What the Economic Crisis Means for IT Security and Risk Management

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[[](http://itmanagersinbox.com/wp-content/uploads/2008/11/pc-and-lock.jpg)](http://itmanagersinbox.com/wp-content/uploads/2008/11/pc-and-lock.jpg)EMA has issued a new advisory that highlights emerging threats in IT Security and Risk Management due to the financial crisis. Including the anticipation of new compliance issues (W3D), “What Washington Will Do”. SOX emerged from a downturn.

Enterprise Management Associates (EMA), a leading IT management research and consulting firm has released a new advisory note titled, “What the Economic Crisis Means for IT Security and Risk Management.” In the advisory note, EMA research director, Scott Crawford, highlights the impact of the current financial industry meltdown, and its implications for the management of security and risk in IT.

“Clearly, the fallout from this crisis poses serious issues for IT security and risk management. Professionals in these fields should be thinking seriously about what they may be facing as a result – but that’s not all,” said Crawford. “They also must understand how this crisis came about in order to be prepared for what will follow – as well as what it says about the mindset of the business when it comes to managing risk in any respect.”

Crawford focused on the increased IT security threats and risk management issues that come into play when the financial industry is unstable. Some examples of the economy’s impact on IT security, risk management and compliance include:

* **Opportunistic attackers will take advantage of many aspects of the crisis.**Examples range from phishing attacks that target desperate individuals seeking debt relief, to more retaliatory attacks launched in frustration and resentment against financial businesses themselves. Some, however, may use the appearance of a retaliatory attack simply to hide what is actually espionage, infiltration, or attempted data theft.
* **Widespread weakness among targets will increase opportunistic risk.** Just as significant is the risk posed by the new weakness of financial institutions – and possibly some governments stretched to cover losses in the private sector – both of which are among the most common targets of attack.
* **Increased M&A activity will complicate security and risk management.** As former financial services competitors take over one another in a wave of mergers and acquisitions, IT as well as security teams on both sides of a deal will find it a challenge to safely integrate a formerly foreign environment.  M&A activity may further open the door to opportunistic phishers who recognize that customers may not know who owns their bank from one day to the next.
* **Businesses should look to the security and risk management values of every management tool and technique in the enterprise.** The need for visibility throughout the network highlights the value and importance of tools not only in security, but in network, systems and application management as well. IT management tools that can enhance security while reducing the cost or complexity of security management – as well as security solutions that improve the management of IT itself – merit closer scrutiny for these values.
* **The crisis will increase the value of “security-as-a-service.”** A now-dire need to move expenditures away from capex and more toward the opex side of the balance sheet presents a new opportunity for security offered as a service. Crawford notes that service-oriented approaches offer ways to keep up with the threat while getting a better-defined handle on the investment.
* **Get ready for “W3D” compliance**. Just as SOX emerged from the previous major downturn, Crawford advises businesses to prepare for the inevitable wave of compliance with “W3D:” “What Washington (or the World) Will Do.”

“The greatest concern the financial crisis creates for IT security and risk professionals lies in the roots of the mess itself,” says Crawford. “If the inclination of the business is always to think first about IT’s primary mission, and only incidentally about the risks that may be exposed, security and risk management may never rise to the level needed to address the truly alarming level of malicious threats in today’s environment. Just as with illusory lending, however, we now have abundant evidence of the impact of poorly managed risk that should motivate us to do better.  The question is, will we?”