How to Implement an Information Security Program

Charles Hornat
www.infosecwriters.com

Contents

Overview

I read an article recently that Stephen Northcut linked to in LinkedIn about how so many jobs today are being posted as “Security Engineers” when in fact that very term was questioned. What is a Security Engineer? While I hope we can mostly agree to what an Engineer is, can we agree to what the security part is?

I teach at a prominent NY university and the first question I ask every one of my classes is, what is security? I get a variety of answers from knowledge of tools like antivirus and firewalls to someone who writes policies and procedures. What fascinates me is that these are part of the job description but not the actual definition of security.

People tend to think of security at so many different levels that we forget or do not realize that it is an art, a process, a mindset that isn’t bought or installed. It’s integrated, accepted and becomes a habit. This paper will outline steps I have taken over the years and have had success with.

So with regards to the article Mr. Northcut provided, should all Engineers be “security” Engineers? Should any job today be defined with “Security” in the title outside of an Officer of the company responsible for it?

This write-up is about my approach to Information Security and based on my own experiences. There are a number of ways to implement a program, but I believe that one has to first identify what they are protecting, understand the risks and associated threats, and then formulate a plan of protection.

What is Information Security?

Definition

Before we dive in to understanding what is in an Information Security program, we need to understand what Information Security is. Let’s define Information Security as reducing risk to an acceptable level by the data owner or the business owner.

Achievable?

I also ask this question to every class, and the answers sometimes surprise me. Most who answer this have no reason to their answer. So I ask that you take a moment and ponder. Is there a point where a security manager can sit back, fold his hands, and be confident that the organization is now secure and their job is done?

The short answer is “no”. Everyday someone is working on new exploits to wreak havoc on your networks and computers. This havoc can result in system downtime, application errors, or impact products and services we offer our customers. Everyday there is a disgruntled employee. Everyday there is the potential for a natural disaster to hit our infrastructure. There are too many threats to list here but you should get the idea.

Knowledge

How does one learn about all the different types of threats or risks? Information Security is more about knowledge than anything else. How does one get this knowledge? They read, study, test, talk to others, and anything else that one can do to expand their knowledge. Luckily, the World Wide Web is here today and a great tool for security. There is so much information out there, and so many great sites like PacketStormSecurity.com or my favorite, Infosecwriters.com. There are great training sites like SANS[1] or Elearnsecurity[2].

There is little excuse to not be aware of zero day announcements in this day and age, and no excuse to not understand how to address them.

Information Security Program

So now that we understand what security is, and how we can learn more, and the fact you are reading this paper, let's take a simple walk through of your first day on the job as a security manager.

The very first thing one should do when starting a role as someone who is in position to protect the "Crown Jewels" and that is understand the "Crown Jewels". What are they, where do they reside, how are they used, who should have access to them. This process would be considered the Risk Assessment process.

It is common to group the parts involved in to three unique areas: People, Process and technology. As you will see below, I have outlined in a very brief format, common core areas that are applicable to this. People contain User Education as well as the individuals and departments involved with creating and enforcing the Information Security Program (ISP). Process includes Risk Assessment and the actual implementation of the ISP. Finally Technology, which would include any software and systems designed to help assist with the enforcement and monitoring of compliance of the ISP.

Risk Assessment

Risk Assessment is the process through which one will identify the Crown Jewels and all the risks, threats, and vulnerabilities associated with them. There are several risk assessment practices available today. I use the Octave[3] method written by CERT but there are alternatives such as the ISO 27005 or the NIST SP 800 30 framework. I prefer the Octave process because one can start at the top and the bottom of the organization to really get a feel for risks and usage of classified data.

Risk assessment should be in alignment with the corporate risk management strategy and circle around to risk treatment. The process in which I refer to here is specific to the identification, analysis and evaluation of risks to an identified crown jewel.

---

[1] http://www.sans.org/

[2] https://www.elearnsecurity.com/

[3] http://www.cert.org/resilience/products-services/octave/

When going through the risk process, it is important to note a few things:

- Should be accepted and approved by top management
- 4 things one can do with risk: Accept, Reduce, Eliminate or Transfer
- Business owner decides what's acceptable, not Security or technology

Be sure to work with the business owners to understand their concerns. Ask them what happens if the data is altered, deleted or disclosed? How will that impact the business overall.

Policy and Procedure

Now that you have performed a Risk Assessment, identified the crown jewels and risks/threats associated with each, you will want to start to formulate some policies and procedures around protecting those jewels.

Through the first process, you have made some allies in the company. Ask these people for assistance to build a standard policy. This policy should outline and include any federal, state or local laws as well as third part requirements such as PCI. If you fall outside of either of those, use best practices. There are some great references like the SANS top 20 Critical Security Controls[4].

To write a policy, you should consider a few things:

- Acceptance company wide and most importantly from owners/CEOs
- Policy should be a list of minimal security requirements to meet legislation, best practice or third party requirements
- Employee education and awareness of the policy
- Enforcement and repercussions for not adhering to the policy
- Exception process
- Should include an overall statement from the CEO/Owner about their commitment to Information Security
- Include the business owners input

Anyone can write a policy, but to get it agreed upon, approved, and implemented so that everyone is aware can be a difficult challenge. How far is management willing to reprimand someone for violating policy? How does one circumvent the policy when business requires it? Also consider who will approve exceptions. It should not be security, legal or HR. It should be the business owner or data owner agreeing to understanding the risk and accepting it.

Frameworks for policies are also available such as the ISO 27002 or NIST. Sans.org and other online resources have templates you can download and fill in the blanks.

[4] http://www.sans.org/critical-security-controls/control/20

Tools and Technologies

Tools and Technologies should be brought in to help enforce, detect and restrict actions by users and attackers. They should not be used outside of policy, but be used to help enforce the policy. Firewalls, antivirus and system/application patches are there to protect users as defined in the security policy. Data Loss Prevention should be used to identify classified data (as defined in the policy) leaving the organization without permission. Proxy solutions should be put in place to block users from downloading programs and infections as defined in the policy. System restrictions should be put in place to prevent alterations to the systems or prevent unapproved software from being installed on systems per the policy.

At this point, be sure to get a valuation on the data you are protecting. This will help put a perspective on how much to spend to protect that very data. While there isn't a magic number or formula for calculating cost to protect versus cost of risk, let your business owner decide this with what they are comfortable with and what they are will to accept.

User Education

Users represent a security officer's biggest concern. They are targeted by attackers all day, every day. Attacks can come as an email with a malicious attachment, a Facebook app, or an advertisement on their favorite site. They are one of our first lines of defense, and it won't cost you yearly renewals or license fees!

When I was at Standard and Poor's, we did something that was received well among staff. We did a program called "Lunch and Learn". The program was simple. I would put together a presentation to cover about an hour worth of topic a user should know and put it in layman's terms. The topics would range from spotting malicious or fraudulent emails to protecting their home computers. We would then send out an email to all staff to sign up if interested, and limit seating so it would be small and intimate. The goal is to teach, but keep it as an open discussion where participants could ask questions as we went through the presentation. We wanted people to be comfortable and not shy, but walk away with any questions they may have had, answered. Lunch would be ordered for them, pizza usually. The time of the presentation was about 45 minutes, but with questions and the like, it would sometimes run over the hour.

Partners

HR and Legal

Your best friends. Work with them in every policy and ensure they have your back from an enforcement and education aspect. They will help by

I was once asked by a senior level Vice President of a major financial institution to allow this person access to one of their employees email. Under US law, a company has the legal right to do this. However, our policy stated that they needed approval from HR or Legal for such a request. This person sought to circumvent that and come to Information Security.

They claimed that we lost a major sale because this employee did not respond to an email from the client. The client claimed they sent it, the employee claimed they never got it. This manager wanted to know who was not telling the truth. The employee was a long standing employee with a solid positive history with the company.

I asked a simple question, what will you do if you find what you are looking for, and what will you do if you don't find what you are looking for? The VP stated that they would not take action regardless of what was found. Then what was the point? I ask this question every time I am requested to grant "snooping" rights. Regardless, I did not approve or deny, but present the request to Legal who denied it based on the answer to my question.

Let these two groups make the decisions, you are just a consultant who understands risk and the policy. If you are asked to do something that imposes on employees or creates an uncomfortable situation, defer to HR and Legal for permission. If anything goes wrong, you did not act alone and without permission. This has saved me more than a dozen times in my career where other management did not take kindly to investigations or data gathering on certain employees.

Physical Security

Team up with this group quickly. They may provide the following:

- Access to security cameras
- Data center or server room access as well as monitor activity in it
- Building and office access
- Enforce clean desk policies
- Store evidence in a secure location
- Provide guidance and assistance during disasters like weather or terrorist activities

Audit

Internal audit can be one of you biggest allies. This group is usually well engrained in senior management and are generally heard well. They should be performing audits of processes and technologies based on the documentation the ISP has produced, best practices and legal guidance.

Once I identified a system put in place by physical security, who did not seek IT or Security help, which was being used for creating building passes. Anytime a visitor or non-employee needed access past the front reception/security desk, they needed to hand over a piece of ID with their picture on it and provide some additional information. The desk clerk would take the Picture ID and scan it in to the system to be saved in a server setup and maintained by physical security. In addition to the picture, they would also record the person's name, phone number and any other characteristics they could at that moment.

One day I received a call from someone claiming to have visited our building that very day, and that they used a new credit card with their picture on it for verification. They claimed to not have used that card anywhere else and that the card was used to make some fraudulent purchases just several hours after they were in our building. I decided to investigate and quickly realized that no one outside of physical security was aware of this system. Human Resources and Legal were not aware either. I had some concerns, not just about this person's credit card being compromised, but what about all the drivers' licenses and other identification information being stored on a potentially non-secure system in the building.

I first approached physical security who basically told me that they were above the law and the system was a directive by Sr. Management. So I contacted my friends in internal audit, and offered them an audit they couldn't refuse. Additionally, I gave them some points to consider. Such as are they recording the person's height, weight, address and driver's license number? Were they storing the credit card with all information associated with the individual? Was encryption used?

Audit performed their assessment and escalated to Sr. Management. Needless to say, Physical Security contacted me a few days later asking for guidance on being compliant with law and best practices.

Conclusion

It is very important to keep in everything you do in perspective with the business. Be sure not to overdo your approach, keeping everything to a minimum level of acceptance. For example, the longer the password and more complex, the more time it will take one to brute force it or memorize while shoulder surfing. Most security people will say to make the password requirement 12+ characters long, but we know from experience that that is a bit extreme for many, and may result in users writing down their passwords creating a new security concern. One must find the balance between security and usability, and that is something that helps make this job so unique.