The HITECH Act: The Teeth and Claws of HIPAA

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

The HITECH Act - Some Background

The Health Information Technology for Economic & Clinical Health (HITECH) act really does 'up the ante' for HIPAA enforcement.

> *Many healthcare and insurance providers require the waiver of HIPAA rights as a condition of service*

In theory, Health organizations have had to comply with the Health Insurance Portability and Accountability Act (HIPAA) since its introduction in 1996. Originally HIPAA was introduced by congress to protect the health insurance rights of employees made redundant. Additional 'Titles' to the act were introduced including 'Title 2' which was designed to protect electronically stored data relating to patient health information – often referred to as 'Protected Health Information' (PHI).

The problem with HIPAA has been the broad interpretation adopted by many healthcare providers and insurers. In fact, many providers require the waiver of HIPAA rights as a condition of service. This has undoubtedly resulted in a varying degree of adoption among providers leaving many unsure as to whether they are or are not considered compliant. But how could you blame them? The requirements aren't specific and there has been little enforcement to speak of.

What is the Impact of HITECH on HIPAA?

The HITECH act as part of the American Recovery and Reinvestment Act aims to change all that with increased penalties for non compliance.

A breach that exposes a patient's confidential data could have serious and lasting consequences. Unlike credit cards for example, which can be cancelled and changed if they are exposed – health care records can't just be changed or re-set. According to data from Forrester Research, criminals are increasingly targeting health care organizations. For security teams within health organizations HITECH's increased penalties may well assist in the justification of funding needed to sure up security and compliance projects that may otherwise have languished under the previously ambivalent and poorly defined HIPAA enforcement.

It is open to debate as to how the federal government will audit compliance with HIPAA's security requirements from here on in, but it widens the number of enforcers by giving State Attorney General's the ability to file federal civil action for harmful disclosures of protected health information (PHI).

There are already cases of lawsuits underway for alleged HIPAA violations due to exposed or breached PHI, likely to end with heavy financial compensation payments being ordered.

Some Good News...

Like all things in life there's usually a process to follow and HIPAA and HITECH are no different. The main headings that will need to be addressed are:

> *"the scope of the standard is quite similar in respect of its approach and its measures to the PCI DSS (The Payment Card Industry Data Security Standard)..."*

- ***Administrative Safeguards*** – Specifically written evidence of measures adopted to ensure compliance. Internal auditing in particular change management processes, approvals and documentation to provide evidence that systems and process is properly governed.
- ***Physical Safeguards*** – Including access controls, restrict and control access to equipment containing PHI information. This will include the use of Firewalls, Intrusion Protection technology and with particular focus on workstation, mobile/ remote worker security.
- ***Technical Safeguards*** - Configuration *'hardening'*, to ensure that known threats and vulnerabilities are eliminated from all systems, with a zealous patch management process combined with anti-virus technology, regularly tested and verified as secure. Strong Monitoring for security incidents and events, with all event logs being securely retained is also a key measure to safeguard IT system security.

Sounds Familiar...?

In fact, the scope of the standard is quite similar in respect of its approach and its measures to the PCI DSS (The Payment Card Industry Data Security Standard), which is another security standard all healthcare providers will now be familiar with.

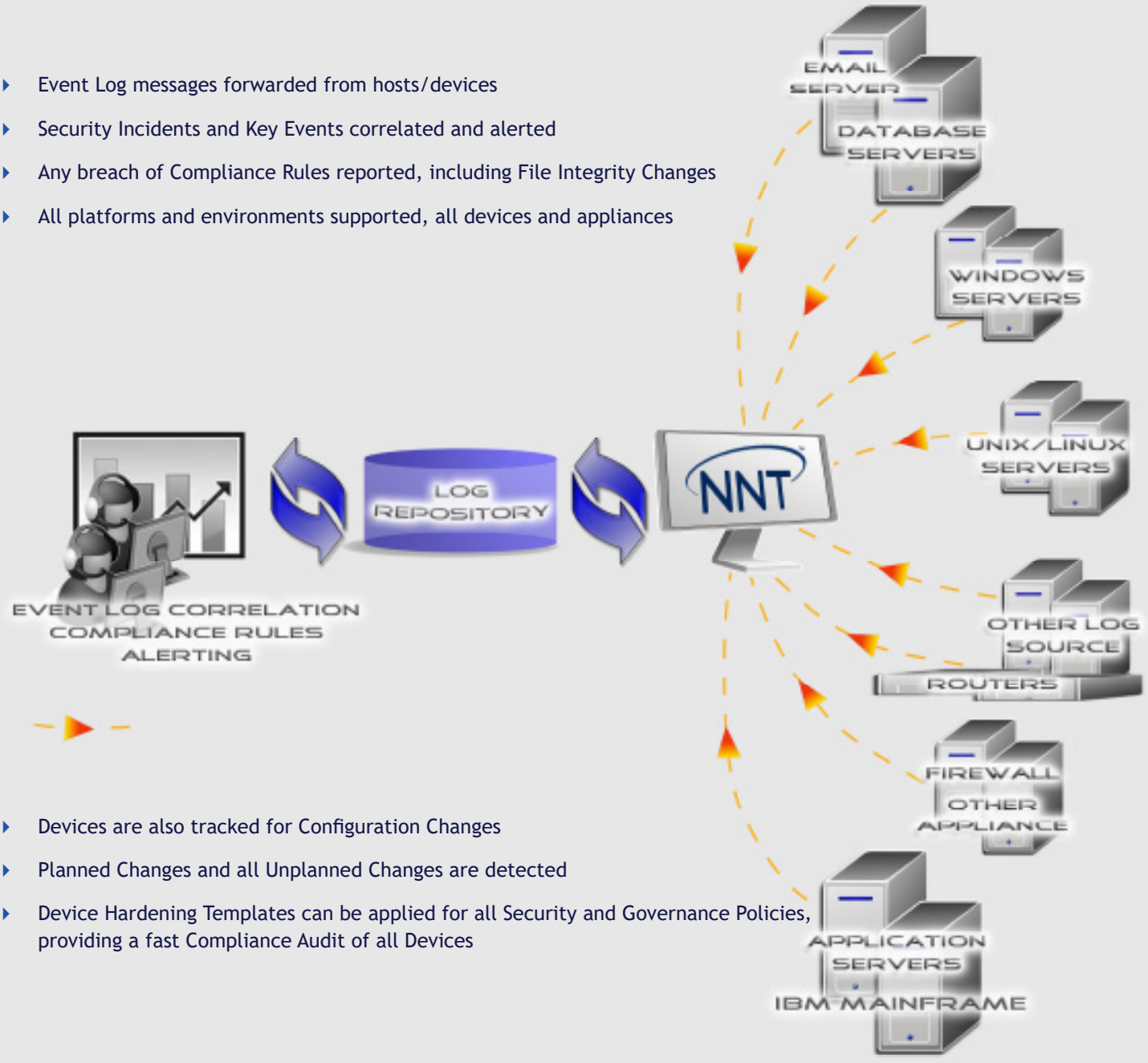
> *"the same technology that helps deliver HIPAA compliance should be relevant for PCI DSS...compliance with one will significantly assist compliance with the other"*

The PCI DSS is concerned with the secure governance of Payment Card data, and any 'card merchant' i.e. an organization handling payment card transactions.

Therefore it makes sense to consider measures for HIPAA compliance in the context of PCI DSS also, since the same technology that helps deliver HIPAA compliance should be relevant for PCI DSS. Or to put it another way – compliance with one will significantly assist compliance with the other.

What Do NNT Provide?

- Event Log messages forwarded from hosts/devices
- Security Incidents and Key Events correlated and alerted
- Any breach of Compliance Rules reported, including File Integrity Changes
- All platforms and environments supported, all devices and appliances



- Devices are also tracked for Configuration Changes
- Planned Changes and all Unplanned Changes are detected
- Device Hardening Templates can be applied for all Security and Governance Policies, providing a fast Compliance Audit of all Devices

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.