SANS Institute
InfoSec Reading Room

Leading the Transformation of a Security Organization as a New Security Manager

Leading the Transformation of a Security Organization as a New Security Manager

GSLC Gold Certification

Author: Robert Mayhugh, rob.mayhugh@gmail.com

Adviser: Dominicus Adriyanto Hindarto

Accepted: August 13, 2008

Table of Contents

1. Introduction

This paper will document my experience and provide insight into my assignment as a new security manager tasked with improving network security and "making things happen." I will discuss how I evaluated current state, defined a vision and mission, created a roadmap, and gained buy-in from senior management to adopt the plan and begin the security team's transformation. The paper will be interesting an insightful for other managers finding themselves in a similar position. It will also be of interest to existing and experienced managers and show what works and what does not work in today's corporate environment when attempting to affect change.

2. Evaluating Current State

What do we do today? The first thing you want to do (i.e. within the first two weeks), irrespective of the team you are moving into, is to take stock of what comprises the team's current responsibilities. Make sure you speak with everyone on the team: as individuals and as a team. It is important that you begin to get the pulse of the people and what makes them tick. I see a lot of managers skip this step and the "us vs. them" mentality begins immediately. Your new team will not feel

included and not feel that their opinions matter. It is the leader's responsibility to begin the building of the trust relationship.

What skills exist on your team? Just as important as understanding your new team's responsibilities is an understanding of what skill sets exist on your team. Giving direction or establishing a vision or mission can be futile until you understand the strengths and weaknesses of your team, and how these might align with your departmental and business objectives. In my situation I discovered that my team was "security" only in name; there were no team members that had received any formal security training, and none were certified at any level.

Look before you leap! This could be the moral of this entire paper. Come in with a positive attitude, talk to everyone, and understand what you are dealing with before moving on to the next step: creating your vision and mission.

3. Vision and Mission

What is your team all about? This is the basis of your vision, the point in the distance that you are driving towards

and it is supported by your organizational mission and values. What is your focus? This is the basis of your mission, what you bring to the business on a daily basis to ensure success. It needs to be simple enough to understand, but uncompromising in its message. As an example, the mission statement I formed for my new team states, "*Operational Excellence through industry-leading security practices.*" Every decision we make needs to measure up to this standard. In comparison, the vision statement is more idealistic and underscores "why we do what we do." Our vision statement reads, "*Network Security protects intellectual property and proprietary customer data to ensure confidentiality, integrity, and availability for the business and our valued customers.*" Do you see the difference? On a daily basis we are striving for "operational excellence" and "industry-leading practices." These guiding principles support the "why we do what we do" perspective of the vision, which is providing the security triad of confidentiality, integrity, and availability to our business and our customers.

You must communicate both your vision and mission relentlessly. These are not "slogans," they are the very fabric that every team member must live by on a daily basis. You talk about it at team meetings, you talk about it when meeting with

other organizations, and you talk about it while getting your morning coffee. Your goal is to have your organization know, without thinking about it, what your team is about and what you bring to the business. Security standards can be forced as a matter of policy and regulations, but think of how much better (and easier) it is when you have a welcoming seat at the table, and everyone knows why you are there.

Are you aligning with the business? This is a critically important question to ask. You might have some great ideas and a passion to implement them, but if you are not aligning yourself to provide the most value to the business you will quickly become frustrated. Others will not see your initiatives as important or worthwhile; you can easily perceive this as a direct affront to your values! You had the best of intentions when you laid out your vision and mission, and to have your ideas rejected is difficult to absorb. Aligning yourself with business objectives gives you a much better chance of achieving your goals and being successful.

4. Creating a Roadmap

As stated previously, you first need to understand the business objectives. Are you detecting a pattern? To be an *effective* security organization you need to be plugged into what the business wants and expects. Understanding what makes the business tick and how you can play a significant role is of vital importance to your success. Just as important are your departmental goals. Is your department aligned with the business? This answer is usually "yes" since your departmental executives will be peers with the executives traditionally considered part of the business: Finance, Sales, Marketing, and Care. Your departmental goals and objectives should be published and known to all; this is your starting point. If you need clarification or further direction you need to engage the executive that owns security, usually your CISO or CIO (or the CEO if you are one of the former), and come to a consensus regarding the posture of the security organization.

Now that you have started the process of aligning your team with departmental and business objectives you can begin creating the team's roadmap. As you go through this process you must keep in mind your team's skill sets and expertise that you

documented earlier; these may or may not match up well with your roadmap. Adding additional resources that have the skills that you desire is not usually an option. This being the situation, you will need to include training requirements within your roadmap. This will include specific training with costs and how that training aligns with your roadmap, mission, vision, and overall departmental and business objectives. For me, this became a parallel roadmap that became a dependency for achieving success with our overall roadmap. As our initial training vehicle we partnered with SANS to help build and justify our requirements.

As security professionals it is extremely important to have credibility in the eyes of the organization. One way we do this is to show the organization that your team has the training and experience by obtaining industry recognized certifications. Requiring certifications also reinforces the training you are paying for, and ensures your employees will take the training seriously. My initial training roadmap yielded 23 individual certifications in the first 18-months, including four CISSP's. Prior to this, there were no formally trained or certified team members.

Figure 1 shows an example of a high-level roadmap, the details of which are explained in subsequent slides.

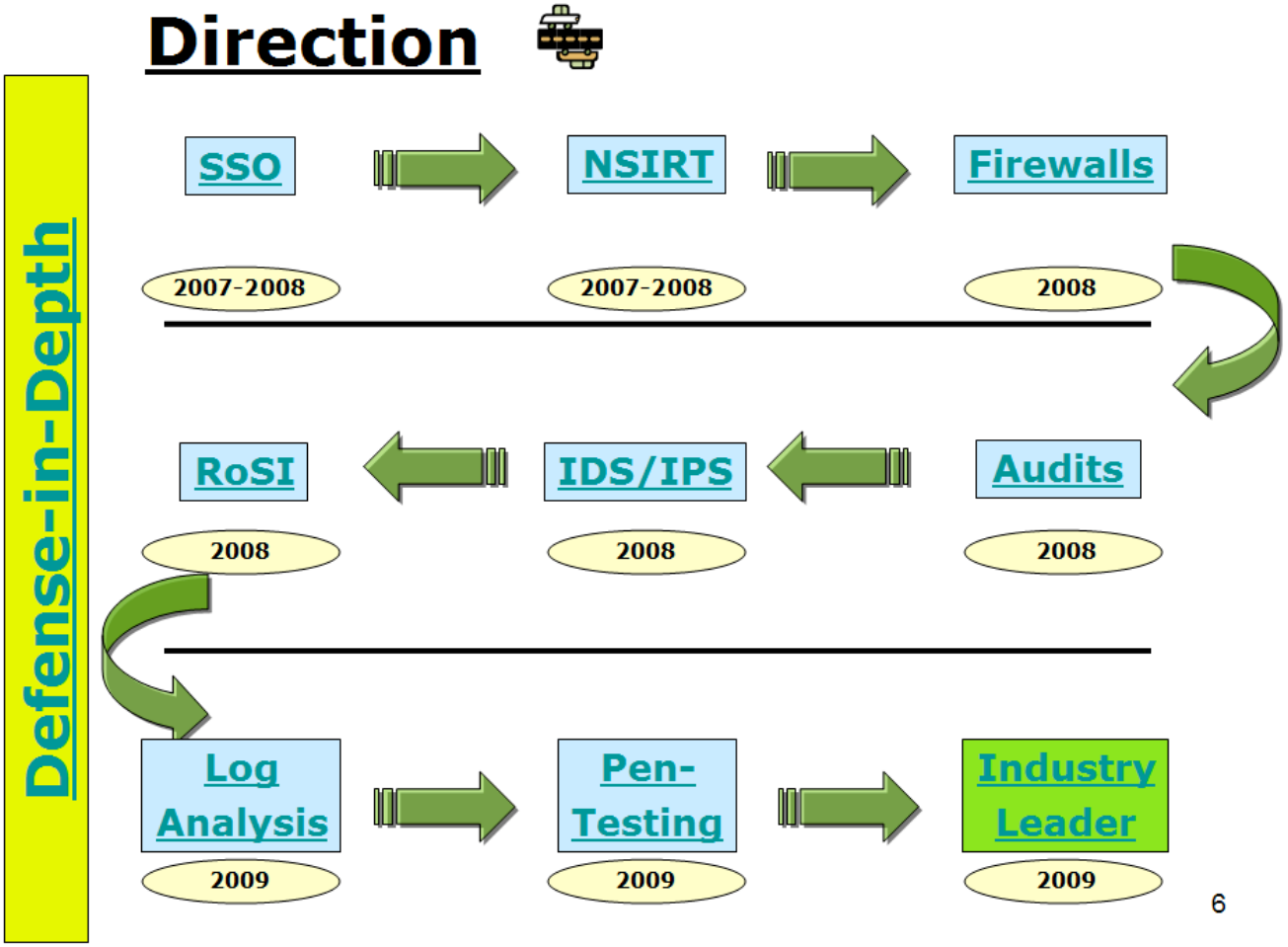

Figure 1

As depicted in Figure 1, the initial roadmap laid out a systematic approach to cover all the major areas of

responsibility:

- **Single Sign-On (SSO):** This was a project to reign-in user access across the network, standardize it, and implement role-based access that was tied into the corporate Identity Management System (IDM).
- **Network Security Incident Response Team (NSIRT):** This was an effort to leverage the existing corporate security incident response capabilities and create a network-centric process. We knew we were deficient with some of our countermeasures, so a plan to react to and contain incidents was critical.
- **Firewalls:** The firewalls were the strength of our security measures, but change management for firewalls was not standardized and did not follow the corporate change management procedures. In addition, there were too many teams that had access to the firewalls. This was an effort to standardize process and limit access.
- **Audits:** Audits were being performed, but they were not regularly scheduled and were usually performed as a reaction to an incident. We formalized this process, created a schedule and made our audits proactive.
- **IDS/IPS:** Intrusion Detection and Prevention was a strength within the company. This was an effort to become part of the IDS/IPS change and management process so that our frontline people understood the rule-sets and what they were doing.
- **RoSI:** The preceding roadmap items were either cleaning up

or enhancing an existing system or capability. We were now entering into items that would require major funding to move forward. Previously, justifications for security measures were largely feared-based presentations or a subjective qualitative analysis. We wanted to minimize this type of justification and move to a more quantitative methodology using the *Return on Security Investment*, or RoSI method. RoSI is discussed later in this paper and an example can be seen in Figure 2.

- **Log Analysis**: We did not have a centralized log management or analysis capability. As of this writing, a corporate policy and standard has been put in place to address this capability. We are currently evaluating vendors and preparing budget justifications for our next fiscal year.
- **Pen Testing**: This was an existing capability that had been allowed to go dormant for fear of negatively impacting a network device. This fear, largely from system and database administrators, was unfounded and we have begun efforts to resurrect the program. This too will require funding to update or obtain new tools, and/or partner with a third party to perform these tests.

The order in which we attacked issues on our roadmap can be debated, but it is largely dependent on the current state of your organization. This is why it is critical that you assess your situation, your team, align with the business, and have an unambiguous vision and mission.

5. Gaining Buy-in

Who are your stakeholders? Ultimately, the major stakeholders are your highest ranking executives; these are the people that will be held accountable by customers and shareholders if the company suffers a security breach. Appealing to the interests of your stakeholders is a process you have already begun if you have taken the steps to align yourself with the departmental and business objectives. This ensures you are looking out for the information and systems that are most important to your company, and keeping your company and its executives safe from negative headlines.

You must seek out and identify your biggest and most vocal critics. This will vary from organization to organization, but it is critical you identify these individuals or teams. Politics within your organization is a realistic and unavoidable consequence of business. Not everyone will agree with your point of view and how you plan to go about doing things. If these individuals or teams feel your agenda threatens their own agenda or position, and you do not recognize it or address it, it can threaten what you are trying to accomplish. The best approach is to acknowledge these individuals or teams and speak to them

directly. As Stephen Covey promotes as Habit #5 in his book, *The Seven Habits of Highly Effective People*, "You must first seek to understand, and then be understood" (Covey, 1989). By giving your critic an audience, acknowledging them, and working to be inclusive of their concerns, you stand a very good chance of not only diffusing the situation, but gaining a new ally.

Who controls the dollars? In most organizations this is the department head. The majority of executives I have worked with have a "better, faster, cheaper" approach to things. By using a Return on Security Investment (RoSI) approach you can appeal to this type of thinking. Security is all about managing risk. Executives do not like surprises, especially when it impacts their reputation or their budget. Identifying the security risks and presenting them in a quantitative format eliminates part of the surprise. Adding to this analysis the countermeasures that could be deployed, what they cost, and the amount of time it would take for these countermeasures to pay for themselves (known as the Return of Security Investment, or RoSI method) is the security manager's responsibility and duty. This eliminates the budget surprise and builds credibility for the security organization. It shows business acumen and a willingness to do what is right…within reason and budget. We could spend millions

upon millions of dollars on countermeasures, but presenting a quantitative analysis that shows where money is best spent should be the goal of every security manager.

Figure 2 shows an example of using the RoSI methodology:

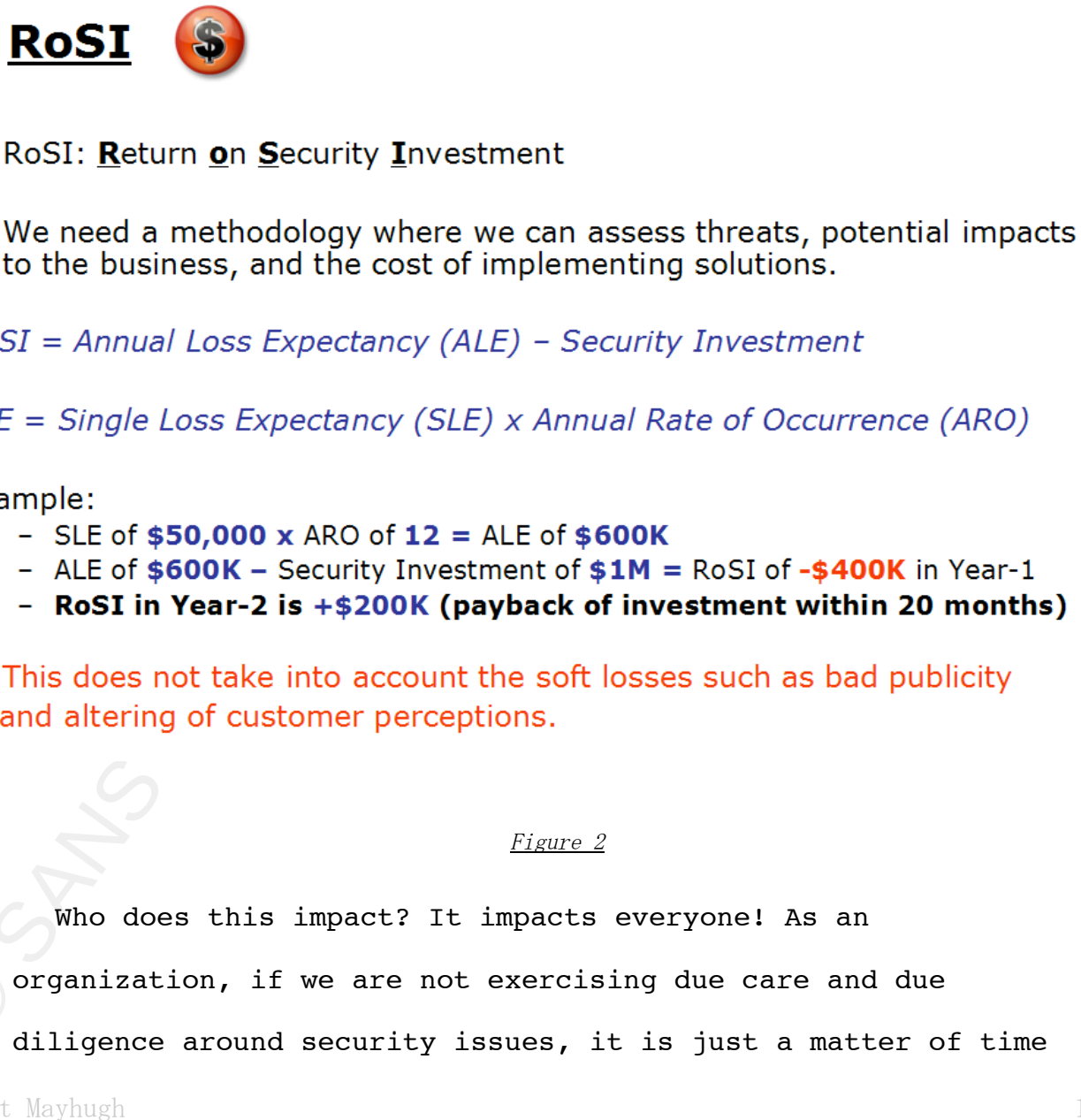

Figure 2

Who does this impact? It impacts everyone! As an organization, if we are not exercising due care and due diligence around security issues, it is just a matter of time

before we experience a breach and end up in a situation like T.J. Maxx (iTnews, 2007). It could truly be the difference between being a relevant company and a company that is no longer in business.

6. Execution

You must be tireless, consistent, and passionate in delivering your message to your team and your constituents. Change is difficult, and if you are not consistent it will open the door for the naysayers and those that want to perpetuate the status quo. Just as important is being consistent and confident with your management chain; managing up is just as important as managing down. I cannot emphasize enough the necessity to "walk the talk." Your team members, peers, and management are always watching and taking cues from your behavior; this is especially true when you are a taking over a new team.

Create and set line of sight (LOS) and stretch objectives. LOS objectives are short term and provide you the opportunity to engage in some quick wins. This will improve your team's morale and begin to build confidence and credibility for the team. Stretch objectives step outside of the SMART (Specific, Measurable, Actionable, Realistic, Time-bound) format in that

they are usually beyond what most would consider "realistic." Meeting LOS objectives is good, but hitting the stretch objective is a tremendous feat and should be rewarded as such.

Figure 3 shows the initial set of goals and objectives formulated from a team brainstorming session.

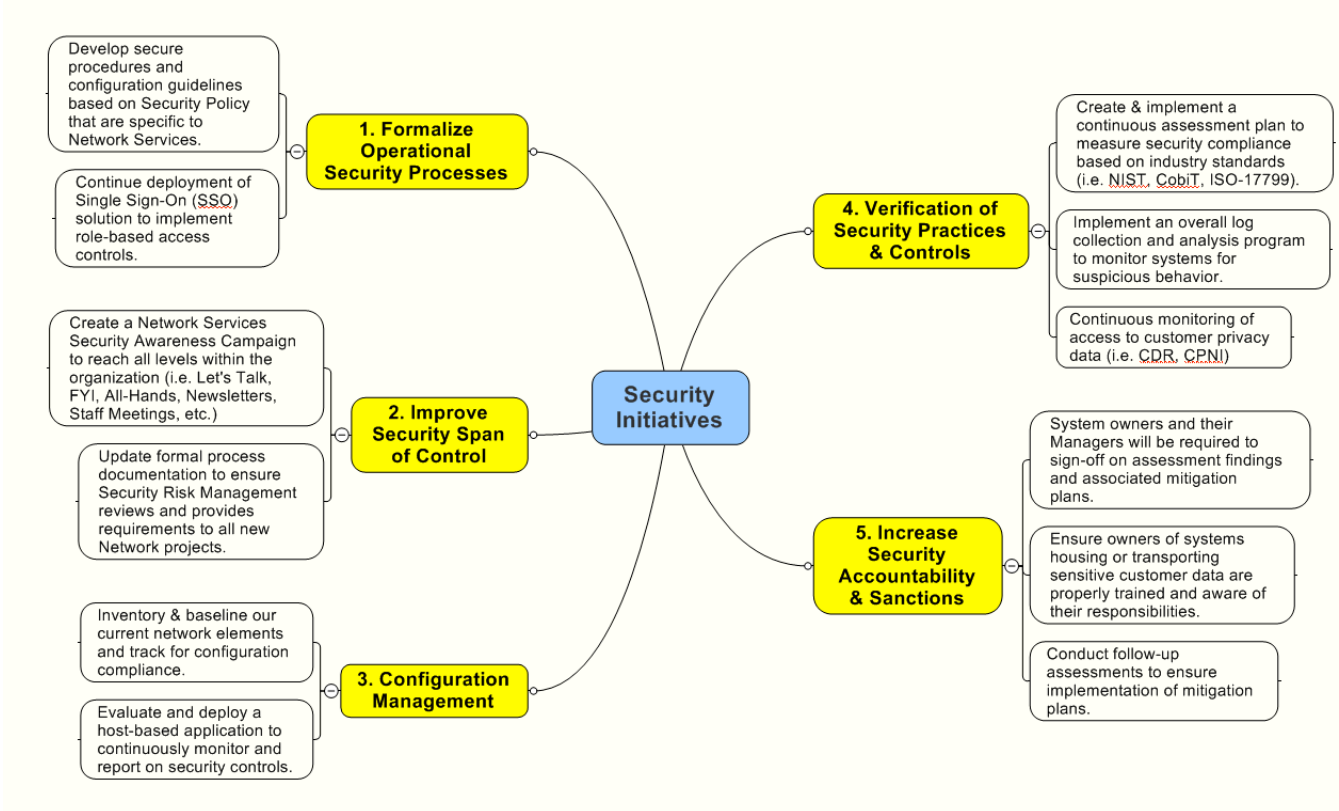

Figure 3

You must measure your progress! If it is not worth measuring,

it is not worth doing. Whether or not you agree with this statement, in a business environment it is true. When you have goals, objectives, initiatives, roadmaps, etc, it is crucial that you measure your progress to know if you are being effective and if what you are doing is producing the desired results. Always remember that you must constantly and consistently show your value to the business. The only way to do this is by measuring performance and providing an honest view of how your team is performing against agreed upon objectives.

7. Lessons Learned

Don't put the cart before the horse! You are new to the team, you are excited, and you want to get right to work implementing all of the great ideas you have. Sound familiar? Many managers are guilty of this and just assume that their new team will be just as excited and willing to implement all of the changes. Wrong! Assuming you do not have any immediate burning fires to extinguish, it is best to take a slower approach, meet and get to know your new team, listen to their ideas, and incorporate them into the process. One thing that I like to do that has been extremely effective is to ask everyone to answer five questions that I picked up from a book titled, *You're in Charge – Now*

What? (Neff & Citrin, 2005, p. 264):

1. **What are the five most important things about this team we should preserve and why?**
2. **What are the top three things we should change and why?**
3. **What do you hope most I do?**
4. **What are you most concerned I "might" do?**
5. **What advice do you have for me?**

I supply these questions to the team in advance and give them a day or two to ponder them. I then will meet with each person individually and use these questions and answers as the basis of our conversation. I am always amazed at the candid and thoughtful feedback I receive. It is also a rare thing when an employee does *not* thank me for asking for their input and listening to their ideas and concerns.

8. Summary

In the great Jim Collins book *Good to Great: Why Some Companies Make the Leap...and Others Don't*, Collins talks about the fact that great organizations always think about "who" before they consider "what or where." In Collins' words, "If

[you] get the right people on the bus, the right people in the right seats, and the wrong people off the bus, then [you can] figure out how to [drive] it someplace great" (Collins, 2001, p. 41). Most of us will not have the luxury of building a team from scratch, and we are put into situations where we need to meet expectations with the resources that we have. Evaluating your resource talent needs to be a continuous exercise, as security threats and technologies are ever-changing. Your resources need to be as passionate about success as you are (the right people on the bus). Those resources that will not buy-in need to find new homes (the wrong people off the bus). This does not imply that you should not be caring about people. After you have set in motion your vision, mission, and roadmap, and put in place SMART goals and objectives, the people on your team that do not fit will quickly realize they are on the wrong bus and will, more times than not, leave on their own accord. The ones that linger can be managed using your company's standard performance management criteria. Once you have identified your best resources, put them in positions of authority, guide them, and help them succeed (the right people in the key seats). In addition to boosting their confidence and morale, it will send a clear message to people who have not yet bought in that they may

be on the wrong bus.

Once you have aligned your team, you can begin to align with the business and departmental objectives. You will have confidence moving forward knowing that you have motivated, capable people in the most important roles. Your constituents will see the motivation and capability and will have confidence in your team's abilities. This will breed confidence in your team and spur them on to do more. Your team's ultimate goal is to be seen as a trusted partner and advisor; someone who has a seat at the table because you protect and enable the business.

Lastly, I wish to share with you my team's five key imperatives. Everything we do must tie into these:

1. **Build security expertise (invest in our people)**
2. **Partner with the business (get a seat at the table)**
3. **Invest dollars where it makes sense (RoSI)**
4. **Be diligent and stay the course (security is not negotiable)**
5. **Operational excellence through industry-leading security practices (our customers expect it)**

9. References

Collins, J. (2001). *Good to Great: Why Some Companies Make the Leap...and Others Don't*. New York: Harper Collins

Covey, S. (1989). *The Seven Habits of Highly Effective People*. New York: Free Press

iTnews. (2007, May 18). *TJ Maxx security blunder will cost US$8.3B*.

Retrieved July 9, 2008, from http://www.itnews.com.au/News/NewsStory.aspx?story=52299

Neff, T., & Citrin, J. (2005). *You're in Charge — Now What?* (pp. 264). New York: Crown Publishing

Last Updated: October 2nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced