Herding Cats:
In or Out?

June 2010

BrandenWilliams
SECURE BUSINESS GROWTH

What's your philosophy? Outsource or insource your security operations management? And more importantly, of all the cold opens I could have chosen, why that one?

We're just about halfway through the 2010 calendar[1], and the economy is showing promise for the rest of the year. Most companies have loosened up their IT and security budgets, but the spend is closely tied to ROI and business growth[2]. At the same time, the number and types of attacks are still growing rapidly. This has forced some companies to take a hard look at the money they spend on security operations management.

With the rise of managed security services in the last decade, companies seemed to take a binary approach to security operations--either it was done in house or by a third party. Mind you, even the companies that outsourced this function still had to follow up on certain events, so it is usually not 100% outsourced unless you also outsource the management of your IT infrastructure. When funds are tight, your hands may have been tied and you were stuck with your current setup. But now that funds may be a little more available, what will you do?

I'm seeing a trend whereby there is a significant uptick in the number of customers looking to insource their security operations management. It's more than just someone looking to have a health check on their enVision or Arcsite installations, it's a serious look at who manages their security operations accompanied with strong business cases for managing it internally.

SIEM tools saw wide adoption from 2005-2009 thanks to compliance initiatives like PCI DSS. According to Anton Chuvakin[3], a prominent PCI DSS and Security Information and Event Management (SIEM) expert, "compliance helped buoy SIEM market dramatically, but many compliance-driven SIEM and log management implementation are stuck in 'comply-land' and are not delivering operational security benefits." The wide adoption seems only half baked. Sure, sales went through the roof, but only to keep auditors and assessors off their backs.

Have companies had enough? Is it time to rethink the approach? Or is the security world still flat?

Back to the philosophical question in my cold open, where do you stand on sourcing security operations management? In or out? Before you can answer on behalf of your company, you must know the overall sourcing strategy[4] set forth by management. If your company is on the "back to core competencies" side of the sine wave, it may be time to consider a good IT partner to which you could outsource this function.

When selecting a provider, focus on overall value as a component of the total cost. I'm not suggesting ignoring cost, but for something like security operations management, the lowest cost provider is probably not the route you want to go. It might be the same as doing nothing. That's not license to go nuts and spend the most amount you can either. The idea is to do a significant deep dive into both your outsourced provider and your own company to make sure you have matched things up correctly.

FOOTNOTES

[1] Though as we all know, we're halfway or more through the year. Thank YOU Chuck Norris! Er, I mean, Thank YOU holiday freeze!

[2] Meaning it is not free money.

[3] http://chuvakin.org/

[4] Even no strategy is still a strategy--albeit a weak and poor one.

For those of you looking to in-source security operations management, you need to take into account a few things. You will need a few tools, some you may already have that may need to be fine tuned and upgraded, and some you may need to procure. You need to invest in people to manage and respond to the operational security events you will face, and you will need to have some kind of 24x7 operational model. Hackers don't just stop attacking you because you went home for the day or weekend. And you will need to do some kind of constant analysis to make sure that things are functioning well and as expected. Don't let a poorly configured tool spell your demise because it missed key security incidents.

Regardless of your choice, your business owners have to take some kind of active role in security operations management. Be sure to propose and execute a solution that fits your company's overall sourcing strategy.

Contact information for requests for permission to reproduce or distribute materials available through this course are listed below.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174

BLOG brandenwilliams.com

EMAIL brw@brandenwilliams.com