Global Information Assurance Certification Paper

Security Risk Communication Tools

GIAC (GSEC) Gold Certification

Author: Andrew Baze, abaze@microsoft.com

Advisor: Stephen Northcutt

Accepted: 9/6/2015

Template Version September 2014

Abstract

The effective communication of risks is a serious challenge faced by every security risk management professional in today's dynamic cybersecurity environement. Business executives expect communication in their language, focusing on financial gain, risk, or loss. Security professionals often speak in technical terms, describing threats or vulnerability in the context of confidentiality, integrity and availability. A key challenge is to translate common security metrics into risk statements using the language of business so that executives with limited security knowledge can make the best, risk-informed decisions.

One of the reasons security risk management is a unique challenge is because the language of security is often relatively technical. An in-depth security discussion often requires a level of engineering understanding that one should not generally expect of executives. It is the responsibility of the security risk professional to translate relevant risk metrics, details, and descriptions into the language of their business leaders, whose understanding could directly affect the future of the business.

A simplistic approach to bridging the communication gap between engineers and executives is to reference the latest security event already circulating in the media, describing how it relates to the business. While this method may garner attention and temporarily enthusiastic support, it is only one piece of the puzzle. Such examples should be part of a coordinated message, accompanied by relevant, appropriately-scoped metrics. "Security Risk Communication Tools" will explore six specific approaches to constructing that critical security risk management message.

1. Introduction

Anyone researching "How to run a cybersecurity program" will find a structure that includes identifying assets and threats, assessing vulnerabilities and risks, mitigating risks, and managing incidents. Most cybersecurity program references focus on technical aspects of program implementation and management, and provide little guidance on one critical component of the program: communicating security risks to key organizational stakeholders. If it is mentioned (most often it is not), it is usually relegated to the "risk management" discipline and treated as if it were a totally separate process.

What should a cybersecurity practitioner, program manager, or director do if his or her company's risk management program is not directly involved with the cybersecurity program? And what if upper levels of management do not understand cybersecurity issues? These are realistic possibilities, and it is therefore necessary for cybersecurity professionals to understand how to effectively communicate security-related risks at all levels of the business hierarchy. "One of the key characteristics of a highly effective security leader is to straddle that fence between technology and business,

Andrew Baze, abaze@outlook.com

and communicate risks in the right language to the different stakeholders in the organization (Au, 2013)."

Support of business leaders is critical. Who authorizes funding for the program? Who authorizes funding for mitigation of security risks? These people must understand and be kept updated on the risks. "Without support at the executive and board level, (and the organizational structure and budget that comes along with it), a security leader cannot execute on his or her strategy (Au, 2013)."

The security program metrics used, their accuracy and relevance, the way they are communicated, and the results of the communication are all critical to the effectiveness of the cybersecurity program. As when communicating risk information regarding any complex topic to a variety of audiences, several essential aspects of communication must be considered, like knowing the audience, being a credible source of information, and placing the risk in perspective (Belloc, 2015).

The effectiveness of the cybersecurity program is tied directly to the survivability of the business. As businesses take increasing reliance on technology, which inevitably includes computer networking, those with inadequate cybersecurity programs are at significant risk of being damaged or destroyed by any number of antagonists (Gardiner, 2015).

To complicate matters, aside from specific metrics and their relevance, communication of risk is a unique challenge. "To calculate risk is one thing, to communicate it is another. Risk communication is an important skill for laypeople and experts alike. Because it is rarely taught, misinterpreting numbers is the rule rather than the exception" (Gigerenzer, 2014). At the same time, demand for this information is

increasing. “In the past, senior executives and boards of directors may have been complacent about the risks posed by data breaches and cyber attacks. However, there is growing concern about the potential damage to reputation, class action lawsuits, and costly downtime that is motivating executives to pay greater attention to the security practices of their organizations” (Ponemon Institute, 2015).

Several tools available in a cybersecurity risk management program will be reviewed in the following sections. These tools will improve the risk manager’s ability to do his or her job effectively, resulting in better decisions being made by key stakeholders. More specifically, these tools will help enable stakeholders to better answer what Lewis (2014) calls the “fundamental question posed by a risk-informed strategy… given limited resources… how should resources (funding) be allocated to reduce risk? How should priorities be set?”

The following tools will be described in detail:

1. A Business Assessment
2. The Stakeholder List
3. Security Metrics and Risks
4. Tailored Communication
5. Communication Verification
6. Security Risk Accountability

Use of these tools should result in more effective and timely communication. This is especially important in an environment when slow or inadequate communication could harm the business. “Never before has the business world moved as fast as it has today – a trend that will only intensify for the foreseeable future. This is particularly true

on technology-related matters. The need for clear and effective communication is more essential than ever. Not only will this problem persist if we ignore it, but it will exacerbate (Simon, 2015)."

2. Communicating Risk

Before describing tools in detail, the context for their use should be understood. In some organizations, the job of communicating risks falls to dedicated risk management personnel. However, regardless of whether the security professional is part of an operational cybersecurity engineering team, a GRC (Governance, Risk and Compliance) group, or a loosely-defined risk management organization, risk data will need to be appropriately packaged depending on unique stakeholder needs.

Risk management will tale place in any business. It may happen explicitly or implicitly, proactively or reactively, competently or as a box-checking exercise. Risks will exist, and some will inevitably be realized. If the security professional is able to effectively communicate those risks, then it is less likely that the risks will negatively impact the business. The following tools will support that mission.

2.1 Tool #1: A Business Assessment

The first step in identifying risks should be to understand the business. Any business project or program run without this context is likely to result in failure or at least waste. An initial review should include the vision, mission, strategy details, and any relevant tactical plans, depending on the expected level of depth concerning the risks being assessed. One useful resources is the organizational context described in Clause 4 of ISO 22301, which includes understanding internal and external issues, including the

organization's activities, functions, services, and the organization's risk appetite (ISO 22301 Portal: Societal security - Business continuity management system, 2015).

One key responsibility of a security administrator is "to convert these business requirements into technical requirements (Sivarajan, 2015)." Communicating in both directions necessarily entails moving information in the opposite direction: translating technical requirements into business requirements. And in this context, this means translating technical risk information into business risk language.

From the perspective of the risk manager as a trusted business advisor, several "must know" elements should be obtained before engaging in a credible discussion with a client: financials, key executives, business units, market position, key competitors, news and press releases, product and service offering, customers and customer segments, previous projects and their outcomes, known issues or needs, and existing contacts and relationships (Parikh, 2015).

In the context of ensuring the continuity of the business in the event of a security incident, a standard practice is to perform a business impact assessment (BIA). It answers the question "what is the impact to the overall business of this service, process, feature, product, etc. being offline for any given amount of time?" Additionally, it provides the basis for investing in recovery strategies (Business Impact Analysis, 2015). In order to realistically answer that question, the overall business and its environment must be understood.

2.2 Tool #2: The Stakeholder List

Stakeholders are those affected by a project or program's outcome. They should be identified at all levels in the business hierarchy, which may include multiple sub-

businesses, services, groups, or feature teams. In addition, external stakeholders such as customers, governments, and investors should be identified.

Not only must stakeholders be identified, but the cybersecurity program's stakeholder list must be regularly updated. This is because the stakeholder environment will change continuously, usually as rapidly as the business itself changes and adapts. In addition, there will be many stakeholders in an area as important and cross-cutting as cybersecurity, adding to the number of potential communication or miscommunication pathways.

How many communication pathways exist? Each time a person is added to the stakeholder list, the number of potential pathways increases significantly. See Figure 1 below. For example, if there are 15 stakeholders, then there are 105 potential communication pathways (calculated as $(n/n-1)/2$, with n as the number of stakeholders, assuming they may communicate with each other (PMII, 2013)). If five more are added, that number goes up to 190.

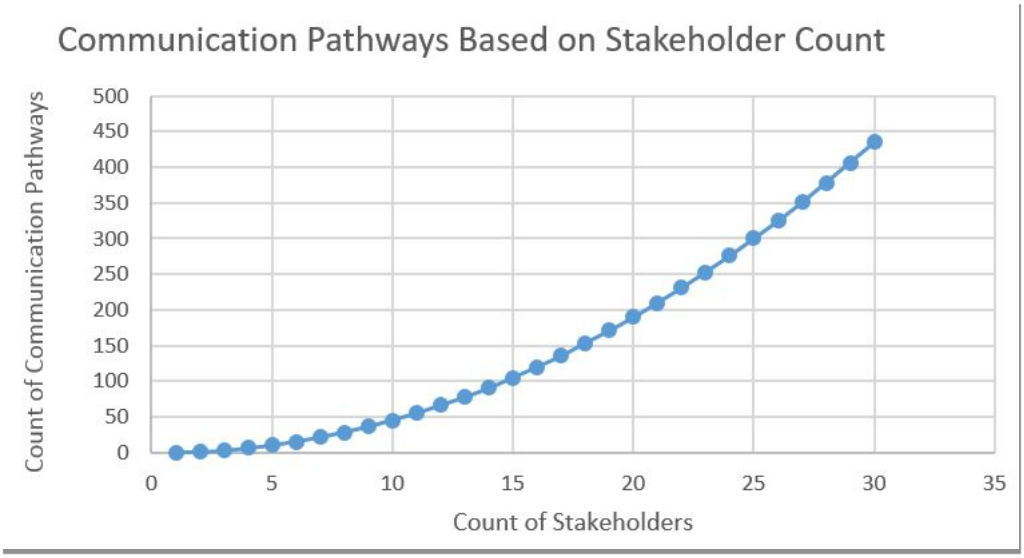

Figure 1. Count of communication pathways based on count of stakeholders.

This illustrates the scope of the communication challenge and the need for a clear, consistent message. If the stakeholder list is not written down, regularly reviewed, and refreshed, it will be very difficult to communicate with the right people at the right time, and the likelihood of the message being misunderstood, diluted or misrepresented increases.

The RACI model is a critical tool in the communication toolbox. This commonly-used acronym stands for Responsible, Accountable, Consulted and Informed.

The following table, Figure 2, illustrates common role definitions in the RACI model.

Responsible	Who is doing the work?
Accountable	Who authorized the work? Who is ultimately responsible for the work, program, or project? Who signs off? Note: only one person may fill this role.
Consulted	Who should be consulted regarding this work?
Informed	Who should be made aware of developments, updates, or status?

Figure 2. The RACI model with descriptions.

A common approach, which is often included as a component of broader stakeholder and communication management plans (depending on the amount of project management rigor in the organization), is to assign one of the letters in RACI to each member of the stakeholder list. See Figure 3 as an example, a variation on a RAM, responsibility assignment matrix (PMII, 2013).

Stakeholder	RACI
Ram Patel, CEO	I
Pat Baker, CISO	A
Pedro Suarez, Project Mgr.	R
Su Lee, Project Coordinator	R
Susan Sharp, VP	C
Jim Alford, VP	I
Company Proj. Mgt. Leads	I
Security Engineering Grp.	R

Figure 3. Example Resource Accountability Matrix (RAM).

Please note that in this example, as in any standard RACI model, there is only one truly accountable person, the CISO. Continuing with the example, a Vice President could assume a variety of roles, in this case either Consulted or Informed. The CEO should only be Informed of key outputs rather than project details. And finally, multiple people are actually doing the work. They are the ones Responsible for getting the work done. Every program's stakeholders model will differ, and it will also likely change frequently, necessitating regular review.

2.3 Tool #3: Security Metrics and Risks

There are many potential metrics a security program could use, and it can be a challenge to determine which ones are best suited for a particular environment. It is more complicated than picking a simple set of metrics, because each metric could be described in multiple ways.

The following metrics could be used in the context of vulnerability scanning: count of scans completed, servers not scanned, Internet-facing servers not scanned, vulnerabilities found, high-priority vulnerabilities found, critical dependency servers

scanned, servers that cannot be scanned because they are temporarily detached from the intranet, or false-positives identified.

Even with this wide variety of measures, there are ways to alter each, providing a different and potentially more useful view. If one substitutes the word "percentage" for the word "count," or if one applies the word "rate" to show changes in these metrics over time, the resulting views could lead to different decisions being made.

The variations above only applies to vulnerability scans. There are dozens of other types of variable to which similar pivots could be applied. Additional metrics to consider include those referencing malware detection, intrusion detection, firewalls, patching, incident management, auditing, training activities, and change management.

With this in mind, there are hundreds of potential metrics to choose from. The security professional must determine which ones matter most, as well as to whom they matter most at which times. In addition, these metrics should be clearly tied to the business' Key Performance Indicators (KPIs). This linkage will help enable clear communication with business leaders.

The combined research of Chew et al. (2008), Jaquith (2007), and several others indicates that IT security metrics need to be bounded, quantified, have obtainable metric input data, be reliable, valid, objective, contextually specific, and automated (Emrah Yasasin, 2015).

On the other hand, the co-author of "Pragmatic Security Metrics," Dr. Gary Hinson, describes seven myths of security metrics, including the myths that these metrics need to be "objective," "tangible," have discrete or absolute values, and most importantly, in his words, that all of the numbers be included (Dr. Gary Hinson, 2006).

These two views are not mutually exclusive, but illustrate different approaches to determining what to track. There is no simple answer to which metrics any organization should track, but whatever the metrics, the security professional is responsible for ensuring that there is a common set that meets the organization's needs, that they are reviewed regularly, and that they are used to help identify risks.

A list of risks is a critical component in a risk management program. However, the quality of the list, the quantity of risks, and the relevance of the data they are based on can cover a broad spectrum. What is the right filter to apply to this data?

The solution has to consider the definition of risk. A standard definition of risk is the potential of losing something of value. Another is the exposure to danger. In the cybersecurity realm, a common definition is "threat times vulnerability times impact." Another is "threat times vulnerability" with an overlay of control effectiveness or velocity (the speed at which a risk could be realized). None are right, wrong, or perfect.

Different organizations will have their own definitions, and a cybersecurity risk manager must determine whether it is appropriate or whether an additional variable applied to the equation may provide relevant insight. In the event that a program is being started from the ground up, the risk manager may be in a position to choose the most appropriate formula.

The components referenced above are critical. No security professional can exclude threats and vulnerabilities from a security risk discussion. However, other components such as impact, likelihood, control effectiveness, velocity (often grouped with likelihood), and average loss expectancy must be included in any risk evaluation,

regardless of an organization's evaluation model. While they may not be explicitly plotted on a risk map, they cannot be ignored.

With the assumption that risks have been effectively identified and analyzed, it is time to move to the next step. What should be done with this information? Considering the stakeholder list, how should information be distributed, and to whom?

2.4 Tool #4: Tailored Communication

In a situation where the business is understood, risk managers understand who their stakeholders are, and relevant metrics are tracked, that is still not enough. A plan must exist for communicating information to various members of the audience in different ways.

The security risk manager should be a trusted advisor, providing customers with useful, risk-related information, ensuring that risk data is understood and included in their decision-making process.

When considering the organization served by the risk manager, information will need to be presented in the context that organization has chosen. In other words, a trusted advisor uses language that the stakeholders understand.

One of the simplest questions asked by stakeholders is: "What are the top priority security risks and what should we do about them?" But even this simple question has critical context. When is the question being asked? What decisions will be made with the information? Why is the question being asked at this time? All of these variables, which change frequently, will determine the best way to answer.

This is not to say that a standard set of metrics has no place, or that these metrics would not necessarily support any answer. It is intended to illustrate the importance of

the question's context, and the needs of the person asking the question. That person, whether he or she asks specifically, is a stakeholder, and different answers will be required for different stakeholders.

Key stakeholders and their associated needs often include a combination of the following:

- The Board of Directors is usually familiar with risk, especially in the context of business strategy. This group usually expects a high-level view, and often does not have time or need for minutiae. The Board needs a consistent, easily-digestible report to consume along with the many other reports it is required to regularly review.
- CEO: The Chief Executive Officer usually needs information at a level similar to the Board of Directors, however, the CEO may need more supporting detail, depending on his or her interest level or technical expertise.
- SLT: A Senior Leadership Team, whether a group of Vice Presidents under the CEO, other C-suite members (e.g. CISO, CIO, COO), or a group of high-level managers under a VP (who also may be business owners), will be more likely to want to see more operational details, at least in summary form. Most importantly, they will likely also be held accountable for these metrics (in the context of RACI, covered previously). Therefore, those details must be made available, especially when organizational goals are not being met as expected.
- Managers or individual contributors with the responsibility to design, implement, operate, assess, monitor, test or audit secure systems will

usually need access to all data, as well as an understanding of how the details are translated into higher-level messages.

This list is not exhaustive, but illustrates the wide variety of stakeholders that may exist at all levels of the served organization, and their unique needs.

Obviously, these stakeholders are quite varied. They may speak different languages or dialects. For example, a product or service owner may spend most of his or her time speaking the language of product quality, service uptime, or customer satisfaction. The people at the next level down in the organizational hierarchy may be more concerned about new feature development velocity or the time required to push a software hot-fix, get a bug patched, re-boot a system, or restore a database in a supply-chain bottleneck. These two groups will use different metrics or collections of metrics (often in scorecard format) to describe the different activities that take place, often in the context of their specific groups' goals. As stated previously and re-stated for emphasis, it is the risk manager's responsibility to understand the business at all its layers, which includes understanding the stakeholders' hierarchy, their perspective on the business, and their needs, as part of understanding the overall business (Tools #1 and #2).

One important consideration when addressing unique groups of stakeholders is to consider the structure of the message. In the context of a message being delivered in written format, it is important to address those who prefer the "forest" view, but one should not neglect those who need the "trees" view. Some people prefer summaries without having to process the raw data, and some prefer reviewing the raw data and creating their own conclusions. Regardless of personal preference, both views are usually

necessary, because a good business case or risk statement requires both a summary (or conclusion) and its supporting data.

During a management seminar several years ago in a large software company, facilitators broke apart a group of managers into two sections, those who had "N (Intuition)" and those who had "S (Sensing)," based on their MBTI ® (Myers-Briggs Type Indicator). The facilitator asked each group to describe the course as it had taken place so far, to write their observations on a large piece of paper. Those in the "S" camp listed several bullets, describing details of the course so far. However, those in the "N" camp listed summarized statements, conclusions. The "N versus S" illustration shows two different aspects of personal preference.

One type ("N") often prefers to provide or read summaries, and the other ("S") often prefers to provide or read details, from which they can construct their own summaries. Using the descriptions from The Myers & Briggs Foundation, the "S" description calls out "I start with facts and then form the big picture." While the "N" description calls out "I like to see the big picture, then to find out the facts" (Sensing or Intuition, 2015). This is an illustration of how a person's preference will likely lean toward one particular communication style.

To accommodate both styles, a common approach in written communication is to provide an executive summary in a few bullets, then a detailed view with supporting detail, sometimes followed by a closing "call-to-action" or final summary. One way to use this approach is to provide an executive summary using concise, summarized, bulleted statements, at the top of an email or report. The details can then consume any

number of pages after that summary, as needed. And the concluding statement should be separated from the body of details.

Another approach using this model in a PowerPoint slide deck is to have a few simple slides with few bullets that describe the key points of the presentation or desired message, with detailed appendix slides available for reference during the presentation or further review after the presentation, when the deck is forwarded to the audience. The conclusion in this case should be included in the initial set of slides, before the appendix.

Another way to communicate risks is to tell a true story. More than ever, there are relevant, high profile examples of serious security compromises. Consider the following examples taken from various industry areas.

Entity Hacked (industry type)	**Scenario**
Target (retail)	Customer credit card payment information stolen
Office of Personnel Management (U.S. government)	Personal information of over 22 million people holding U.S. security clearances compromised
Premera and Anthem (health care)	Personal data of 90 million people exposed
Tinder (popular application/service)	Online dating customer private data exposed
Chrysler (auto manufacture)	Researchers demonstrated their ability take over various vehicle controls
Sony (entertainment)	Hackers stole company data and destroyed IT infrastructure

Figure 4. Recent high-profile hacking scenarios and consequences.

Different business have used multiple aspects of the Sony incident (or more accurately, a long, ongoing series of incidents) to provide reasons for better employee training (e.g. anti-phishing training), even when experts were not sure how the hackers broke into Sony's networks (Kerner, 2015). While it should not be difficult to justify

basic training or to get funding to remediate serious network security gaps, an example such as this one should help.

A quick Internet search will provide several examples that relate to almost any business. It may even be challenging to winnow down the list, depending on the industry. The examples in Figure 4 are not meant to provide a complete list, nor are they intended to provide fodder with which someone could pressure management into budgetary submission, but instead provides examples of real scenarios that can be used to better illustrate related risks in one's own organization.

A week or so before Stephen Northcutt, a security author and researcher, presents a keynote, he goes to: http://www.privacyrights.org/data-breach and http://www.sans.org/newsletters/newsbites/ to find recent examples related to the industry to which he is presenting (Northcutt, 2015). Examples at these and many other reputable sites should carry a lot of weight, especially if the researcher is able to compare cybersecurity program components (or deficiencies) between the example and served organizations.

With all of the discussion of metrics, risks, and communication options, it is important to remember that providing the appropriate message may mean excluding some details, and that this can be an effective way to clarify (or not muddle) what is being communicated.

One of the most common and critical metrics of business is money. Using Benjamin Franklin's well-known, centuries-old axiom, "Time is Money" (Franklin, 1719), how could one deliver a risk message in these terms? What if time and money were the only two metrics allowed? Whose needs would they address? In today's

business environment, it is unlikely that very limited data will suffice to effectively inform any competent decision-maker in any business with significant Internet or intranet dependencies. However, ensuring that some metrics focus clearly on and time and money will certainly appeal to senior executives, and help reinforce the security professional's trusted advisor role.

2.5 Tool #5: Communication Verification

Even when the business is understood, its stakeholder list is clearly defined, and relevant metrics are being used to communicate the message in the best possible format, communication is still not complete. An email may never be read, a PowerPoint may have too many bullet points or too many pictures, or the same "red" (versus "green" or "yellow") data in a scorecard could be interpreted as either good (critical issues uncovered) or bad (critical issues not fixed). There are myriad ways in which a message may be diluted, distorted, retransmitted or misunderstood. The message originator must verify that the message has been understood by key stakeholders.

One reliable method of ensuring communication has taken place is to ask that the receiver repeat the message in his or her words. This likely will not happen so directly with many stakeholders. Instead, one should gauge understanding based on the questions that are asked during discussions, or the directives that are issued as a result of the communication.

A lack of response could be an indicator of failure to communicate. Perhaps a variation of the following may be necessary: "Did you understand these details?" An logical follow-up option is "Do you have any questions?" If no response is obtained, it is

safest to assume that communication did not take place, and that a different approach may be necessary.

Aside from changing approach to adapt to an individual, there is another potential reason to the messaging approach. Anyone actively involved in a cybersecurity program will be aware of the rapidly-changing nature of the threat and vulnerability environment. And if the business is heavily reliant on or otherwise directly tied to technology, it must constantly adapt. This constant adaptation not only includes the fluctuations in the data measured, but the makeup of the stakeholder list, the business's strategy and tactics, its competition, and even legal or regulatory requirements. As the business changes and adapts, so must communication regarding the business risks.

Once it has been determined that the message has been understood (while adapting as needed), the risk manager may also have the charter of driving risk accountability in the organization.

2.6 Tool #6: Security Risk Accountability

A well-understood list of risks is a major accomplishment, however, it must eventually be matched with a list of planned mitigations for those risks accepted, transferred, or avoided. This includes understanding whether the mitigation plans are on schedule and are delivering the expected results.

The mitigation verification process could take a variety of forms, from consuming an organization's internal scorecard to one-on-one follow-up interviews with the risk owners or other accountable parties. In a worst case scenario, or if there is no charter to ensure or drive for security risk accountability, a cybersecurity risk manager

should at least have an understanding of the mitigations' effectiveness during a regular (possibly quarterly, at least annually) risk refresh.

"As the saying goes, 'security depends 30% on technology and 70% on management.' … Although the plan can seem wonderful, it still needs to be inspected for its effectiveness" (Wu, 2015).

If the security organization is chartered with reporting on risks, it must consider that one of the most important metrics to report on broadly is the extent to which accountable risk owners are executing as expected on their risk mitigations.

3. Conclusion

The cybersecurity environment is rapidly changing. Because of businesses becoming more reliant on technology and the need for rapid shifts in business strategies to adapt to other changes, cybersecurity risks will change in scope, potential impact, likelihood, and velocity just as quickly. Consequently, the risk surface will expand and the security professional must be prepared to communicate effectively in this challenging environment, using the best data for the right audience at the right time. The consequences of ineffective communication, resulting in misunderstanding security risks, can be catastrophic.

Understanding the business objectives, the stakeholders, their needs, and the risks themselves will position the security professional to provide a clearly-understood, relevant message. However, it is still important to ensure that risk data is appropriately tailored for the right stakeholder group, and then to verify that it has been understood. The ultimate measure of understanding will be the planned and realized mitigation of

critical security risks, and increased resilience of the business in the face of inevitable attacks.

By using the available tools, the security professional has a much better likelihood of guiding his or her stakeholders to make better informed and more timely decisions, to the benefit of the business.

Andrew Baze, abaze@outlook.com

References

A Guide to the Project Management Body of Knowledge (PMBOK (R) Guide) - Fifth Edition. (2013). Newton Square: Project Management Institute, Inc.

Au, D. (2013, November 11). The New Language Of A Highly Effective Cybersecurity Leader. Retrieved from Security Week: http://www.securityweek.com/new-language-highly-effective-cybersecurity-leader

Belloc, H. (2015, August 17). Risk Communication. Retrieved from Risk Communication: http://www.soc.iastate.edu/sapp/soc415RiskCom.html

Business Impact Analysis. (2015, August 15). Retrieved from Ready.gov: http://www.ready.gov/business-impact-analysis

Dr. Gary Hinson, P. (2006, July). Seven myths about information security metrics. Retrieved from NOTICEBORED.com: http://www.noticebored.com/html/metrics.html

Emrah Yasasin, G. S. (2015, April 7). Requirements for IT Security Metrics - An Argumentation Theory Based Approach. Retrieved from ResearchGate: http://www.researchgate.net/publication/272943474_Requirements_for_IT_Security_Metrics__An_Argumentation_Theory_Based_Approach

Franklin, B. (1719, May 18). The Free-Thinker. The Free-Thinker, p. 128.

Gardiner, B. C. (2015, March 03). Case study: When a hacker destroys your business. Retrieved from CIO.com.au: http://www.cio.com.au/article/569410/case-study-when-hacker-destroys-your-business/

Gigerenzer, G. (2014). Risk Savvy: How to Make Good Decisions. New York: Penguin Books.

Andrew Baze, abaze@outlook.com

ISO 22301 Portal: Societal security - Business continuity management system. (2015, August). Retrieved from PECB.org: https://pecb.org/iso22301/#c4

Kerner, S. M. (2015, April 21). Sony Hackers Used Apple ID Phishing Scheme, Researchers Claim at RSA. Retrieved from eWeek: http://www.eweek.com/security/sony-hackers-used-apple-id-phishing-scheme-researchers-claim-at-rsa.html

Lewis, T. G. (2014). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation (2nd Edition). Hoboken: Wiley.

Northcutt, S. (2015, August 15). (A. Baze, Interviewer)

Parikh, S. (2015). The Consultant's Handbook: A Practical Guide to Delivering High-value and Differentiated Services in a Competitive Markeplace. West Sussex, UK: Wiley.

PMII. (2013). PMBOK Guide, Fifth Edition. PMII.

Ponemon Institute. (2015). 2015 Cost of Data Breach Study: Global Analysis. Ponemon Institute.

Sensing or Intuition. (2015, August 17). Retrieved from The Myers & Briggs Foundation: http://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/sensing-or-intuition.htm

Simon, P. (2015). Message Not Received: Why Business Communication Is Broken and How to Fix It. Hoboken: Wiley.

Sivarajan, S. (2015). Getting Started with Windows Server Security. Birminghan, UK: Packt Publishing Ltd.

Andrew Baze, abaze@outlook.com

Wu, H. Z. (2015). Web Security: A WhiteHat Perspective. Boca Raton: CRC Press.

Andrew Baze, abaze@outlook.com