



An Elemental Approach to HIPAA-compliance Measures

By Doug Torre, CISSP

The April HIPAA security deadline has passed, but most health care organizations consider that date to be a starting point instead of a deadline.

I was on a call recently with more than 100 New York hospitals, and not one of them said they were completely HIPAA-compliant. Now is the time for testing and validating security measures that will lead health care organizations closer to compliance.

A major issue shared throughout the health care community is a lack of up-to-date visibility into our networks. Because of this, there's no way to know how compliant we are at any point in time, nor what we need to do to bring out-of-compliance systems back in line. Without proper surveillance, there is no way to know how a machine is configured, which patch levels are running, what a machine has access to and which machines communicate with it, its policies, etc. Not knowing what's out there on your network or what's happening prevents you from managing your compliance or risk.

Wanting automation

Another hurdle to HIPAA compliance is a lack of automation -- the ability to roll out necessary policies, check for current compliance status and enforce policies to bring systems back into compliance. At Catholic Health Systems (CHS) in Buffalo, N.Y., where I am director of networking and technical services, our systems and network have changed frequently. Manual updates were labor-intensive, and manual checks on compliance were slow and inefficient. We were looking for tools to automate compliance checks and facilitate our network updates.

These issues are not new. But at CHS we've found a new information security tool that provides sound security policies and practices and can help lead organizations in addressing HIPAA compliance.

With so many products on the market claiming to solve HIPAA-compliance problems, we had considered several security aids for CHS. For example, we evaluated host-based firewalls and configuration controls. We also looked at network management and surveillance tools, such as security event management products. We also considered port-level protection to examine systems and quarantine non-compliant machines.

However, we found a security compliance management solution from San Mateo, Calif.-based Elemental Security that costs about as much as one of those other alternatives, but provides their combined security and compliance functionality, and more.

The Elemental Compliance System is client/server technology that gives visibility into all computers on, or communicating within, our network. It also gives us the means to control or contain machines through automated security policies. We found it unique in that it unifies policy management, host configuration, network access control and discovery/inventory in one tool.

Elemental's centralized view into our dynamic network and policy baselines helps us track and improve our security and compliance posture. The technology takes our stated security plans and policies and implements them throughout our network to automate our discovery of what's going on in our network and how we measure up to our stated policies. It also automates our security and compliance controls. We can measure our performance over time, and evaluate our security confidence level. Security is implemented and maintained without operator intervention.

The solution gives us moment-to-moment information as to what's happening with our computers on the network, all in a unified view. This helps us address the HIPAA requirement to record and examine activity in systems that contain or use electronic protected health information (PHI). Elemental also helps us understand how the network operates and changes over time. It gives us new levels of information, and delivers a new approach to managing security and risk -- not with a quarterly snapshot, but with a current daily view.

If one computer or group of computers does not meet security policy settings, the computer/group can automatically be partitioned to protect sensitive systems and data. If a computer's configuration changes, Elemental can affect policies without our intervention. If a security vulnerability is detected within Windows, we can quickly find out which computers are at risk, and we'll know what to do to fix them.

Elemental also provides granular access controls, based on a computer's current compliance status. This helps us approach the HIPAA regulations to secure electronic PHI and grant access only to those users or software programs that have been granted access rights.

Automatic grouping

One of the technology's features is its automatic dynamic grouping. If security on a computer degrades (e.g., its anti-virus software stops running), it is no longer allowed to communicate with our database server. New computers can either be automatically segregated or added to the network, based on the configuration of the system.

We are interested in building multiple layers of security on our network. In the past, a wall around our network was good enough. However, in today's dynamic environment, we need to take a different approach to monitoring and enforcing security. Security at multiple levels -- the network, groups and individual hosts or users -- makes sense.

Unlike some other solutions we evaluated, this technology complements protection at the perimeter of our network by adding security around every host. Defining and defending the CHS network borders and peering points had been an exercise in futility and decreasing returns. Defending the perimeter alone isn't viable due to our dynamic network and mobile users and hosts. Now we can define security policies where our information resides as well, right down to the host or virtual host grouping.

With Elemental's technology, we are also better prepared for audits, and can now report how our network and hosts are operating at any moment. The technology demonstrates our compliance against policy baselines, and creates a warehouse of compliance details with its logging so we can show what's going on over days, weeks or months.

Even though the HIPAA security deadline has passed, there is still a lot of variability in implementing compliance systems. Some organizations are satisfied with a quarterly or annual vulnerability analysis, but our new technology provides more frequent and more in-depth analysis. This is important because we are always assessing our rules, and how our organization stands against those rules.

HIPAA compliance

Can one tool make you HIPAA compliant? No.

Can you ever be totally compliant or secure? No organization can be 100-percent secure or risk-proof; it's a matter of the tools you use to reduce your risk.

With the necessary visibility into what's going on in your network, and automated controls to fix issues, your organization's IT structure can be stronger than it was before.

Keep in mind that security is a process; there are always opportunities for improvement.

Mr. Torre is director of networking and technical services at Catholic Health Systems in Buffalo, N.Y.