CHAPTER 11

Engineering Your Organization to Be Privacy Ready

Action springs not from thought, but from a readiness for responsibility.

—G. M. Trevelyan

This chapter provides a methodology for assessing and implementing privacy awareness and readiness in the enterprise as a whole. It also discusses the privacy roles and responsibilities typically found in nonengineering groups throughout the enterprise and their contribution to an organization's privacy awareness and readiness.

Some may think the term engineering cannot cover organizational structure, input, and expected output. Nonetheless, an organization, like a series of hardware and software elements, can also be considered a "metasystem" and, as such, it needs to be designed and tooled (and in some cases, retooled) to function properly. This type of engineering work (i.e., organizational or industrial engineering) is instrumental in establishing an environment and cultural context in which privacy engineering can flourish and one in which data is recognized as an asset and is respected as a matter of ethical as well as financial importance.

It is just as important to engineer an organization for privacy as it is to engineer processes, products, systems, and services for privacy. In fact, the effectiveness of privacy engineering systems or programs depends on the privacy readiness of the overall organization. This is because processes, products, services, and systems are not built, licensed, deployed, implemented, or supported in a vacuum.

All tasks within an enterprise are ultimately performed against a backdrop powered by personal information use and management. This is true regardless of the percentage of PI related to employees vs. customer data processed by an enterprise or a subunit of an enterprise. In other words, almost anything requires uses of personal information throughout an enterprise.

This organizational engineering includes establishing privacy governance (which will be discussed in detail in Chapter 12) and creating privacy awareness and readiness throughout the organization (i.e., communication and training), functional alignment, and staffing. This staffing includes new and emerging privacy-focused roles, as well as more established roles such as the chief privacy officer (CPO)[1] and chief information security officer (CISO).

A good example of emerging privacy roles may be drawn from the experience of many CPOs in the early 2000s when the notion of organizational privacy roles was in its infancy. Many early CPOs first established a privacy council. This virtual organization consisted of business owners of required datasets (i.e., marketing and human resources), IT representatives, disaster recovery staff, legal representatives from outside the privacy function, business continuity, mergers and acquisitions groups, and risk and dedicated privacy professionals. The group would bring intelligence and best practices together on a regular basis and would be the central sharing point for information or workflows that required coordinated efforts from different owners. The levels of individuals on the privacy council often varied wildly to include security savvy junior programmers as well as high-placed officers who commanded large budgets and resources but who also were dependent on a constant flow of sanctioned and safe data. In many cases, a privacy council acted collectively in the enterprise system where distributed technologies and authority would not or did not exist.

Making an organization privacy ready is not solely the domain of privacy engineering teams any more than making sure an organization is ready to release a new product or deploy a new system is solely the domain of product engineering.

Privacy Responsibilities in Different Parts of the Organization

Every organization's strategy for addressing its coordination and improvement requirements to become more data and person centric will be a bit different. These differences evolve as the privacy programs mature and as metrics for success become more ubiquitous. As such, there is no one-size-fits-all answer to what roles and areas of focus different departments will have in tuning an organization for privacy operational readiness; however, there are some typical roles and functions that are more than likely to appear in any organization.

Table 11-1 provides an overview of the high-level responsibilities of data privacy professionals in nonengineering departments (i.e., not IT or product development).

[1] We are talking about the CPO role. The job title may be different.

Table 11-1. *Privacy Responsibilities Throughout the Organization of Nonengineering Groups*

Organization/Function	High-Level Privacy Responsibilities
Legal	Provide support for contractual documents and help privacy engineering staff stay current on new legislation and regulations, including assessing laws as they relate to privacy policies.
Marketing or business development and sales	Manage and safeguard customer data to protect its privacy and help ensure that customers' personal information is accessed and used only as authorized. Build trust in the organization so customers are comfortable sharing their data. Plan and address sales team playbooks for selling privacy engineered products or services or demonstrating to potential customers how their data will be subjected to high levels of protection and respect.
Vendor management	Ensure that if vendors collect, manage, or use PI on behalf of the organization, that the PI is accessed and used only as authorized and that appropriate safeguards are maintained.
Audit	Help develop a privacy compliance audit model as well as identify and track privacy risks during the audit process. Conduct audits in a privacy-compliant manner.

Privacy Awareness and Readiness Assessments

Awareness starts with an assessment. Those concerned with an enterprise's privacy preparedness must determine what is already in place (if anything) and what needs to be put in place for the enterprise to be privacy aware and ready. If an enterprise has engaged a CPO, this effort should be led by that CPO. If the enterprise does not yet have a privacy accountable executive such as a CPO, we recommend any one of these options:

- Create and staff the role as soon as possible as a permanent position with funding and executive support and buy in
- Fill the role temporarily until the assessment is completed and then fill it as a permanent chartered position based on the results of the assessment project
- Get the tasks, requirements, and responsibilities integrated into each relevant function

The process for making this assessment is called a *privacy awareness and readiness assessment* (it could also be called a Proactive Assurance Review [PAR], in internal audit terms). A privacy awareness and readiness assessment is similar to a privacy assessment of a process, product, or system, which is done through a Privacy Impact Assessment (PIA) (as discussed in Chapter 10).

The difference between a PAR and a PIA is typically one of horizonal vs. vertical scale. Where a privacy awareness and readiness assessment (the PAR) covers the organization as a whole, a PIA typically covers a system, a process, or a particular tool or feature.

A good privacy awareness and readiness assessment requires focused leadership, a budget, executive buy in, and a lot of finesse to convince stakeholders that they are, indeed, stakeholders and to gain an understanding of a data asset that may have gone unnoticed and uncurated for years.

In the experience of many privacy officers, one of the grumpier members of any executive staff may be the loveable yet cynically analytical chief financial officer. At first blush, the CFO should be the most excited and engaged in the notion of unearthing unleveraged assets and identifying potential liabilities, after all, this is the crux of his or her job. In reality, the CFO may consider a discussion of data risks and outcomes as the exclusive domain of the CIO and his or her only concern, the now well-trod notion of risk under the financial controls requirements.[2] Reaching and teaching teams that calculate financial worth in a world where data asset values are not yet competently reported can be a challenge. Be patient with them. The CFO and his or her team will ultimately report and leverage data valuation and risk for data assets, including personal information.

Nonetheless, performing a privacy awareness assessment and leveraging its results can create a significant contribution in building a sustainable privacy-ready enterprise. Think of a preliminary assessment as gathering the "requirements" for the enterprise metasystem as any good privacy engineer would also do for a product, process, or system.

A privacy awareness and readiness assessment provides the means to accurately map out an organization's current situation and understand how well the organization is currently executing the necessary controls and measures to mitigate risk or to create opportunity. It includes identifying organizational roles that are present or missing and defining the level of data utilization, privacy awareness, and readiness throughout the various functions involved in utilizing, managing, or manipulating data as well as those involved in developing products and services.

Remember that risk should always be compared with the value to the business, so the real objective here is to determine the current state of the controls and measures used to manage and protect (i.e., process) personal information so that unacceptable risk can be managed. The ultimate goal, however, is to make sure that risks taken before collecting, processing, or sharing data are all proportionally lower than the value of what is being assessed or achieved by processing those data. After all, if the costs to mitigate data-related risks are greater than the ultimate asset value, processing will not be a good business proposition, nor will the incentive to maintain and protect that data remain at the appropriate level.

A good privacy awareness and readiness assessment should not only define and document the existing situation but should also identify steps for remediation where unacceptable risks and opportunities for innovation are discovered.

[2] The Sarbanes-Oxley Act of 2002 is the most notorious legal requirement for publicly traded companies in the United States, but nearly every jurisdiction worldwide has similar requirements to protect financial reporting from fraud and shenanigans.

Define Existing Systems and Processes

Because the use of personal information in an enterprise can be so vast and pervasive, it is rare for any one individual to understand it all. Many organizations have no map that defines the existing data flows for all personal information. Those that do have some mapping often proudly produce a spaghetti-looking diagram of existing databases and data markets and, perhaps, a key to identity management systems and corresponding role definitions. Rarely, if ever, do data elements have corresponding policies dated and marked to reflect timing and processing requirements for data within the enterprise map.[3] Rarer still are data element maps created for data flowing to and from third-party systems and vendors.[4] The privacy engineer should dance an unseemly and ungainly privacy jig if he or she encounters such a map, as the basic assessment and privacy readiness of such an enterprise would then be much easier.

The first step in a privacy awareness and readiness assessment is to define the current business processes and data flows as well as the existing privacy policies and notifications in use. The idea behind this first step is to document the current situation for analysis from a strategic perspective and to identify where additional controls might be needed. This step also allows the privacy professional to discover exemplars to hold up as models for emulation by others—competition is a strong cohesive force in most organizations.

This can be accomplished with a succession of high-level interviews with stakeholders that will culminate in sufficient information to chart activity diagrams or use-case diagrams that take into account the elements in the enterprise management lifecycle, as shown in Figure 11-1.

[3] Note the activity diagrams showing privacy requirements (Figures 9-3 and 9-7) in Chapter 9. There will often be enterprise data models in well-managed enterprises.

[4] An encrypt and forget legacy is a strong one that actually represents some of the more advanced organizations' early attempts at proactive data protection. This type of scenario is the likely result of a strong IT security group or an unfunded CPO who has been assigned under the CISO organization where the best-case protection for personal data has been deemed encryption for any suspected regulated data.

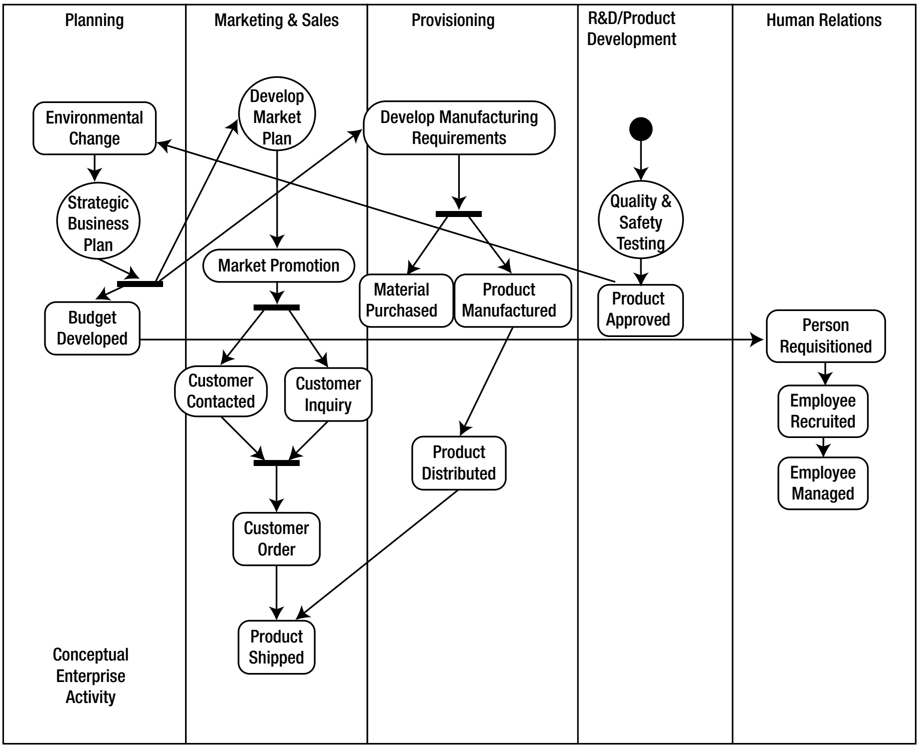


***Figure 11-1.** UML activity diagrams can be used to document the existing high-level process flows and data flows*

Such activity diagrams capture a snapshot of how personally identifiable information flows within and between the existing processes products, services, and systems. They show how the information is currently being used, managed, collected, controlled, and safeguarded throughout the organization. Such diagrams also provide a good management snapshot to show where resources and tasks are owned and where more resources may need to be deployed.

HIGH-LEVEL PRIVACY IMPACT ASSESSMENT QUESTIONS

Here is a sample set of questions you can use to interview key stakeholders and collect information about the data-processing activities of a group or division of an enterprise. The idea is to start at the executive level and begin to travel down the chain of responsibility until sufficient information has been collected and stakeholders at the management and execution levels have been interviewed.

Date:

Name:

Business Unit (BU):

Department:

1. Please describe the general functions of your department or group.
2. How much annual revenue is driven from this BU or supported by this BU?
3. Is there a product or services breakdown of the revenue?
4. What is the overall "value" of the information that is used or processed as part of this BU?
    a. Is there another way that you measure value for information (Example: churn, subscriptions/newsletters subscribed to)?
5. What is the volume of the information your team manages?
6. What are the elements, types, or categories of data? (i.e., customer e-mail addresses, credit card numbers)
7. What information is critical to your BU for success?
    a. What information helps with product or services or business development?
    b. What information, if not delivered on a timely basis, creates risk?
    c. What information, if not properly managed or stored, creates unwanted risk?
8. Which data elements are important (i.e., highly valued, but not critical) to your business?
9. What are the sources of the data (i.e., internal human resources, payroll systems, products, end users)?
10. Is the source of the data internal, external, or both?
11. What are the systems, applications, interfaces, or other tools your BU uses in performance of its functions?
12. Who are the data subjects?
13. With whom is the data shared?
14. What is the source of the data (i.e., systems, applications, APIs from which the data is gathered)?
15. Where do you see [insert name of company]'s information risk overall?

16. Who at [insert name of company] is doing a great job of data protection?

17. What type of training would be best for your team?

18. When you think about information and data, what worries you most?

To get started creating activity diagrams and enterprise data models, first engage with key stakeholders to understand the "stuff" that is managed[5] and the business processes, their purpose(s), and their value. Then as the business data flows are clarified and are ready for more granular information, begin to work with the IT organization to create activity diagrams and data models. An enterprise IT organization may already have an inventory of the majority of existing systems and may also have a starting point for defining data flows between systems and within business processes. They may not have the contents of various systems documented down to the data element (although they should), but knowing the type and ownership of systems is a great place to begin.

MAPPING DATA FLOW HAS MULTIPLE BENEFITS

In every enterprise, everyone is busy. Everyone has their own set of goals and deliverables. Often, getting resources for a project is not easy, even when everyone realizes it is the right thing to do. Finding resources to map data flows may be similarly challenging and often requires working across multiple groups (at a minimum two—IT, who can tell you what data, and the business owners or data stewards of the systems, who can tell you how the data is used[6]).

Here are some benefits that mapping data flows provides IT, which can be useful in building the business case for IT resources and IT involvement:

- Clear picture of where the enterprise's information assets actually reside and a groundwork for data value assessments
- Quick understanding of risk in the enterprise
- True picture of which IT systems require more or less protection
- Fast analysis of issues when systems are updated or end-of-lifed
- Opportunity to remove redundancy in systems and reduce storage overhead

[5] The class or data models discussed throughout Part 2 are often available for most systems.

[6] Between IT and business organizations, it may sometimes seem that IT is the hardest to get involved. Sometimes this is because IT leadership falsely believes that the mission is complete after encryption of some of the incoming data or, more tragically, they do not believe that the stores of data they do collect, process, and manage is personal information. Perhaps a holiday gift of *The Privacy Engineer's Manifesto* may help with this common quandary!

Equally important, if not more important, is gaining an understanding of the data flows, models, and activities that involve service providers or are hosted at third-party facilities or data centers. When mapping data, it is important not to put blinders on and assess only what is within an enterprise's physical control. All the data flows and activities connected to the enterprise should be considered part and parcel of the same. This is particularly true for small to medium organizations where many off the shelf cloud instantiations or applications may be used to manage a business or organization or just a process. The data models in these cases may not be as complete on the backend, but even the smallest teams can understand which data they use for value and where they send them initially.

Consider the Context

As part of the analysis, it's a good idea to consider the context in which a privacy initiative will operate. What are the aspects of data control that already exist and what is the understanding of privacy from the most senior management to middle managers, functional departments, and administrative personnel? Just getting a handle on the basic concepts and an understanding of privacy at these different levels of the organization will indicate the point from which a privacy awareness and readiness campaign must start.

Another critical factor in establishing context is the organization's overall bias toward risk. If the organization has a high tolerance for risk,[7] then making the business case to close gaps, protect data, and developing internal enthusiasm to do so will be more difficult. However, if the tolerance to undertake risk is low, then creating a business case and developing internal enthusiasm may be easier to engender.[8]

Ultimately, if privacy programs are perceived as providing value to the business or if an organization has made a strategic decision that embedding privacy controls into all of its systems and processes will improve its brand image or provide a competitive advantage, then IT, human resources, product marketing, engineering, legal, leadership, and other teams will likely be quite supportive of the overall privacy initiative.[9] An initial assessment can provide adequate detail to begin this effort.

If, on the other hand, senior management has mandated a privacy initiative to mitigate risk but lower levels of the organization are not yet onboard with the idea, then much more upfront effort will be required. In this example, the privacy professiona would need to spend more time educating engineering and marketing teams about what their risks are and how implementing better controls can provide value.

[7] This type of "risk" is risk that is not based in fact and data. A true risk-based organization would ideally take in relevant facts and then take action. This type of idealized organization can, arguably, make broader leaps forward because the risk is taken with data and not exclusively chest-bumping bravado.

[8] It should be noted that an excessive desire for too much detailed data or an overly conservative appetite for risk may also cause decision paralysis, and unnecessary paralysis can transform once innovative organizations into sleepy dinosaurs.

[9] This is more about corporate values and views of risk. Google and Facebook, for instance, have high thresholds for privacy risk and thus it has taken FTC sanctions for them to beginning toeing the privacy line. Whereas a bank like RBC has always understood privacy risks and implementing and managing privacy controls have always been relatively more straightforward.

Privacy awareness and readiness can also have implications for a business strategy. For example, where there is limited awareness and readiness in marketing and the business strategy depends on consumers opting in to an online community, there will be a need to bring greater maturity to the marketing team's privacy awareness and readiness. Without such readiness, it will be necessary to alter the business strategy to avoid the risk that marketing will not properly protect consumer data or will misuse that data to create whole-enterprise risk rather than a risk of a failed marketing campaign.

An organization's strengths and weaknesses with regard to privacy awareness and readiness should be documented so this knowledge can inform privacy strategy, help prioritize tasks in the privacy initiative, and can serve as a benchmark and starting point for improvement for the entire organization.

Skills Assessment

The skills component of the privacy awareness and readiness assessment is a review of where these various responsibilities are currently hosted in an organization and to what degree skill sets currently meet or are capable of meeting desired objectives.

In most cases, there will be holes, meaning that some of these responsibilities are not currently being carried out in the organization or may not even have an assigned responsibility. Several factors can affect how well the responsibilities are carried out. The most common reasons for poor execution of privacy responsibilities include:

- *Lack of awareness and readiness:* The responsible party may not fully understand privacy risks or how to alleviate them. In this case, privacy awareness and readiness education is needed.

- *Lack of resources:* The responsible party will often be wearing multiple hats, and if there are limited resources to properly perform the privacy duties and responsibilities, they can fall by the wayside. Similarly, a lack of financial resources can stymie efforts to get proper local legal counsel, hire vendors for efficiency and outside perspective, and limit face-to-face communication, which is necessary for a strong (often virtual or matrixed) team.

- *Lack of incentive:* Other tasks that are more directly related to the charter of the department in which the person resides are likely to get more attention unless there are explicit incentives for privacy engineering support work.

Organizational alignment can fill these gaps through a matrix organizational structure or by getting buy in from management to assign goals and objectives related to privacy engineering.

In summary, the skills assessment identifies and documents the responsibilities that are currently unfulfilled as well as those that are already being carried out. It also identifies opportunities for improvement in how the existing responsibilities can be executed more efficiently or more effectively.

More detail about specific roles needed for successful privacy engineering can be found in Chapter 12.

Building the Operational Plan for Privacy Awareness and Readiness

Based on the findings from the privacy awareness and readiness assessment, an implementation strategy and operational plan can be built.

Goals and objectives for privacy awareness and readiness can be organized to provide short-, medium-, and long-term focal points. They should include quantifiable metrics for success so that the privacy professional can measure progress of the program. The goals and objectives should take into consideration the existing business risks from known privacy vulnerabilities as well as the levels of privacy awareness and readiness throughout the organization.

The general level of understanding about privacy throughout the organization is a key factor in deciding which can be accomplished and the proper timeframe for goals and objectives. The initial data-gathering phase of the privacy awareness and readiness assessment should uncover the existing level of awareness and readiness in the organization. During this analysis phase, the privacy team should come up with a prioritized list of actions to improve privacy awareness and readiness.

SAMPLE PRIORITIZED ACTION LIST

Here is a sample list of prioritized actions paired with the associated finding to which the action is a response.

Overall Awareness or Understanding of Personal Information

- General awareness communication and training across the organization to help apply clarity and consistency to how PI is defined
- Specialized or targeted training efforts to support specific roles (i.e., product development, human resources, sales and marketing)

Documenting Knowledge or Expertise

- Continued coordination between privacy and engineering teams to complete PIAs and translating results to formalized policies and procedures to guide the business on how to handle PI

Developing Data Lifecycle Model

- Coordination with corporate strategy or BU teams to help build a model on how to monetize the data utilized across the enterprise
- Company-wide effort to establish data retention and deletion requirements

Privacy Engineering

- Privacy teaming with engineering, IT, and operations to put in process gates or assessments to ensure privacy-related areas are considered in product development or project implementations
- Development of standards or guidance that will be business enabling and not business stifling
- Align roles and responsibilities with counterparts at parent company and other subsidiaries

Marketing Privacy-Related Products

- Privacy collaborating with corporate development, strategy, portfolio or product management, professional services, and go-to-market teams to segment out privacy-related products as a separate part of product solutions
- Focus on both organic and inorganic growth for privacy-related solutions

Privacy awareness and readiness are only two components of an overall privacy program that must make efforts toward improvements across a broad array of people, process, and technology issues. However, there is always some need to improve privacy awareness and readiness before other factors can be properly addressed. For example, if there are myths about privacy that have proliferated throughout the organization, these must be dispelled before the organization can successfully adopt the right privacy practices. Privacy awareness and preparedness are ongoing processes for the enterprise to remain strategically positioned and resilient in the face of changing legal requirements, external events, customer and business changes, and overall enterprise resilience.

FIVE BIG MYTHS ORGANIZATIONS HAVE ABOUT PRIVACY AND THE RESPONSE SHOULD BE TO DISPEL THEM

Myth 1: We don't have any personal information to worry about.

Response: If you have employees or customers, you have PI.

Myth 2: Security has it covered.

Response: Security's focus is ensuring confidentiality, integrity, and availability of proprietary information, not all that privacy requires. Security can be, but is not always, a help. (See Chapter 3 for a discussion of this.)

Myth 3: No one gets in trouble if we screw up.

Response: Facebook, Google, Microsoft, and Eli Lilly are all currently under 20-year consent decrees from the FTC and need to submit to biannual audits. Fines and sanctions are growing every day. It may not always make headlines, but people and organizations are both getting into trouble. The recently passed European Regulation calls for a downside 5% of worldwide turnover for privacy failures with few specific guidelines regarding how individual member-states may attempt to assess such a fine. Even if this law and others like it do not stand, legal costs battling even speciously assessed fines will be the future for many years to come. Trouble.

Myth 4: Privacy people always say no to fun business ideas.

Response: This is the one myth that may be grounded in some truth and a failure of imagination. Unless the fundamental premise of that which is proposed is against the law, a good privacy person will answer: Yes, it may be done and here is how, or, at least, here are a few ideas. Although the hoops that must be jumped through to get something done may equal "no" in terms of a risk vs. reward calculation, the decision not to move forward with a bright shiny object is a sound business risk decision.

Myth 5: Privacy gets in the way of marketing or connection.

Response: In the era of customer engagement and e-marketing, it has been proven time and again that privacy-based permission and context-based marketing provide *better* results and return on investment.

Common approaches for building privacy awareness and readiness include internal publications, newsletters, custom apps, employee-specific goal setting, and formal training for specific audiences.

An operational plan should include a prioritized list of action items intended to advance privacy awareness and readiness. This prioritized list should be accompanied by a schedule for execution and an associated budget.[10]

[10] Ordering multiple copies of this book would be a good idea!

The privacy awareness and readiness operational plan should also include success metrics for each step of the plan as well as descriptions of the planned review processes that will help determine if additional steps are needed as time goes on.

Building a Communication and Training Plan for Privacy Awareness and Readiness

To create awareness and build readiness into the enterprise, there must be a "there" there. For this reason, privacy policies must be defined, written, and communicated to employees. They also should be extended into standards and guidelines that are practical and both directional and instructional as needed. All such policies must be effectively communicated throughout the enterprise. Communication and training are crucial to building awareness and ensuring readiness and ownership.

IT'S ALL FUN AND GAMES UNTIL SOMEBODY LOSES PI (PERSONAL INFORMATION)

By Ruby A. Zefo, Chief Privacy and Security Counsel, Intel Corporation

Does your enterprise have a bring-your-own-device (BYOD) program? If you work for a sizable company, the answer is likely "yes," whether you know it or not. Chances are that if you do not launch an "official" BYOD program, savvy employees who prefer using their own smartphones and other mobile devices will launch their own. When that happens, your intellectual property and your employees' PI could be at risk. BYOD programs should not be the reason you suddenly dust off your processes for data breach management or trade secret loss. Proper cross-company planning and maintenance of BYOD programs can make all the difference between a cherished employee and employer benefit vs. rogue devices and networks, employee complaints, and employee data loss.

Prohibiting employees from bringing their personal devices to work is not the answer. History shows that Prohibition didn't work the first time; alternative compute options only become more tantalizing if a company is overzealous in prohibiting their use. A recent study found that one of three respondents said they would gladly "contravene a company's security policy that forbids them to use their personal devices at work or for work purposes."[11] Many younger employees view using their own mobile devices at work as a right, not a privilege. An employer may find it difficult enough to stay ahead of the curve when it purposefully launches a new BYOD program, no less when the program "starts itself."

[11] InfoWorld report on Vision Critical study, "Young employees say BYOD a 'right' not 'privilege.'" www.infoworld.com/d/consumerization-of-it/young-employees-say-byod-right-not-privilege-195901

Embracing BYOD programs is the right answer. These programs are not only about employee convenience and satisfaction; BYOD programs can also provide corporate benefits, such as increased employee productivity. Right or wrong, employees use mobile devices to work while on vacation, in bed, during travel, on weekends, and while they are multitasking on the phone with old Aunt Marge who is droning on about the neighbor's barking dog. Managed properly, these programs can be a win-win for employers and employees.

So, you wisely decide to launch a BYOD program. What could go wrong? It's all fun and games until somebody loses PI. Even a company attempting an effective plan to launch a new BYOD service can get it wrong by failing to understand employee preferences and device usage habits, privacy and data security impacts, culture, environment, law, and so forth. When that happens, a company may see history repeating itself in the form of bootlegging: more rogue behaviors, networks, and devices.[12]

Even initially cherished implementations may grow stale; a company may erroneously expect a properly launched BYOD service to thereafter "run itself," and that it will remain static and rarely need changes in how it is administered. That can lead to a lack of funding and program management, gaps in security as technologies, user behaviors, and devices change, and increased risk.

Without a well-organized cross-functional launch plan, BYOD programs can create insecure devices, networks, apps, and behaviors that all risk company assets and create privacy problems, including:

- Lost, stolen, or misused PI, including sensitive PI—people store all kinds of sensitive data on their mobile devices
- Lost or stolen intellectual property
- Malware or intrusions that can impact the corporate network and assets and provide a route for illegal access to third-party data and assets connected to the corporate network
- Employee escalations over personal data loss and resulting harm
- Data protection authority or enforcement agency inquiries
- Lawsuits, including class action lawsuits can occur

[12] According to an iPass Mobile Workforce Report, nearly 25% of mobile workers say they bypass IT controls to access corporate data, claiming IT is slow in responding, they needed to do something immediately and could not wait for IT, and so forth. "BYOD mobile workers thumbing nose at IT security." www.zdnet.com/byod-mobile-workers-thumbing-nose-at-it-security-7000003519/

What can a company do to properly prepare, launch, and maintain a BYOD program? BYOD programs are more of an art than a science. So while in the BYOD context one size never fits all, a company can still prepare for the inevitable privacy issues that can Creating a cross-functional team that will gather data on employee preferences, beta test the services prior to broader launch, address any gaps in service and data protection, and manage employee expectations, awareness, and consent are important steps to getting it right. Nobody wants to be the employee that leaves the CIO holding the liability bag because he realized after the launch that he accepted more risk than he thought by failing to have requested or accepted a comprehensive risk analysis from all the key stakeholders. That should be part of the return on investment analysis prior to service launch.

In addition, a company can take a number of practical steps for proper planning and management of a BYOD program, including:

- Identify all key global stakeholders, including employees from IT, privacy, security, legal, employee communications, training, e-discovery, and human resources
- Ask the launch team to conduct a real return on investment analysis to evaluate the tradeoff of service value vs. cost and privacy risk
- Prioritize global rollouts according to import and ease of offering the service, considering privacy and related laws, enforcement schemes, types of data involved, ease of giving employees notice and obtaining consent, number of employees, operational readiness in each location, and importance of the service to the employees
- Find the right balance when monitoring employee data: failure to monitor can lead to loss of intellectual property, PI loss, excess cost (e.g., bandwidth use), and lawsuits (e.g., employee harassment). Overmonitoring can lead to decreased morale, covert rogue behavior, and lawsuits (e.g., privacy violations)
- Remember proportionality—for example, many data-protection authorities frown on using biometrics or location tracking for employee monitoring when something less will suffice
- Leverage existing corporate policies, such as acceptable use of electronic devices and the corporate network, information security policies, software licensing policies, etc.;
- Don’t forget cultural differences – both jurisdictionally and within the company; and
- Ask the launch team to create global program managers for proper ongoing maintenance of the program.

Finally, employee behaviors in the BYOD context can make or break the program. With proper planning and execution, a company can do a number of things to create the right employee behaviors and make the service a better experience for everyone:

- Make BYOD policies and guidelines easy for employees to find and understand
- Create short, understandable employee agreements
- Create and launch employee trainings—you need real employee awareness, not just constructive notice, of how the program works and the expectations the company has on employees to participate in the program
- Technology can help: separate work and personal data, secure the device (e.g., strong passwords) and data (e.g., mobile device management technologies), create trusted access based on context (employee and location)
- Regularly revisit the program specifics—authorized types of devices, technologies, employee behaviors and agreements, laws and regulations, enforcement

By embracing BYOD programs instead of avoiding or ignoring them, companies can focus on the fun and games of a great place to work, and not on the loss of PI.

Communicating

Once the privacy strategy and operational plan have been completed, a strategic plan document should be published internally so that all stakeholders involved can gain a better understanding of the objectives of the plan. These reviewers likely will have excellent suggestions for improvements before a final plan is adopted.

The benefit is that it makes the stakeholders part of the process and owners of a stake in the outcome. An auxiliary benefit is that the process of receiving stakeholder input also provides a sense of who will be willing participants, who is going to be dragged along (or cajoled into compliance), and where each type of party's interests lie.

It is important, however, to not let the process of gathering feedback derail the process. Be prepared to set limits to the number of review cycles and timing of the assessment phase so things do not get out of hand.

Once the strategic plan document is considered final, the key ideas of the plan should be communicated broadly within the organization and, where appropriate, with outside parties or stakeholders who may have access to the organization's data.

Another step in the process is to identify the parts of the plan that can be made public, and—if practically and strategically important—make a big public relations deal about it. For example, where a business model is built offering a product or service that benefits from having a strong publically articulated privacy policy (i.e., it requires a great deal or unexpected types or uses of personal information), it may be strategically important to broadcast what measures the enterprise has taken. Because data privacy is synonymous with trustworthy management and sharing of personal information, similar tactics of truthfulness and transparency often work for the enterprise as they do in person-to-person communication and relationship building.[13]

Internal Communications

Concurrent to the policies, procedures, standards, guidelines, and privacy rules being developed, a communications plan should be developed to ensure that all members of the enterprise know that the privacy policies are, which standards and guidelines exist, where to find them, what they are, why they are available, and what their responsibilities are.

Once things are ready, the privacy team should focus on working with the key privacy stakeholders, explaining things and providing training where needed. The availability of this information through such things as internal web sites, newsletters, all-hands meetings, and leadership training will also help people who are new to the enterprise or new to privacy to become educated more quickly.

As much as possible, privacy materials should be written to the specific audiences and avoid too much legalese and jargon (even for lawyers). This will help everyone see the issues in their own areas and recognize that it is also their responsibility and not just the specialized domain of privacy professionals or legal teams.

To this end, it may be helpful to leverage both human resources and communication specialists within an enterprise or organization. Having this information easily accessible and available will also enable those within the company interested in doing so to make helpful, constructive suggestions.

External Communication

As important as the internal community is, external parties of interest—including customers, partners, suppliers, consultants, media, industry analysts, and regulators—are important targets of the communication plan.

There must be an external communication plan delivering the right messages to these audiences to help build awareness of the enterprise privacy program and its benefits. Because regulators and policymakers look at privacy material published by the enterprise, these externally communicated messages need to be well orchestrated and transparent.

Customers and other impacted parties of interest will review these external privacy communications to ensure that their personally identifiable information and the confidential data related to it are handled in an acceptable way. Reasonable fears of these parties of interest should be anticipated. If people fear that their personal data will be sold, for example, the information transfer and sharing policies need to be communicated as clearly as possible to alleviate such fears.

[13] The opposite is true as well. Hiding the type and kind of processing and collection performed, even for the most virtuous of intentions, may cause a rift in respect that may never be repaired. The “trust” that is thus engendered is a trust that this company will always be a jerk. Individual customers and businesses will only remain with jerks until alternatives inevitably appear.

The best outcome for a data subject from an enterprise perspective is one in which the data subject knows which PI is needed, why it is important to engage with this enterprise with this type and amount of data required for the task, and how it is being used and protected. Most important, the data subject should not be surprised by unexpected practices or creeped out by inappropriate or excessive data practices. The more clear, engaging, and complete the communication, the more likely it is an actual asset to the overall program.

A Word About What Are Usually Important, but Boring Words

It is time for an overhaul of how enterprises design privacy notices. As much as regulators and advocates demand transparency and simplicity, they also have become much more demanding about adding required elements and magic language to data subject–facing privacy notices. As a result, the Privacy Notice has drifted in function and efficacy from a document intended to teach and illuminate the user to an element of enterprise self-insurance. The shift in external requirements has also caused the external Privacy Notice to become a creator of risk rather than a means of engagement (which it *should* be in a privacy-engineered environment).

As privacy engineering practices become ubiquitous, so too can the Privacy Notice become an object of innovation and community creation in context rather than lead undercoating for the enterprise.

As with technology innovation, notice and policy innovation can benefit from a multidisciplinary approach. For example, there are vast resources available outside enterprise legal teams focused exclusively on learning, communication, and persuasion. Large enterprises often have internal communications, public relations, marketing, learning, designers, user interface, branding, human resources, and other similar professionals from whom an intrepid privacy engineering team can benefit.

THE PRIVACY NINJA: PRIVACY NOTICE AS GRAPHIC NOVEL

McAfee’s turning its external Privacy Notice into a graphic novel is one such example of a privacy-engineered notice. The inspiration for this approach came from several divergent requirements to explain a very complex data relationship between security services and data subjects. The Privacy Notice needed to transcend many different international contexts.[14] It is needed to respect and provide a counterbalance to the research that said that no users were ever actually taking the opportunity to read policies. Finally, the comparisons in the technology—and most other vertical marketplaces—were comprised on privacy notices that were heavy, confusing, and not the first impression McAfee hoped to make with its customers.

[14] In full disclosure, two of this book’s authors, Michelle Dennedy and Jonathan Fox, are employees of McAfee and were responsible for the creation of the Ninja and the graphic novelization of the McAfee Privacy Notice. We and many others who have since contacted us and well as Tom Finneran, our third coauthor, think they happen to be awesome.

Figure 11-2 shows examples of the illustrations used by to communicate privacy information to customers and web site visitors in its graphic novel Privacy Notice.

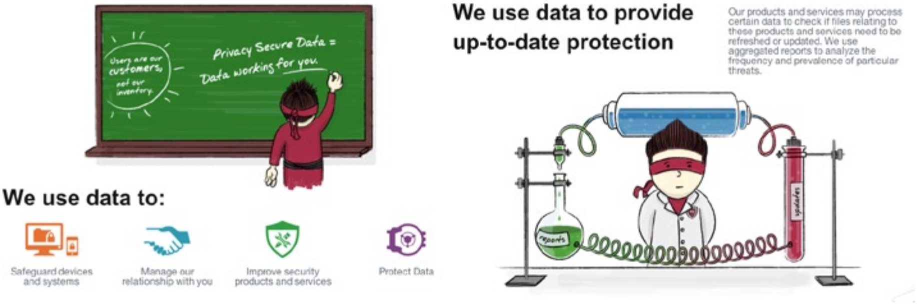

Users are our customers, not our inventory.
Privacy Secure Data = Data working for you.
We use data to:
Safeguard devices and systems
Manage our relationship with you
Improve security products and services
Protect Data
We use data to provide up-to-date protection
Our products and services may process certain data to check if files relating to these products and services need to be refreshed or updated. We use aggregated reports to analyze the frequency and prevalence of particular threats.
reports
updates

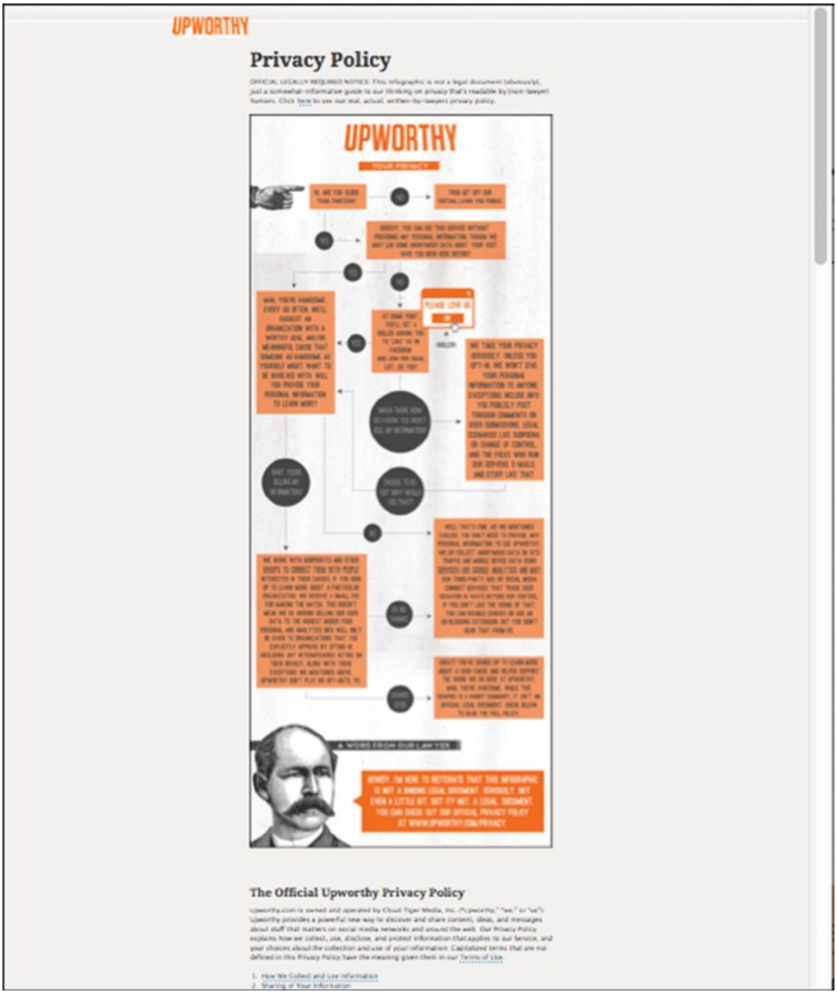
***Figure 11-2.** Animated Privacy Notice example from the McAfee Privacy Notice*[15]

The process benefited from collaboration with McAfee's Chief Design Officer who happened to have a PhD in psychology (sometimes you just get lucky and the combination of one professional with creative and communication expertise is powerful). The team also included international data privacy external counsel to control the risk of innovation, information architects and designers, as well as the McAfee Privacy Team.

The McAfee notice benefited from concepts in two excellent books: *Blah Blah Blah*[16] by Dan Roam and *Resonate*[17] by Nancy Duarte. Both are examples of sources from which to draw, or begin drawing, visual representations of complex ideas such as PI and security data flows. Also, the project team benefited from research such as that performed by Carnegie Mellon regarding policies and the survey performed by the trustmark firm Truste regarding the abysmal record of policies engaging users in toto.

Finally, the idea to work up a visual notice was also inspired by School House Rock, a series of animated musical short films that aired in between Saturday morning cartoons in the United States from 1973 to 1985. In that series, American children learned to recite the US Constitution Preamble, cite their three's multiplication tables, and learn a wide range of sometimes complex facts and ideas in 3-minute segments set to music and animation. As of the first printing of this book, the McAfee Ninjas remain silent though illustrative. The future may be more melodious for the Ninjas as data use continues to grow, business models become more complex, and users of security software become more sophisticated (Figure 11-3).

[15] `mcafee.com`/privacy, December 7, 2013
[16] `www.danroam.com/blah-blah-blah/`
[17] `www.duarte.com/book/resonate/`



UPWORTHY

Privacy Policy

OFFICIAL LEGALLY REQUIRED NOTICE: This infographic is not a legal document (obviously), just a somewhat-informative guide to our thinking on privacy that's readable by (non-lawyer) humans. Click here to see our real, actual, written-by-lawyers privacy policy.

UPWORTHY
YOUR PRIVACY
A WORD FROM OUR LAWYER
HOWDY. I'M HERE TO REITERATE THAT THIS INFOGRAPHIC IS NOT A BINDING LEGAL DOCUMENT. SERIOUSLY. NOT EVEN A LITTLE BIT. GOT IT? NOT. A LEGAL. DOCUMENT. YOU CAN CHECK OUT OUR OFFICIAL PRIVACY POLICY AT WWW.UPWORTHY.COM/PRIVACY.

The Official Upworthy Privacy Policy

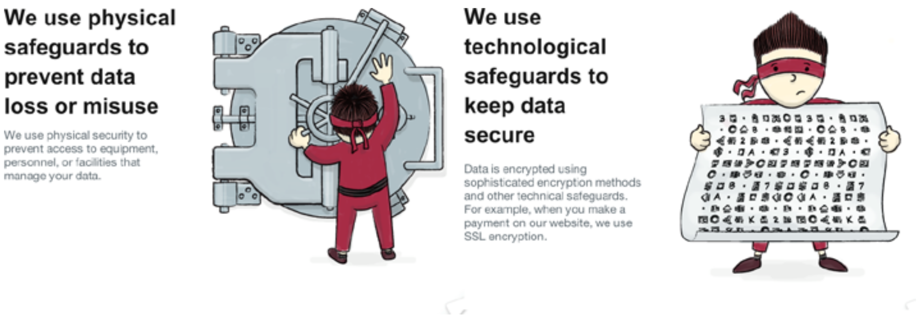
Upworthy.com is owned and operated by Cloud Tiger Media, Inc. ("Upworthy," "we," or "us"). Upworthy provides a powerful new way to discover and share content, ideas, and messages about stuff that matters on social media networks and around the web. Our Privacy Policy explains how we collect, use, disclose, and protect information that applies to our Service, and your choices about the collection and use of your information. Capitalized terms that are not defined in this Privacy Policy have the meaning given them in our Terms of Use.

1. How We Collect and Use Information
2. Sharing of Your Information

***Figure 11-3.** Another great example of a graphic depiction of a privacy policy. This one comes from* `Upworthy.com`

The basic requirements for privacy policies and a public-facing privacy notice include legal requirements, acknowledgment of evolving standards, and global requirements regarding data processing. The other critical role of the public facing notice is to provide transparency to users of systems and services. In the case of security products and services or other complex data intensive services[18], extensive use of aggregate data processing to predict, protect, and block informational threats on multiple platforms should also be described as clearly as possible.

The need for clarity and simplicity in the Privacy Notice was driven by the requirement to raise understanding and engagement in a business where data—sometimes personal data—is necessary to protect all data (Figure 11-4).



We use physical safeguards to prevent data loss or misuse

We use physical security to prevent access to equipment, personnel, or facilities that manage your data.

We use technological safeguards to keep data secure

Data is encrypted using sophisticated encryption methods and other technical safeguards. For example, when you make a payment on our website, we use SSL encryption.

Figure 11-4. *More Privacy Notice examples from the McAfee Privacy Notice on* `mcafee.com`[19]

Timothy Pilgrim, the Australian privacy commissioner, stated that we need to innovate for privacy to be more effective and accessible to consumers at an Industry and Government Privacy Conference in Australia in 2013 Celebrating Data Privacy Week. He cited, as one example, McAfee's use of animated Ninja characters to encourage people to read and understand their Privacy Notice.

Even when privacy engineers commit to innovation, when considering the best approaches for communicating to any audience, keep communications concise and use simple language. Playful and fun communications will generally get good results, as long as they are honest, accurate, and respectful. However, iconography and illustration and other techniques are not yet expected and accepted as best practices. Until these are best practices, infographics, images, or graphic novels are best done in *addition* to full text of privacy notices and related documents for those who may want detail in a more traditional format.

It is also absolutely crucial to note that playfulness and humor do not always translate across cultures or demographics. Privacy notice creation must include the requirement of learning for the intended audience of the notice, designing it according to those preferences and biases.

[18] Data intensive services may include things like what is currently called the Internet of Things (IoT) or Cloud services. However, even well known traditional services like retail or real estate may require massive amounts of data processing, particularly given how much data is available for analytics and other services.

[19] `mcafee.com`/privacy, December 7, 2013

DATA CLASSIFICATION AND RISK ASSESSMENT

By Ed Glover, Client Services Director, Security and Privacy at Resources Global Professionals (RGP)

Too often, senior management who are responsible for the business units view their data needs as unique from other areas of their enterprise. Failure to come to a consensus on common data classification has potential risk implications. Even if they do come to a consensus about the criticality of the data, are their classification standards documented and communicated across the company's business units? Are the metadata used to describe the data consistent across systems? Unfortunately, this is usually a onetime event, and as the nature of the data changes within the business units, management does not reassess the critically of their data to determine if appropriate safeguards are in place or enforce consistent data definitions.

The first step to address risks implications of the data is to ensure that information receives an appropriate level of protection in accordance with the importance to the organization. The company should develop an information classification standard that considers legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the data.

When determining data classification, ISO 27001/2 (ISO/IEC 2013) provides an excellent framework for identifying organization assets and defining appropriate protection responsibilities.

The process of compiling and classifying a list of information assets is an important first step for performing a risk management assessment to identify the level of risk to the information. One needs to understand the criticality of the data in order to assess the risks to the data.

Although there are many ways to classify data, the following list is an example of an information classification standard:

- *Public information*: Any information that, if disclosed, causes no harm or embarrassment to the company. An example of this could be the company's address or main phone number, published annual report, or approved press releases.

- *Internal information*: Any information not approved for general circulation outside the organization, where its disclosure would cause minor embarrassment or operational inconvenience, but more than likely will not result in financial loss or serious damage to credibility or reputation of the company. An example of this could be internal memos, internal project reports, or minutes of meetings.

- *Critical information*: Any information that is considered critical to the organization's ongoing operations and could seriously impede or disrupt them if shared internally or made public. An example of this type of information could be accounting information prior to the approved quarterly and annual announcements, corporate or divisional business plans, customer information of banks, patients' medical records, and similar highly sensitive personal data. Some of these data elements could have privacy implications and should be assessed and evaluated against local or regional laws.
- *Sensitive and confidential information*: Any information that has a serious impact on long-term strategic objectives of the company. This could put the company at risk, if disclosure, and could result in violations of various domestic and international Laws and Regulations. For example: customer databases that include personal information of the employees, etc., pending mergers or acquisitions, investment strategies, intellectual property that could seriously damage the organization if lost or made public. Information classified as sensitive and confidential should have a very restricted distribution/usage labels assigned to it, and must have the appropriate safeguards in place at all times. This information should be identified, assessed for the level of risk, and appropriate safeguards are in place to mitigate the risk to an acceptable level.

Once you understand the importance of data the corporation is responsible for protecting, one should perform a risk assessment to understand the potential threats and vulnerabilities of disclosure of the data. When assessing risk in business terms, there are a number of different methodologies you can use. The following are a few of the many risk assessment frameworks that can be used when assessing risk.

CobiT (© ISACA) Information Criteria[20] consists of seven information criteria in expressing IT Risk in business terms. They are:

Efficiency, Effectiveness, Confidentiality, Integrity, Availability, Compliance, and Reliability

[20] Information Systems Audit and Control Association (ISACA) publication "The Risk IT Practitioner Guide."

The four A's (Westerman) is another way to express risk in business terms. This defines IT risk as the potential for an unplanned event involving IT to threaten any of the four interrelated enterprise objectives[21]:

- *Agility:* Process the capability to change
- *Accuracy:* Provide correct, timely, complete, information
- *Access:* Ensure appropriate access to data and systems, so that the right people have access to the information they need and the wrong people do not
- *Availability:* Keep the systems running and the ability to recover in a timely manner

The COSO ERM – Integrated Framework lists the following criteria[22]:

- Strategic criteria consist of high-level goals, aligned with supporting the enterprise mission
- Operations criteria pertain to the effectiveness and efficiency of the enterprise's operations
- Reporting criteria pertain to the reliability of reporting, including both internal and external reporting.
- Compliance criteria pertain to adherence to relevant laws and regulations

These are just a few options to consider when expressing IT risk in business terms. There are many other risk frameworks to use, and it boils down to choosing a framework that best fits what your company is trying to accomplish when performing a risk assessment.

Having a data classification standard and a holistic risk management process in place to assess risk is a huge challenge and, in most instances, is not addressed or incomplete. Most of the time, corporations at one point in time have developed a data classification definition standard and have not revise it since its inception. This alone is a huge issue because as the business grows and evolves, the original definition may no longer pertain to the business and can result in not addressing, through a risk assessment, the potential threats and vulnerabilities to the corporation's data.

[21] Westerman (Westerman, G.; R. Hunter, *IT Risk—Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007)

[22] COSO (© by the Committee of Sponsoring Organizations of the Treadway Commission) Enterprise Risk Management (ERM)

An example of this is when a company started a professional services organization and provided services to their clients. Their consultants would use laptops (company owned or their own personal laptop) to download client data in order to perform their work. Depending on the nature of the engagement, the data may contain personal information of the employees, network topology maps, credit card information, among others. In most cases, there was information that would be considered private and confidential residing on the personal laptop of the consultant. When performing a risk assessment, it was identified that their consultants were exposing their customers' data to risk of disclosure because they did not understand their clients' data classification and security requirements for data and how to ensure that appropriate security measures were in place depending on the criticality of data.

Furthermore, not every client assessed the criticality of data in the same manner. This proved to be a huge risk issue for the professional services group and the potential impact to their reputation and resulting lawsuits were identified as high or critical. The result of the risk assessment's finding was to encrypt all company-owned laptops to protect client information that is stored on it. Furthermore, a policy was developed to prohibit the use of personal laptops while performing work on behalf of a client. Although this is somewhat restrictive in today's environment, especially with the push for BYOD, it was necessary to ensure that the clients' data was protected and did not expose the company to potential lawsuits if a disclosure were to happen.

There are many stories like this out there. Has your company performed a recent review to determine the criticality of its data, assessed the risk to the company if this data element is disclosed, and implemented the necessary security to reduce the risk to an acceptable level?

Monitoring and Adapting the Strategy

Ongoing review processes are needed to monitor progress in the area of privacy awareness and readiness so that the program can be adapted as needed. Monitoring can take many forms, but objective metrics must be used so that progress can be measured. For example, one metric might be the number of privacy issues that are uncovered in a privacy impact assessment. This particular metric may arise initially as management teams become more aware of privacy issues and thus spot them in PIAs. However, this knowledge will flow down through the ranks over time and the number of privacy issues discovered in PIAs should then begin to decline.

Other metrics to consider are:

- Number of real and unfounded incidents reported
- Program maturity model level
- Percentage of employees who have completed training
- Size and coverage of the "volunteer" army helping the privacy program

Another way that privacy awareness and readiness can be monitored is through a privacy audit, a thorough annual review of the privacy program and its results done in conjunction with either the internal audit team or a certified third-party auditor versed in privacy. In addition to identifying privacy vulnerabilities and areas for improvement in privacy engineering practices, the audit might also be used to monitor the level of privacy awareness and readiness based on a set of agreed-upon metrics. The audit may be conducted by a third party or by an internal audit group and may include a gap analysis that compares an ideal future scenario against the current environment.

Most organizations will not be able to do all of the privacy awareness and readiness assessment steps outlined in this chapter due to resource or time constraints. They are included in this chapter to provide an overview of what should be considered within the context of your organization's needs.

A summary of the phases and key activities of a privacy awareness and readiness assessment is provided in Table 11-2.

Table 11-2. *Summary of the Phases and Activities in a Privacy Awareness and Readiness Assessment*

Phase	Key Activities
Information gathering	• Document existing business processes and data flows. • Document privacy awareness and readiness maturity levels across different organizational functions and across different levels of management. • Assess skills throughout the organization. • Determine how well the organizational structure supports privacy engineering objectives.
Analysis and strategy	• Define a privacy awareness and readiness strategy, including goals and objectives with metrics for success. • Communicate the strategy throughout the organization.
Operational plan	• Develop a privacy awareness and readiness operational plan with a prioritized list of actions and a timeline for execution. • Define the budget needed to execute the privacy awareness and readiness operational plan.
Monitor and adapt	• Ongoing reviews to monitor privacy awareness and readiness can be used to identify additional action items and adapt the program as needed.

Conclusion

This chapter presented a foundation for how to begin to assess the work to build an organizational privacy development structure. We will continue to build on the actual organizational structures in the next chapter.