Join the Discussion Connect

De-Operationalizing InfoSec: Living in an Imperfect World

By Benjamin Tomhave – ISSA member, Northern Virginia, USA Chapter

This article explores those functions historically classified under the "security operations" header and questions whether these functions really do belong labeled as "security."

Abstract

Historically, most information security operations have been owned by IT and/or the security department (which is, itself, often part of IT). Today, though, we have to wonder if this really makes sense. In the realm of operations, what is core to security vs. just being security-related? This article explores those functions historically classified under the "security operations" header and questions whether these functions really do belong labeled as "security."

Which came first: Information security[1] or information technology?[2] Depending on how you define either topic area, the answer may be surprising. Computation as a practice has been around for eons, but so has the practice of protecting information (Caesar cipher[3] anyone?). Assuming for a moment that information technology is limited to the fairly recent evolutions in technology-based computation, it would then seem clear that information security has been around for far longer. Yet somehow we find ourselves in a position today where infosec is consistently subjugated as a sub-component of IT.

The good news is that the past decade has seen a change in this approach, and with good reason. However, it would seem that we have not come far enough. In many organizations, operational activities with a security-related function are still "owned" by the security team or organization. One has to wonder if this is still a good practice, or if it is just an extension of institutional inertia. Should infosec own parts of operations, or are we undermining our credibility by continuing down a path that does not support a proper security focus?

Commoditized functions

The key to this argument is the differentiation between *commoditized* and *specialized* knowledge and solutions. Early in the emergence of new solutions specialized knowledge is required for proper support and management. As the solution becomes more mainstream, so does the requisite knowledge for support and management. Over time we then see that a specialized area becomes a generalized, commoditized area. It is at this point that we find many security technologies today.[4]

Consider a variety of solutions – AV, firewalls, VPNs, IDS/IPS – and think about what it takes to install and support these platforms. Now break down those responsibilities into two camps: operations and security. In the traditional mind set everything is assigned under security, but this approach belies an underlying bias toward maintaining the status quo – toward maintaining and building turf. The simple fact of the matter is that a firewall is just another network appliance; AV is just another desktop or server software component.

This conclusion may not sit well with certain segments of the industry. For one thing, the broader point here is nothing short of telling people and businesses that what they do is less about security than it is about IT operations. There are fundamental practices that ought to be – and in many cases are – ingrained in standard operating procedures for IT organizations. Why, then, do security teams still oftentimes continue owning operational responsibilities? More importantly, what is the impact of segregating certain operational

1 See http://en.wikipedia.org/wiki/Computer_security or http://csrc.nist.gov/publications/history/ for more on the history of computer security.

2 See http://en.wikipedia.org/wiki/History_of_computing for more on the history of computing.

3 See http://en.wikipedia.org/wiki/Caesar_cipher for more on the Caesar cipher.

4 Andrew Stewart, "Information security technologies as a commodity input," *Information Management & Computer Security* (2005).

duties out of the department that is charged with optimizing IT operations?

Enablement culture

By taking and holding control of certain commoditized security operations, infosec has set a bad precedent and created an enablement culture. An enablement culture is a social context in which bad behavior is empowered by a third party.[5] In the case of infosec, we have held onto commoditized security technologies that no longer require specialized knowledge for so long that IT operations – and the business practices they support – have lost any sense of what is right and wrong behavior. We then find ourselves in this cat-and-mouse game of playing the heavy when someone asks to do something that should not be allowed (e.g., developers active in production environments, office networks with full access to production networks, improper handling of sensitive data).

Simply put, we have a credibility issue in infosec today. Rather than focusing on core security functions, we instead let ourselves get dragged into the operations trenches, losing resources and precious time slogging through battles that were long-since decided. Do you need a firewall? Yes. Do you need a VPN for remote access? Yes. Do you need network segregation? Yes. Do you need to judiciously and cautiously handle sensitive data? Yes. Do you need to encrypt your most sensitive data? Yes. Do you need to write clean, tight code that takes into account the OWASP Top 10[6] and the SANS/CWE Top 25?[7] Yes.

The enablement culture is a direct result of taking away the direct responsibility from true operations teams.

If all of these questions seem obvious, then why are we still having arguments about these measures? Why is there even a question? Because of the enablement culture that is a direct result of taking away the direct responsibility from true operations teams. Moreover, there is a potential conflict of interest here where we in infosec are writing the rules, enforcing the rules, and – oh yeah – we are also operationally implementing the rules. Who gets punished in the case of a security breach due to bad behavior? Operations? The business? Even if they do not have direct ownership of executing their security duties? We have created the conditions for security failures, enabling bad behavior and removing a direct connection to consequences.[8] [9] It is time we reconsider our place in the business.

You redefine me

At this point we need to ponder what exactly is core to security. If you subtract out direct operational responsibilities for commoditized technologies, then what does that leave? Do not despair – there is still a plethora of specialized security responsibility to cover. Following is a brief breakdown of some common topic areas where infosec must still maintain an active role, either as an owner or as a primary stakeholder.

Technologies

Specialized security technologies will continue to emerge, evolve, and occasionally go mainstream. DLP is a prime example of a security technology that is already quickly reaching the transition point from specialized to generalized. Assuming the technology still exists, in a decade it seems quite likely that it will make a full transition to a commoditized operational solution. On the other end of the spectrum we

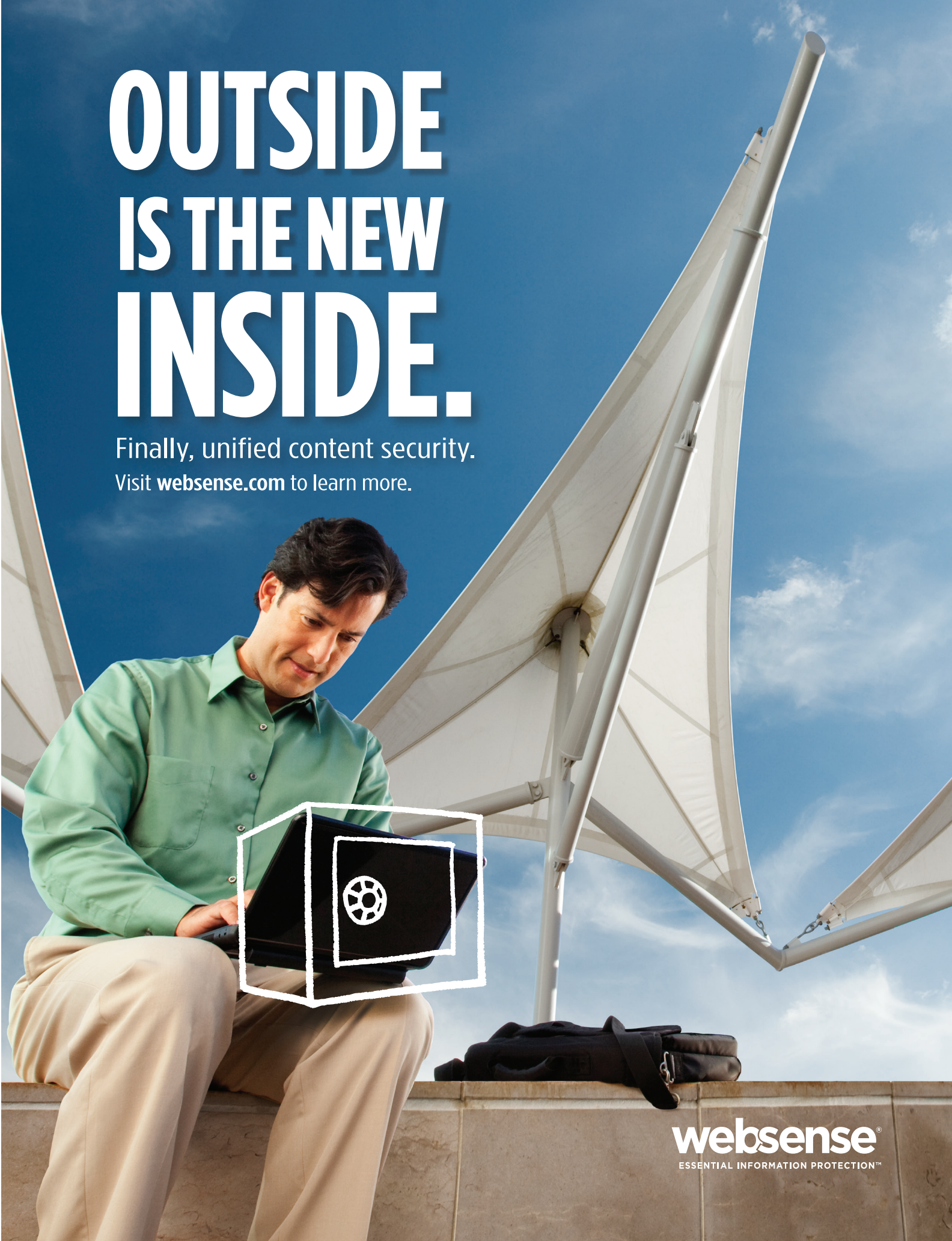
5 See http://en.wikipedia.org/wiki/Enabling for the negative sense of "enabling."

6 See http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project for more information.

7 See http://cwe.mitre.org/top25/ for more information.

8 Mikko Siponen, et al, "Compliance with Information Security Policies: An Empirical Investigation," *IEEE Computer Magazine* (February 2010), available online at http://www.computer.org/portal/web/csdl/doi/10.1109/MC.2010.35.

9 Lance Spitzner, "Ticket or Click-It," available online at http://www.honeytech.com/blog/ticket-or-click-it.


OUTSIDE
IS THE NEW
INSIDE.
Finally, unified content security.
Visit websense.com to learn more.
websense®
ESSENTIAL INFORMATION PROTECTION™

can look at forensics tools. It seems unlikely that they will ever transition into general practice because they support specialized competencies and practices. If they have not transitioned already, access management technologies should quickly move into operational realms, leaving only the governance activities within infosec.

Competencies

Certain competencies will always be endemic to infosec, because the infosec mind set tends to be unique in the world. Incident response management (security incidents in particular), security testing methodologies (e.g., penetration testing, hardware hacking, exploit and vulnerability research), and risk assessment and management are all examples of competencies that have, and will likely retain, specialization under the infosec heading. On the other hand, key areas like software development lifecycles and project management, while important to security, are not core competencies to security. While we may have worthwhile insights to bring to the table, we are not the owners, nor should we be.

Practices

There are many areas of practice that logically make sense to remain under the infosec moniker, though operations is clearly not one of them. As already discussed, forensics and related investigations activities are specialized practice areas that will inevitably continue under the infosec heading. Other important areas like governance, risk management, compliance, and training and awareness will also continue under the infosec header to one degree or another, as will technical practices around assessment, testing, application security, and security architecture. Other practices core to infosec include the processes and approvals around access management and security policy definition and enforcement.

It seems unlikely forensics tools will ever transition into general practice because they support specialized competencies and practices.

The above list is by no means complete, and it is intended to cause a little chaffing. Not the least challenging is the notion that marketing may have gotten it right a few years ago (I know, blasphemy!). Is it possible that infosec really has matured to the point that GRC is in fact the core of our industry? If you abstract out operations and audit, then this leaves governance, risk management, and compliance covering a large portion of core infosec duties. Yes, there is more to infosec than just GRC (security research, incident response management, and forensics chief among them), but one must wonder if we might not benefit from redefining our industry from the GRC perspective and then branching out only where necessary, relegating the rest to other areas of focus.

Conclude this

Historically, information security programs have taken on operational duties, often in the name of "doing things right." The result has been the creation of an enablement culture that undermines credibility and creates resource duplication and discrepancies. The argument presented here – to de-operationalize security – is in no way perfect or complete, but it is key to the future of the infosec industry. It is time to refocus on what is core to the industry, starting with higher-level functions like GRC and branching out as necessary. As Huey Lewis sings:

> *Try to remember and understand*
> *Ain't no living in a perfect world*
> *Keep on dreaming of living in a perfect world* [10]

About the Author

Ben Tomhave, CISSP, is a Senior Security Analyst with Gemini Security Solutions in the Mid-Atlantic region of the U.S., specializing in solutions architecture, security planning, program development and management, and other strategic security solutions. Ben holds a Master of Science in Information Security Management from The George Washington University. He may be reached at tomhave@secureconsulting.net.

10 Huey Lewis & the News, "Perfect World" (1988 *Perfect World* album).