The

Pragmatic
C S O

INTRODUCTION

12 Steps to Being a Security Master

By Mike Rothman

ii

**SECURITY
INCITE**
SECURITYINCITE.COM

Intro to the Intro

Thanks for downloading the Pragmatic CSO Introduction. You can see the full table of contents, and also read the introduction chapter, which sets the stage for the Pragmatic CSO methodology. You'll get a good feel for the book, and what value it can add to your efforts to build a world-class security program. But first, let me tell you a bit about why I wrote the book.

First, for those of you not familiar with my style – I'm basically an open book. If I'm thinking it, I'm writing it – both good and bad. I've spent the last year building an audience through my Daily Incite newsletter (which is available through both email and RSS at http://www.securityincite.com/BSP-landing) and listening. For those who read the Daily Incite, I know it seemed like I was talking most of the time, but I've got lots of surprises up my sleeve.

I listened to the problems that folks had. I heard their frustrations. At times, I felt more like a shrink than an analyst. But that is all part of the process. The one thing that became crystal clear to me was that CSOs of mid-sized companies (and lots of large enterprises too) were just trying to get through the day.

Life is too short to just be getting through the day. These folks weren't having fun, but rather spending time chasing the latest vulnerability, filling out useless reports to justify their existence, and groveling for funding every time they wanted to do something. And then the auditors would show up to inflict more misery on our beloved CSOs.

Is it any wonder that most CSOs I spoke to were basically miserable?

I figured there had to be a better way. There had to be a plan, a roadmap to help CSOs figure out what they should be doing and how they should be doing it. I went looking for a simple program that would get CSO's heads in the right place. I found things like ISO 27001 and COBIT, but I wouldn't term either of those frameworks "simple." So I wrote one. That's what the Pragmatic CSO is all about – simple, focused and achievable. You know, PRAGMATIC.

The first thing you'll notice is that this isn't your run of the mill technical book. In fact, it's not a technical book at all. Believe it or not, that was very intentional. I believe that the role of the CSO is no longer just technical. If you want technical stuff you are in the wrong place. There are hundreds of books and training courses for you to choose from. Maybe even thousands. But the Pragmatic CSO is not one of them.

But if you want a management-training program for a CSO, you are home. If you are looking for a structure to build a repeatable and effective security program, you are in the right place.

What's next? Check out the intro and then buy the book. That's the first step to becoming Pragmatic.

Good luck.

Mike Rothman (mike.rothman@securityincite.com)

December 2006
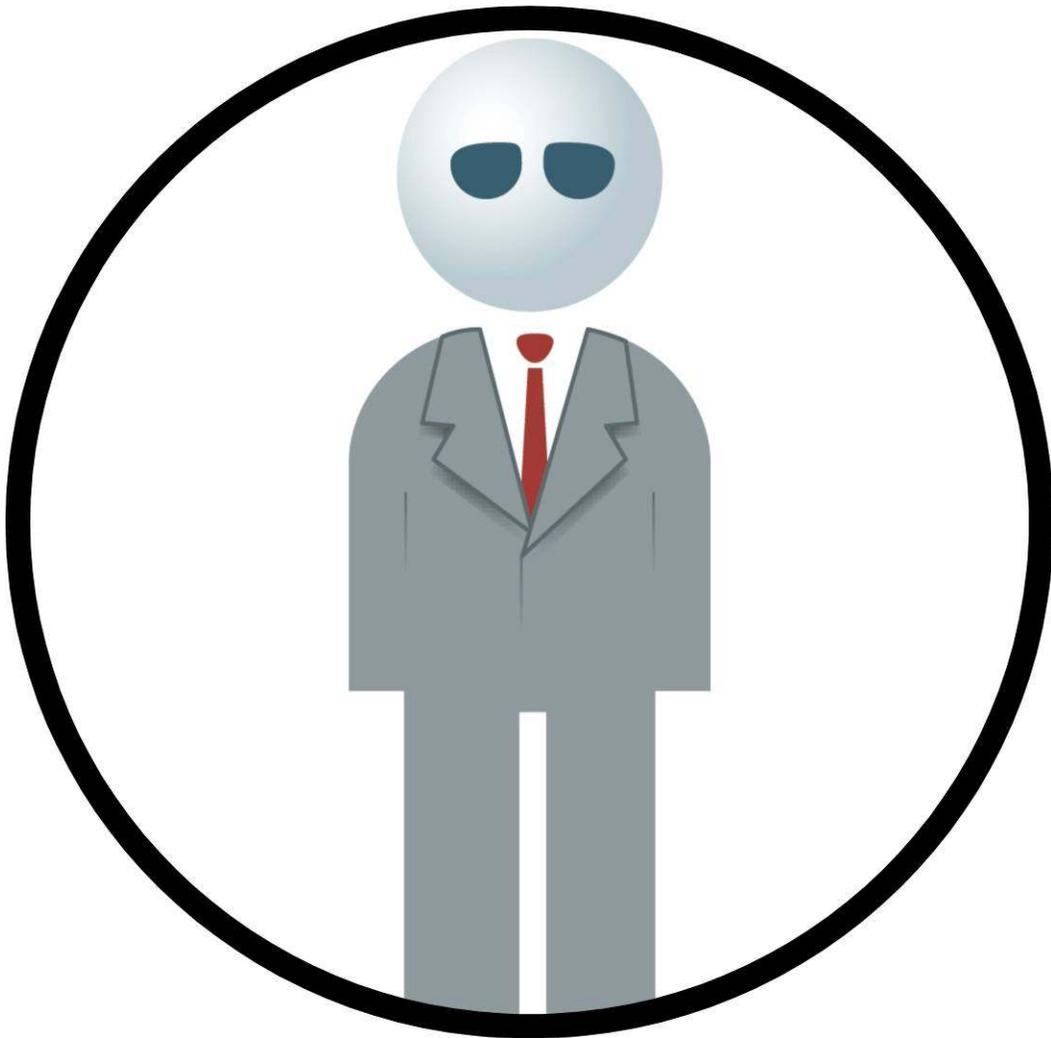Alpharetta, GA

TABLE OF CONTENTS

Introduction

CSO Conversations

Mike: Hi, I'm Mike and I think I'm an addict.

Group: Hi, Mike

Facilitator: Welcome to the group Mike. Tell us a little about yourself.

Mike: I'm a CSO for a mid-sized electronics manufacturing company. We do a lot of business with high-tech companies, so we are held to the same standards they are from a security standpoint. We rode through the boom and bust of the first Internet bubble, and I lived to tell about it.

We also have a small direct to consumer business, which requires us to accept credit cards and integrate systems with our banks. So we get to deal with all of those niceties, like PCI, as well. Thankfully we are privately held, so I don't worry directly about Sarbanes-Oxley.

Facilitator: We should all be so lucky. SarbOx is a bear and still largely unknown. But that's a topic for another day. Why are you are here at *Security Products Anonymous*?

Mike: The reason I'm here is simple. I'm in pain and I'm hoping this group can help me. The world has changed. My job used to be pretty easy and exciting. The bad guys spent their time trying to take down my network, and I worked my butt off to stop them.

I got addicted to the rush of constant battle. I got accustomed to bringing in new equipment every 3-4 months to solve another problem that appeared. I got used to just doing my job. But now I'm finding it harder and harder to do that.

Facilitator: Why?

Mike: Hackers have changed. It's not about putting another notch in their belts anymore. They no longer seem interested in taking down my network. They are trying to compromise

my devices and stay undetected. It's about fraud, and the best way for them to do that is to compromise machines on the down-low. It used to be easy; they'd come through the front door. Now they don't want me to know they are even there.

Senior management seems to have had a change of heart. Getting budget to buy new security tools never used to be an issue, but now the CFO is looking for a business case for everything we are buying. He wants to understand what the security investments of the last 3-4 years have bought them.

And then you have the auditors. Those guys want everything documented: What I'm doing, how I'm doing it, what is working and what isn't. We haven't had any kind of issue in over two years, so what we're doing is working, but that's not good enough for the auditors. *I just want to do my job, and it seems all I do is fill out reports, spreadsheets for business cases, and sit in meetings with auditors.*

Facilitator: Mike, would it kill you if I said what you just described is your job?

Mike: Do you have any hemlock handy?

Facilitator: [Laughs] On a more serious note, have these issues affected you personally?

Mike: I've been dramatically impacted and that's why I decided to take action and come to a meeting. I'm not home enough, so my kids feel like strangers. When I am home, I'm worried about what is going to go wrong at work, so I've got my "Crackberry" nearby at all times, which really pisses off my wife. The 3 AM calls tend to create some friction with the wife as well.

You know, I'm just not happy, so that impacts all aspects of my life. I've even considered leaving my CSO position and joining a vendor or becoming an analyst. Those jobs seem pretty easy compared to what I'm doing now. But I

don't want to give up. I still love security and I want to figure out a way to get my mojo back. That's why I'm here.

Facilitator: It does always seem the grass is greener on the other side. More importantly, we are glad you are here Mike because we can help you. Clearly you are addicted to fighting fires as opposed to protecting your systems and data. Security is still a battle for you, not a business function. The good news is that you understand that things need to change and that you have the ability to change them. That's why you are here.

The Pragmatic CSO process practiced by our members is a 12-step program (yes, like those other 12-step programs) **to put you back in control of your security environment**. You'll be able to focus on strategy, as opposed to fire fighting. You'll be able to position security's contribution to business imperatives and make a compelling value case to your senior management. And if you do things right, over time you'll get a seat at the table to be consulted on new infrastructure and application processes.

Mike: I don't believe you. I've been doing this for 15 years, and I don't know of any CSOs who have a seat at the table. They are always the last to know and the first to lose budget when things get tight. Security is perceived to be overhead, and that always puts us behind the 8-ball, no?

Facilitator: I know. You have every right to be skeptical. But you haven't been hanging around with the right people. It's as simple as that. Our risk-centric program teaches you how to talk about security in business terms. We show you how to fund your projects by finding the real power bases in your organization. We will be right there with you every step of the way, helping you envision how the program will work in your environment.

To be clear, this is NOT an easy process nor is it something that you do in a week. This is a program and it requires permanent change. You'll do a lot of extra work at the beginning because basically you are trying to change the

tires of the car as you are speeding down the hill. But the alternative of not taking any action is much worse, I assure you. The status quo is not your friend.

Mike: OK, I'm sold. I'll suspend my disbelief long enough to give this a try. The alternative of becoming a painter or basket weaver isn't the right answer for me. Let's get started.

The Evolving Role of the CSO

As we follow the path to become a Pragmatic CSO, we will keep tabs on Mike as he learns each step of the program and even practices what we preach in his own (fictional) organization. But let's take a step back and highlight some of the things that Mike pointed out about how the job of the Chief Security Officer has changed over the past few years.

First and foremost, the motivations of the hacking community have changed. It's no longer about mayhem and bringing networks to their knees; it's about compromising machines to gather personal data to commit financial fraud. The hacker's objective is to remain anonymous. The longer they remain invisible to you, the better it is for them.

Second, security practitioners are under significantly more scrutiny nowadays. As Mike pointed out, for years we had carte blanche to buy whatever we wanted. Whether it was worm mitigation or compliance, we always had reason for some new widget to address some new attack vector, and senior management said OK and wrote a check. After five years of this, the reality is that executives don't feel more secure now. Actually, many feel LESS secure. This has led the bean counters to start asking questions and contracting budgets. What are they getting for all that money they are spending? Why should they spend more? Drat! Now we need to justify what we are doing.

Third, there is still the specter of compliance out there. Regulations like HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act), SOX (Sarbanes-Oxley Act), and now the PCI DSS (Payment Card Industry Data Security Standard) standards have been out there for a while, but it's not clear what "compliance" with these regulations really means. Without some definitive enforcement actions, it's hard to say when you are "done." Senior executives are sick of paying through the nose when it's not clear whether they've spent enough already.

Suffice it to say, few CSOs are having fun nowadays. The swashbuckling days of battling hackers are over. Now the CSO is more of a management position, and if it walks like a duck, it better talk like a duck. So we need to talk like managers, sell our strategies, and document the progress we make. We have to earn our seat at the table through thoughtful, consistent action and the demonstration of results. Unfortunately, many CSOs are not prepared to make this change. They have not been trained in the finer art of management. And let's be clear, it is an art. That's what the Pragmatic CSO is about.

What about that CIO?

For better or worse, most CSOs report into the technology department, thus the Chief Information Office (CIO) tends to be your boss. There are exceptions to that, especially in the financial industry, but for the purposes of the Pragmatic CSO – let's assume that your boss is the CIO.

That means that the CIO is the first stop in any of the key initiatives that you need to accomplish. He/She will be a key influencer and needs to be a supporter of your initiatives. The Pragmatic CSO is designed to make the CIO look good because security is discussed within the context of the business drivers that govern investment. If you look good (and you will), the CIO looks good. It's a win-win situation.

But as with all successful executives, the Pragmatic CSO does need to spend a lot of time managing up. One of the first steps is to define success (which is discussed in detail in Step 1) and along with that it's imperative to define roles and responsibilities. Typically you see the CSO taking responsibility for all security activities, which may include physical security as well. What's on the list is less important than that the list actually exists.

Reasons to Secure

The first step in understanding the transition that you'll need to make is to define what your job. And if you think it's about stopping hackers, then we've got a lot of work to do.

In a nutshell, your job is to *protect the assets of the organization and ensure that business can operate*. Note that the job description does not mention firewalls or intrusion prevention or services or any technology. **It's not about technology – it's about business**. Five "reasons to secure" have emerged from our work with many CSOs and senior management over the years. This is why you are employed, so take good notes.

- *Maintain business system availability* – If hackers are successful in compromising your systems and taking down your networks, systems or applications, then you can't do business. That's a bad day. So Job #1 for the security professional is to make sure that this doesn't happen. Period. The systems must remain up or at least not go down because of a security issue.

- *Protect intellectual property* – In today's digital age, the bulk of most organizations' intellectual property is in digital format. That means that your company's deepest, darkest and most valuable secrets can be stolen with a click of the SEND button or a data download onto a seemingly innocent iPod. Whether it's customer data, transactions, product plans, financials, or whatever – it's getting easier to steal it. So another key priority is to protect that intellectual property.

- *Limit corporate liability* – Whether you are keeping porn from showing up in someone's inbox, blocking the leak of private data that would result in significant notification and clean-up activities, or allowing the corporate to take more judicious risks relative to with whom and what kind of business is transacted, another job of the security professional is to limit corporate liability. By ensuring that policies are clear, communicated and enforced, most organizations can insulate themselves from the actions of employees and contain the risks of everyday business. There is no reason a few bad apples should take down an entire organization, as we saw with Arthur Andersen back in 2002.

- *Safeguard the corporate brand* – Building your corporate brand takes years and significant investments. And it can go poof in a matter of seconds. Just ask any of the organizations that have had to disclose that they lost back-up tapes or laptops with millions of private customer records. Instilling the correct behaviors with employees, protecting private data and enforcing acceptable use policies could avoid many of these branding "train wrecks".

- *Ensure compliance* – Ultimately, compliance continues to be a major driver for the security professional, not so much to get funding (that game is pretty much over), but to provide an objective third-party assessment of your security posture and program. Many security professionals view auditors as adversaries, but in reality they are partners who are trying to achieve the same thing you are – protecting the assets of the organization. Harness compliance as a way to improve your security and you win not only with the auditors, but also with your senior management.

What's your plan?

Today's CSOs need a plan. You must execute on a structured program that keeps you focused on the Reasons to Secure. Showing the value of security to the organization and proving the safety of the computing environment to internal and external auditors are no longer optional activities; your longevity in the CSO position is directly related to how well you sell your strategy, show progress, and manage to your budget.

The Pragmatic CSO process has been designed to achieve these goals. It's about economy of effort and leverage. You'll be setting goals and systematically achieving them. You'll define success within the context of your security program and you'll show how you get there, every step of the way. It's about protecting your environment, safeguarding your data, and communicating what you've done to the business leaders that need to know.
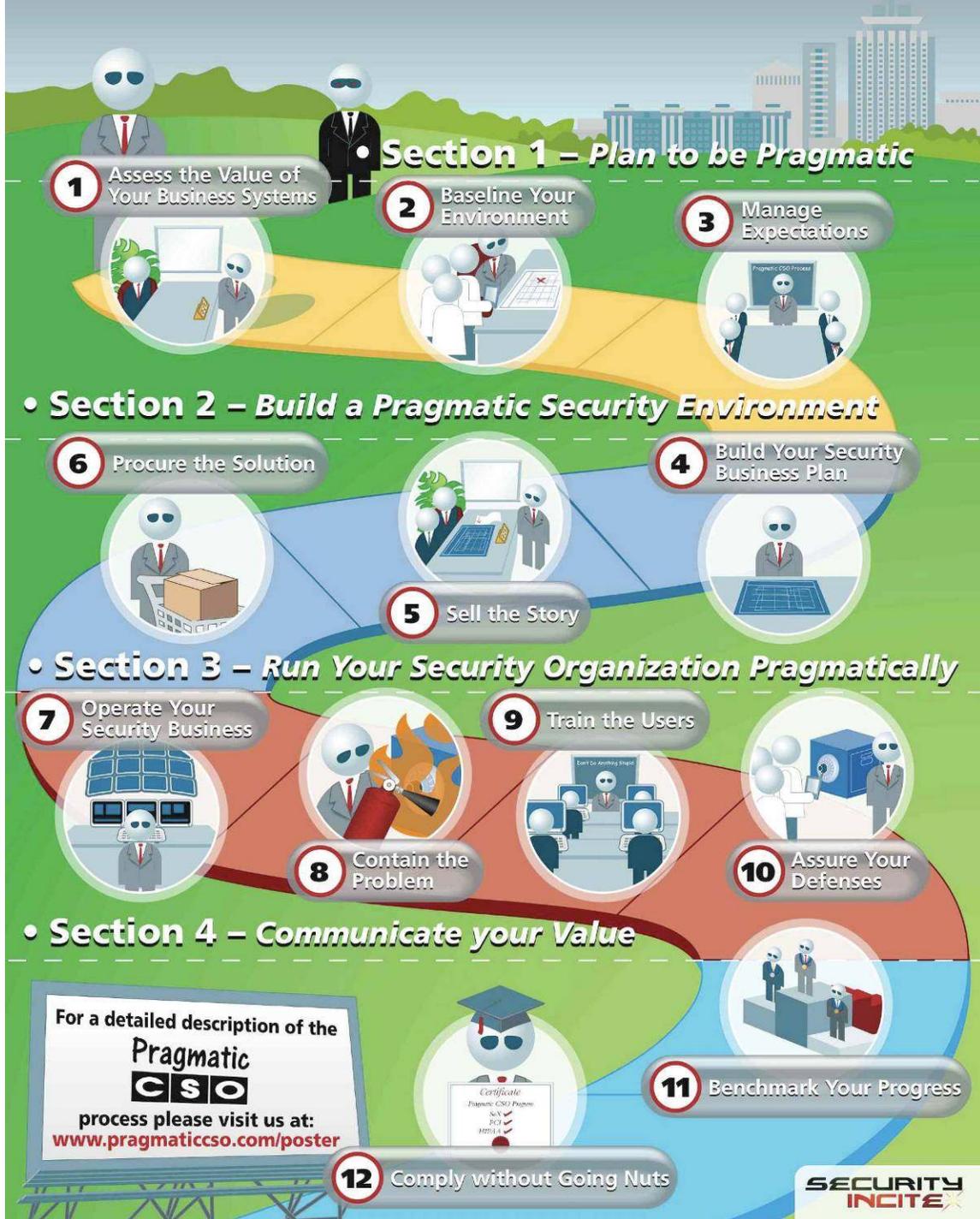
Let's discuss some specifics about the Pragmatic CSO methodology:

- Section 1 – Plan to be Pragmatic

  - Step 1: Assess the Value of Your Business Systems
    - You can't protect what you don't know about, so the first step is to figure out what you have. Likewise, you don't want to spend $50,000 protecting a $2,000 business system, so in Step 1 you talk to senior management and discern how important each system is to the operations of the business. Then you can figure out how much to invest in protecting it.

  - Step 2: Baseline Your Environment
    - If you don't know where you are, it's pretty unlikely you'll know that you've made progress. In Step 2, you gather data to understand your current state, where your most significant exposures are, and how much work you need to do.

  - Step 3: Manage Expectations
    - Managing executive expectations are the most critical responsibilities of the CSO. You must be very clear about what you are going to accomplish and how you are going to do it. In Step 3 you see the power of speaking security in the language of business, and how you can get everyone on the same page regarding what the security program does.

- Section 2 – Build a Pragmatic Security Environment

  - Step 4: Build Your Security Business Plan
    - Every business needs a plan, and yours is no exception. In Step 4, you prepare a high-level business plan, laying out the reasons your business exists and presents a high level architecture, committed service levels, and the milestones that you plan to achieve.

- o Step 5: Sell the Story
    - ▪ You need money to secure anything, in Step 5 you package your business plan, associated service levels and milestones and sell the program to senior executives getting the funding you need to protect your corporate assets.

- o Step 6: Procure the Solution
    - ▪ A structured procurement process is critical to getting the right products, at the right time, for the right price. In Step 6, you learn about Security Incite's Buying Security Products methodology and how that should be applied to how you buy the products and services you need for the Pragmatic CSO process.

- Section 3 – Run Your Security Organization Pragmatically

    - o Step 7: Operate/Monitor
        - ▪ Now that parts of the solution are implemented, you need to make sure they're doing what they're supposed to. In Step 7, you learn how to fortify your perimeter defenses, what you should be monitoring, and how to navigate the change control process.

    - o Step 8: Contain the Problem
        - ▪ Inevitably you will have a compromise or breach situation. Dealing with that will make the difference between a CSO with a job and one collecting unemployment. In Step 8, you learn how to recover as gracefully as possible and use a structured incident response process to make sure you live to fight another day.

    - o Step 9: Train the Users
        - ▪ Users are the weakest link in the security chain, so all the technology in the world will not help if a user gives up a password to the bad guys. In Step 9, you learn why a structured user awareness training process is critical to educate users to think and act securely and avoid many of the easy attacks used every day.

- o Step 10: Assure Your Defenses
  - ▪ It doesn't matter if you say something is secure, you need third-party validation. In Step 10, you'll engage third parties to try to penetrate your defenses, both to see where you are really exposed and also to make the case for more funding.

- Section 4 – Communicate your Value

  - o Step 11: Benchmark Your Progress
    - ▪ Quantitative measurements prove your worth and ensure your program is moving in the right direction. In Step 11, you'll benchmarking your program by tracking the right metrics and comparing what you are doing relative to your peer group and other businesses your size.

  - o Step 12: Comply without Going Nuts
    - ▪ Compliance with a variety of both internal policies and legislative regulations is a critical aspect of every CSO's job. In Step 12, you see how compliance is a benefit of implementing the Pragmatic CSO program and how by generating a set of hard-hitting reports, the auditors will be gone in a fraction of the time it used to take.

Of course, not all steps within the Pragmatic CSO methodology will make sense for your organization. You need to figure out for yourself how to build your own program to achieve your own goals. The Pragmatic CSO will outline a framework to kick-start your efforts, and you'll also have an opportunity to participate in the web-based Pragmatic CSO community, which provides access to templates and discussion forums for each step in the process, as well as getting security research from Security Incite.

The key message you should take away is you are not alone. Everyone involved in the Pragmatic CSO is vested in your success. Good luck on your own journey and get ready to change pretty much everything you know about security.

Why Buy the Pragmatic CSO?

Actually, you don't need to buy the book. Perhaps you like to spend your days with a fire extinguisher strapped to your back, trying to make sure the house isn't burning down. Maybe you enjoy the attention of getting emails and calls at all hours telling me about potential security issues and things you need to add to your To-Do list. Lots of people take joy in groveling to get a new piece of equipment to stop the latest attack vector. And maybe you are one of those folks that looks forward to the bi-annual ritual of the auditors telling you that you are an idiot.

But probably not. The job of the CSO isn't much fun anymore.

If you are tired of spending your days filling out reports, making spreadsheets for business cases, and sitting in meetings with auditors, then by all means keep doing that. But that's not why most people became CSOs in the first place, now is it?

The Pragmatic CSO changes everything

The Pragmatic CSO will show you that most CSOs are addicted to the heat of the battle. Many thrive on reacting to the latest attack and would pull out all the stops to get that new piece of equipment that was going to change everything. But nothing ever changes, does it?

Until now, that is. The Pragmatic CSO takes you through a 12-step program [http://www.pragmaticcso.com/poster] that will get you back on top of your game. To be clear, it's a lot of hard work and you will really have to change the way you think about security.

What if you could close your eyes and envision exactly how you'd like your security group to operate? Would it be something like this?

- Senior management asks your opinion – Security is part of the team now, so before a new initiative or application gets rolled out, you are consulted to make sure there aren't any critical holes.

- You run a business – Through the Pragmatic CSO, you build a business plan for your security operation, which will help to get the funding that you need in order to the job. As long as you hit the objectives you have laid out, you get the rope you need to execute on the plan.

- No more chasing the attack de jour – It's crystal clear what's important to protect and you focus on making sure those business systems are protected. There is no question about what your priorities are on a daily basis.

- The auditors are your friends – By changing your perspective on how you deal with the auditors, you can give them what they need and they help you accomplish your goals. Who would have thought it possible to get a win-win with auditors?

Being a security professional, you are probably a bit skeptical of crazy claims from yet another pundit trying to tell you what time it is with your own watch. That's fine; don't take our word for it. Look at what Ken Camp (www.ipadventures.com) has to say about the Pragmatic CSO:

> *Mike Rothman's the Pragmatic CSO presents a fresh, human approach to the intimidating world of managing enterprise security. It provides real-world examples and lays out the basics any Chief Security Officer needs to succeed. It's an easy, entertaining read that every business executive with an interest in securing their enterprise should have. If there's a "must read" book for business managers grappling with broad enterprise security challenges, this book is one of the best I've seen.*

Who is this Rothman guy, anyway?

The author of the Pragmatic CSO program, Mike Rothman, was META Group's first network security analyst, and was advising clients on security topics before the Internet was even called the Internet. For over 15 years, he's had a front row seat as the attacks changed – but the results stayed the same. Most organizations are still woefully unprepared to protect their corporate assets.

It was Rothman's idea that CSOs need to act more like business people in order to thrive. So the Pragmatic CSO is designed to make sure that regardless of your skill level and management chops, you'll be able to proceed through the program. He's also designed this cool Web community (available in February 2007) that provides Pragmatic CSOs with a place to ask questions and get more information about the program.

Still Skeptical? You have Nothing to Lose!

Still sitting on the fence? Let's go through what you can achieve with the Pragmatic CSO – one more time:

- You'll get a seat at the table – Senior managers will be consulting you before they rolled out an application. It's not a pipe dream.

- Users will get it – Your employees will no longer be the bane of your existence. Many will stop doing stupid things because they'll actually understand what not to do.

- You'll know what not to get done – No longer will you need to spend all of your waking hours trying to get everything done, no matter how trivial it seems. A clear idea of priorities will make sure you stay focused at all times.

- You'll live to fight another day – Security incidents are part of the territory, but you'll be prepared. You'll learn how to know something is up and what to do, who to call and how to recover – without fatally damaging your credibility.

To be clear, the Pragmatic CSO is not cold fusion. The idea of a security program has been around for a long time. But the Pragmatic CSO takes a different tack on the security program – how it's packaged, who the audience is, and how to give senior executives what they want.

You can pay your favorite auditor to park 5 bodies on site and execute on a security program for you. You've probably done that already. Did it help your credibility? You can also consult some of those high-priced analysts that will charge you $50,000 to send you a few research notes and spend an hour on the phone with you. That will make sure your ass is covered ("the analyst said it was a good idea"), but is it going to help you execute on a security program?

As was said in the very beginning of this section, you don't need to buy the book. You don't need to join the community. You can keep on keeping on and hoping that things will get better. But is hope the best strategy for you and your security organization? That's the question you need to answer.

For $97, you can give the Pragmatic CSO a try. That's less than you probably spend at Starbucks each month. And you have nothing to lose. If don't see how you will receive 20 times the value, just ask for your money back. That's right, anytime within 30 days, you can ask for your money back – no questions, no heartburn.

So what are you waiting for? Go back to www.pragmaticcso.com and click the BUY NOW button. You have very little to lose, except maybe the status quo.

Other resources for the Pragmatic CSO

- *Pragmatic CSO Web Community* – Your long-term success as a Pragmatic CSO is dependent on your support group. Joining the Pragmatic CSO community will give you a place to dig deeper into each of the steps and stay current on what's going on in the world of security. The community will feature the following sections, and much more:

  - Pragmatic CSO support – Members working through the 12 Step process will find specific forum for each step, with templates to kick-start efforts, and discussions to help ensure the successful completion of the step.

  - Security Incite research –Security Incite will publish 8 "Battle Plans" in 2007 that help members to wade through the hype and learn what they need to know about solving the most critical problems they are facing.

  - CSO and Hot Seat interviews – Each month Mike will also do 2-4 interviews to get some field-level insight about what is working and what isn't. These detailed interviews go far beyond today's podcasts and pull no punches about what you should be doing and what is a waste of time.

- *Pragmatic CSO Coaching* – For those uncomfortable interacting and sharing information in the Pragmatic CSO forums, one-on-one coaching can be arranged with Mike Rothman, the author of *The Pragmatic CSO* and the President of Security Incite. Coaching engagements involve a monthly conference call to track progress and discuss your specific situation as well as the ability to ask questions via email.

- *Pragmatic CSO Training* – The 12 Step Pragmatic CSO methodology will be delivered in an intensive 2-day boot-camp program, and attendees will be able to work with Mike Rothman on their adoption of the Pragmatic CSO project via a one-year coaching relationship to assist in applying the lessons learned in the boot camp.