Overcoming Upper-Management Resistance

by Paul J. Brusil, PhD
Adjunct Professor, Information Assurance
Norwich University, Northfield VT

Note from M. E. Kabay: In working with students in the online Master of Science in Information Assurance (MSIA) program of Norwich University <http://www.msia.norwich.edu/>, professors contribute to the weekly discussions. One of the questions in the first week of the second seminar, which focuses on management, presents a scenario in which management dismiss security concerns. Professor Paul J. Brusil, PhD, commented on his students’ interchanges as follows and I think readers will appreciate his insights.

* * *

A number of you have made good suggestions for overcoming lack of support by upper management. I’d like to summarize, to highlight some and to put a couple more possibilities on the table for your consideration in overcoming management blockage to security policy development.

- You need to know what upper management opinions to counter. Try to find out what piece of “knowledge” is used by resistant management for them to arrive at the fear-uncertainty-doubt (FUD) conclusion regarding the value of information security and associated policies to your enterprise. Once you know what is really bothering the executive(s) who is(are) blocking action, then you have a better chance at discussing and exploring how to counter or accommodate the objection.

- Be prepared to talk about the potential pluses and minuses of instituting or not instituting each policy.

- Have a business case, not just a regulatory case, and, when possible, a return-on-investment (ROI) case for each potential security policy.

- When possible, develop and use a business impact analysis (BIA) matrix to show business impact to the enterprise if a security incident were to occur because of a lack of a particular policy.

- Have real-world examples of vulnerabilities created by lack of policy and examples of the business impacts of exploitation of such vulnerabilities.

- Analyze the marketplace and your competition. What are other enterprises in your field doing with respect to security policies? What are the media and trade magazines saying? Circulate headlines (and eventually whole news stories) of the look-what-happened-to-some-other-enterprises-and-how-they-got-burned-doing-what-we’re-doing-now sort about enterprises similar to yours. In some sense, justify that fear is real. Circulate strategy-oriented headlines (eventually whole news stories) about security policies that enterprises similar to yours institute to show that your proposed approach is accepted by others.
Make sure executives have a growing, and eventually complete, understanding of the responsibilities they have under current laws, including mandatory reporting (e.g., under California SB1386) to customers of even potential threats, the personal accountability they face, and the potential litigation facing the enterprise (including litigation associated with indirect liabilities that may arise because of business relationships between your enterprise and other enterprises that may knowingly or unknowingly violate Federal, state and local laws and regulations that pertain to information security).

Get some real proof and evidence from your own enterprise for the need for security policies. Install free open source security monitoring tools such as an IDS (and if possible buy/borrow/install other security monitoring tools such as honeypots, event logs, etc.) to develop a picture of the security-related vulnerabilities and attacks happening now within your enterprise’s IT structure because of lack of policies. That is, put together a picture of current incident activity and current potential/real direct asset losses and indirect asset losses (e.g., possible future customer losses due to negative publicity, diminishing reputation, or decreasing customer confidence) specific to your enterprise. It ought to be hard for a CFO to ignore asset losses.

Seek and expand upper management/C-level support where ever and when ever you can find it.

Have the various conclusions from the activities above available as 25-words-or-less impromptu, “elevator pitches” that you could give to a C-level manager you meet casually. Take every opportunity to bring home the points that real-world security-related problems do exist, that personal and enterprise risks are real, that a certain amount of fear is justified, and that security policy is one of the first steps in the right direction.

Stay positive, but keep telling it as you see it.

* * *

Paul J. Brusil, PhD (brusil@post.harvard.edu) founded Strategic Management Directions, a security and enterprise management consultancy in Beverly, Massachusetts, USA. He has worked for MITRE, NIST, NSA, and many other US government agencies on security standards and other high-technology issues including especially medical informatics and the Common Criteria. Dr Brusil is an editor of the Journal of Network and Systems Management <http://www.cstp.umkc.edu/jnsm/> and is the author of more than 100 papers and book chapters.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.