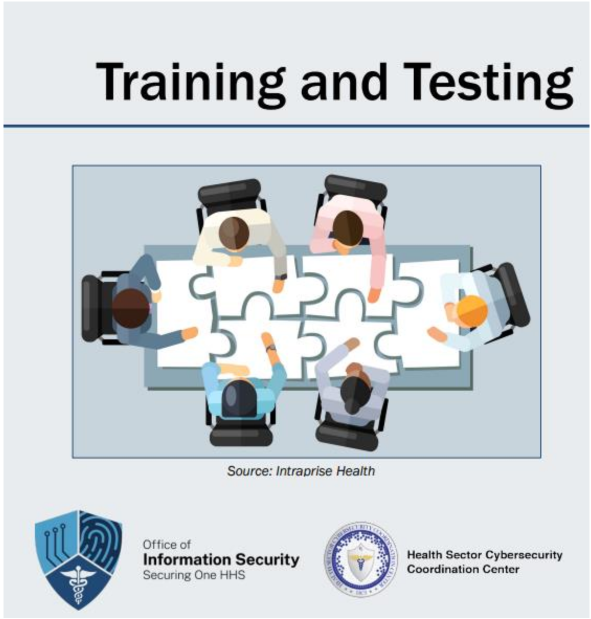
Host Security

Office of Information Security Securing One HHS

Health Sector Cybersecurity Coordination Center

(*Id. p31)

The Cybersecurity Lawyer has a fundamental role in the training and tabletop exercises to test and prevent all the plans created to identify any weakness before any cyber-attack occurs. Before an incident occurs, it is imperative to test established procedures and policies to ensure their efficacy.



Training and Testing

Source: Intraprise Health

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

(*Id p32)

Training and Testing involves various steps:

- Validation of accuracy and usefulness to ascertain their practicality.
- Communication testing to ensure a smooth flow of information during crises.
- Verify the functionality of tools required for implementation.
- Conducting tabletop exercises to simulate real-life scenarios and evaluate response mechanisms.
- Non-IT functions should be considered, such as reverting to pen and paper for documentation and diverting patients if necessary. These measures collectively ensure preparedness and effectiveness in managing potential incidents. (Id. p32)

2. Detection & Analysis:

Secondly, understanding the organization's tools and establishing a baseline normal state is crucial. By knowing the typical functioning of systems and networks, anomalies indicating potential breaches can be detected more readily. It is relevant to understand that when a possible security breach is noticed, it has to be investigated because it can lead to discovering that the organization is hacked. It happens with the ransomware attacks that are in place long before the organization notices it.

In Cybersecurity, understanding the most common types of attacks is crucial for effective defense strategies. Among these, some stand out for their prevalence and potential impact. Phishing, often executed through email, remains one of the most pervasive threats, where attackers use deceptive messages or attachments to trick recipients into divulging sensitive information or unwittingly installing malware. Another significant attack vector is external or removable media, such as USB drives, which can carry malware and initiate unauthorized access when plugged into a system. Web-based attacks, including cross-site scripting and redirection to malicious sites, exploit vulnerabilities in websites or web applications to compromise user data or spread malware.

Additionally, impersonation attacks, like spoofing or man-in-the-middle attacks, undermine trust by masquerading as legitimate entities or intercepting communications. These attacks highlight the diverse tactics that cybercriminals employ to infiltrate systems. Cybersecurity measures to mitigate risks and safeguard digital assets are critical solutions to prevent these attacks.

3. Response: Containment, Eradication, and Recovery and the Cybersecurity Lawyer Role

In their place, determining whether a response should be "live" or "static" is paramount but as critical as the other points. This decision hinges on whether immediate action is required to contain an ongoing breach or if a more methodical or systematic approach, such as forensic analysis, is appropriate.

The response has fundamental steps: Containment, Eradication, and Recovery. Even if these steps require heavy technical work, the Cybersecurity lawyer can organize the response to the press and users, manage the legal response to the incident, and report to the agencies involved according to the law. This work eliminates pressure on the IT Department and helps them concentrate on the technical incident response.

Some of the Best practices recommended by NIST and the Health Sector Cybersecurity Coordination Center are:

- Timely response: A swift response is essential to contain and eradicate the threat.
- Detailed Analysis: Conducting a post-incident analysis to understand how the breach occurred is essential.
- Patch Management: Keeping software and systems up to date helps prevent known vulnerabilities from being exploited.
- Monitoring and Validation: Monitoring the network after eradication to ensure the threat has been eliminated." (Id p40)

4. Post-Incident Activity

Some of the best practices recommended previously give plenty of room to the lawyer Cybersecurity to help the organization and be an asset working in collaboration with the IT Department: A detailed analysis and post-incident activity is a field where the Cybersecurity lawyer can help powerfully to improve the policies and prevent future incidents.

While elaborating on these points is beyond the scope of this article, it is evident that the Cybersecurity Lawyer, in coordination with the IT Department, has a pivotal role in each aspect of this response framework.

The Cybersecurity Lawyer is a linchpin in orchestrating the organization's response to cyber threats. They contribute to developing and refining the Cybersecurity Plan, ensuring legal compliance and alignment with industry best practices. Moreover, their expertise allows them to effectively navigate the organization's tools and establish a baseline normal state. In the event of a breach, the Cybersecurity Lawyer plays a critical role in determining the appropriate response strategy, weighing legal considerations and potential ramifications.

Their involvement is indispensable in safeguarding the organization's interests and ensuring a swift and effective response to cybersecurity incidents. Thus, while the intricacies of these response elements may vary, the presence of a skilled Cybersecurity Lawyer is essential to bolstering the organization's cyber resilience. (* 2).

XIV. Conclusion

In conclusion, including the figure of a Cybersecurity Lawyer is a necessity for the new digital world to manage the law and the legal response in coordination with the IT Department: (1) preventing cybersecurity attacks, creating strong policies and contingency plans before the incidents that comply with the laws, regulations for the industry and best practices, (2) during the attacks the lawyer can handle the response to the press, users, hackers and establish a legal strategy to mitigate damages, and (3) after the incident the lawyer must improve the policies and prevention plans in coordination with the IT department and the directors of the organization.

The medical industry and all organizations could manage cybersecurity risks and incidents more efficiently while ensuring compliance with regulatory requirements and industry best practices.

References

*** 1 NI**ST Information Technology Laboratory. COMPUTER SECURITY RESOURCE CENTER
Retrieved from Internet 4/15/2024
https://csrc.nist.gov/glossary/term/Cyber_Attack
(Source CNSSI 4009-2015 under attack / NISTIR 8323r1 under attack from CNSSI 4009-2015 /NISTIR 8401 under attack) and (NIST SP 1800-10B from NIST SP 800-30 Rev. 1, NIST SP 800-30 Rev. 1 from CNSSI 4009, NIST SP 800-39 from CNSSI 4009).

*** 1.4** American Bar Association. Description. Speaker *Linn F. Freedman*, Partner, and Chair of Data Privacy & Cybersecurity Team, Robinson & Cole LLP, Providence, RI.
Retrieved from Internet 4/15/2024
https://www.americanbar.org/careercenter/career-choice-series/cybersecurity-law/

*** 2** Conferences of Mary Frantz from Enterprise Knowledge Partners LLC at Nova Southeastern University. Winter 2023.

*** 3** (See HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414

Retrieved from Internet 4/15/24
Publication of US Department and Human Services:
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html#:~:text=These%20individual%20notifications%20must%20be,the%20breach%2C%20the%20steps%20affected Retrieved 7/7/23)

* 4 See Summary of the HIPAA Security Rule, U.S. Department of Health and Human Services. (2016). Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Retrieved from Internet 4/15/2024
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html and HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414

*** 5** 7 Cybersecurity Frameworks That Help Reduce Cyber Risk POLICY & REGULATIONS by Eric Cisternelli March 31, 2023, Retrieved on 7/7/23 7 Cybersecurity Frameworks To Reduce Cyber Risk (bitsight.com))

*** 7** Ransomware Attack: Incident Response Plan and Action Items By Anusthika Jeyashankar July 9, 202 / Retrieved from Internet 4/15/2024
https://www.socinvestigation.com/ransomware-attack-incident-response-plan-and-action-items/

* 8 The Cyber Resilience Act
https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html
* 9 **Advant Beiten** - Daniel Trunk March 22, 2024
Retrieved from Internet 4/15/2024
The Cyber Resilience Act: What You Should Know Now
https://www.lexology.com/library/detail.aspx?g=94ed5607-d8d0-40ac-944c-ca1bfc3ec6c9#:~:text=Almost%20unnoticed%20in%20the%20shadow,Parliament%20on%20March%2012%2C%202024.

*10   Incident Response Plan from NIST :
National Institute of Standards and Technology (NIST) 10/12/2023 Page 25
202310121300_Cybersecurity Incident Response Plans_TLPCLEAR
Retrieved from Internet 4/15/2024
https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf

*11 Incident Response Plan Policy from NIST :
National Institute of Standards and Technology (NIST) 10/12/2023 Page 21
Retrieved from Internet 4/15/2024
202310121300_Cybersecurity Incident Response Plans_TLPCLEAR
https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf

*12 NIST Special Publication 800-63: Digital Identity

Retrieved from internet 4/15/2024 Guidelines: https://www.nist.gov/special-publication-800-63

*13 HHS 405(d) Task Group: Health Industry Cybersecurity Practices (HICP) Resources: Retrieved from internet 4/15/2024 https://405d.hhs.gov/resources

*14 NIST Cybersecurity Insights: Phishing Resistance – Protecting the Keys to Your Kingdom, Retrieved from Internet 4/15/2024:

https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom

*15 Incident Response Plan Policy from NIST :
National Institute of Standards and Technology (NIST) 10/12/2023 Page 28-40
Retrieved from Internet 4/15/2024
202310121300_Cybersecurity Incident Response Plans_TLPCLEAR
https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf

*16 Famous Ransomware Attacks in History
Written by: **University of Tulsa** • January 22, 2024
Retrieved from Internet 4/15/2024
https://online.utulsa.edu/blog/famous-ransomware-attacks-in-history/#:~:text=WannaCry%20(2017)&text=However%2C%20many%20users%20hadn't,cost%20an%20estimated%20%244%20billion