



# The State of Application Security

Are Compliance Regulations Lagging?



## Introduction

Sony, Facebook, Twitter, WordPress, Iranian State sites. As the hacking continues through Cloud and Web applications, one has to wonder who's on first? With over 250M websites out there and mobile apps being published continuously, most of which are insecure, hackers have a huge pool of targets. Inertia, budget and lack of knowledge are the common reasons behind lack of efforts in securing applications. If the risk of getting hacked isn't enough of a motivating factor, what would drive companies to protect their applications? What about regulations?

Let's look at some of the existing regulations and see why these haven't been a driving force for organizations to improve security for their Cloud, Mobile and Web applications.

## Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA), also known as The Financial Modernization Act of 1999, was enacted to ensure protection over customer's records and information. Rules and provisions make up the requirements for financial institutions to (a) ensure protection of the security and confidentiality of customer's nonpublic personal information, (b) implement administrative, technical, and physical safeguards, (c) protect against anticipated threats and hazards to information security, and (d) protect against unauthorized access to or use of information. Sounds good, right?

If we just focus on the sections on Access Control (as clarified by FFIEC), there are various subsections that provide guidance on Authentication, Network Access, Operating System Access, Application Access and Remote Access. If we zoom in further into Application Access, here's roughly what we get: "Financial institutions should control access to applications by:

- Using authentication and authorization controls appropriately robust for the risk of the application
- Monitoring access rights to ensure they are the minimum required for the user's current business needs
- Using time-of-day limitations on access as appropriate
- Logging access and security events
- Using software that enables rapid analysis of user activities

All valid points but no mention of secure code or application vulnerabilities.

## Health Insurance Portability and Accountability Act (HIPAA)

In 1996, the Health Insurance Portability and Accountability Act or the HIPAA was endorsed by the U.S. Congress. The HIPAA Privacy Rule, also called the Standards for Privacy of Individually Identifiable Health Information, provided the first nationally-recognizable regulations for the use/disclosure of an individual's health information.

Without going into all the other details, if we just look at the Technical Safeguards of the HIPAA law, here's what's covered:

### Access Control

A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information

### Audit Controls

A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI;

### Integrity Controls

A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.



### **Transmission Security**

A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

Again, a lot of details about access controls which are good and required but no details on web applications and securing the code.

### **The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)**

The North American Electric Reliability Corporation (NERC) is a nonprofit corporation designed to “ensure that the bulk electric system in North America is reliable, adequate and secure.” NERC maintains comprehensive reliability standards that define requirements for planning and operating the collective bulk power system. Among these are the Critical Infrastructure Protection (CIP) Cyber Security Standards, which are intended to ensure the protection of the Critical Cyber Assets that control or effect the reliability of North America’s bulk electric systems. In 2006, the Federal Energy Regulatory Commission (FERC) approved the Security and Reliability Standards proposed by NERC, making the CIP Cyber Security Standards mandatory and enforceable across all users, owners and operators of the bulk-power system. Here’s the description of a requirement 4 in CIP: Cyber Vulnerability Assessment – the Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually.

The vulnerability assessment shall include, at a minimum, the following:

#### **R4.1**

A document identifying the vulnerability assessment process

#### **R4.2**

A review to verify that only ports and services required for operations at these access points are enabled

#### **R4.3**

The discovery of all access points to the Electronic Security Perimeter

#### **R4.4**

A review of controls for default accounts, passwords, and network management community strings

#### **R4.5**

Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan

Again, there is no specificity on web applications and finding vulnerabilities or including a remediation plan, etc.

### **The Federal Information Security Management Act (FISMA)**

The Federal Information Security Management Act (FISMA) requires that all federal agencies document and implement controls for information technology systems that support their operations and assets. Standards and guidelines have been developed and published by the National Institute of Standards and Technology (NIST). FISMA and NIST guidelines do a fairly reasonable job of defining various controls under System and Communications Protection Controls. Some of the controls in this section include cryptography, mobile code, virtualization, session authenticity, information at rest etc. The standard and the NIST guidance also talks about security controls to assess and monitor all systems on a regular basis.

Although this regulation is better about security than others, it falls short of calling out comprehensive application security processes.



## The Payment Card Industry (PCI) Data Security Standard (DSS)

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. PCI has come closest to defining and emphasizing web applications security in its standard.

Requirement 6.6 clearly defines the requirement for securing web applications: For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes
- Installing a web-application firewall in front of public-facing web applications

A couple of issues that continue to plague PCI DSS as it relates to web application security are:

1. Option of having a web-application firewall (WAF) or assessment of web applications
2. Enforcement. For the first issue, this option encouraged a lot of companies to just install a WAF and get compliant without going through a rigorous process of assessing applications.

The actual requirement should be to assess all applications on a regular basis and either fix the critical vulnerabilities or use a WAF to block until those are fixed. In other words, you need both. As far as the second issue goes, enforcement is supposed to be done by the five credit card companies (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.) through acquiring banks. But enforcement of these standards has been focused on only the big merchants leaving millions of non-compliant merchants with insecure web applications.

## Other Regulations

In addition to these, there are a number of other regulations like SOX, California SB 1386 and AB 1950, Massachusetts Data Privacy Laws, and many others. Most of these are at a much higher level in terms of data breaches and consumer information protection. None of these specifically go into application security issues.

## Summary

So, what does this all mean? Do we really need more regulations? While too many regulations can be bureaucratic and costly to administer, sometimes you have no choice. Desperate situations require desperate measures. With over 75 percent of attacks occurring through the web application layer, more emphasis needs to be placed on protecting this infrastructure.

As billions of users are going on the Internet and shopping or entering their personal information into Cloud, Mobile and Web applications, most of which are insecure, it is only a matter of time before their information will be stolen. Our critical defense infrastructure and intellectual property is also susceptible to major cyber war types of attacks which have been occurring on a regular frequency now. For smaller merchants, we should provide tax incentives and loans to encourage them to protect their applications.

We don't necessarily need another new regulation, but it's time to update all the old standards to provide more clarity and enforcement guidelines around protecting applications.



## About Cenzic

Cenzic provides an application security intelligence platform to continuously assess Cloud, Mobile and Web vulnerabilities. This helps brands of all sizes protect their reputation and manage security risk in the face of malicious attacks. Today, Cenzic secures more than half a million online applications and trillions of dollars of commerce for Fortune 1000 companies, all major security companies, government agencies, universities and SMBs.

## Cenzic Products

Cenzic Enterprise	Cenzic Enterprise is a software solution that assesses the security of Cloud and Web applications and supports security risk management throughout the software development lifecycle. Cenzic Enterprise provides a company-wide view of security vulnerabilities and status to executives as well as customized views for other users from a Web-based dashboard.
Cenzic Desktop	Cenzic Desktop is a single-user version of Cenzic Enterprise. It is designed for the power user that wants to run their security assessments on Cloud and Web applications from a single system.
Cenzic Managed Cloud	With Cenzic Managed Cloud, Cenzic's security experts remotely perform full vulnerability testing on Cloud, Mobile and Web applications. From a Web-based dashboard, users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Cloud	Cenzic Cloud allows users to test their own Cloud and Web applications for basic attacks and receive actionable results all within their own Web portal – no security experts needed.
Cenzic Hybrid – Software + Cloud	Cenzic Hybrid provides access to both Cenzic Enterprise software and Cenzic Managed Cloud services. Vulnerability testing can be done either by using the software on premise or by leveraging Cenzic's expert security services team.
Cenzic Mobile	Cenzic Mobile service is delivered as a managed service. Cenzic's security experts remotely perform full vulnerability testing on mobile applications. All testing is managed from a Web-based dashboard where users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Services	Cenzic services and training help those responsible for Cloud, Mobile and Web application security to implement best practices and procedures to protect data from hacker attacks.