

white paper

To Eliminate IT Security as a Reportable Condition or to Eliminate Conditions That Make IT Security Reportable

William H. Kirkendale, CISSP

proactive

To Eliminate IT Security as a Reportable Condition or to Eliminate Conditions That Make IT Security Reportable...that is the Question!

If William Shakespeare were around today he'd probably be concerned with things more humanly than information security. But sit him in a room full of senior corporate or government managers talking about the subject and you might hear him puzzle the question; "Doth not security — the return by good compliance, prefer, compliance — the return by good security?"

You'll have to look long and hard at that line. And looking long and hard is exactly what many organizations are doing at their responsibility to report about the measures they are taking to protect themselves. Protect themselves from the auditors that is, not necessarily the audacious.

Recently, Federal Civilian Agency IT working group labeled itself, "Eliminating IT Security as a Reportable Condition" — a noble title that exhorts with command, determination, and perseverance. A quick, gloss over gives you the sense that officialdom is taking IT security seriously. Read it again, slow it down, focus and, as will often happen reading Shakespeare, you're suddenly enlightened to realize that they're serious about the reporting. "The worst is not, So long as we can say, 'This is the worst.'" ¹

It's really about a priority to get rid of the nagging, painful, and never ending, reportable condition of faulty IT security conditions, or "findings".

Federal managers do a lot of reporting. Due to the stepped up demands to comply with Federal IT security and privacy laws, significant resources are being appropriated to automating reporting tasks and centralizing disparate reporting sources. Unfortunately, the end game of these initiatives is not efficiencies and effectiveness in operations, business processes, or risk management (information security); it's usually efficiencies and effectiveness in reporting.

So what about the "findings"? What are they founded upon and who finds them?

In the United States, information security and privacy law holds Civilian government agencies responsible to FISMA. Defense agencies are primarily governed by DITSCAP (soon to be DIACAP) and NIACAP. The US financial services sector is beholden to GLBA and Health Care organizations answer to HIPAA. Commercial, government, and non-profit organizations alike, must comply with these information security and privacy regulations as pertains to their business conduct and affairs.

Each is required to report the state of their security and privacy compliance. Public companies get the double whammy having to comply with Sarbanes-Oxley (SOX).

Though there are starkly different business drivers, the best security practices for confidentiality, integrity and availability, comprise a common thread in the regulations. HIPAA and GLBA address specific industries. SOX is concerned primarily with accounting integrity (see WorldCom & Enron), and DOD for obvious reasons, lends extra weight to confidentiality. Federal Civilian Agencies have broad information security requirements and are best as a group, to illustrate the taming of this shrew.

We all need a little taming from time to time. The ubiquity and increasing speed and expanse of global networks (Internet) combined with our reliance on the advanced applications screaming to market to take advantage of them, has placed us in a precariously vulnerable position. Criminal hackers and domestic and international terrorists happen to have access to the same global network, application code, and documented, proven hack methods and tools.

Software has bugs, flaws, and insecure default security settings. Network architects did not consult with hacker and cracker documentation before they built out their infrastructure. Passwords are sometimes the word "password", and our love affair with email is neglect of attachment (opening savvy, that is). Our personal, financial, and health data is a nanosecond away, and our 401K's can be wiped out, as a byproduct of a few clicks by some corporate accounting scoundrel. "Love all, trust a few, do wrong to none" ²

So, in 2002, Congress enacted FISMA, The Federal Information Security Management Act, to govern the information security practices of Federal Civilian agencies. With good sense, FISMA directs agencies to look to the extremely well thought out guidance of NIST (the National Institutes of Standards and Technology) to develop and maintain their security programs, and to certify and accredit their systems. As an information security program matures, NIST advises, its measurement (findings) will be based on the “effectiveness and efficiency of its implemented security controls”.

The measurement is carried out by auditors from regulatory oversight bodies and Inspectors General, all of which have come to know and love the pentest (penetration test) and vulnerability scan as their latest measuring tools of choice. (some say, the perpetrators of their existence). These tests reveal granular conditions that demonstrate the effectiveness and efficiency of controls. They could be any number of things and usually are. "When sorrows come, they come not single spies, but in battalions" ³

Controls such as patch management, access control policies, or configuration management may be found inadequate because critical security patches are missing, simple passwords are allowed, and unnecessary daemons are running. Seems reasonable were it not that patch management as a whole and seven missing security patches often get thrown, on equal footing, into the same “findings” hopper,. Findings need to be remediated, their progress towards this end reported upon, and eventually closed. The more closings the seemingly better reports.

For departmental management, accommodating the auditor’s reporting requirements is mandatory and is an imperative that outweighs that of implementing any proactively mitigating control. This is especially so when one considers proceeding through a bureaucracy encumbered procurement and/or contractually (see outsourcing) debilitating deployment of a control. The auditors want results and it is at this juncture that they have actually become the “implemented security control” — the one that they must also measure! Confused? You should be.

There’s very good rationale and useful material in the body of FISMA, but first impressions are lasting and after you read its first six paragraphs defining its purpose (you must read it as you would read Shakespeare), you’ll have no question about its priority. FISMA wants to know what’s going on — not as a result of — but at the expense of, if need be, — rational and prudent IT security practices. These overtones flat out “exploit” NIST’s intentions by causing the enforcers and compliers to pull out the guidance to help them “report” not “protect”. Additionally, FISMA’s fizz is getting a bit flat. It should accommodate change, be dynamic, and demand this of itself.

One of the more increasingly illuminated deficiencies among government information security efforts, is not knowing the “inventory” — servers, desktops, their operating systems, applications — their versions, changes, patch status, etc (see configuration management). For one lawmaker, it’s the finding of all findings!

Florida Representative Adam Putnam sharply criticized federal managers at a panel discussion for exactly that. “Nobody seems to know what they own”; said Putnam. Obviously, if you don’t know what you have, you can’t know what’s wrong with it and you can’t make plans to correct it. “for they say every why hath a wherefore.” ⁴

Once agencies have the ability to know what they have and know what’s wrong, on their own...does the auditor go out of business? Probably not, because, as IT folks often say, “there’s always something”. But security will no doubt be improved and isn’t that what it’s all about?

It is, according to a 2004 GAO report on Software Patch Management. The GAO found only 4 of 24 agencies “monitor all of their systems on a regular basis”. Not too good, and in this age of zero-day exploits, frightening.

Elected officials are in business to protect us. They want our data secure, our privacy ensured, and they want to know that organizations are complying with the laws they created to accomplish this. Congressman Putnam’s lashing about knowing the inventory, may one day be reflected upon as the second most important observation in the history of

the Federal IT security struggle. Continuously, and in as near real-time as possible, know what you have — match it against a current known vulnerability database — assess the risk, and prioritize — take action to mitigate/remediate. Carnegie Mellon's CERT Coordination Center says 95% of network intrusions could be avoided by keeping systems up to date with appropriate patches.

The first most important observation will be the one that leads to a reform of regulations so that they insist that (a) prudent protection is not encumbered by laws that make reporting, CYA, or any other bureaucratic dynamic take preference, (b) software vendors and developers, deliver secure products, and (c) those responsible for information security — whether lawmakers, senior business managers, or system administrators – when they come to the fork in the road to destination compliance — have incentive to take the prudent and proactive protection route.

Eliminate the conditions (first know them) and the reporting can take care of itself. It's a mindset that has to be changed and there's no better place, to set the example and make it happen, than at the top. "Delays have dangerous ends".⁵

About the author:

Bill Kirkendale is a Certified Information Systems Security Professional (CISSP) and Senior Security Architect with Unisys Corporation's Federal Security Solutions Practice.

¹ Shakespeare's King Lear Act IV, Scene I

² All's Well That Ends Well (Act I, Scene I)

³ Hamlet (Act IV, Scene V).

⁴ Comedy of Errors (Act II, Scene II)

⁵ King Henry The Sixth – Part I (Act III, Scene II)

For more information, please visit our Website at:
www.unisys.com/public_sector

Specifications are subject to change without notice.

© 2005 Unisys Corporation.

All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands or products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

