

2008 Security Incites

What are the Security Incites?

Annually, Security Incite publishes a list of the key “trends” in the security business for the next year. Called “Security Incites” and written from the perspective of the end user (or security consumer), Incites provide direction on what to expect, assisting the decision making process. Each Incite provides a clear position and distills the impact on buying dynamics and architectural constructs. Incites also set the stage for Security Incite’s upcoming research agenda.

2008 Security Incites

1. Express Your Inner Bean Counter

Substantiating the value of security continues to plague practitioners, who still can’t specifically answer the question: “Are we secure?” Structured security programs (ISO 27001/2, COBIT, Pragmatic CSO) help align programmatic activities, and look for significant advances in the area of security metrics – where the industry begins to gain consensus about what can and should be tracked.

2. It’s time for an audit revolution

Contrary to popular belief (and desire), compliance is far from dead and remains a major buying catalyst (and funding source) for all sorts of information security tools, services and the like. Yet, the acrimonious relationship between the auditor and the audited continues to create problems and needlessly burn resources. Forward-thinking security professionals jump on the bleeding edge of innovation treating the auditor as a peer and viewing the audit as a learning opportunity.

3. Best of Breed DOA

As security matures as an industry, the concept of “best of breed” goes the way of the dodo bird. Mature technologies such as firewalls, IPS, and anti-virus get subsumed and integrated into bigger “suites” making the individual performance and feature set of a specific function less important. Emerging functions still stand-alone, but not for long as the innovation/consolidation cycle accelerates. Security management offerings also consolidate, driven by the fact that most customers don’t have time to deal with one management hierarchy, certainly not 2 or 10. This continues to reinforce the “big is the new small” trend that has predominated security buying for the past 2 years.

4. Weaving security into the network fabric

Network security hits the tipping point where it's no longer considered novel or a "must-have," but rather it's just there – truly becoming a feature of the network fabric. Network Access Control remains a proxy for all things network security, and makes minor inroads in 2008 – largely as people stop talking about it. Independent NAC vendors either sell or struggle, as the big networks force their will on locked-in customers. The NAC standards battle turns out to be much ado about nothing.

5. Night of the Internet Dead

With a majority of attacks (like drive-by downloads) no longer requiring user interaction; the number of active zombies continues to exponentially multiply. Organized fraud networks increasingly use targeted, social engineering-based attacks because they work, forcing users to put a premium on REACTING FASTER and training users to stop doing stupid things, as opposed to hoping a new shiny product will solve the problem.

6. Laptop encryption hits the big leagues

Since remote employees insist on losing laptops and the Government insists on notifying customers when private information is lost, security teams respond by rolling out full disk encryption far and wide. Within two years, this market disappears, first because every endpoint security suite will include a FDE option (2008) and later because the operating system makers (Microsoft and Apple) do a good enough job (2009) to kill stand-alone offerings.

7. The SDLC is your friend

As innovation in web application scanners is crushed by consolidation and web application firewalls still can't find its sea legs, security professionals finally get religion about building secure applications, largely to avoid the PCI stick in the eye and embracing the reality that applications remain the path of least resistance. A long, hard cultural struggle ensues between security and software development personnel, but by focusing on building the most critical applications securely, the tide turns regarding the secure systems development lifecycle (SDLC).

8. Protect the Vault (that's where the money is)

The hackers continue to go where the money is by increasingly targeting the databases storing private information. Database vendor's disdain for security doesn't help, and creates an opportunity for database monitoring and security solutions to gain a foothold before this capability is subsumed into the DBMS and/or network fabric. Encryption infrastructure makes little to no progress in 2008, despite regulatory pressures – largely due to complexity and the nebulous compensating controls clause.

9. Get the jumper cables for DLP

Data leak prevention stalls in 2008, continuing to be a solution looking for a problem. Given its complexity, limited ability to protect intellectual property, and early consolidation by Big Security, the technology is stuck in the early adopter phase. Significant regulatory catalysts are balanced by an uncertain spending environment, which forces users to utilize the built-in filtering within email and web gateways. These solutions are largely good enough to make sure a dimwit doesn't send a SSN# (or other regular expression) outside of the organization.

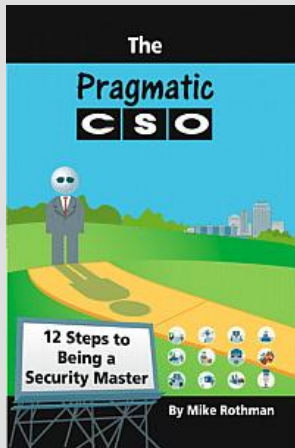
10. Hack thyself

Given that there is no panacea on the horizon, security professionals start to understand the concept of risk management, as opposed to throwing money down the security toilet on the latest, shiniest widget. Security organizations must start to put a premium on prioritizing activities, based upon what's important to the business, as well as what is really exploitable in their environment. The only way to figure out the latter is through a new function called "security assurance," which focuses on breaking stuff (networks, systems and applications) before the bad guys do.

About Security Incite

Security Incite is an industry analyst firm specializing in the information security market. Our mission is straightforward: Help subscribers protect their information assets more effectively by making better decisions. Security Incite was founded to address a real need to provide objective, relevant and inciteful security research by focusing on what's right, as opposed to what pays well. Focusing on bold, thought-provoking and irreverent analysis, Security Incite helps organizations make better decisions. Our tagline is "No Bias. No Bull. Real Incite," which does a good job of explaining our philosophy and our focus.

Security Incite publishes *The Daily Incite*, a unique, refreshing, no holds barred newsletter about the information security business. And you never know who is going to be on the receiving end of one of President Mike Rothman's famous rants. As a bonus, subscribers also receive Security Incite's BUYING SECURITY PRODUCTS ebook. To subscribe, send email to dailyincite@securityincite.net or visit <http://securityincite.com/dailyincite>.



The attacks have changed. Why are you doing the same old security stuff?

Chief Security Officers have been locked in a LOSING BATTLE with the bad guys. Senior management is losing faith and scrutinizing security activities. We need a new way to "do" security - a program that gets you to focus on protecting what's important, to stop chasing the attack de jour, and to keep the auditors in check.

This new way is **The Pragmatic CSO.**

Buy the new Book from Security Incite's Mike Rothman and learn a 12-step program to become a better CSO. It's available now at www.pragmaticcso.com.

I strongly recommend buying and reading The Pragmatic CSO. All CSOs should also have a copy, period.
- Richard Bejtlich

This is the first time I have read a book about security that not only made sense, but actually gave some decent advice on how to do something about it.
- Mike Murray (www.episteme.ca)

Mike Rothman's The Pragmatic CSO presents a fresh, human approach to the intimidating world of managing enterprise security.
- Ken Camp

I think the Pragmatic CSO will go down as a milestone in the security management arena.
- Alan Shimel