SecureState
What State Are You In?

SOLUTION

April 8, 2013
Version: 1.0

SUBMISSION TO

National Institute of Standards
and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
www.nist.gov

Adam Sedgewick
t: 202.482.0788
e: Adam.Sedgewick@nist.gov

PREPARED BY

SecureState
23340 Miles Road
Cleveland, OH 44128
www.SecureState.com

Framework For Reducing Cyber Risks to Critical Infrastructure RFI Response

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

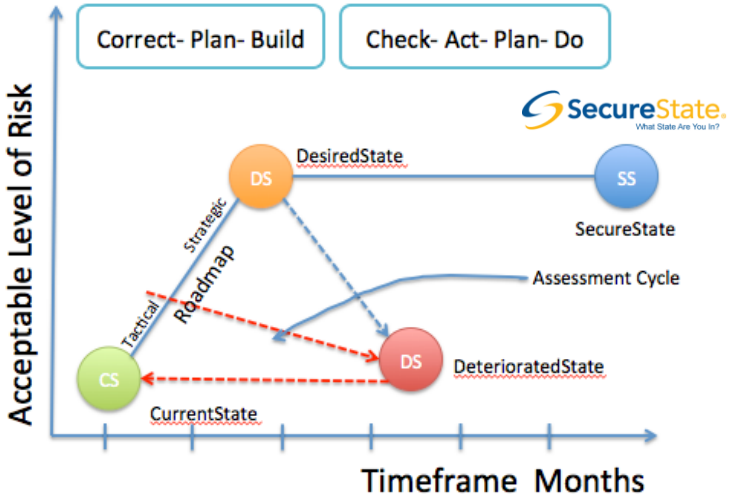
Request for Information Response

Dear Mr. Sedgewick,

SecureState is pleased to provide our response to the Framework for Reducing Cyber Risks to Critical Infrastructure. If there are any questions regarding the information provided, please contact SecureState Federal Director, Matthew Franko. The information provided herein includes SecureState thoughts, opinions and suggested approach for properly implementing a framework that will reduce Cyber risks to Critical Infrastructure in accordance with the Executive Order set forth by President Obama.

SecureState is a management consulting firm that specializes in information security. We believe in a different approach to security, partnering with organizations to understand their business and align security in a way that objectives can be easily accomplished. SecureState works with organizations to solve complex information security problems by using technical services to facilitate strategic decision. Ultimately, SecureState's value is in our ability to bridge the strategic and tactical approaches to Security that helps organizations at a Program Level. The way we guide our customers is twofold: First, we work to identify the problem in a causal relationship to your problem and second, we provide strategic recommendations to make appropriate business decisions that addresses the problem. This is evident in the work we do within several of the Critical Infrastructure Sectors including Chemical, Communications, Commercial Facilities, Critical Manufacturing, DIB, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Transportation and Water.

No matter the service, our team works together to determine the underlying problem. We then craft a strategic solution, coupled with a tactical approach that gets organizations to the level of managing a desired state of security, where we are able to build a program that equips organizations with the knowledge and resources that account for the Principle of Three Forces (Time, Resources, and Change). This includes seamlessly addressing projects which require multi-practice integration, discipline and management. Combine our sizeable breadth of knowledge with the experience of our six distinct practices and you will receive a unique problem solving experience with each individual client engagement.



The key to SecureState's innovative approach is in our consultants' ability to work together and leverage their unmatched expertise in their individual focus area.

- Each individual that makes up our team has a specialized focus in at least one of our

service offerings that include penetration testing, application security reviews, vulnerability assessments, audit and regulatory assessments and audits, incident response/forensics and security program building.

- During each engagement our team collaborates to identify underlying problems and develop strategic solutions to mitigate those problems.
- We focus on research and innovation to be able to provide our clients with forward thinking and innovative approaches that are on the cutting edge.

SecureState would like to thank you for the opportunity to respond to this request and look forward to working with you. Should you have any questions please let us know.

Best Regards,

SecureState
What State Are You In?
23340 Miles Road | Cleveland, Ohio 44128 | 800.903.6264

Table of Contents

Current State of Cybersecurity Across Sectors 5

The Desired State of Cybersecurity Across Sectors 6

Summary.....6

Current State of Cybersecurity Across Sectors

The Government recognizes the need for organizations to adopt a framework that helps better manage security within Critical Infrastructure. However, it is important to note that there are a multitude of security frameworks that have already been developed and in some cases have already implemented and begun managing their security with the use of a standards based framework. The development of yet another framework an organization would have to apply would cause an unwarranted stress that would likely not be adopted in mass. Looking at the frameworks, standards or regulations that are currently being enforced upon individuals within Critical Infrastructure include: National Institute of Standards and Technology (NIST) – 800-53 and 800-66, Electric Sector - Cybersecurity Capability Maturity Model (ES-C2M2), Health Insurance Portability Accountability Act (HIPAA), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), Payment Card Industry Data Security Standards (PCI DSS), Graham-Leech Bliley Act (GLBA), Sarbanes-Oxley (SOX), International Organization for Standards (ISO) 27001. And this is just a short list of the standards and frameworks that organizations have to worry about when building an overarching program.

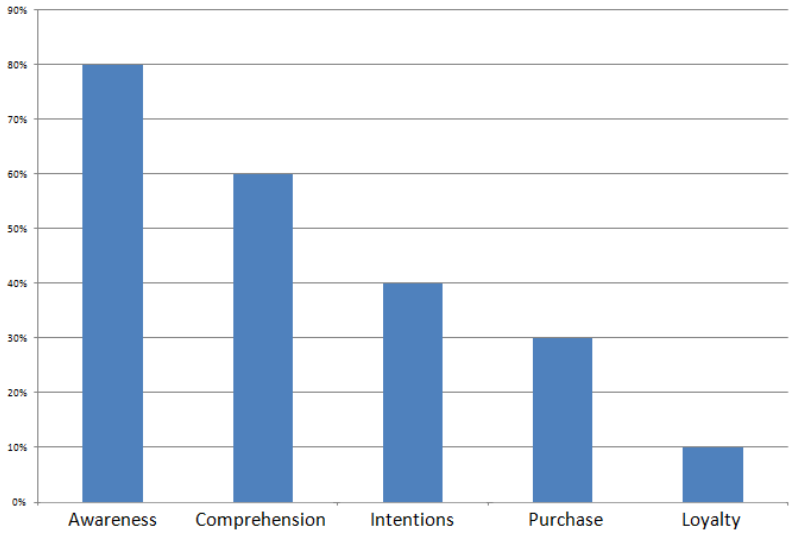
Another issue plaguing Critical Infrastructure is the position of Security within these organizations. Often times these individuals do not reside at the executive level, are focused in Information Technology or do not come into contact with the Organization's Enterprise Risk Management Program. More often than not, there is not a full Enterprise Risk Management Program within organizations, only individual department risk management practices with nothing rolling up to the full enterprise. For example, the finance department of an organization may have a risk management program that is worried about financial loss, while the security department may have its own Risk Management Program focused on security risks. Without an overarching program that rolls up to the enterprise, each group is making a decision without accounting for the other. For example, reliability is the main concern of most Energy Organizations, while within the Healthcare Sector the main concern is on patient safety. Even at the point that in a rare case there is an Enterprise Risk Management Program that does include Security as a factor, the bar of entry where a risk even gets considered has an extremely high dollar value.

A big reason for this is with the individuals assigned to manage the security in the Critical Infrastructure sectors. Often times, these individuals have come through the organization with very deep technical expertise, as an IT Administrator or Information Security Analyst. Typically these individuals do not have the training or the understanding of the business to relate the security risks to the executives in a way that they can comprehend or understand the business impact. To this point it is not a matter of whether or not executives understand the need for security, as many organizations have a dedicated security team in some facet, the issue lies on the security professionals to become better at communicating risks and aligning them with the overall business strategy.

The Desired State of Cybersecurity Across Sectors

It is key to ask the question, "If so many standards exist, why has there not been a wide-scale adoption." When leveraging the Customer Response Index (CRI)" model for market awareness of products, it can be related to the adoption of an information security standard within the Critical Infrastructure Sectors.

When looking at this model, the information flows left to right. The first stage for a product to gain market share is that it must have an increased amount of awareness. Once the awareness is prevalent, then the market must understand the product and its uses. From there the intentions of the product must be understood. If all three of these factors are high, only then can a product move into Purchase (implementation) and loyalty. If not, then the product will struggle to gain wide-adoption and acceptance.



If the industry were to take this model and apply it to information security and the standards and frameworks that currently exist, it will help to identify the shortfall and the lack of implementation and loyalty. Awareness and comprehension of the current standards and frameworks are high in information security, especially with sector specific standards and frameworks. Which begs the question, why not try to increase the understanding of the intentions of the standards and frameworks for a more wide scale implementation and loyalty. This issue will not get fixed by inventing a new framework; it will only be remedied by findings a way to increase the comprehension, intentions and ultimately implementation and loyalty.

The key in this area is to focus on the audience. Currently the audience that comprehends and understands the intentions and wishes to adopt these frameworks or standards are in the wrong position within the organization. They are failing in relaying this message to the executives who make the decisions that impact spending and the business. If the Government wishes to have wide scale adoption within the Critical Infrastructure industries, it would be a good choice to leverage current standards and just shift the audience of the message. The executives need to understand that security can be aligned with the strategic goals of the companies, and building a security program that is focused on the framework.

Summary

As the government continues to strengthen its focus on the private sector and working to secure the critical infrastructure, it is important for the Federal Government to understand the current

state of the private sector and co-develop a desired state that is achievable by all. While there has not been wide scale adoption of a single framework among all critical infrastructure sectors, the primary reason has not been because the frameworks are not strong enough, simply because the right audience does not have the awareness, comprehension or understanding of the intentions behind them. If the government shifts the focus from building yet another framework that will not be fully adopted; to awareness and comprehension with the right audience (senior executives), only then will progress be made in truly securing the critical infrastructure.