



PERITUS
SECURITY PARTNERS

The Peritus Approach to Information Security Compliance

Complying with new MA Resident Personal information Regulation 201CMR17

By: Charles Christianson, President Co-Founder, Peritus Security Partners

ABSTRACT

Peritus Security has developed an innovative approach to information security compliance as it relates to both federal and state regulations. Specifically, we have assembled the resources that businesses need to achieve compliance with 201CMR17 – the new MA Resident Personal Information Security Regulation. In this document, we will discuss the assessment, WISP creation and remediation processes that virtually every business in the state will need to follow in order to ensure compliance with the very comprehensive regulation.

Information Security protects your most valued asset – your customer!

As business owners and executives, we all have a tendency to push back against regulation of any kind. In fact, I agree that we are largely over regulated. Aside from all of the business hurdles that this regulation will undoubtedly create, look at this from the consumer's side. In the past year and a half, there have been approximately 470 breaches reported to the State of MA compromising over 700,000 MA residents personal information (yes folks, that is you and me) and that is with only about 1/3 of all breaches actually being reported. So when you go to the corner store and hand out your debit card, think twice about how responsible that company is with your personal information and how you would react when you find out that your information was stolen or leaked to a third party who may try to steal your hard earned money or even worse your identity. 700,000 represents approximately 10% of your friends and neighbors statewide, maybe even you! It takes a nationwide concerted effort on behalf of business to protect consumer information and the State of MA felt the need to get this on the books so that there is recourse for those that handle this information improperly.

Information Security is more than any one product – it is a process

Information Security is more than any product or service, it is a combination of technological solutions that physically secure a network, properly developed and implemented policies, procedures and controls; and equally important - employee training and awareness.

Each of these components represent a key to the puzzle and each are equally important in a well-crafted Written Information Security Program (hereinafter WISP). Peritus has developed

a modular system whereby we address all of the key components of a sound information security strategy and also the long-term management of the WISP.

When a business is faced with complying with a state or federal information security regulation such as Massachusetts 201CMR17, the first reaction is usually to ask what do we need to do to comply? This is of course a reasonable question and to answer this requires a formal Information Security Compliance Assessment. Through the Assessment process, we can determine where our strengths and weaknesses are and most importantly where risk lies.

What Makes Peritus Different?

The Peritus team is made up of highly skilled professionals who have been working in the IT industry, specifically the Information Security sector, for many years. We pride ourselves in taking the complex and breaking it down into the understandable.

Peritus begins by taking an internationally accepted Information Security Framework known as ISO 27001 and applying it to the new regulation. The value in taking this approach is that it applies a known set of principals to the regulation so that the resulting Written Information Security Program (WISP) is consistent with industry standards. ISO27001 is a very broad and detailed standard that, in its entirety, exceeds the scale and scope of 201CMR17 and is beyond the reach of most small to medium businesses. However, Peritus has taken key parts of the ISO and mapped it directly to various regulations, most recently to 201CMR17 resulting in a repeatable, actionable document that can predictably guide a business toward compliance.

The Peritus team comes from a variety of IT backgrounds giving us a unique

insight into best practices and the application of technology to mitigate the various threats and risks that are identified in the assessment process. Coupled with our extensive knowledge of Information Security compliance with a variety of state and federal regulations, we are in a position to provide practical yet effective recommendations along with a roadmap to compliance that is both technically sound but also within reach. We also focus on common sense recommendations for remediation and implementation of various controls.

With almost 25 years experience running our own businesses, we understand the challenges of training staff and creating the necessary level of awareness for IS best practices. We also understand the challenges we all face when it comes to allocating hard earned resources to regulatory requirements.

Compliance Assessment (PHASE 1)

Peritus has developed an innovative approach to providing businesses with the most comprehensive assessment that has been specially designed to meet the compliance requirements of the MA 201CMR17 regulation. This easy-to-use tool empowers the client to compile the necessary information to provide a comprehensive assessment. Peritus has broken down the complex regulation into a series of simple yes/no questions. Each page of the questionnaire includes:

- A copy of the specific provision being addressed as it appears in the regulation.
- A detailed discussion of the provision in layman's terms that helps you understand what the State is asking, why they are requiring the provision and the underlying intent.
- A video discussion of the provision with the necessary background to help the client truly understand what is being asked of them. This

component is important and will count toward education requirements in the regulation.

- A single yes/no/I don't know question and the ability to upload information when appropriate

The resulting information is then collected and transmitted to Peritus for review and analysis. Upon completion of our analysis, Peritus creates a formal compliance assessment report that includes our findings along with recommendations and a roadmap to remediation (SOLUTION). This document shall be reviewed and signed by an Information Security professional who holds the designation of (CISA) Certified Information Systems Auditor.

The document will then serve as your guide to complying with the complexities of the regulation and will act as a concrete record of your efforts to embark on a path to compliance.

We also realize that an assessment is not a one size fits all process. If your organization is complex and exceeds the scope of the Peritus online compliance assessment, we recommend that you engage a security professional (Peritus) for a formal third party IS Assessment.

Written Information Security Program (WISP) (Phase 2)

In accordance with 201CMR17.03, *"Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information."*

A written information security program is basically your handbook to compliance. In it, you will have all of the policies, procedures and controls necessary to

implement, manage and monitor your WISP.

Some businesses may already have all or part of a WISP while others may need to start from scratch. For those with all or part of a WISP, it is critical that it be reviewed by a qualified IS professional who can help you modify it as necessary to become compliant with 201CMR17. Those who need to start from scratch will need help from an IS professional to ensure that the WISP is comprehensive and meets all of the requirements outlined in the regulation.

In either case, Peritus is in a position to help you. Whether reviewing what you have and making recommendations or providing you with a WISP, Peritus has a program that will ensure that this key component is addressed properly and in a cost effective manner. It is essential that this document be written properly to ensure that you are both compliant and more importantly creating a truly secure environment.

Remediation (Phase 3)

Peritus is focused on providing you with quality compliance documentation and procedures but more importantly actionable recommendations that will not only satisfy regulators but will actually improve your information security posture.

In our effort to provide a complete compliance solution, Peritus has assembled a group of trusted partners to help with various technological solutions to help bring your organization into compliance. Our goal is to create a one stop solution to your compliance efforts.

Training and Education:

Our greatest challenge in moving our organizations toward compliance will likely be the changing of our culture. Getting staff to understand the need to

use, much less, change passwords or to restrict access to regulated data, encryption, etc., will be a challenge. We have been conditioned into making convenience the highest priority and we are now being asked to put security before convenience. Once people are educated on the need for security, the threats that exist and the repercussions of failing to comply, it becomes much easier to change culture. Peritus can provide you and your employees with the knowledge necessary to understand the compliance requirements and use a best practices framework to protect valuable MA resident personal data.

Ongoing Maintenance and Review

Part of the compliance process is to provide for frequent review of the WISP. The review process is important because it needs to take into account any changes in the business that require modifications to the WISP. It is highly recommended that an objective third party perform an annual IS Compliance Assessment to ensure that you maintain an adequate level of compliance.

Who Should I Look to for Help?

IS Compliance is multifaceted. To create an effective WISP or accurate assessment, it is necessary to have someone who is trained in information security compliance. Your local "computer guy" may be helpful during remediation but he is not likely to be qualified to assist in writing policy or rendering opinion on compliance. Likewise, any work that is done by a qualified IS professional should be reviewed by your attorney for legal accuracy. Once in place, the WISP should be relatively easy to enforce, maintain and revise. But, it is critical that you get it right in order to mitigate the risk of being fined as a result of a breach or error in reporting. These fines could easily put you out of business and/or prove damaging to your company's reputation.