Social Engineering Impact on Risk Assessments

Edward Escobedo

Lewis University

CPSC-59700 Project

One University Parkway, Romeoville, IL 60446

TABLE OF CONTENTS

ABSTRACT

Information security risk assessment is a continuous process of detecting, correcting and preventing security problems. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information systems. Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organization from some failure of its computer systems. My job as a security control assessor for the Department of Navy, all software and hardware systems that are deployed out onto Navy ships and shore establishments comes through my office. We see systems from simple applications to full enclaves that span between ships and shore stations. These systems also use a variety of networks that access the Internet and pass information which will be discussed further in this paper. It is paramount to understand that these systems are also classified which adds another layer to consider. For this research, I will focus only on unclassified information which will more than cover the research necessary for this paper. Recently, our office received information from the Navy Certifying Authority asking for the security control assessors to start considering social engineering into the risk assessments. The Navy has thousands of personnel either active duty or civilians that touch these systems daily. We do have a process (checklist) that covers the minimum when it comes to conducting an assessment. How does this in social engineering? We do not have anything that dictates this process. For the fifteen assessors in my office, we all look at this differently. There are general guidelines out there but nothing that is official. The National Institute of Standards and Technology has asked the control assessors to come up with a general checklist to include social engineering. This research paper will discuss social engineering and risk assessments according to the Navy, and attempt to provide information that will generalize a checklist that will include variables to consider for a security control assessor standpoint.

CHAPTER 1

INTRODUCTION

Information security risk assessments are a necessary element of a sound cyber-security program and are required for all Navy Department of Defense systems that will be deployed out the ships and shore establishments. The ultimate goal of a risk assessment is for an organization to understand the cybersecurity risk to organizational operations organizational assets, and individuals [1].

Conducting a risk assessment typically includes the following six steps: identify and document asset vulnerabilities, detect and record all threats, acquire vulnerability and threat information from sources, identify potential organizational likelihoods and impacts**,** determine enterprise risk by reviewing threats, vulnerabilities, likelihoods, and impacts and detect and prioritize risk responses. The goal is to be proactive. Best practices for conducting a risk assessment is adequate preparation. However, what does this require? Risk assessments preparation means establishing rules and having an understanding of the purpose of evaluation and scope, constraints and assumptions, information sources, and whether a risk model or analytic approach is being used.

There are several options for conducting the assessment itself, all of which will have some combination of reviewing the threats against your assets, identifying vulnerabilities, and consequences. The most useful risk assessments are informed by strong knowledge of the real tactics, techniques, and procedures that already have been used to target your organization or industry and that are likely to emerge from it.

Social Engineering is an often overlooked threat but regularly exploited; to take advantage of what has long been considered the weakest link in the security chain of an organization, the

human factor. An example follows [2]: In 1994, a hacker named Anthony Zboralski called the FBI pretending to be an FBI employee working in the U.S. embassy in Paris. He persuaded the person at the other end of the phone to explain how to establish a connection to the FBI's phone conferencing system. Then he ran up a $250,000 phone bill in seven months. This is just one many examples, and there are many ways that social engineering is conducted.

Figure 1illustrates a typical cycle of social engineering.

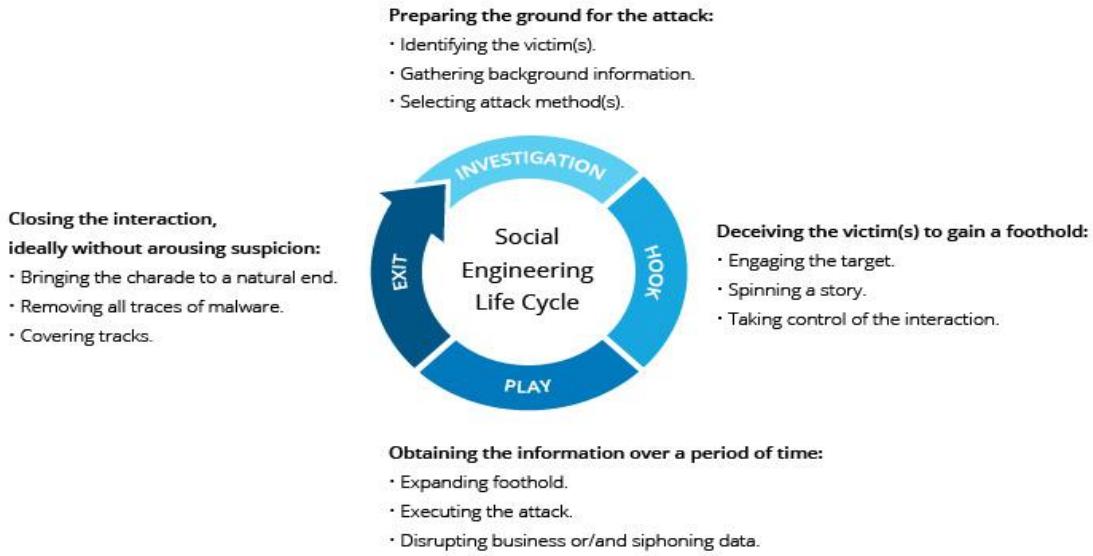

Figure 1.1 Social Engineering Life Cycle [2].

This paper will discuss the risk assessment cycle process conducted by the Navy Security control assessor from the technical standpoint but also include information on the human standpoint and provide some general considerations that can be applied throughout the risk assessment process.

CHAPTER 2

SOCIAL ENGINEERING TYPES

A commonly overlooked factor in cyber security is the human factor and more importantly the manipulation of a user to compromise security posture. This research will focus on making

the risks of social engineering transparent. Helping organizations manage these risks through a social engineering risk management model is the primary goal. Techniques used in social engineering are commonly used to deliver malicious software, but there are many other parts for, as an enabler to gain additional information, commit fraud or obtain access to secure systems. Social engineering techniques range from indiscriminate wide-scale attacks, which can usually be identified, through to sophistication and tailored multi-layer attack which can be almost indistinguishable from genuine interactions. Social engineers are creative, and their tactics can be expected to evolve to take advantage of new technologies and situations. This paper outlines some of the most shared and effective forms of social engineering.

2.1 Phishing

A phishing attack is the most common form of social engineering attack, which accounts for nearly 77% of all attacks with over 37 million users reporting phishing attacks in 2013[3] [4]. Phishing is an attack to try and steal personal or sensitive information by masquerading as a well-known or trusted contact. While email is the most common, other attacks can also be conducted via text messages, phone calls and fax, as well as other methods of communication, including social media. A large number of wide scales email phishing attacks remains unsophisticated and will be recognized by most computer users as credible. However, as email phishing is rapidly becoming sophisticated, attackers will use many different techniques to make the email appear authentic or to lure the victim into acting before thinking. Attackers may disguise the address the email is sent from so that it seems to be a reputable organization and common ones include banks, utility companies, couriers, recruitment agencies, and government. Better designed phishing emails will appear to be very similar imitations of legitimate emails from these organizations.

Other common techniques are to make use of the main news events by posting as updated information that is new on the event or asking the recipient to act on to the event.

2.2 Baiting

Another form of wide-scale attack is baiting using online advertisements and websites. As with phishing, these offers are too good to be true or advice of urgent warning. This includes websites that will allow the user to download or stream videos, or pop-ups that state to have detected an issue with the victim's system and by clicking on the link will resolve. Once the links provided in the bait are clicked, a user may then be tricked into giving away personal or sensitive information, or their machine may automatically download malware. These attacks can be crude, but others are sophisticated and persistent. Another common form of baiting is the use of free Wi-Fi hotspots. The attacker creates a Wi-Fi hotspot that is clearly labeled as free, typically in public areas such as airports, coffee shops, and hotel rooms. While they may provide a victim with an internet connection, any data sent in this context intercepted by the attacker, this is considered a man-in-the-middle attack. The ability to intercept the victim's data can even be conducted to secure connections such as online banking. The attacker can also install malware onto the system, allowing a range of further exploits to be carried out.

2.3 Spear Phishing

Spear phishing is a sophisticated attack that limits the target to a specific group, usually changing the information within the message along with sensitive information only the team would know, such as a business sector, employees in the same company, or the same department, or who share some other common attribute will make it look legitimate. A spear phishing email can even target one specific individual if they are seen to be of sufficient to the attacker. While this does decrease the number of potential victims, it can result in a higher damaging fallout from

the compromise. Some spear phishing attacks are difficult and remain easy to spot as they contain some of the indicators listed above. Others can appear legitimate and are tough to identify as malicious. A competent attacker will research their target to maximize their chances for success. Finding out information about the organization, including organizational charts, contact details and combine this with information obtained from their social media profiles and other publicly available information. Rather than a generic greeting, a recipient is likely to be addressed by name and the message will probably include other personalized details. An attacker will probably use the identity of a third party that is to be known or of interest to the intended victim, such as a maintenance technician or supplier, to leverage or establish trust. The another method is the attacker trying to replicate an external party's email address and assume the identity of an individual who is employed by the third party, potentially someone whom they believe their victim recognize. They may even have established access to the external party's email account. The following statistics provide a summary of metrics of the discussed social engineering attacks [4]:

- 107 million emails sent in which 90% contained SPAM or Viruses
- Phishing represents 77% of all socially based attacks
- Clicking links within e-mails account for 88% of all phishing attacks (Most common attacks are mimicking bank institution.)
- 1.8 million victims are medically identified theft
- The work area accounts for 80% of thefts which is the largest vulnerability by disabling or bypassing controls.

CHAPTER 3

NAVY SECURITY CONTROL ASSESSOR

The previous chapter discussed issues and concepts used to conduct social engineering. Although it seems trivial, it is important to understand what social engineering is and how it affects systems whether it is hardware or software. With this understanding, trying to incorporate it into a risk assessment of a system is complicated. As a security control assessor, we are at the mercy of programs to provide all documentations and diagram needed to conduct an assessment. We can only address what we can see, so there is already a disadvantage because the most program will not list any high-risk information in fear of not being able to field their system. I see this constantly and usually after the system is in operation then a compromise happened and an investigation is conducted, and we are required to provide all information that was used to conducted a risk determination.

3.1 Risk Management Framework (RMF)

The specification and selection of security controls for a system are accomplished as part of an organizational cyber-security program that involves the management of risk that is, the risk to the organization or individuals associated with the operation of a system. The administration of organizational risk is a major factor in the organization's information security program and provides an efficient framework for selecting the appropriate security controls for a system. The security controls are a necessity to protect individuals and the operations and assets of the organization. The Risk Management Framework(RMF) is a process that integrates risk management and security activities into the product life cycle. This approach to security control selection and specification considers efficiency, effectiveness, assumptions and constraints due to executive orders, applicable laws, directives, policies, standards, or regulations. Figure 3.1 shows the six-step process of RMF:

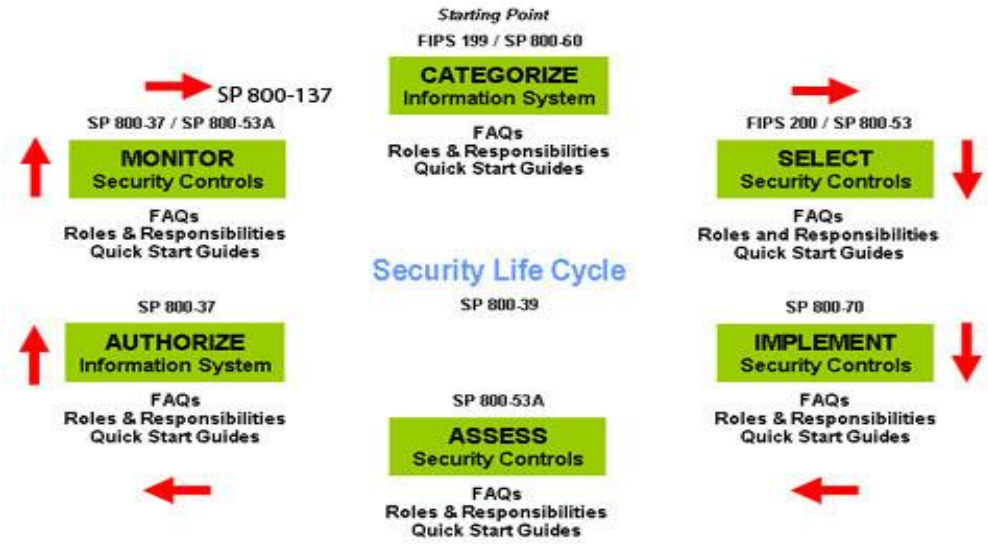

Figure 3.1 Risk Management Framework Process [5]

Looking at this process, the security control assessor has output requirements at steps 2 and step 5 of this process. Step 2 deals with assessing the Security Assessment Plan (SAP) of the systems and must be approved before the program moving forward. The SAP is prepared by the information system owner and the testing required before a risk determination can be conducted. Areas such as IP addresses, web applications, databases, roles, assumptions, and methodology are listed. This step is critical because without approval the program may conduct inadequate testing which will waste time and money.

Looking at the process and step 2, where does social engineering fall into? RMF is very detailed as far a security control required, but it does not have a control for social engineering. Since the Navy has now asked the assessors to incorporate social engineering into the risk determination. A standardized guideline needs to be created to accomplish the best possible assessments. Further along this paper, I will address some variables that should be considered and my hope that it will contribute to creating a checklist within the office. The issue here is step 2 is where this need to be addressed. Because once approval of the SAP is obtained, then the program

will conduct to testing and scans needed at step 5 for assessment. At step 5 a risk determination is provided to the Certifying Authority (CA) for a final decision.

3.2 Security Controls

To stop the social engineering threat from succeeding or damaging assets, the program will need to apply measures to mitigate social engineering attacks and techniques. Programs can change the environment, choose to act on occurring attacks or mitigate the social engineering risk by the structured implementation of countermeasures. The function of control is related to its place and effect in the security management process. Consideration of this controls is broken down into Strategic, Tactical and Operational controls. Some control considerations are:

Strategic	• Security culture and Polices • Security Documentation and Planning • Incident response • Recovery Policies • Risk Management
Tactical	• Data Classification • Authentication/Authorization • Recovery Procedures • Logging Procedures
Operational	• Security Awareness training • Access Control Enforcement • Intrusion detection • Malicious software removal

Table 3.2 Security Controls Affected by Social Engineering [6]

As most program already have security controls in place a comparison of these controls along with the list of possible controls related to social engineering can be used to measure the current level of security. As stated, these are just some of the controls that are affected by social engineering. It will be almost impossible to have program flip all controls affected to non-complaint due to this. We have a hard time convincing a program that their control is non-

complaint when the testing and scans show compliance. The major control families are listed below:

AC- Access Control	AU- Audit and Accountability	AT- Awareness and Training
CM- Configuration Management	CP- Contingency Planning	IA – ID and Authentication
IR- Incident Response	MA- Maintenance	MP – Media Protection
PS- Personnel Security	PE- Physical and Environment Protection	PL- Planning
PM- Program Management	RA- Risk Assessment	CA- Security Assessment and Authorization
SC- System and Communications Protection	SI- System and Information Integrity	SA- System and Services Acquisition

Table 3.3 RMF Security Family of Controls [7]

Looking at the controls that the security control assessor must evaluate, there are multiple controls that social engineering can affect. Since there is no general guidance to address when a control is non-complaint due to social engineering, this becomes and subjective risk determination. If I provided the same system package to review to different SCA assessors, most of the reviews would be different. Let's take an example: We have a system that is software only and resides on an infrastructure on a ship. Looking at social engineering into the assessment my initial determination would be controls IA and PS will be a consideration. Another assessor looks at the same system and determines controls AC and AU should be considered. Who is right in this instance? Both have valid arguments for which controls should be addressed. We can also look at some of the other controls that should be assessed as well. There inlays the problem which a risk assessment considering social engineering. In the next chapter, I will provide some variables that should be considered and a generation of a metric to help provide some general guidance to help the assessors.

3.3 System Design

The last consideration that security controls assessors look for is the design of the system. How does this apply to determining risk for social engineering? A program needs to be designed with security in mind. We have addressed this through this course, so I just want to summarize some key points. Most of the today's system projects, though modest in size and scope, using aggressive technology for performance and competitiveness. The success of these programs must seek an optimal investment in people, time, and resources. There is a need for system design environments which enable a small number of system designers to define, implement, verify and deliver such a product on time. Technology tools suppliers must fully understand and be able to exploit the capabilities of the underlying technology. The overall responsibility of the system engineer is to provide a level of abstraction, which supports the system development process. To maintain system design correctness, all tools must be verified accordingly. To enhance design correctness, all tools should be made extensible where appropriate. Tool development must grow to stay viable. Size, limits and update requirements in the tools should be aggressively tested in advance of usage. Formal verification proves or disproving the correctness of intended algorithms underlying a system on a certain formal specification, using formal methods in math. Formal verification will help demonstrate the accuracy of systems such as combinational circuits, cryptographic protocols, internal memory, and software expressed as source code. The audit of these systems is done by providing a formal proof of an abstract mathematical model of the system, the relationship between the mathematical model and the nature of the system being otherwise known by construction. Design errors are the major factor bad system design. An engineer needs to consider the following common mistakes [8]:

- Miscommunication on specifications
- Interface and protocol mismatch

- Incomplete or erroneous exception and error handling
- Mishandling of boundary conditions for operations or algorithms
- Missing features
- Incorrect initialization or unreliable state
- Missing testability coverage

By addressing system correctness and using the tools available to provide assurance of system design will help to address and curtail social engineering. It is a small aspect of determining risk but ensuring the system is working as requested along with security build in is a step in the right direction.

CHAPTER 4

VARIABLE CONSIDERATIONS TO DETERMINE RISK WITH SOCIAL ENGINEERING

Social engineering risk management process is influenced by a senior management and applied across the program, designed to identify risk and manage this risk to an acceptable level, to provide assurances regarding the achievement of overall objectives of the system or program. There is no special tool used to help define the risk social engineering imposes and the countermeasures needed to mitigate these risks. The following main question defines the problem a system should address:

- What are the risks involved with social engineering
- Which countermeasures can be taken by an organization to protect themselves from the threats of social engineering
- What measures can be used to mitigate the risks it poses

4.1 Security Controls and Policies and Procedures

This is where it all starts. As an assessor, there is a section in the repository that mist programs do not fill out. It has been difficult to assess, and when we do address it, a program is held up because they will need to address their policies and how often they are updated. A clear security policy addressing social engineering is necessary to build the complete security upon. The social engineering policy should contain the guidelines and standards requirements to achieve the overall security objective, and how to mitigate the risks of social engineering attacks. This policy can be used as a reference in the underlying procedures. The security policy should be defined and documented, for consistency and maximum effectiveness. It should be available to all employees such as in a program intranet page. Social engineering security procedures are the operational translation of the policy set out by management into a possible series of activities, tasks, steps, decisions or processes to achieve fixed outcome, in this case, the prevention, detection, and recovery of an attack. These procedures form the basis for mitigation based on the security objectives. Employees will have to make decisions quickly, and by having these procedures, it will decrease the opportunity for an attacker to manipulate them. This reliance on procedures makes document control critical, to review the procedures regularly and keep them up to date.

4.2 Security Awareness

The security awareness program should create constant awareness of the social engineering risk among users and their responsibility in protecting the organization's assets. The program should consist of training with clear reference to policies and procedures of the program, psychological principles, and tactics used by social engineers and information that they target. This security awareness training teaches the trainees to recognize an attack when it occurs and prevent it from causing harm by the following policy and set procedures. Users should receive training on the specific systems that they use so they can be aware if something suspicious is

occurring. This increases the chance of detecting an attack by a social engineer or coworker and recovery from an attack.

4.3 Number of Users

This category is where the discussion come in on the size of the of the program. The number of users is a factor. Also, the number of administrators or privileged accounts allotted and the rights that are posed with owning a privileged account. [9] For example, one system I was assessing was a software only applications located on a shore establishment that had all its users with privileged access. That is one of the core rules of cyber security is the least privileged concept.

4.4 System Complexity

In today's world of technology, the complexity of systems is a major disadvantage in risk assessments. Critical Infrastructures can be considered complex systems. For example, a ship's warfighting infrastructure which is dependent upon the network, internal/external connections, communication systems, and power systems is one example of a complex interconnected infrastructure. Most current risk analysis methodologies take a highly holistic view of the system. This look often misses the areas and detail needed where the risk may reside. Additionally, inexperience and the data of complexity of the systems tend to derive any such holistic view of risk. As stated above security risk assessments is difficult in the best of circumstances, let alone in these scenarios. The risks arising from the complexity of a system, along with operational and financial pressure; these factors are themselves major influences to the data collection and analysis necessary to gain an understanding of risk at the necessary levels. On the other hand, attempts to predict risk behavior from other programs and lesson learned data is negated by the limited experience and understanding of the models, and the minimal data available to cover the large area

within risk scenarios. Below is an unclassified diagram that an assessor tries to breakdown. This is an unclassified chart. Also, note that this is just internal to a ship and shows how quickly the complexity of a system can be.

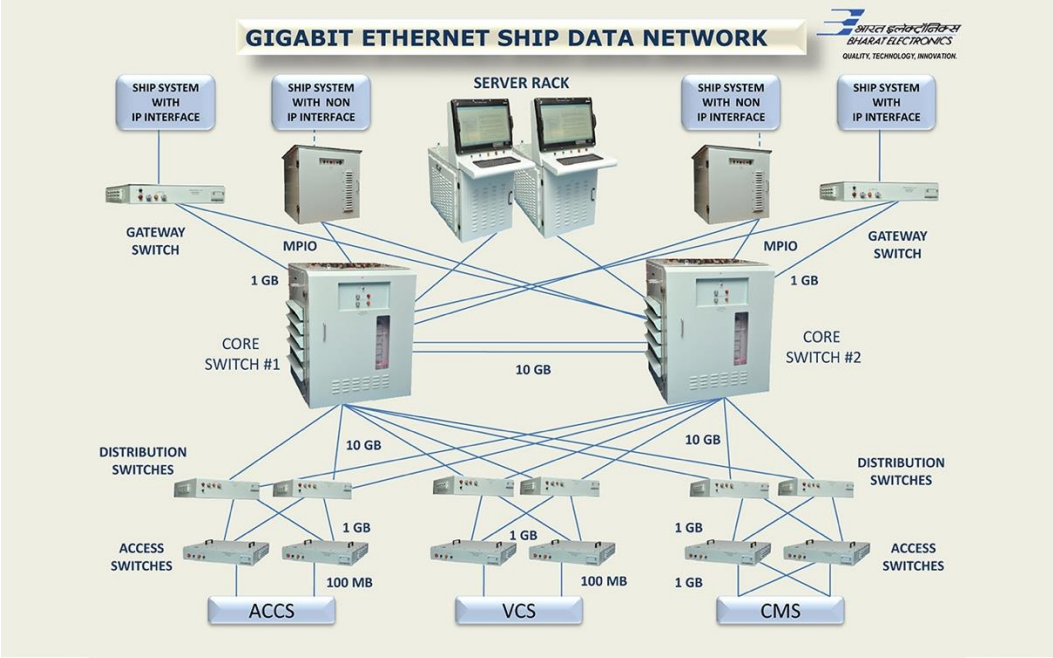

Figure 4.4 Example of ship diagram review

CHAPTER 5

SOLUTIONS

Trying to determine a risk assessment with social engineering in mind is challenging task. There are so many individual variables that are at the discretion on the assessor. The intention of this research is to generate a basic list of standards that can be followed and be able to justify why a certain risk determine is made.

The first step is the categorize a system. In this step, the system is characterized which can be an entire organization, division, department, process or even a specific system. The categorization will set a clear definition of what the system is used for and dictate the selection of controls. The system consists of the processes occurring within this system and the information

and data handled by this system. This organizational environment in which the personnel operates needs to be described. The characterization, therefore, generates essential information on the system for following steps as well as information on the environment that influences it. In RMF, system categorization is focused on the CIA triad (confidentiality, integrity, and availability). The three categories of categories are high, medium and low. As the system and environment characterization set the overall scope of the system, the process scope should also be set, which necessitates the objectives of the social engineering risk management process to be clarified.

The next step in a checklist should be vulnerability identification. A social engineer needs to have the opportunity to obtain the desired information; as long as there is no vulnerability, then the risk is minimal. The social engineers target people and can use a variety of psychological principles. Every place users can obtain access is therefore potentially at risk and creates a vulnerability when this location contains the targeted information. So, from this standpoint, some privileged users and the number of regular users' needs to be considered. We address this already in the process. Usually, we look for no more than three privileged users per site, but we may need to reassess this theory and consider the number of users and what kind of information they have access to. Along these lines, access control measures are important. We address this requirement with PKI or dual authentication methods. This will not be necessary to mitigate the threat of social engineering, but accountability is important.

The next item on the checklist for the assessor to address will be external connections to the program. Is the program public facing or internet capable? This will obviously affect the risk determination. There is some program within the Navy infrastructure that is isolated and is not public facing. The DOD has a requirement that all systems must comply with the Host Based Security System (HBSS) and obtained a waiver is unable. HBSS is a suite of software applications

to monitor, detect and defend networks and systems. The assessor should look at things like printer defense such as firewalls, intrusion prevention, and detection equipment.

Another item of defense is an incident response. This is critical so that the network is not just waiting for the social engineer to find someone in the company who does not know or care about security. There needs to be a clear process that an employee can begin as soon as there is suspicion something is wrong. This process needs to be aggressive and go after the hacker and proactively inform other potential victims. If there is no incident response, every employee that deals with a hacker is fighting a new battle. In the meantime, the hacker is getting better at understanding the organization's defenses. The incident response procedures stop that process. As soon as a social engineer is discovered in any part of the organization, the attack is characterized, and the employees are alerted that he or she is there and what to expect in an encounter.

Another major item on the checklist should include training and security awareness. Most commands within the Navy are required to hold quarterly training for its sailors. What we seem to notice as assessors are that this portion often is not conducted. As mentioned above this is probably the most important factor. No matter the security posture of a system, people are the weakest link in the chain, and a compromise is almost certain if the sailor does not know what to look for in regards to phishing email attempts or a phone call from an so called helpdesk employee wanting the user to give up their credentials.

The solution that I would recommend would for a separate section in the checklist that only addresses social engineering. I would look something like this:

Social Engineering Risk Checklist		
Risk Factor	**Variables**	**Comments**
System Characteristics	• Understand purpose • Number of General User/Privileged Users • Is system public facing	

Access Control	• Is PKI used • Dual Authentication • Biometrics	
Security Polices	• Written set of Social engineering policies • Visitor Management • Internet usage policy • User ID and Password Policy • Mobile Technology Use	
Physical Security		
Data	• Hard and Soft Copy Materials	
Applications	• Black and Whitelisting	
Awareness and Training	• How often Security Training/Awareness conducted • How does program track compliance	
Incident Response	• How does program track incidents • Reporting and Incident Response Procedures	

Figure 5.1 Proposed Social Engineering Risk Checklist

This checklist is a beginning starting point. As we proceed along and develop accurate metrics on how to address social engineering in a risk assessment, modifications can be made accordingly.

CONCLUSION

Social engineering is a very dangerous threat and one that currently has free reign. The office of the security control assessor has been tasked with providing standards to help in the development of risk assessments for Navy systems. Although the Navy does understand the seriousness of this task, the goal here is to provide a basic starting point for the assessors to address. The risk assessment process only allows for about four hours per system per employee within the office. Funding is constantly being cut as the Navy looks for efficiencies but how does adding additional requirements to the security control assessor and many systems that need to be assessed. This is the challenge that we currently face, and I believe that implementing a standard process for evaluating the social engineering threat is a start.

References

[1] Schmittling, R. (n.d.). Performing a Security Risk Assessment. Retrieved May 7, 2017, from https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx

[2] Allen, M. (2006, June). SOCIAL ENGINEERING A MEANS TO VIOLATE A COMPUTER SYSTEM. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

[3] MERCY, M. (n.d.). An Introduction to Social Engineering. Retrieved May 7, 2017, from https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf

[4] Courtney, W. B. (2014, April 28). The Social Engineering Infographic. Retrieved May 7, 2017, from https://new.social-engineer.org/social-engineering/social-engineering-infographic/

[5] (2017, February 1). RISK MANAGEMENT FRAMEWORK (RMF). Retrieved May 7, 2017, from http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/

[6] Osterloo, B. (2008, March). Managing Social Engineering Risk. Retrieved May 7, 2017, from http://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf

[7] N. (n.d.). NIST Special Publication 800-53 (Rev. 4). Retrieved May 8, 2017, from https://nvd.nist.gov/800-53/Rev4/

[8] Fu, P. L. (1997, November). Design Methodology for System Correctness. Retrieved from http://www.hpl.hp.com/techreports/tandem/TR-87.7.pdf

[9] F. (2015, June). Cybersecurity Assessment Tool. Retrieved from https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf