THE CISO GROUP

Compliance For Compliance Sake: A False Sense of Security

January, 2010

Alan Shimel, CEO

Compliance and Security

- Compliance ≠ Security
- Information security compliance represents a regulatory agency's attempt to ensure a reasonable level of security.
- Information security compliance regulations are usually based on best practice security practices
- Good security practice usually leads to being in a compliant state.
- Being compliant does not necessarily lead to being secure
- Security is difficult to legislate

What Is Compliant?

From the Merriam-Webster online dictionary –

com·pli·ant

Pronunciation: \-ənt\

Function: *adjective*

Date: 1642

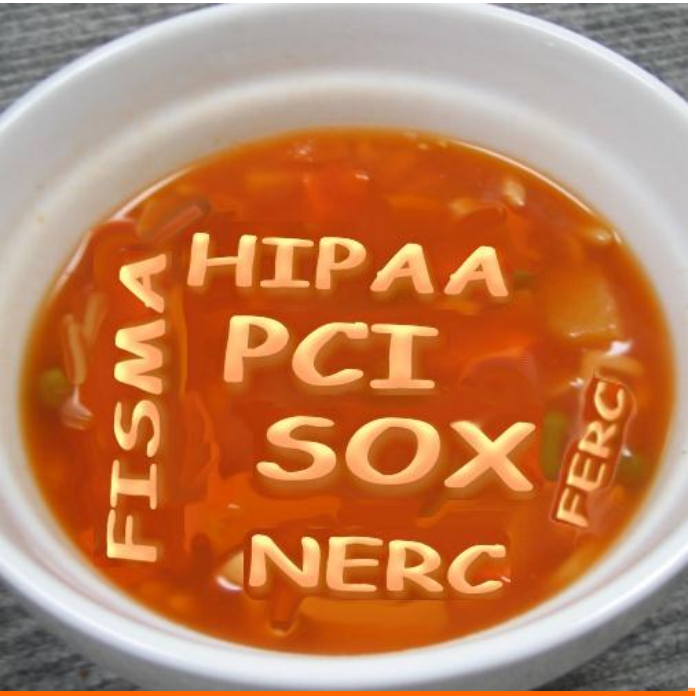
1 : ready or disposed to comply **:** submissive <a corrupt regime aided by a compliant press>

2 : conforming to requirements <compliant software>

Sounds pretty straight forward, right? WRONG!

The Alphabet Soup of Compliance

- Compliance has become a Tower of Babel with everyone speaking different tongues
- Overlapping regulations sow confusion
- The race is on to comply for compliance sake alone
- In conforming to compliance requirements we lose sight of why those requirements are there to begin with?



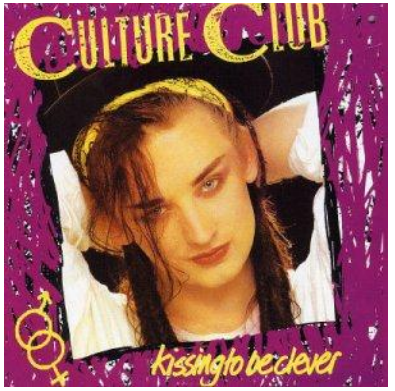
- The answer seems to be even more regulation

- What is a government security Czar going to bring? More regulation!

- Are all of these regulations making us more secure?

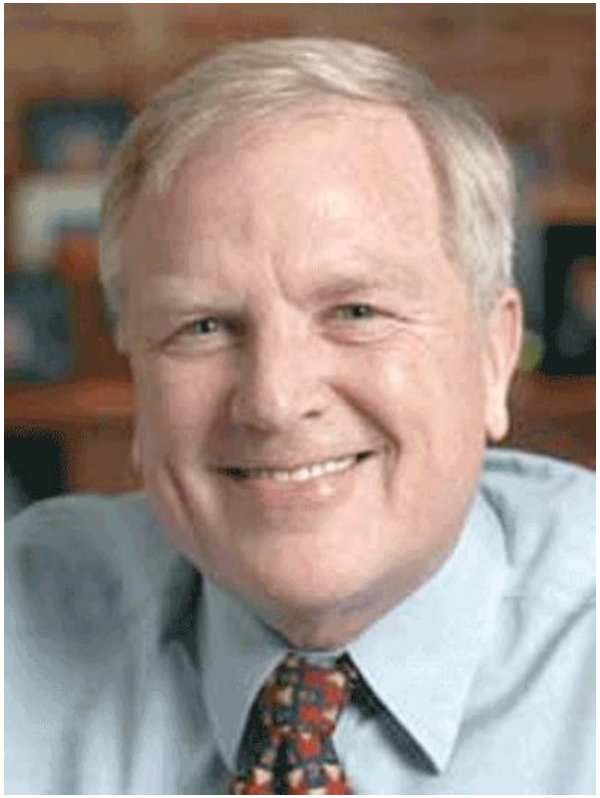
The Compliant Culture Club

- We have created a culture of compliance
- Substituting conforming with regulations for being secure
- Compliance audits become the key driver for resource allocation
- Priorities are set based upon what is needed to pass audit, not what will result in best security.
- In this culture compliance equates with security
- Compliance and security are viewed as a “tax” on the business. No positive impact to bottom line
- Leads to the “checkbox” culture. Minimal effort
- Over time compliance equates to security



This is the Result?

Blind reliance on compliance, equating it with security, leads to this:



Robert Car, Chairman and CEO, Heartland Payment Systems

Heartland CEO says data breach was 'devastating'

Heartland CEO on Data Breach: QSAs Let Us Down

… Robert O. Carr, Chairman and CEO of Heartland Payment Systems - the subject of potentially the world's biggest data security breach earlier this year - declared that the model used by quality security assessors (QSA) is "broken".

So now it is the auditors fault we are not secure?

Even 4 years after the fact?

- Merrick Bank sued QSA Savvis in 2009 for an audit done in 2005 on processor CardSystems Solutions.
- Merrick said they relied on Savvis “certifying” CardSystems.
- CardSystems subsequently had a vulnerability which led to a breach
- They were storing credit card numbers
- Issues around “snapshot in time”, 3rd party reliance and liability of an auditor are all new legal theories in IT security audits.
- Was CardSystems in compliance at time of audit?
- If so, what if any liability should Savvis incur?
- Does Merrick have a right to sue Savvis anyway?

If the Shoe Fits . . .

- The CardSystems - Savvis suit is the first where a PCI auditor is being sued due to a breach at a audited company.
- Traditionally, financial audits can be relied upon by 3rd parties, but can an IT security audit be relied upon by 3rd parties? What about by the audited parties?
  - *"We're at a critical juncture where we need to decide . . . whether [network security] auditing is voluntary or will have the force of law behind it," says Andrea Matwyshyn, a law and business ethics professor at the University of Pennsylvania's Wharton School who specializes in information security issues. "For companies to be able to rely on audits . . . there needs to be mechanisms developed to hold auditors accountable for the accuracy of their audits."*
- Clearly in Heartland and CardSystems, the audited company relied upon passing audit as proof of being secure.
- If the IT auditor is going to be held liable, what should the standard be?
  - The auditor certifies that the audited entity meets the minimum standards of a regulation OR
  - That the audited entity is now "secure"?
- Of course it is lunacy to think you can audit out insecurity
- Are auditors becoming the final word on security?
- Is this fair to the auditor?
- Does the auditor now need to be a security expert?

What is the Auditor to do?

- No matter the outcome of CardSystems-Savvis, the liabilities of IT security auditors are going to change.
- Of course there will be even more disclaimers in any auditing agreement to limit any liability, but hiding behind the fine print isn't going to do it
- At the end of the day it is really all about the regulations. We need to be an agent for change of the regulations themselves
- Being PCI or SOX compliant is not any guarantee of being secure or hacker proof.
- Make sure that your client understands this. Don't hide behind fine print, shout it out!
- Can you use the opportunity to actually make them more secure?
- Your clients "fear the auditor more than the attacker"!
- You have the power to change the equation

The Auditor as Superman

- The bright side of potentially increased exposure, is greater power for change
- If you are more feared than the hacker, use it to accomplish good.
- In your audit findings point out the minimum, but strongly suggest best practice security strategies.
- More than suggest highly recommend
- Move your clients beyond the checkbox
- Most security administrators don't know how to make management pay attention, you do. Work with them, not against them
- Make sure that policies and process are actually in place, not just talked about
- Make sure that technology solutions are not only installed, but being maintained and used.
  (when was the last time the logs were actually looked at, the firewall rules updated?)

YOU HAVE THE POWER!

Thanks

For more information about The CISO Group contact us at:

Alan Shimel
alan@thecisogroup.com
561 206-4512

The CISO Group
info@thecisogroup.com

South Florida
1081 Holland Drive
Boca Raton, Fl 33487
561.206.4512

Denver, Colorado
2100 16th St
Suite 311
Denver, CO 80202