Security Standards Participation

By Jeff Stapleton – ISSA member, St. Louis Chapter **and Phillip H. Griffin** – ISSA Fellow, Raleigh Chapter

This article describes the benefits for both the employer and the employee when participating in the development of industry standards. The possibilities for company advantages and the potential for personal and professional growth are significant.

Abstract

This article describes the benefits for both the employer and the employee when participating in the development of industry standards. Employers profit from awareness, influence, diversity, and education. Employees benefit not only from gaining knowledge and having opportunities for continuing professional education (CPE) credits, but also networking and development of both technical and soft skills. The possibilities for company advantages and the potential for personal and professional growth are significant.

Figure 1 – Standards influences

Why Standards?

Everyone knows that security standards are a good thing. They promote industry interoperability and provide baselines for reasonable, effective security controls. Manufacturers can follow standards when building products. Implementers can deploy products to enable services that comply with standard requirements. Administrators can manage services according to standards; auditors can assess whether lines of business (LOB) comply with standards; and regulators can evaluate when corporations are following best practices based on standards.

Further, information security standards are written by security professionals. The employers (corporations) of these individuals allow them to participate in the development of international, national, vendor consortium, or even corporate standards. This article discusses the advantages to corporations for following industry standards and the benefits that accrue to employers and security professionals participating in the development and maintenance of security standards.

Figure 1 shows the influences between international, national, and corporate standards, along with the security professionals employed by the variance corporations. Some countries adopt international standards and do not have their own national standards. Other countries (e.g., United States) might adopt international standards where applicable, but adapt or maintain national standards when there are differences. Further, some international standards might originate as a national standard submitted by a member country (e.g., United States) through their national standards organization, such as the American National Standards Institute[1] (ANSI) while others are developed only as an international standard.

International standards represent the consensus of multiple countries that include standards, technical specifications, and technical reports. Each country has its own relatively different cultures, industry markets, laws, regulations, and national standards that are represented by the various country subject matter experts (SMEs). Respectively, each country SME is approved by its associated national standards body for international representation. For example, in figure 2 the national standards body for the United States is the American National Standards Institute (ANSI), which accredits other national standards organizations (e.g., ASC X9, INCITS) to develop international standards and approve US representatives as SMEs in international committees.

National standards represent the consensus of multiple companies that include standards, guidelines, and technical reports. Company participants might be researchers, government agencies, manufactures, service providers, audit firms, or other businesses. Each company represents its own cul-

1 www.ansi.org

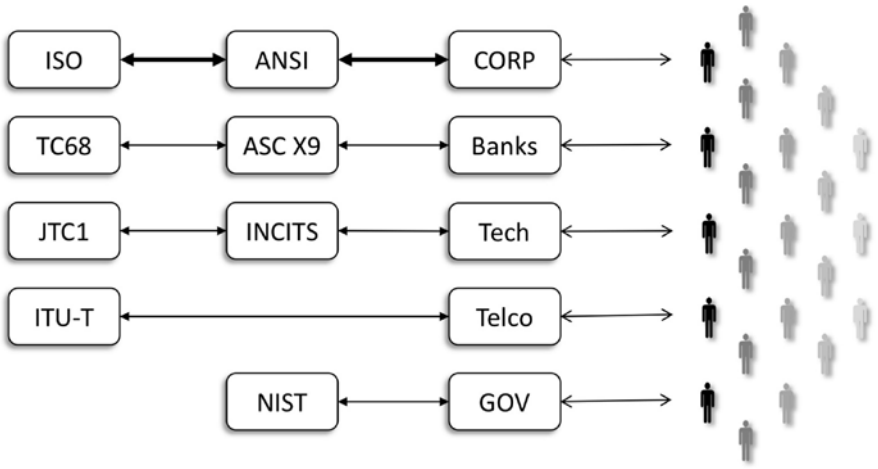

Figure 2 – Standards associations

ture, industry market(s), federal laws, industry regulations, and organizational standards that are represented by the various company SMEs. Respectively, each company SME is approved by its employer and the standards organization to develop national standards and approve corporate representatives.

Industry standards represent the consensus of companies or individuals that might include standards, specifications, guidelines, and reports. Participants might be academicians, researchers, government agencies, manufacturers, designers, developers, service providers, audit firms, or others. Each company or individual reflects its culture, industry segments, laws, regulations, and experiences. Industry standards organizations such as OASIS[2] or W3C[3] focus on various industry segments.

Corporate standards are internal to each company. Hopefully these internal standards are based on industry, national, and where applicable international standards, but also influenced by federal laws, industry regulations, and other contractual obligations, such as the Payment Card Industry Security Standards Council[4] (PCI SSC). Each corporation typically designates internal SMEs from its various lines of business, legal, and security professionals to develop and maintain corporate standards.

Security professionals are SMEs internal to each company. Skills learned or honed from developing international, national, or industry standards are applicable to their daily jobs. They might also be acknowledged as a national SME to develop and maintain national standards, and further recognized as an international SME to develop and maintain international standards. Individuals will typically specialize in one or more information technology (IT) or information security (IS) areas. These individuals help develop and maintain the corporate standards.

Figure 2 expands the standards influences into variance associations. ANSI is the national standards body for the United States to the International Standards Organization[5] (ISO), but ANSI does not develop national standards. Rather ANSI accredits other organizations to develop national standards by industry segments. Members of ANSI include companies, government agencies, other standards organizations, industry consortium, and even individuals.

Accredited Standards Committee[6] (ASC) X9 is accredited by ANSI for financial services. Thus, X9 develops national X9 standards and is the US Technical Advisory Group (TAG) to ISO Technical Committee 68 Financial Services. X9 standards address retail banking, paper and electronic checks, wholesale banking, securities, and information security. Members of X9 include payment brands, financial institutions, merchants, manufactures, service providers, government agencies, law firms, accounting firms, and other financial service providers.

International Committee for Information Technology Standards[7] (INCITS) is accredited by ANSI for information technology (IT). Originally named X3, INCITS develops national standards and is the US TAG to the Joint Technical Committee One (JTC1) Information Technology. Members of INCITS include manufactures, service providers, government agencies, and other standards organizations.

International Telecommunication Union[8] (ITU) is the United Nations specialized agency for information and communication technologies (ICT). The ITU Telecommunication (ITU-T) is its standardization sector that develops industry recommendations. Members of ITU-T are companies organized by country. ITU hosts focus groups that study new technologies (IoT, blockchain, digital currencies, etc.) and develop recommendations for standardization. Participation in ITU focus groups is free to anyone in a member country.

National Institute of Standards and Technology[9] (NIST) is a United States government organization that promotes US innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST develops Federal Information Processing Standards (FIPS) and a variety of Special Publications that are freely available. NIST is a participant of X9, INCITS, and many other national and international standards organizations, and its Information Technology Laboratory (ITL) is an ANSI-accredited standards developer organization (SDO).

2 www.oasis-open.org/standards
3 www.w3.org
4 www.pcisecuritystandards.org
5 www.iso.org
6 www.x9.org
7 www.incits.org
8 www.itu.int
9 www.nist.gov

There are far too many international, national, and industry standards organizations to discuss within a single article. The standards organizations discussed here provide a fair representation for an overview and introduction. Suffice it to say that standards are fundamental to any industry, and knowledge of security standards and their application should be an integral part of any security professional's tool kit.

Why participate?

From a company perspective, organizations depend on standards for their security and privacy in many aspects of their information security management and operations. Standards provide a basis for defining the security policy, practices, and procedures of the organization. Compliance with standards is often one of the measures used by assessments and audits to determine compliance with policy. These checks produce results that are fed into the Plan-Do-Check-Act (PDCA) quality cycles of the organization Information security management system (ISMS). These results may also be used to provide evidence to regulators and business partners of compliance to industry norms.

Standards enable products from multiple vendors to interoperate. It is true that standards do not guarantee that products that comply with their requirements will interoperate. It seems that vendors can find many ways to prevent interoperability from happening, sometimes by error and sometimes by design. However, standards can make interoperability possible, and without standards, interoperable products are nearly impossible to achieve and maintain.

Standards also influence legislation that can impact the organization for good or ill. As people all over the world become more likely to possess smart phones rather than computers, these standardized, interoperable devices have provided new opportunities for commerce, social media, banking, education, and awareness. They have the promise of connecting remote or underdeveloped communities to the developed world and providing increased access to modern services, such as banking and medical care. As the Internet of things (IoT) continues to increase worldwide, communications and security need standardization.

Standards are developed by a group of participants with common interests, but with varied expertise, interests, and goals. These participants often include vendors and competitors that may not share the same concerns as the organization. Such subject matter experts come from a wide diversity of individuals and expertise. It is important that the organization has input into the standards development process in order to ensure the standard that results addresses its specific requirements. Left alone, the committee will reach consensus among themselves and those not participating will not be able to influence the outcome.

The company SME that participates in developing national or international standards can influence its development, represent employer interest, and share information to other employees. Issues can be discussed, information can be digested, and alternatives can be determined. Problems or possibilities can be escalated to senior management that might affect a company's IT and IS strategy.

Why contribute?

From a security professional perspective, standards activities are personally beneficial. As mentioned earlier an SME can only specialize in a few IT or IS areas and so can learn from other SMEs. Gaining knowledge within a standards group is very different than being in school. Information learned in school lags behind actual industry evolution, and while standards are typically not the cutting edge, they are often groundbreaking. SMEs can bring their own experience to the table, subject to their employer's intellectual property rights,

of course. Meeting and working with peers from other companies is a fantastic networking opportunity.

Standardization groups need researchers, writers, and reviewers. Contributing to standards helps build an individual's ability to understand technology and security concepts. Reviewing and commenting on draft material is an integral part of developing standards. Participants can learn how to read and write technical documents, which is a difficult skill set and a rare commodity. Such skills are reusable for an individual's day job and other ventures. SME participants might only review drafts, actually write material, or even become an editor for the development of a standard. Participants might also submit requests for continuing professional education (CPE) credits.

Other potential skills include time management and project management. Since standards developers are typically volunteers and everyone has a day job, coordinating standards work with company work can be a challenge. Likewise, when an SME becomes an editor or even a work group chair, coordinating tasks with all the other SMEs who have day jobs is another interesting challenge. The successful SME who actively engages in developing standards learns many skills.

Getting involved

If your employer is already a member of a standards development organization (SDO), you may be able to participate at no cost. You can search your company website for a contact or look at the list of members on websites of the SDO of interest. If you find your employer, you can contact the SDO directly and get contact information for your company representative.

There are SDOs such as IETF,[10] OASIS,[11] and W3C[12] that are freely open to participation. You only need to register for a project or complete a membership application to get started. Some of these require paid membership in order to vote or to receive marketing benefits. However, individuals can contribute to the work and influence the outcome.

The INCITS (International Committee of Information Technology Standards[13]) organization serves as the US Technical Advisory Group (TAG) to many ISO/IEC standards development organizations. These groups are organized by sub committee (SC), such as SC37 Biometrics and SC27 Information Security, Cybersecurity, and Privacy. X9[14] develops security standards for the financial services and serves as the US TAG to ISO TC68 and the SC2 Security group. Both INCITS and X9 require paid membership to participate.

The ITU-T (International Telecommunication Union -Telecommunication Standardization Sector) develops security standards in Study Group 17 (SG17). The work of this group covers the X.500-series directory standards that include X.509 certificates. SG17 also covers ASN.1, telebiometrics, identity management, cryptography, security architecture, and more. Membership in ITU-T is expensive for voting members. However, ITU-T has many liaison relationships, some with ISO and ISO/IEC groups, and these liaison groups can be less expensive to join.

10 https://www.ietf.org/standards/.
11 https://www.oasis-open.org/standards.
12 https://www.w3.org/participate/.
13 http://www.incits.org/.
14 https://x9.org/.

There are face-to-face meetings, often in Geneva, but meetings provide remote video and audio access. An inexpensive way to participate is to register for an ITU-T Focus Group (FG).[15] These are free to anyone in any ITU-T member country, which covers most of the world's countries. The current FG topics include financial services, digital ledger technology (DLT), digital currency including digital fiat currency, artificial intelligence for health, data processing and management for the Internet of things (IoT), machine learning in 5G systems, and more.

Conclusion

Company benefits include awareness, influence, and education. Awareness of what standards are under development allows an organization to better prepare for change. Influencing standards development allows an organization to protect itself and its industry. Education of its employees makes for better workers, happier workers, and helps with worker retention. The possibilities for company advantages are far reaching from the individual to the whole company.

Personal benefits include education, networking, and skills. Education by peers who know more about a subject or know other areas is invaluable. Networking with professionals from other companies or even other countries is irreplaceable. Learning or honing skills to manage one's time, coordinating with others, and negotiating compromises, can be indispensable. The potential for personal and professional growth is astounding.

About the Authors

Jeff Stapleton has been an ISSA member and participated in X9 standards for thirty years. He has contributed to the development of more than three dozen X9 and ISO security standards, and has been the chair of the X9F4 Cybersecurity and Cryptographic Solutions work group for over 20 years. The X9F4 work group's program of work includes security requirements for authentication, biometrics, cloud, cryptography, Internet, mobile, PKI, pen testing, timestamps, and wireless areas. He can be reached at jjs78023@yahoo.com.

Phillip H. Griffin, CISM, has over 20 years of information assurance experience. He has served as a trusted security adviser, security architect, and consultant with leading corporations, and acted as committee chair, editor, and head of delegation in the development of US national and international security standards. Phillip has served on the ISSA Educational Advisory Council and the ISSA Journal Editorial Advisory Board, and actively participates in ITU-T SG17 Security, ISO TC68/SC2 Security, ISO/IEC JTC1/SC27 Security techniques, and X9 Financial Services standards development. He may be reached at phil@phillipgriffin.com.

15 https://www.itu.int/en/ITU-T/focusgroups/Pages/default.aspx.

ISSA CAREER CENTER

The ISSA Career Center offers a listing of current job openings. Among the current 803 job listings [6/29/19] are the following:

- **Cybersecurity Program Manager**, Emerson – Sidney, OH
- **Information Security Program Lead,** William Blair – Chicago, IL
- **Cyber Security Analyst**, IDA – Alexandria, VA
- **Desktop Support Engineer,** William Hill – Jersey City, NJ
- **Lead Software Engineer**, Product Security, Hill-Rom/Welch Allyn – New York, NY
- **Information Systems Security Officer ISSO**, Pennsylvania State University – Reston, VA
- **Information Security Tech**, Franciscan Alliance Information Services – Beech Grove, IN
- **Sr Cybersecurity Engineer**, McGraw-Hill – East Windsor, NJ
- **Information Security Analyst**, Minnkota Power – Grand Forks, ND
- **Chief Information Security Officer,** North Carolina Administrative Office of the Courts – Raleigh, NC
- **Corporate Director of Security and Resiliency - Health Care,** Orlando Health – Orlando, FL
- **Sr. Information Security Analyst**, Abiomed – Danvers, MA
- **Senior Information Security Analyst**, Nasdaq – Philadelphia, PA
- **Security Analyst / Risk Assessment**, University of California San Francisco – San Francisco, CA
- **Senior Information Security Analyst**, UC Davis Campus – Davis, CA
- **Cybersecurity Program, Director/ Full Time Faculty**, Immaculata University – Immaculata, PA

2018 Journal – Past Issues

Past Issues – digital versions: click the download link:

Best of 2017 | Impact of Malware
Legal, Regulations, Ethics | Privacy
Operational Security — the Basics of Infosec
Internet of Things | The Next 10 Years
Health Care & Security Mangement
Practical Application & Use of Crypto
Standards Affecting Infosec
Foundations of Blockchain Security
Security Challenges in the Cloud