Realtime publishers

The Shortcut Guide™ To

Understanding Data Protection from Four Critical Perspectives

sponsored by

CREDANT®

We Protect What Matters

Rebecca Herold

Copyright Statement

Chapter 3: How Information Security Leaders Need to Address Data Protection Within the Business Context

A few years ago, in a large financial services organization that had around 15 different business units selling different products and services, the marketing folks got what seemed like a great idea to feed people's growing appetites for new technologies. They decided that they would give a free Blackberry phone (not nearly as common as they are now) to all brokers that reached a specific sales goal for the upcoming month.

To the marketers' great joy, almost all of the approximately 800 brokers met their goal! Along with the Blackberrys, the marketers sent instructions along with this magical and delightful gadget that described how the brokers could synchronize their email with the device. They advised in the instructions that the brokers should not try to do the synchronization until 9:00am PST on a specified Monday so that they would be sure to have staff on hand from any of the time zones in case the brokers had problems. Sound like good preplanning?

That Monday came, and mysteriously the response time of a section of the corporate network not only ground to a standstill but also the call center was flooded with calls, primarily from brokers saying that the synchronization did not work. The brokers basically inadvertently performed a nicely coordinated Denial of Service (DoS) attack by flooding the network all at the same time with the synchronization attempt. Oops.

New Technologies: The Good, the Bad and the Ugly

New technologies have always provided great potential opportunities for businesses to make improvements upon how business is done. Technologies can provide new ways to improve productivity in everyday work activities. These technologies were often created as consumer goods first but then wholeheartedly embraced by business leaders. These new technologies include everything from DVDs to iPods; from Blackberrys to iPhones; from CDs to super tiny, high-storage USB memory devices; from Facebook and other Web-based services to online virtual networks; from instant messaging to texting and tweeting.

Although all these new technologies bring with them the potential for improving business, the bad news is that every new technology also brings with it new and unforeseen information security and privacy risks. It makes sense; the majority of new technology is not developed with security in mind but rather ease of use accompanied by how cool and unique they can be. All these cool and unique features inherently bring with them new and unique threats, and can introduce unanticipated vulnerabilities into a business, creating new risks that businesses had never anticipated or prepared for.

What makes these good, new technologies—along with the really bad new accompanying risks—really ugly is that usually the risks are not addressed until after something bad happens. Or, if some forward-thinking information security leader anticipates the risks and then creates policies for the use of the new technologies, the ugly truth is that significant portions of personnel choose not to follow policies if they perceive the restriction as infringing upon their personal rights.

Three Things Necessary to Make Policies Effective

Multiple studies done in the past year show that growing numbers of personnel are purposefully choosing not to follow policies, particularly when the policies impact their personal use of email, texting, instant messaging, tweeting, and general talking on the phone.

> **Note**
>
> Messages sent using Twitter are called "tweets." People who use Twitter are called "peeps," and their active use of Twitter is called "tweeting."

A late-2008 RSA survey reported that the majority of workers polled said they regularly do not follow corporate security policies in order to get their jobs done. Many others indicated that they did not even know what their information security policies covered, or what they allowed and disallowed.

These situations reveal significant information security management problems:

- The policies are not being enforced. People choose not to follow policies because 1) they're inconvenient and 2) they know that they will suffer no negative consequences.
- The policies are not being communicated. If people do not know what the policies are, how can they follow them?

Is it any wonder policies are perceived as being ineffective?

The already existing risks are significantly magnified when rampant, and employee-perceived innocent policy breaking occurs on a daily basis by otherwise well-intentioned employees. If you want your information security and privacy policies to be effective, you must:

- Obtain strong and visible executive support for them.
- Provide regular training and ongoing awareness communications so that personnel know how to protect information as required by policies.
- Consistently enforce policy compliance.

In the next few sections, I'll discuss the growing common areas where policies either don't exist, the policies are not communicated, or personnel overwhelmingly choose not to follow them.

Mobile Devices

Consider these statistics:

- According to research from the National Center for Health Statistics, at the end of 2007, nearly one in six homes (16.6%) did not have landline phones; only cell phones (Source: http://ecircuitonline.com/index.php?option=com_content&task=view&id=692&Itemid=834).
- In March 2009, the Centers for Disease Control and Prevention estimated that in the US, 17.5 percent of households use cell phones only; a slight but significant increase in a one year span (Source: http://www.thenorthwestern.com/article/20090327/OSH0101/903270442/1128).

As these statistics reveal, most people now feel the need to be able to talk, or communicate in some other way, on their mobile phones. Although this enables personnel to get their work done anywhere, it also allows personnel to do personal tasks anywhere, including at work.

Not long ago, while doing a project for a large financial organization, I was sitting at an empty desk in the aisle where all the contracted workers, doing security access changes, were sitting. Two of the eight people sitting in that aisle were talking or texting on their cell phones most of the day. They justified their non-work activities during the hours they were getting paid by saying, "Hey, we're just contracted; we could get cut at any time. Of course we're going to try and find permanent positions at other organizations while we're here so that we can be covered when we have to leave." Do you have workers with this kind of attitude?

Personnel are also increasingly using USB storage devices within the workplace, and without, to store and carry large amounts of business information. Much of this is personally identifiable information (PII). Do you have enforced policies in place for such devices?

The more mobile PII becomes—being stored upon smart phones, Blackberrys, laptops, and mobile storage devices and being accessed by people who work from home, work while traveling, or work for other companies—the more risk there is that PII will be involved in a breach. Every day, literally, I read news reports about lost or stolen laptops. On June 18, 2008, I read a news report, "A Misconfigured Laptop, a Wrecked Life," which chronicled how one man had his first work laptop stolen, then was fired when the second work laptop he was issued as a replacement was found to have pornography on it; either it was pre-loaded when he got it or lack of prevention software allowed someone to remotely load it on his computer while he was online.

It is very important to provide training and ongoing awareness communications to personnel about the risks of mobile computing and how to protect mobile computers as well as implement protections for mobile computing devices.

Online Activities

Growing numbers of personnel are using online networking sites and tools. Not only are social networking sites, such as Facebook, more popular than ever but also new communications tools, such as Twitter, are increasingly being considered as a necessity. Do you have information security and privacy policies, procedures, and tools in place to control the participation in and use of these types of sites and technologies to help ensure valuable business information is not leaked out through them?

Organizations must create policies for the use of online social networks. You and your personnel need to understand the security and privacy implications of these sites to prevent accidentally exposing information intended to be private.

Consider Twitter. Today, I spent just a few minutes doing some searches to see if I could find any information posted related to business. I was curious to see how much PII, or other sensitive information, I cold find.

Here are some of the tweets I found, with sensitive and otherwise inappropriate information redacted, when doing a search for “password”:

- [TwitterID redacted]: [redacted] is online. http://[redacted URL] (password is still fiddler).
- [TwitterID redacted]: [redacted URL] password: It's "password"
- [TwitterID redacted]: Accidentally hacked a Comcast account last night. Sorry, [email address redacted]. Shame on you, Comcast, for weak password reset function. pw="funnymoney"
- [TwitterID redacted]: [TwitterID redacted] ServerName: [redacted] Username: [redacted] Password: ICVjIijD
- [TwitterID redacted]: [redacted] knows my password is "hooters". but i do love her perfect [redacted].
- [TwitterID redacted]: 'You need to fill in your Kerberos password', your what? It's Tv34Nov
- [TwitterID redacted]: Strengthening passwords on a bunch of websites. Up until a minute ago, the password to my Yahoo! email account was "123456"

There are also a huge number of company- and boss-bashing messages. In fact, boss bashing seems to be a rampantly popular type of tweet to make while at work. Here are just a small fraction of boss-mentioning tweets, with appropriate parts redacted, that I also found within just a few minutes:

- [TwitterID redacted] my boss has this really nasty habit of blaming me for things she effed up. Today I found irrifutable proof that...
- [TwitterID redacted] she did this one all on her own. -rocky balboa dance-
- [TwitterID redacted]: Dear nephew of my boss... F[***]k you. [URL showing map to location redacted]
- [TwitterID redacted] My boss is trying to drive me crazy!!!!! I know that is his evil plan!
- [TwitterID redacted]: My boss just put me in a headlock. Not sure how I feel about that.
- [TwitterID redacted]: Heading to lunch with the boss today! Celebrating my anniversary with my firm! Love my job! Great to be me!
- [TwitterID redacted]: Need to go bust my boss in just a bit for not doing what he said he'd do yesterday. Yup, I'm that a[**]hole.
- [TwitterID redacted]: work is busy today and i'm about ready to slay my boss cause he's an idiot.
- [TwitterID redacted]: grrrrr.... someone have a short cliff for my boss to take a long walk off of?
- [TwitterID redacted]: my boss needs explanations said to him Sesame Street style
- [TwitterID redacted]: my boss keeps glaring at me and is listening at top volume to some conference, replete with boring speakers. WANT TO CLOSE DOOR. gah.
- [TwitterID redacted]: enjoying hummus and fresh pita and listening to the rain. Hope my Boss is outta the office.
- [TwitterID redacted]: [name redacted] oh and my boss is a prick...
- [TwitterID redacted]: My new boss is suuuchhhhhh a geek lmao
- [TwitterID redacted]: Boss is riding with me... No music... No texting... No twitter... Dude in my way all day... Boo... Very boo... [link to map of twitterer's location]

Not only are many of these career-limiting types of messages, they could also have legal implications for the companies where these folks work. Just because they usually did not name names in the tweets, it was trivial to go to the profile of the associated TwitterId and often find the name of the company where the individual works. That very quickly led to knowing much more about who the boss could be. Do your personnel understand or realize how easily their tweets could be linked back to them and to your organization? It is your responsibility as the organization's information security and privacy leader to make them aware of this possibility.

In mid-April 2009, more than 14 million people used Twitter. A recent MarketingProfs survey of 425 Twitter users revealed that they spend an average of almost 3 hours a day on Twitter. And from what I've seen in 2 months of using, and often just lurking on, Twitter, most of this activity is during normal business hours. Business leaders, do you know what your personnel are actually doing throughout the day? Are they linking to business information that should not be made public? Are they naming names that should not be named? It is important to think about all the possibilities and address the identified concerns, and associated risks, with effective and enforced policies; not only for Twitter, but for any of the new and emerging social networking sites.

Perceived Need for Personal Activities Within the Workplace

Not that long ago, personnel never really expected to do any type of personal activities at work. Well, maybe make a quick phone call or two during the course of an exceptional day when a doctor's appointment needed to be made or a school appointment set, but otherwise, for the most part, they came to work expecting to focus on getting their jobs done and then leaving. Occasionally, workers would justify doing such things as writing personal letters at work or taking work supplies home with them. They still do.

But new technologies have brought along new attitudes about what perceived acceptable activities should be at work. Not only do people now expect to use their own mobile phones and computers within the workplace and visit whatever Websites they want to visit whenever they want, it is even becoming the expectation of children in elementary and secondary schools.

I was recently at a conference and heard Jason Dorsey, "The Gen Y Guy," give a keynote about the wants and perceived needs of the four generations of workers that he had defined. He indicated that the youngest generation, the "Gen Y" workers, frankly just expect to be able to do personal activities and use their own personal computers and data storage devices at work unless they are explicitly told by their work managers, through policies and on an ongoing basis through other communications, that they could not.

Various studies also show that the ability to use personal technology tools and Web sites while at work is a feature that growing numbers of workers look for in an employer. If they do not have these abilities, even in these hard economic times, many actively search for a new employer.

Information security and privacy leaders need to keep this perceived need for personal technology use in mind as they create policies and governance programs. Look over your policies, procedures, processes, and technologies and consider the following:

- You will have a small, to possibly large, percentage of employees who have a perceived need to use their personal technology devices (such as smartphones, laptops, USB drives, iPods, and so on) and personal communications (such as email, instant messaging, blogging, tweeting, social network sites, and so on) while they are at work. Do your information security and privacy policies address all these types of technologies, sites, and associated activities?
- Is personnel retention important for your organization? If so, have you looked at the impact of retaining employees by addressing their perceived technology needs and implementing appropriate security transparently and without perceived unnecessary restrictions?
- Are your information security controls and safeguards balancing the wants of personnel with the needs for security? Have you determined acceptable controls and corresponding acceptable levels of risk to meet personnel wants and security needs?

You Must Establish Requirements and Expectations to Effectively Protect Information

It is critically important to effectively establish information security and privacy requirements if you want to successfully manage data protection to support business. Why?

- You must know WHAT the types of information are within your business that require safeguards and controls; often referenced as sensitive and confidential information.
- You must know WHERE these sensitive and confidential pieces of information, in all forms, are collected, accessed, processed, copied, shared, stored, and disposed of in order to be able to safeguard the information in all those places.
- You must document and communicate HOW to protect the sensitive and confidential information, in all forms and locations, to all personnel who have job responsibilities that give them access to such information.

Establishing and implementing documented, thoughtful, risk-based information security and privacy policies provides the safeguard directions and goals necessary to effectively control security. Documented policies also demonstrate and establish management expectations as well as responsibilities and accountability for personnel to implement the safeguards.

Do not assume that personnel will innately know that they must protect information, let alone how to protect it—especially when they are using new and emerging technologies. Were you born with the knowledge for how to cross the road safely or how to ride a bike? People have to be told, and reminded often, how to protect information. Documented policies, supported by appropriate procedures and ongoing training and awareness communications, are necessary to effectively protect information in all forms.

Additionally, persuasive, new, and emerging laws and regulations as well as government and business partner retention and archiving requirements call for formally documented information security and privacy requirements, internal compliance, litigation, and e-discovery support. These must be regularly reviewed and updated appropriately to address risks created by new and emerging technologies that personnel use within the business environment.

The Key Components of Data Protection

Most experienced information security practitioners know that the three generally accepted primary components of information security are confidentiality, integrity, and availability. They are commonly referenced as the CIA triad.

As far back as 1990, Donn Parker expanded upon this typical CIA triad model to provide what, in retrospect, was a more tenable information security model within the context of all these new technologies. Parker called these six elements the "six atomic elements of information," which Dr. Mich Kabay subsequently coined the phrase "Parkerian Hexad," which is now the more popular label. These elements included not only confidentiality, integrity, and availability, but also the additional components of authenticity, utility, and possession (or sometimes referenced as "control"). Certainly with the business-to-business and person-to-person connections new technologies now allow, these additional three components are more apparent than in 1990 when we were a basically larger, unconnected world.

Let's consider how personnel use of a new technology, such as social networking sites, impacts business through each of the Parkerian Hexad components.

- Confidentiality—Confidentiality refers to limits on who can get specific kinds of information. When considering the growing numbers of data protection laws, regulations, and industry standards, let's consider the confidentiality of PII and who may be able to get to that information through the use of social networks. Could customer PII end up on social networks from your company's network?
- Possession or Control—This refers to ensuring that only authorized persons are able to access or have possession of specific types of information, such as PII. What if one of your personnel, authorized to access a client file containing huge amounts of PII, downloaded it and, somehow unbeknownst to him, placed it on his Facebook page. Then one of his friends obtained a copy of it, effectively taking possession and control of the file. Does your company have controls in place to keep your corporate files from being posted to public sites? What if the customer file were password protected? Even if individuals who obtained the file did not break the password, the individuals whose PII was in the file would understandably and legitimately be concerned that those in possession of the file could get access to the information at any time through any number of freely available password crackers without the control of your company.
- Integrity—Integrity refers to being correct or consistent with the intended state of information. Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity. For example, what if one of your personnel decided that they wanted to update client files, necessary for work purposes, by posting a copy of it to their Facebook page so that they could then easily download it and update it later from their home? This has actually been done! What if the file got changed by someone else who had access to that individual's Facebook page? Do you have any policies or technologies in place to keep confidential information and PII from being posted to such sites?
- Authenticity—Authenticity refers to correct labeling or attribution of information. For example, what if an internal email is forwarded to an online Web 2.0 site, then someone who has access to the site forwards it back into your network and makes it look as though it came from someone else? What if they changed the contents and made it look like an official email from your company's CEO? Do you have any controls in place to ensure the authenticity of electronic messages and other data used during business? Authenticity is breached because the email is incorrectly attributed to someone else. Similarly, misusing a field in a database to store information that is incorrectly labeled is also a breach of authenticity. For example, storing a customer's Social Security Number in a field labeled as the customer's credit card number would violate the authenticity of the information.
- Availability—Availability refers to having timely access to information. For example, could your personnel use social networking sites, or download information from them, in ways that would effectively create a DoS situation for your network? Do you have policies addressing this risk?

- Utility—Utility means usefulness. For example, suppose personnel stored a decryption key for a business file in their personal computer they primarily use for accessing their social networks. Then, their computer crashes because of malicious code that was downloaded through one of those sites and they lost all their data, including that one, unbacked-up decryption key. You may still have the encrypted customer file, but without that decryption key, the file is worthless; it has lost all its utility. Have you thought about the possibilities for this type of situation and implemented safeguards to prevent it from happening?

Now let's consider a different type of technology that is just as pervasive as social networking site use—cell phones with texting and photo capabilities—as they apply to the Parkerian Hexad components. We'll use an iPhone for ease of referencing:

- Confidentiality—To review, confidentiality refers to limits on who can get specific kinds of information. So what types of confidential business information can your personnel store on their iPhones? And who has access to their iPhones? Is the data stored on their iPhones encrypted? Should it even be there?
- Possession or Control—This refers to ensuring that only authorized persons are able to access or have possession of specific types of information, such as PII. Who has access to the iPhones that your personnel use? What can others do to the data on the iPhone if they get possession of it?
- Integrity—Integrity refers to being correct or consistent with the intended state of information. Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity. What kind of business data can be changed through the iPhones your personnel use?
- Authenticity—Authenticity refers to correct labeling or attribution of information. How can the authenticity of messages and data files possibly be changed through iPhones used for business purposes?
- Availability—Availability means having timely access to information. Are any files stored on your personnel iPhones that should more appropriately be stored on business systems on your network, such as email messages with attachments? Would they be available if necessary for e-discovery purposes?
- Utility—Utility means usefulness. Will the data stored on your personnel's iPhones retain its usefulness for business purposes? If one of your worker's decryption key is stored on the iPhone and the iPhone is lost, what encrypted business data could lose its utility?

Desperate Times Call for Diligent Measures

A bad economy requires more information security diligence. That is worth repeating: whenever there is a bad economy, information security practitioners must be more diligent and more aware to ensure security controls and safeguards are effectively working.

The economy has a profound impact on the information. Chapter 1 described the many recent studies that business leaders need to know about that provide compelling evidence that information security and privacy incidents dramatically increase as a result of desperation, with those committing the crimes convincing themselves that they are justified in their criminal actions. The studies reveal that many of the incidents will occur from insiders with authorized access to valuable information.

The economy has a noticeable impact in increasing information risks around data protection activities:

- Increasing crimes
- Increasing mobility
- Increasing cutbacks in security protections

I attend several information security and privacy professional group meetings, seminars, and conferences. A recent seminar was held with information security and privacy officers from numerous agencies and organizations. The facilitator asked the group of around 50 in attendance to name four major technical changes that were on the horizon that would affect their organizations.

Even within this very knowledgeable group of folks, the responses revealed that many to most attendees were unaware of emerging technologies that could have significant impacts on their organizations. In general, they were knowledgeable about current developments in laws and regulations and new compliance products but were unaware of dramatic changes to existing technologies, and brand-new technologies, that would certainly have a major impact with their organizations in the coming months. Significant numbers of the attendees had never heard of the following:

- Twitter
- Virtual worlds
- Cloud computing (yes, really!)
- Geo-coded data
- Semantic-aware technology

The challenge to keep up with new and emerging technologies that personnel throughout the organization are widely and quickly using, even while doing business activities, is a weakness among many organizations. Most information security and privacy leaders are overwhelmed by the need to do daily operational and tactical planning.

All these variables result in the need for more proactive data protection activities, including diligent risk assessment activities, which include consideration and forecasting of the new technologies that personnel will be bringing in-house and using prior to having safeguards established.

Assessing Risk to Provide the Best Data Protection

Information security risk assessments for facilities, infrastructure, applications, operations, and PII use need to be performed to ensure that threats and vulnerabilities associated with these new technologies have been identified, the recommended controls implemented, and management has accepted the residual risk or transferred applicable risks to another organization. When performing risk assessments for new and emerging technologies, be sure to think out of the box. (Yes, I used an overworked cliché; but it is applicable here.) Information security and privacy practitioners cannot just look at how the new technologies are currently being used; they must also look at how they COULD be used!

> **Note**
>
> Determining risks to PII is commonly and increasingly done through privacy impact assessments (PIAs).

Remember, information security exists to SUPPORT the business. To effectively support the business, information security professionals must apply safeguards that are appropriate to mitigate risks to a level that is acceptable to BUSINESS; this will vary from one organization to another based upon each organization's unique environment and circumstances. This is why you cannot just put out a cookie-cutter information security policy or use an exact copy of a policy that a friend of yours who is also a CISO is using.

Information Security Leader Responsibilities

There are a number of data protection issues and responsibilities that information security leaders must understand. If poor decisions are made, it could have significant negative impacts upon the organization. Table 3.1 provides a listing of the ways in which information security leadership decisions can impact the business.

Exemplary Leadership Results: Positive Impacts	Poor Leadership Results: Negative Impacts
Regulatory, contractual, and industry standards compliance	Fines and other sanctions for legal, regulatory, and standards non-compliance, along with bad publicity and lost customers
Efficient use of staff, resources, and budget	Wasted resources because of duplicated activities, conflicting tasks, numerous versions of code used to do the same type of security task, and so on
Efficiently prioritizing information security activities based upon risk and need, resulting in projects being delivered on time with little to no security mishaps	Lack of project information security prioritization, resulting in missed due dates and leaving more critical tasks unaddressed
Standardization of information security products, technologies, processes, and activities makes security actions more efficient and saves time and money	Lack of standardized information security products, resulting in increased time to correct problems and fight fires
Standardization of information security technologies results in having to support significantly fewer types of products as opposed to trying to keep up with many different products	Lack of standardized of information security processes and procedures, resulting in confusion and loss of momentum
Centralized information security leadership that applies to all parts of the enterprise ensure security is addressed consistently, resulting in more efficient security	Lack of clear direction and objectives results in lackluster information security leadership, perceived lack of information security importance, and too many areas of the enterprise doing too many types of information security activities; this situation creates conflicts in some areas and leaves gaps in others
Including specific information security checks and activities throughout the entire systems development management process will help to ensure the most secure applications and systems possible, and ensures that they will handle security controls consistently throughout the enterprise network	Lack of a defined systems development management program that includes information security requirements results in haphazard applications development and applications with poor or completely lacking security controls and poor documentation
Working on applications and systems based upon criticality and risk will help to ensure the most business-critical vulnerabilities are addressed and implemented before those that are less critical	Lack of organization-determined application criticality results in the unavailability of the most critical applications

Exemplary Leadership Results: Positive Impacts	Poor Leadership Results: Negative Impacts
Effective information security controls and requirements will more effectively secure PII and other sensitive information, preventing costly incidents and privacy breaches from occurring	Ineffective information security controls will lead to unauthorized disclosure of sensitive information, including PII, resulting in costly incidents, privacy breaches, bad publicity, lost customers, and fines and other potential penalties
Effective information security controls help to ensure proper use of information resources in compliance with applicable laws, regulations, industry standards, contractual requirements, and policies	Ineffective information security controls usually results in improper use of information resources
Effective information security controls help to manage efficiently and in a cost-conservative manner the large numbers of information security threats for which all organizations constantly must be on the lookout	Ineffective information security controls allow a barrage of information security threats, including intrusions, DoS attacks, malicious code (such as viruses, Trojans, worms, spyware, and key-loggers), bots, phishing messages, content spoofing, spam, and related forms of electronic pestilence and mayhem to enter the enterprise infrastructure

Table 3.1: Information security leadership impacts.

Set a Course and Stick with It

Privacy and trust are essential to maintaining good relationships with customers, employees, and business partners. It is also necessary to address privacy issues to comply with a growing number of privacy regulations worldwide. An effective information security program is necessary to ensure privacy expectations, and trust, are maintained with your customers, employees, and business partners.

For smooth, or at least the smoothest possible, sailing with your information security initiatives, create a governance plan and stick with it. Your organization must stay aware of compliance not only with your information security and privacy policies and practices but also to ensure the policies and practices cover applicable laws and contractual requirements. Implement procedures and documentation to monitor the information security and privacy program on an ongoing basis.

Cross-Reference

For additional information about compliance requirements, refer back to Chapter 2.

The following are leading practices organizations increasingly follow to help ensure an effective privacy program as well as to help demonstrate due diligence:

- Provide ongoing visible security and privacy support, commitment, and participation from upper management. Your personnel will truly follow the examples of business leaders, so business leaders must set good information security and privacy examples.
- Implement security and privacy policies, based upon the results of risk assessment, that reflect business goals and mission. Security must benefit business, not unnecessarily prohibit it by implementing controls that are not risk based.
- Diligently stay aware of new and updated security and privacy-related laws and regulations that are applicable to the organization. Make sure you know how each truly is applicable to your organization. Interpret the spirit of the laws and regulations in the context of your organizational environment, not by the letter of the law interpreted by someone who does not understand how information truly is used within your business.
- Develop and implement procedures, standards, technologies, and processes that support information security and privacy policies, ensuring security and privacy that are consistently addressed throughout the organizational culture and support applicable legal requirements.
- Establish formal personnel responsibility for information security and privacy policy compliance by incorporating security and privacy responsibilities into job descriptions and including it within the annual performance appraisals.
- Effectively market and communicate security and privacy issues and requirements to all managers, personnel, and business partners. Yes, successful information security and privacy professionals know how to market and sell the need for safeguards and controls! You cannot expect that everyone in your enterprise will blindly do what you say needs to be done. Everyone will need to know how security is beneficial to them and their job responsibilities.

- Provide regular training and ongoing awareness communications. Give information security and privacy education in small digestible chunks, not in one huge, overwhelming banquet where most of the learning gets scraped off the plate into the dog dish after the training meal. You must keep information security and privacy guidance in the forefront of personnel minds if you expect them to perform their daily work in a secure manner. Be sure to provide training and awareness to your business partners, contracted workers, and other third-party partners as well.
- Use a comprehensive and balanced system of measurement to evaluate performance in information security and privacy management and compliance and make appropriate changes based upon the results.

The entire enterprise organization, from senior executives down to entry-level staff, must consider security and privacy as in integral part of the business, not as an after-thought. Implementing an effective information security and privacy program is more than important; it is a key component of business success.