DEVELOPING A FRAMEWORK TO IMPROVE CRITICAL INFRASTRUCTURE CYBERSECURITY

RESPONSE TO DOCUMENT # 2013-04413

SUBMITTED BY: DONALD M. EDWARDS
DMEDWARDS@COMPUTER.ORG
512-497-4678

DEVELOPING A FRAMEWORK TO IMPROVE CRITICAL INFRASTRUCTURE CYBERSECURITY

The National Institute of Standards and Technology (NIST) has requested input from stakeholders in the Critical Infrastructure Sectors regarding the development of a voluntary Cybersecurity Framework for reducing cyber risks to critical infrastructure and services. A key factor in the success of any voluntary framework is that it must be both practical and desirable to adopt. Small businesses are heavily involved in the Critical Infrastructure Sectors and are particularly sensitive to the short-term practicality of any expenditure of effort and resources. The focus of this response is to share some of the insights I have gained from implementing technology solutions and information security programs. I have 17 years of experience in information technology in the Critical Infrastructure Sectors, most of which has been focused on improving the confidentiality, integrity, and availability of sensitive data and the systems that manage it. In particular, my focus for the last three years has been on implementing information security programs based on the framework described in the NIST SP 800 (FISMA) series and the Payment Card Industry Data Security Standard (PCI-DSS). I am a Certified Information System Security Professional (CISSP) as well as a long-time member of the Institute of Electrical and Electronics Engineers (IEEE) and its associated Computer Society.

BACKGROUND

Over the last decade, small business contribution to non-farm nominal GDP has been in general decline. However, small businesses in certain industry sectors have actually gained ground and are accounting for an increasing percentage of the U.S. economy. In particular, small businesses in the Finance & Insurance and Health Services sectors each accounted for about 4.5% of non-farm nominal GDP, for a combined total of over 9%.

Finance & Insurance and Health Services are only two of the sixteen industry sectors designated as Critical Infrastructure Sectors in the Presidential policy directive (PPD-21) that was issued as a companion to the Improving Critical Infrastructure Cybersecurity Executive Order (EO-13636). With a minimum of 9% of the U.S. economy at stake, it is imperative that special consideration be given to the impact that the Cybersecurity Framework will have on small businesses.

THE SMALL BUSINESS CHALLENGE

The very characteristics that define a business as being small are those that present the most significant hurdles to implementing an effective information security program: limited workforce and revenue. The vast majority of administrative and technical controls designed to assure the confidentiality, integrity, and availability of information resources rely on highly-skilled and well-paid people implementing checks and balances through separation of duties. A well-defined, methodical approach to the design, testing, and implementation of changes in business processes and technology systems is necessary to prevent the introduction of the sorts of security lapses that are commonly exploited in Cyberattacks. Unfortunately, adhering to strong methodology necessarily results in lowered business agility, which removes one of the major market advantages on which small businesses rely.

DEMONSTRATING THE VALUE OF CYBERSECURITY TO SMALL BUSINESSES

Small businesses, with their limited resources, are extremely sensitive to the return on investment of every endeavor they undertake. Return can be measured in many different ways, but small business owners and managers are typically focused on increasing revenue, lowering expenses, and improving marketability. Investing time and money in an information security program is a hard sell because on the surface it appears to decrease marketability, given the impact to agility, while dramatically increasing expenses. In fact, absent outside influence, the return on an investment in an information security program can only be measured in terms of potential losses avoided. Without some kind of incentive that speaks to revenue, expenses, or marketability, small businesses will be extremely reluctant to implement the Cybersecurity Framework.

submitted by: Donald M. Edwards
dmedwards@computer.org
512-497-4678

CYBERSECURITY AS A DIFFERENTIATOR

Since small businesses are, ironically, huge players in these Critical Infrastructure Sectors, it is important that the Cybersecurity Framework provide an incentive to make participation desirable to them. With very little effort from NIST, DHS, or whichever agency ultimately administers the Cybersecurity Framework, certified compliance could become an extremely desirable market differentiator for small businesses. Specialized skill certifications have long been used in the information technology labor market to demonstrate proficiency and to stand out from others applying for the same job, and there is every reason to believe that the same would hold true in small business competition.

FEATURES OF AN EFFECTIVE CERTIFICATION PROGRAM

In order to entice small businesses to participate, the Cybersecurity Framework Certification Program should include several features which have proven to be valuable in existing private-sector certification programs:

LOW COST OF ENTRY

The return on investment of an information security program is hard to quantify, so it is important that the first steps to implementation require as small of an initial cash outlay as possible.

GRADUATED CERTIFICATION PATH

Implementing an information security program can be as much of a psychological challenge as a fiscal one. One way to help a certification program gain acceptance is by offering several levels, with the first one within easy reach for small businesses. As business owners become more comfortable with the value of certification they will be more likely to increase their investment in their information security program.

ACHIEVEMENT BADGES

Businesses looking to certification as a differentiator will want to wear their certification like a badge on their business cards, website, signage, etc. It is important that each level of certification come with the right to use a graphical symbol as a sign of their commitment to information security. Examples of this kind of badge include the logos used by professionals holding certifications from the International Information Systems Security Certification Consortium and the “Norton Secured” seal.

PUBLICITY FOR THE VALUE OF CERTIFICATION

A certification’s value as a differentiator is only as strong as its reputation in the marketplace. The organization responsible for administering the program will need to invest time and money in public service announcements or marketing campaigns to encourage people and businesses to look for certified service providers. If consumers value the certifications, market pressures will encourage businesses to participate in the program.

DIRECTORY OF CERTIFIED BUSINESSES

Both consumers and businesses will place more value on a certification if it is easy to find qualified businesses. The organization responsible for administering the program should create a searchable directory of certified businesses that is kept up to date.

SEARCH RESULT RANKING

If possible, the organization responsible for administering the program should partner with major search engines and business directories to rank certified businesses higher in search results than uncertified businesses.

submitted by: Donald M. Edwards
dmedwards@computer.org
512-497-4678

On a personal note, I would like to thank President Obama and NIST for giving the stakeholders in the Critical Infrastructure Sectors this opportunity to provide input into the Cybersecurity Framework. The threat of Cyber attack is one of the greatest challenges we face, and I am encouraged that we are taking this bold step towards a more secure future.

If I may be of any assistance, I am happy to serve.

-- Donald M. Edwards, CISSP

submitted by: Donald M. Edwards
dmedwards@computer.org
512-497-4678