

# The COMPUTER & INTERNET *Lawyer*

Volume 27 ▲ Number 11 ▲ NOVEMBER 2010

Ronald L. Johnston, Arnold & Porter, LLP Editor-in-Chief\*

## Developing a Comprehensive Written Information Security Program

By Thomas J. Smedinghoff

Implementing legally compliant “reasonable security” requires the development of an appropriate comprehensive information security program.<sup>1</sup> While much has been written about developing an information security program from a technical perspective, this article will focus on the legal requirements.

---

**Thomas J. Smedinghoff** is a partner in the Privacy, Data Security and Information Law Practice at the law firm of Wildman Harrold in Chicago. He is Co-Chair of the Federated Identity Management Legal Task Force of the American Bar Association (ABA) Section of Business Law, and Chair of the International Policy Committee of the ABA Section of Science & Technology Law. He is also the author of *Information Security Law: The Emerging Standard for Corporate Compliance* (IT Governance Publishing, 2008). Mr. Smedinghoff is a member of the US Delegation to the United Nations Commission on International Trade Law (UNCITRAL), where he participated in the negotiation of the United Nations Convention on the Use of Electronic Communications in International Contracts. He can be reached at [smedinghoff@wildman.com](mailto:smedinghoff@wildman.com).

Developing a legally compliant information security program involves an iterative process that requires a company to do the following:

- Identify its information and system assets;
- Conduct periodic risk assessments to:
  1. Identify the specific threats to those assets that the company faces:
    - a. Identify its vulnerabilities to those threats, and
    - b. Estimate the resulting harm if a threat materializes and exploits a vulnerability.
  2. Identify and implement security controls by considering:
    - a. The results of the risk assessment and other relevant factors, and
    - b. The *categories of security controls* identified in applicable laws.
  3. Monitor and test the program to ensure that it is properly implemented and effective;
  4. Continually review and adjust the program in light of ongoing changes; and



5. Oversee third-party service provider arrangements.

The following sections discuss each of those requirements in detail.

## Structure of the Security Program

As a threshold matter, it should be noted that the security program must be in writing. Numerous regulators take the view that, “if the security program is not in writing, it does not exist.” More importantly, however, many laws and regulations expressly require that the security program be in writing.<sup>2</sup>

### Step 1: Identify Information Assets

In order to protect something, you need to know what it is, where it is, how it is used, how valuable it is, and so forth. Thus, when addressing information security, the first step is to identify the information assets to be protected so as to define the scope of the effort. This involves taking an inventory of the data and information that the company creates, collects, receives, uses, processes, stores, and communicates to others. It also requires examining the systems, networks, and processes by which such data is created, collected, received, used, processed, stored, and communicated.

This step requires more than merely identifying data and systems, however. It is also important to understand where the data and systems are located. This means identifying where in the company (*e.g.*, which office and which department), the data, and systems are located and who controls them. It also requires identifying in which jurisdictions (country and state or province) they are collected, processed, and stored, as this will impact which laws require compliance.

As is often the case, little known but sensitive data files are often found in a variety of places within the company. Moreover, it is also important to consider company data that is in the possession and control of a third party, such as an outsource service provider, as the company is responsible for the security of all of its data regardless of who has actual possession of it.

### Step 2: Conduct Risk Assessment

Implementing a comprehensive security program to protect a company’s information assets requires a thorough assessment of the potential risks to the organization’s information systems and data. Thus, once a business has identified the systems and data to be protected, it must undertake a risk assessment process to identify and assess the risks to those systems and data.

Assessing risks requires consideration of threats and vulnerabilities.

- A **threat** is anything that has the potential to cause harm. It can be an act of nature, such as a fire, flood, or tornado, or it can be man-made, such as a computer virus, the actions of a hacker, or the negligent mistake of an employee.
- A **vulnerability** is a flaw or weakness that can be accidentally triggered or intentionally exploited by the threat to endanger or cause harm to an information asset. It might be a hole in the roof, a system with easy-to-guess passwords, unencrypted data on a laptop computer, disgruntled employees, or employees that simply do not understand what steps they need to take to protect the security of company data.

The likelihood that a threat will exploit a vulnerability to cause harm creates a risk. Stated differently, when a threat intersects with a vulnerability, risk is present. For example, if the threat is rain and the vulnerability is a hole in the roof, risk is the likelihood that it will rain, causing water to enter the building through the hole in the roof, and doing damage to the building and/or its contents. Similarly, if the threat is a hacker and the vulnerability is open Internet access to a server containing sensitive data, risk is the likelihood that a hacker will enter the system and view, copy, alter, or destroy the sensitive data.

In other words, **risk** is the likelihood that something bad will happen that causes harm to an information asset. Somewhat more precisely, “Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.”<sup>3</sup>

**Risk assessment**, then, is the process of identifying vulnerabilities and threats to the information assets used by the company and assessing the potential impact/harm that would result if a threat materializes. This forms the basis on which the company determines what countermeasures (*i.e.*, security controls), if any, it should implement to reduce risk to an acceptable level. Thus, a risk assessment requires:

- Conducting a threat assessment to identify all reasonably foreseeable internal and external threats to the information and system assets to be protected;<sup>4</sup>
- Conducting a vulnerability assessment to identify the company’s vulnerabilities;
- Assessing the likelihood that each of the threats will materialize, and if so, the probability that it will

exploit one or more of the vulnerabilities to cause harm—*i.e.*, identifying the likelihood that threat sources with the potential to exploit weaknesses or vulnerabilities in the system will actually do so;

- Evaluating the potential damage that will result in such case; and
- Assessing the sufficiency of the security controls in place to guard against the threat.<sup>5</sup>

This risk assessment process will be the baseline against which security controls can be selected, implemented, measured, and validated. The goal is to understand the risks that the business faces and determine what level of risk is acceptable in order to identify appropriate and cost-effective safeguards to combat that risk.

Traditional negligence law essentially takes the same approach. That is, in assessing what qualifies as reasonable care in a given case, negligence law identifies the relevant factors as: (1) the probability of the identified harm occurring (*i.e.*, the likelihood that a foreseeable threat will materialize), (2) the gravity of the resulting injury if the threat does materialize, and (3) the burden of implementing adequate precautions.<sup>6</sup> In other words, the standard of care to be exercised in any particular case depends upon the circumstances of that case and on the extent of foreseeable danger.<sup>7</sup>

Numerous security laws and regulations expressly require a risk assessment as part of a comprehensive security program. Laws and regulations that do not expressly include such a requirement typically do so impliedly.

In the United States, a risk assessment is expressly required by a variety of statutes and regulations, such as the Graham-Leach-Bliley Act (GLB),<sup>8</sup> the Health Insurance Portability and Accountability Act (HIPAA),<sup>9</sup> and Federal Information Security Management Act of 2002 (FISMA).<sup>10</sup> It is impliedly required by most other security statutes and regulations by imposing an obligation to provide “reasonable” security. Likewise, the consent decrees entered in all Federal Trade Commission (FTC) enforcement actions have expressly extended the banking and healthcare sector-specific requirements for a risk assessment to all industries generally.

In addition, several US courts have held that a risk assessment plays a key role in determining whether a duty will be imposed and liability found. In *Wolfe v. MBNA America Bank*, for example, a bank issued a credit card to an imposter who had stolen the plaintiff’s identity.<sup>11</sup> The court held that the injury to the plaintiff resulting from the bank’s negligent issuance of a credit card was both foreseeable and preventable and that as

a consequence “the defendant has a duty to verify the authenticity and accuracy of a credit account application.” In other words, when a risk assessment would have identified a risk of harm, a company has a duty to defend against it.

Similarly, in *Bell v. Michigan Council*, the court held that when a harm was foreseeable, and the potential severity of the risk was high, the defendant was liable for failure to provide appropriate security to address the potential harm.<sup>12</sup> On the other hand, in *Guin v. Brazos Education*, the court held that, when a proper risk assessment was done but a particular harm was not reasonably foreseeable, the defendant would not be liable for failure to defend against it.<sup>13</sup>

In the European Union and other countries, a risk assessment is almost always a required element of the obligation to provide appropriate data security. Many data protection laws expressly require a risk assessment, including the data protection laws in Iceland, Italy, Norway, and the Slovak Republic.<sup>14</sup> Most such laws, however, impliedly require a risk assessment. They typically do this by requiring that the company provide a level of security “appropriate to the risk.” Countries that take this approach include Albania, Austria, France, Hong Kong, Ireland, Isle of Man, Italy, Jersey, Lithuania, Mauritius, Philippines, Poland, Portugal, Romania, Singapore, Spain, United Arab Emirates, and the United Kingdom.<sup>15</sup>

In most cases, however, the law does not generally specify how to do a risk assessment. In the United States, the banking regulators have referred financial institutions seeking general information on risk assessments<sup>16</sup> to: (1) the “Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards”<sup>17</sup> and (2) the “FFIEC IT Examination Handbook, Information Security Booklet.”<sup>18</sup> The US National Institute of Standards and Technology (NIST) also offers guidance on conducting risk assessments.<sup>19</sup>

### Step 3: Select and Implement Security Controls

The next step in the process of developing a comprehensive information security program is to select and implement appropriate physical, technical, and administrative security controls to manage and control the risks that the company faces.<sup>20</sup> This involves considering the *categories of security controls* identified in the applicable security laws (and any additional categories that are suggested by the risk assessment), in light of the results of the risk assessment and other relevant factors, to select specific security controls that will reduce the company’s risks and vulnerabilities to a reasonable and appropriate level.<sup>21</sup>

## **Factors Affecting Selection of Security Controls**

In determining what specific security measures should be implemented within each of those relevant categories of security controls, virtually all of the existing precedent recognizes that there is no one-size-fits-all approach. Which security measures are appropriate for a particular organization will vary depending on a variety of factors.

The primary factor, and the key to providing legally compliant security, is the requirement that the specific security controls selected and implemented must be responsive to the company's fact-specific risk assessment.<sup>22</sup> In other words, merely implementing seemingly strong security measures is not, by itself, sufficient for legal compliance. Those security controls must be responsive to the particular threats that a business faces and must address its vulnerabilities.

Posting armed guards around a building, for example, sounds impressive as a security measure, but if the primary threat that the company faces is unauthorized remote access to its data via the Internet, that particular security measure is of little value. Likewise, firewalls and intrusion detection software are often effective ways to stop hackers and protect sensitive databases, but if a company's major vulnerability is careless (or malicious) employees who inadvertently (or intentionally) disclose passwords or protected information, then even those sophisticated technical security measures, while important, will not adequately address the problem.

In addition to the risk assessment, the following factors are most often cited in security statutes and regulations as relevant to determining what security controls should be implemented in a given case:

- The company's size, complexity, and capabilities;
- The nature and scope of the business activities;
- The nature and sensitivity of the information to be protected;
- The company's technical infrastructure, hardware, and software security capabilities;
- The state of the art regarding technology and security; and
- The costs of the security measures.<sup>23</sup>

Interestingly, other than a risk assessment, cost is the one factor mentioned most often and certainly implies recognition that companies are not required to do everything theoretically possible.

This point was also stressed by the US banking regulators in their response to questions relating to its regulations for strong authentication. When asked whether a financial institution could forgo a risk assessment and move immediately to implement additional strong authentication controls, the regulators responded with an emphatic "no." As they pointed out, the security requirements for authentication are risk-based, and thus a risk assessment that sufficiently evaluates the risks and identifies the reasons for choosing a particular control should be completed before implementing any particular controls.<sup>24</sup>

The bottom line is that the legal appropriateness of any particular security control is not determined in the abstract. Instead, it must be determined on the basis of a risk assessment specific to the company and its business. Each security control should be appropriate and reasonable from a business perspective in light of the reasonably foreseeable risks.

This means, of course, that the standards for legally appropriate security controls will vary across businesses and applications. It also means that what constitutes legally appropriate security controls may also change over time as new threats arise and better technology is developed to address them. Thus, a single risk assessment is never sufficient. Companies must implement an ongoing process to regularly review threats and technology in order to ensure that appropriate changes are implemented as needed.

## **Categories of Security Controls to Consider**

Most security statutes and regulations do not require companies to implement any specific security measures or use any particular technology. As expressly stated in the HIPAA Security Regulations, for example, companies "may use any security measures" reasonably designed to achieve the objectives specified in the regulations.<sup>25</sup>

Nonetheless, security statutes and regulations seem to consistently require that companies consider certain *categories* of security measures, even if the way in which each category is addressed is not specified. For example, many laws require companies to implement access control measures to ensure that only authorized persons can access sensitive data. But the laws typically say nothing about which access controls should be used. At most, they will sometimes define objectives or criteria that must be achieved (such as restricting access on a need-to-know basis or requiring that access be terminated when an employee leaves the company). Thus (in the example of access controls), companies are free to select any types of access controls that achieve those objectives and are reasonable for the business in light of the results of its risk assessment.

The specific categories of security measures that security statutes and regulations often require companies to consider are listed and discussed below.

#### **Step 4: Monitor and Test the Controls**

Merely implementing appropriate security measures is not sufficient. Companies must also ensure that the security measures have been properly put in place and are effective. One only need look to the security breach involving the TJX Companies—a breach that reportedly involved the compromise of 90 million credit card numbers—to see the need for testing. All of the compromised credit card data in that case was apparently encrypted; a fact that might lead many to assume that it was adequately protected. But the weak nature of the encryption used in that case was apparently easily broken by the hackers.

Thus, conducting an assessment of the sufficiency of the security measures in place to control the identified risks, and conducting regular testing or monitoring of the effectiveness of those measures,<sup>26</sup> is an important component of the legal standard. Existing precedent also suggests that companies must monitor compliance with their security programs. To that end, a regular review of records of system activity, such as audit logs, access reports, and security incident tracking reports,<sup>27</sup> is also important.

#### **Step 5: Review and Adjust the Program**

Perhaps most significantly, the legal standard for information security recognizes that security is a moving target. Businesses must constantly keep up with changing threats, risks, vulnerabilities, and with the security measures available to respond to them. It is a never-ending process. As a consequence, businesses must conduct periodic internal reviews to evaluate and adjust the information security program in light of:

- The results of the testing and monitoring;
- Any material changes to the business or arrangements;
- Any changes in technology;
- Any changes in internal or external threats;
- Any environmental or operational changes; and
- Any other circumstances that may have a material impact.<sup>28</sup>

In addition to periodic internal reviews, best practices and the developing legal standard may require

that businesses obtain a periodic review and assessment (audit) by qualified independent third-party professionals using procedures and standards generally accepted in the profession to certify that the security program meets or exceeds applicable requirements and is operating with sufficient effectiveness to provide reasonable assurances that the security, confidentiality, and integrity of information is protected.<sup>29</sup>

It should then adjust the security program in light of the findings or recommendations that come from such reviews.<sup>30</sup>

#### **Step 6: Oversee Third-Party Service Providers**

Finally, in today's business environment it is important to recognize that companies often rely on third parties, such as outsource providers, to handle much of their data. When corporate data is in the possession and under the control of a third party, this presents special challenges for ensuring security.

Laws and regulations imposing information security obligations on businesses often expressly address requirements with respect to the use of third-party outsource providers.<sup>31</sup> And first and foremost, they make clear that, regardless of who performs the work, the legal obligation to provide the security itself remains with the company. As it is often said, "you can outsource the work, but not the responsibility." Thus, third-party relationships should be subject to the same risk management, security, privacy, and other protection policies that would be expected if a business were conducting the activities directly.<sup>32</sup>

Generally, the developing legal standard for security imposes three basic requirements on businesses that outsource: (1) they must exercise due diligence in selecting service providers,<sup>33</sup> (2) they must contractually require outsource providers to implement appropriate security measures,<sup>34</sup> and (3) they must monitor the performance of the outsource providers.<sup>35</sup>

#### **Security Controls to Consider**

Set forth below is a list and explanation of the *categories* of security controls most often cited in security laws and regulations. No single law or regulation expressly requires that all of these controls be addressed, but when all of the security laws and regulations are viewed as a group, the categories of controls identified here emerge as the set most likely to be required for global legal compliance.

Moreover, given the process-oriented nature of the legal standard for security, there is a good possibility that a requirement to at least consider many of these controls will be read into security laws and regulations that do not expressly identify them. Thus, if some of these

# Security

---

categories of controls are not addressed by a company's security program, a court or regulator may well conclude that the company has not satisfied its obligation to implement "reasonable" or "appropriate" security under the applicable law.

It is important to stress, however, that while the law will likely require that a company's security program address the controls listed here (even if they are not expressly mentioned in the applicable law or regulation), the law does not typically specify how that must be done. Moreover, if the company "considers" a security control but finds it to be unnecessary in light of its own risk assessment, that may well be sufficient, so long as the fact that the control was considered, and the reasons for not adopting it, are adequately documented.

Even when a particular control category is deemed to be relevant, the manner in which it is addressed, and the approach or technology used, is typically up to the company. The law does not require companies to implement security controls in a particular way or use a particular technology. As expressly stated in the HIPAA security regulations, for example, companies "may use any security measures" reasonably designed to achieve the objectives specified in the regulations.<sup>36</sup>

The organization of the categories of security controls listed below is subject to many different approaches. Thus, some of the labels used here may not be used in other listings, or certain controls may be grouped under different headings. With respect to each control, a footnote reference to the description of the control category in applicable ISO<sup>37</sup> and NIST standards is also included.

## Physical Security Controls

### Facility and Equipment

Security regulations frequently require companies to protect the security of their facility, their physical equipment comprising the information system, and the physical media on which their information is stored against destruction, loss, or damage.<sup>38</sup> Such physical and environmental security controls typically fall into three general categories: physical access restrictions, protections against technological failures, and protections against environmental threats.<sup>39</sup>

Physical access controls are common. Security laws and regulations frequently require that the company implement security measures and procedures to prevent unauthorized persons from gaining physical access to the buildings, computer facilities, and records storage facilities containing the equipment and the media.<sup>40</sup> This includes restricting physical access to the premises where the information systems used for processing

personal data are located<sup>41</sup> and restricting physical access to the data processing equipment used for storing, accessing, and processing the data.<sup>42</sup> It may also include controlling physical access to system devices that display information to prevent unauthorized individuals from observing the display output, such as procedures that govern the use and security of physical workstations.<sup>43</sup>

Controls to protect against technological failures are often important. This may include, for example, requirements to implement controls such as providing short-term uninterruptible power supply for emergency power, automatic emergency lighting systems, and temperature and humidity controls.<sup>44</sup> Requirements to protect equipment and media from water damage resulting from broken plumbing lines and other sources of water leakage may also be included.<sup>45</sup>

Environmental controls are also important. This includes, for example, controls to protect against environmental incidents, such as deploying fire suppression and detection systems.<sup>46</sup>

### Media

Media protection security controls are often necessary to ensure that security is not compromised through the improper handling of storage media. Thus, security laws and regulations may require companies to implement security controls to prevent data media from being read, copied, altered, or removed by unauthorized persons.<sup>47</sup> Security controls relevant here include the following:<sup>48</sup>

- **Media access:** ensuring that only authorized users have access to information in printed form or on digital media.
- **Media storage:** securely storing removable media in a manner designed to prevent unauthorized access and processing.<sup>49</sup>
- **Media transport:** ensuring that devices and media that are taken outside of the premises are secured in a manner that guarantees the confidentiality and integrity of the data<sup>50</sup> and ensuring that all media accessible to repair personnel have all data removed in a way making the recovery of the data impossible or are repaired under appropriate supervision.<sup>51</sup>
- **Media destruction and disposal:** ensuring that the deletion/destruction of the data and/or the media on which it resides is secure (*i.e.*, to ensure that the data cannot be recreated)<sup>52</sup> and procedures for removal from media before re-use of the media;<sup>53</sup>

The issue of media destruction and disposal has been the subject of several new laws and regulations. These laws typically do not require the destruction of data, but seek to regulate the manner of destruction when companies decide to do so. They require companies to properly dispose of personal information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

With respect to information in paper form, this typically requires implementing policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that the information cannot be read or reconstructed. With respect to electronic information, such regulations typically require implementing policies and procedures that mandate the destruction or erasure of electronic media containing consumer personal information so that the information cannot practicably be read or reconstructed.<sup>54</sup>

In the United States, both the banking regulators and the securities regulators have adopted rules regarding security requirements for the destruction of personal data. Similarly, at the state level, many states have adopted analogous requirements. Several other countries also have adopted requirements to destroy removable media containing personal data no longer used or alternatively to render personal data on such removable media unintelligible and not capable of reconstruction by any technical means before re-use of such removable media is allowed.<sup>55</sup>

## Technical Security Controls

### Access Controls

Access controls include security measures to (1) prevent unauthorized persons from gaining access to systems and data and (2) appropriately limit and control the scope of access granted to any authorized person.<sup>56</sup>

Numerous laws and regulations require companies to implement security measures and procedures to control access to their information systems and data.<sup>57</sup> This includes procedures to determine who is authorized to access the system;<sup>58</sup> procedures for granting and controlling access to the system in accordance with applicable policy;<sup>59</sup> such as authentication procedures (*e.g.*, user ID and passwords); procedures for regularly verifying that the relevant authorization profiles still apply;<sup>60</sup> and procedures for terminating access when it is no longer authorized (*e.g.*, a person's employment has terminated or role within the company has changed).<sup>61</sup>

Other laws impose requirements that data cannot be read, copied, modified, or removed without

authorization<sup>62</sup> and that measures be taken to prevent unauthorized persons from gaining access to the information systems when personal data are processed or used.<sup>63</sup>

Regulations often require companies to implement security measures and procedures to establish an appropriate level of authorization for persons entitled to access the personal data. This includes measures and procedures to ensure that personnel will have access only to the data and resources that they need to know to perform their duties and only to the data within the scope and to the extent covered by their respective access permission.<sup>64</sup> Procedures to prevent information systems from being used without (or in excess of) authorization are also required in some cases.<sup>65</sup>

Some regulations also address the authorization process itself. Specifically, they require that the company ensure that only authorized personnel may (1) create, modify, or cancel the rights of access of other employees, agents, and contractors and (2) access the hardware and computer components where the authorization databases are processed.<sup>66</sup>

### Identification and Authentication

Controlling access to systems and data requires determining whether a person (or device) seeking access is someone previously authorized to have access. This requires properly authenticating the identity of persons and devices seeking access to verify that they are authorized. Thus, it is important to implement appropriate identity management security procedures to identify those persons and devices authorized to access the system and its data and to authenticate the identity of persons and devices claiming to have such authorization when seeking online access.<sup>67</sup>

Such a requirement is expressly addressed, for example, in most US information security laws and regulations, including HIPAA, GLB, the Homeland Security Act,<sup>68</sup> Food and Drug Administration regulations,<sup>69</sup> and state information security laws.<sup>70</sup> Likewise, in April 2007 the Federal Communications Commission (FCC) issued an order that imposes specific authentication requirements on telephone and wireless carriers to protect personal telephone records from unauthorized disclosure.<sup>71</sup> Numerous laws in other countries impose similar requirements.<sup>72</sup> In a recent case involving identity theft, a court found that there was a common law duty to authenticate the identity of a person submitting a credit card application.<sup>73</sup>

In all cases, the key issue is not whether authentication is required, but rather, what form of authentication is legally appropriate. Security laws and regulations take varying approaches.

## **System and Services Acquisition Controls**

Acquisition of new systems and/or software for internal use, as well as acquisition of outsourced services that will access or process company data presents significant security risks.<sup>74</sup> Accordingly, security laws and regulations often require a company to adopt appropriate security policies and procedures to address system and services acquisition. Such controls should include the following:

- For internal system acquisitions, this should include (1) imposing appropriate security requirements and/or security specifications in information system acquisition contracts, (2) properly designing and implementing information systems using appropriate security engineering principles, and (3) properly testing and evaluating the security characteristics of such systems.
- For outsourced services, most security regulations require companies to ensure that the third-party providers of information system services employ adequate security controls in accordance with applicable laws and to monitor compliance.

## **System Configuration and Change Management Controls**

Configuration controls address the security of the configuration of the various hardware and software components comprising the information system on which the data is used or stored.<sup>75</sup> This generally has two high-level components.

First, the company should identify and maintain records on the devices and software that comprises its information system<sup>76</sup> and verify that the system and software configuration are appropriate from a security perspective.

Second, it should establish procedures to control any changes to the configuration to ensure that system modifications are consistent with the company's security program.<sup>77</sup> This includes, for example, protecting personal data in the event of changes to, movement of, or replacement of any hardware, computer component, software, or information related to the processing of personal data.<sup>78</sup>

## **System and Information Integrity**

It is important to implement appropriate security controls to protect the integrity of the system and the information that it contains. Such controls generally include checking data input validity and accuracy, data error handling, malicious code protection, intrusion detection tools, and procedures to verify software integrity.<sup>79</sup>

Various security regulations expressly require controls to address system and data integrity, including the following:

- **System integrity:** Software integrity procedures to detect and protect against unauthorized changes to software and to ensure that system modifications are consistent with the company's security program.<sup>80</sup>
- **Data integrity:** Procedures and measures to protect information from unauthorized access, alteration, disclosure, or destruction during storage;<sup>81</sup> to ensure data integrity;<sup>82</sup> and to prevent the unauthorized or erroneous recording, alteration or erasure of personal data.<sup>83</sup>
- **Malicious code protection:** Procedures for preventing, detecting, and reporting malicious software<sup>84</sup> and protecting the data against the effects of viruses, Trojan horses, worms, and other forms of malware.<sup>85</sup>
- **Intrusion detection:** Tools, techniques, and procedures to monitor log-in attempts and report discrepancies;<sup>86</sup> measures to detect actual and attempted attacks on or intrusions into company information systems;<sup>87</sup> and provide identification of unauthorized users. Ensure that personal data is protected against the risk of intrusion,<sup>88</sup> including by the installation of physical or logic-based safety systems providing protection against unauthorized access.<sup>89</sup> This might include, for example, limiting the number of unsuccessful attempts that are made to enter the information system or access the personal data.<sup>90</sup>

## **Data Communications Protection**

It is important to implement appropriate controls to protect the confidentiality and integrity of data in the process of transfer or transmission.<sup>91</sup> This applies both to the transfer of data via hardware devices, such as laptops and USB drives, as well as to the transmission of data electronically, such as via the Internet.

This requirement is raised in several regulations, which address this concern in a variety of ways.<sup>92</sup> Perhaps the most common approach is to require procedures designed to ensure that the data cannot be read, copied, modified, disclosed, deleted, or otherwise unlawfully processed by unauthorized persons before it is allowed to leave the company.<sup>93</sup> Some regulations focus on laptops and require special precautions when transporting, storing, and using the equipment outside of the company premises, including such measures as encryption of the processed personal data.<sup>94</sup> Others

focus on Internet communications, and require encryption of such communications.<sup>95</sup>

Some regulations also focus on requirements for procedures that ensure that no personal data is moved outside the premises without authorization of the company.<sup>96</sup> Others focus on the use of methods by which it is possible to check and establish when and to whom sensitive data is transferred by means of data transmission facilities.<sup>97</sup>

## **Maintenance**

System hardware and software maintenance requirements raise a variety of information security concerns.<sup>98</sup> They generally fall into two general categories.

First, system maintenance is critical to ensure that the software is kept up-to-date so that others are not able to exploit newly-discovered vulnerabilities. In particular, this often requires procedures to identify, report, and correct information system flaws and potential vulnerability resulting from those flaws such as by ensuring that newly released software security patches are identified, tested, and promptly installed.

Thus some regulations expressly require that the company implement security measures and procedures for the regular updating and patching of computer programs to eliminate vulnerabilities and remove flaws that could otherwise facilitate security breaches.<sup>99</sup> In one US case, failure to promptly install security patches resulted in liability for a telecommunications company.<sup>100</sup>

Second, it is important that appropriate policies and procedures be in place to ensure that the process of doing hardware and software maintenance does not compromise security. For example, when it is necessary to remove system components or storage media from the facility for repair, the company should have procedures in place to ensure that the receipt and removal of hardware and electronic media into and out of a facility does not compromise security.<sup>101</sup> This might include removing all information from media before it leaves the premises and checking hardware and software security features after maintenance is performed to ensure that they are still functioning properly.<sup>102</sup>

Likewise, when maintenance is conducted remotely, the company should approve, control, and monitor remotely such activities to ensure that security is not compromised in the process. And of course, only authorized personnel should be allowed to perform such maintenance.

## **System Activity Monitoring and Audit Records**

Information system and database events should be monitored and audit logs and accountability records should be maintained in order to track system use and

activity to assist in the detection and investigation of potential security issues.<sup>103</sup> This includes implementing security measures and procedures for monitoring access to sensitive data and for monitoring additions to, and alterations, deletions, and copying of, such data. Some regulations require, for example, that it be possible to determine when, by whom, and which personal data were recorded, altered, or erased.<sup>104</sup>

Based on its risk assessment, the company should decide which system events require auditing on a continuous basis and which events require auditing in response to specific situations. Companies should also consider the content of audit records, audit processing and storage procedures, audit monitoring, analysis, and reporting procedures, the protection of audit information, the retention of audit information, and establishing the auditing process in a manner such that it supports non-repudiation.<sup>105</sup>

For example, some regulations require monitoring of access to PCs, workstations, or other units, indicating the specific equipment or machine accessing the information system or personal data, the date and time of access, the name of the user, the number of concurrent users, the kind of access, the files accessed and kind of information processed, which personal data were recorded, copied, altered, or erased, transmissions of data and name of the recipient, and acceptance or rejection of such access by the information system or personal data.<sup>106</sup>

## **Administrative Security Controls**

### **Personnel Security**

Personnel security controls are designed to address risks associated with individuals.<sup>107</sup> Thus, these controls apply not only to employees but also to third-party personnel employed by contractors, technology service providers, and outsourced application providers. The focus is on the risks presented by persons who are not properly trained or qualified for the job, persons who may be dishonest, and persons who may be otherwise motivated to do inappropriate or destructive acts.

To address these concerns, security laws and regulations frequently require companies to verify that their employees, agents, and contractors have the technical expertise and personal integrity required for their position<sup>108</sup> and take steps to ensure the reliability of employees who have access to the information system or sensitive corporate data.<sup>109</sup> They may also require the screening of individuals requiring access to information to ensure that granting them access is appropriate, including, when appropriate, requiring background checks for employees with access to sensitive information.<sup>110</sup>

Security regulations may require clearly specifying the obligations of all employees, agents, and contractors entrusted with access to sensitive data.<sup>111</sup> They may also focus on work process, recommending consideration of dual control procedures, segregation of duties, and other personnel management procedures for employees with responsibility for or access to information to be protected.<sup>112</sup> Some regulations require appropriate supervision of workforce members who work with sensitive information or in locations where it might be accessed.<sup>113</sup> Controls to prevent employees from providing information to unauthorized individuals who may seek to obtain this information through fraudulent means are also important.<sup>114</sup>

Sanctions are an important part of personnel controls as well. Thus, some regulations expressly require that companies employ a formal sanctions process for personnel failing to comply with established security policies and procedures.<sup>115</sup>

Policies relating to personnel termination are also a critical component. Personnel security controls must address issues such as prompt termination of system access, exit interviews, insuring the return of all company property, (*e.g.*, keys, ID cards, building passes), and ensuring that appropriate personnel have access to official records created by the terminated employee that are stored on information systems.<sup>116</sup>

## **Employee Awareness and Training**

Training and education for employees is a critical component of any security program. It is the primary vehicle for disseminating security information that employees need to do their jobs and for providing them with the information and tools needed to protect the company's vital information resources.

Numerous audit reports, studies, and surveys confirm that people are often the weakest link in the security chain. Even the very best physical, technical, and administrative security measures are of little value if employees do not understand their roles and responsibilities with respect to security. For example, installing heavy duty doors with state-of-the-art locks (whether of the physical or virtual variety) will not provide the intended protection if the employees authorized to have access leave the doors open and unlocked for unauthorized persons to pass through.

Thus, the legal standard for reasonable security mandates appropriate security awareness training and education for employees.<sup>117</sup> The goal is to ensure that all employees, agents, and contractors are aware of and comply with the relevant security measures implemented by the company to protect the data. A good example is the regulations issued under the US Computer Security Act,

which require federal agencies to provide mandatory periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of a federal agency.<sup>118</sup>

Employee security awareness and training is, in many cases, the only security control that can minimize the inherent risk that results from the people who use, manage, operate, and maintain information systems and networks. Thus, security education should be provided for all employees who are involved with the management, use, or operation of a computer system or who access information contained therein. This includes contractors as well as employees of the company.

Security education<sup>119</sup> begins with communication to employees of applicable security policies, procedures, standards, and guidelines, as well as the requirements of the laws applicable to their activities and the data with which they will be working.<sup>120</sup> It also includes periodic training in computer security awareness and accepted computer security practices,<sup>121</sup> periodic security reminders, and developing and maintaining relevant employee training materials, such as user education concerning virus protection, password management, and how to report discrepancies.

Each user should be versed in acceptable rules of behavior for the application before being allowed access to the system. Training should also inform the user on how to get help when having difficulty in using the system and procedures for reporting security incidents.

## **Contingency Planning: Backup and Disaster Recovery**

Security laws and regulations often require that the company develop and implement a contingency plan for the information system and data.<sup>122</sup> Such a plan should be designed to ensure that the company is able to continue operations and that the data will be available in the event of an emergency. This includes not only environmental emergencies, such as fire, flood, hurricane, and earthquake, but also other potential threats, such as equipment failure, denial-of-service attacks, or sabotage.

Such a contingency plan<sup>123</sup> should include system and data backup procedures and a recovery plan that specifies the procedures to be followed in case of emergencies, such as fire, vandalism, system failure, and natural disasters.<sup>124</sup> This often requires providing alternate secure storage site(s) to permit the storage of back-up information; alternate processing site(s) to facilitate the resumption of system operations for critical functions; alternate telecommunications services to support the

information system; and entering into necessary agreements to establish the foregoing.<sup>125</sup> Back-up and retention procedures should also ensure that regular back-up copies are made and properly stored and that they are properly deleted immediately after they cease to be of any use.<sup>126</sup>

It should also provide for appropriate mechanisms to allow the information system and the data to be recovered and reconstituted to its original state after disruption, failure, destruction, or damage.<sup>127</sup>

The plan should also designate appropriate personnel and specify their roles, responsibilities, and activities associated with restoring the system after a disruption or a failure. Training for designated personnel in their contingency roles and responsibilities with respect to the information system is critical.

Testing of the contingency plan on a regular basis to determine its effectiveness and the company's readiness to execute the plan is also important and often required by security regulations.<sup>128</sup> Likewise, regulations often require that the plan be reviewed on a regular basis and revised as necessary to address system or organizational changes or problems encountered during plan implementation, execution, or testing.<sup>129</sup>

## **Incident Response Plan**

In addition to contingency planning, security laws often require companies to develop and implement incident response policies and procedures.<sup>130</sup> The goal is to provide a plan for taking responsive action (including notification, management, and response procedures) in the event that the company suspects or detects that a security breach has occurred.<sup>131</sup> Such incident response policies and procedures typically address the following:<sup>132</sup>

- Incident reporting: procedures to ensure that appropriate persons within the organization are promptly notified of security breaches and that (when appropriate) external authorities are notified as well.
- Incident handling and response: procedures to ensure that prompt action is taken to respond to the breach, including detection and analysis of the breach, containment of the breach to stop further information compromise, eradication of the problem, recovery procedures, and procedures for working with outside experts and law enforcement when appropriate.
- Incident monitoring and recordkeeping: procedures to track and document each security incident on an ongoing basis and to create appropriate records that include date and time of the incident, nature of the

incident, impact of the incident, persons involved in responding to the incident, and procedures followed to resolve the incident.<sup>133</sup>

- Incident response assistance: policies for obtaining both inside and outside support and assistance for the handling and reporting of security incidents and policies for notifying appropriate persons who may be potentially injured by the breach.
- Training: appropriate training for relevant personnel in their incident response roles and responsibilities.
- Testing: periodic testing of the incident response plan to determine its effectiveness and document the results.

## **Special Rules for Specific Data Elements**

Some security statutes and regulations are also beginning to focus on specific data elements and imposing specific obligations with respect to such data elements. Prime examples include so-called sensitive personal data, Social Security numbers, and credit card transaction data.

## **Sensitive Data**

From its inception, the EU Data Protection Directive has required special treatment for particularly sensitive personal information. Specifically, the Directive prohibits "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life," unless certain exceptions apply.<sup>134</sup> Those exceptions include "explicit consent" by the data subject and carrying out obligations under applicable employment laws.

But even with consent, processing such sensitive data, according to EU interpretation, requires that "special attention" be given to data security aspects to avoid risks of unauthorized disclosure. In particular, "[a]ccess by unauthorized persons must be virtually impossible and prevented."<sup>135</sup> To that end, some EU country laws require that sensitive data be encrypted, logically separated from other data, or protected by other technical means that make such data illegible to any unauthorized third party.<sup>136</sup>

In the United States, a *de facto* category of sensitive information has been defined by the various state security breach notification laws. These laws require special action (*i.e.*, disclosure) in the event of a breach of security with respect to a subcategory of personal data generally considered to be sensitive because of its potential role in facilitating identity theft.

## Social Security Numbers

Separately, in the US the security of Social Security numbers has also been the focus of numerous state laws enacted during the past few years. The scope of these laws ranges from restrictions on the manner in which Social Security numbers can be used to express requirements for security with respect to the communication and/or storage of Social Security numbers. For example, several states have enacted laws that prohibit requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the individual's Social Security number is encrypted. The law in Maryland and Nevada goes further and prohibits initiating any transmission of an individual's Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.<sup>137</sup>

The bottom line is that if a company wants to continue collecting, maintaining, and transferring data with SSNs, it will have to provide special treatment for the protection of that data (at least for the SSN number portion), such as encryption, using secure communications media, controlling access, and adopting special security policies.

## Credit Card Data

For businesses that accept credit card transactions, the Payment Card Industry Data Security Standard (PCI Standard)<sup>138</sup> imposes significant security obligations with respect to credit card data captured as part of any credit card transaction. And at least two states (Minnesota and Nevada) have also enacted laws imposing specific security obligations with respect to credit card data.<sup>139</sup>

## Notes

1. Mass. Regulations 201 CMR 17.03(1).
2. In the US, *see, e.g.*, Mass. Regulations 201 CMR 17.032(1); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A; HIPAA Security Regulations, 45 C.F.R. § 164.316(b)(1); Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(b). In other countries, *see, e.g.*, Argentina Regulations of the National Bureau for the Protection of Personal Data; Austria Act, Article 14(2)(8); EU Directive, Article 17(4); Iceland Rules, Article 3; Italy Act, § 34(1); Liechtenstein Ordinance, Article 12; Lithuania Act, Article 24; Netherlands Act, Article 14(5); Norway Act, § 13; Philippines Act, § 8.1; Poland Act, Article 36; Portugal Act, Article 14(4); Slovenia Act, Article 25(2); Spain Royal Decree 1720/2007, Article 88.
3. National Institute of Security and Technology (NIST) Special Publication 800-30, *Risk Management Guide for Information Technology Systems* (July 2002) at p.8.
4. *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(1); Mass. Regulations 17 CMR 17.03(2)(b).
5. *See, e.g.*, FISMA, 44 U.S.C. §§ 3544(a)(2)(A) and 3544(b)(1); GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(2); Mass. Regulations 201 CMR 17.03(2)(b).
6. *See, e.g.*, *United States v. Carroll Towing*, 159 F.2d 169, 173 (2d Cir. 1947).
7. *See, e.g.*, *DCR Inc. v. Peak Alarm Co.*, 663 P.2d 433, 435 (Utah 1983); *see also Glatt v. Feist*, 156 N.W.2d 819, 829 (N.D. 1968) (the amount or degree of diligence necessary to constitute ordinary care varies with facts and circumstances of each case).
8. Also known as the Financial Services Modernization Act of 1999, 15 U.S.C. § 6801, *et. seq.* (1999).
9. 42 U.S.C. § 201, *et. seq.* (1996).
10. 44 U.S.C. § 3541, *et. seq.* (2002).
11. *Wolfé v. MBNA America Bank*, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007).
12. *See Bell v. Michigan Council*, 2005 Mich. App. LEXIS 353 (Mich. App. 15 Feb. 2005).
13. *See Guin v. Brazos Higher Education Service*, Civ. No. 05-668, 2006 U.S. Dist. LEXIS 4846 at \*13 (D. Minn. Feb. 7, 2006) (finding that when a proper risk assessment was done, the inability to foresee and deter a specific burglary of a laptop was not a breach of a duty of reasonable care).
14. *See Iceland law*, Article 11; *Italy law*, Annex B, § 19.3; *Norway regulations*, § 2-4; and *Slovak Republic law*, § 16.5.
15. *See, e.g.*, *Albania law* Article 9, *Austria law* § 14(2).8, *EU Data Protection Directive* Article 17(1), *France law* Article 34, *Hong Kong law* Principle 4, *Ireland law* § 2C.-(1), *Isle of Man law* Schedule 1, *Italy law* § 32(1), *Jersey law* Seventh Principle, *Lithuania law* Article 24, *Mauritius law* § 27(1), *Philippines law* Article 8.1, *Poland law* Article 36, *Portugal law* Article 14(1), *Romania law* Article 20(2), *Singapore Model Code* Principle 7, 4.7.2, *Spain law* Article 9, *United Arab Emirates law* Articles 15(2) and 16(2), and the *United Kingdom law* Seventh Principle.
16. FFIEC (an abbreviation for Federal Financial Institutions Examination Council), *Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment*, August 8, 2006 at p.5, available at [www.ffiec.gov/pdf/authentication\\_faq.pdf](http://www.ffiec.gov/pdf/authentication_faq.pdf).
17. *Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards*, Dec. 14, 2005, available at [www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/default.htm](http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/default.htm).
18. FFIEC, *IT Examination Handbook, Information Security Booklet*, July 2006, available at [www.ffiec.gov/ffiecinfobase/booklets/information\\_security/information\\_security.pdf](http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf).
19. *See NIST Special Publication No. 800-30*, "Risk Management Guide for Information Technology Systems," available at <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

20. *See, e.g.*, US, GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.A; HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(1)(ii)(B); FISMA, 44 U.S.C. § 3544(b); Mass. Regulations 201 CMR 17.03(1); Belgium Act, Art. 16(4); Denmark Act, Section 41(3); Estonia Act, § 19(1); EU Data Protection Directive, Article 17(1); Finland Act, § 32(1); German Act, § 9; Greece Act, Article 10(3); Hungary Act, Article 10(1); Lithuania Act, Article 24(1); Netherlands Act, Article 13; Philippines Act, Article 8.1; Portugal Act, Article 14(1); Russia Act, § 19(1); Slovakia Act, § 15(1); Spain Act, Article 9; Sweden Act, § 31; United Arab Emirates Act, Articles 15(1) and 16(1); UK Act, Schedule 1, Part I, Seventh Principle.
21. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(1)(ii)(B).
22. Mass. Regulations 201 CMR § 17.03(2)(b).
23. *See, e.g.*, US, HIPAA Security Regulations, 45 C.F.R. § 164.306(b)(2); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A and Part II.C; FISMA, 44 U.S.C. §§ 3544(a)(2) and 3544(b)(2)(B); Mass. Regulations 201 CMR 17.03(1); Finland Act, § 32(1); Ireland Act, § 2C.-(1); Netherlands Act, Article 13; Portugal Act, Article 14(1); Sweden Act, § 31; United Arab Emirates Act, §§ 15(2) and 16(2).
24. *See* FFIEC, “Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment,” Aug. 8, 2006, at p.5, available at [http://www.ncua.gov/letters/2006/CU/06-CU-13\\_encl.pdf](http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf).
25. HIPAA Security Regulations, 45 C.F.R. § 164.306(b)(1).
26. FISMA, 44 U.S.C. § 3544(b)(5); Eli Lilly Decision at II.C; GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III(c)(3); Mass. Regulations 201 CMR 17.03(h).
27. HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(1)(ii)(D).
28. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.E; HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(8); Microsoft Consent Decree at II, p.4; Eli Lilly Decision at II.D.
29. Microsoft Consent Decree at III, p.5.
30. Ziff Davis Assurance of Discontinuance, Para. 27(h), p.7.
31. *See, e.g.*, US, GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(2); HIPAA Security Regulations, 45 C.F.R. § 164.308(b)(1) and 164.314(a)(2); Mass. Regulations 201 CMR 17.03(f); Belgium Act, Article 16(1); Denmark Act, Article 42(2); ED Data Protection Directive, Article 17; France Act, Article 38; Japan Act, Article 22; Netherlands Act, Article 14; Philippines Act, § 8; Spain Act, Article 12; United Arab Emirates Act, Articles 15(3) and 16(3).
32. *See, e.g.*, Office of the Comptroller of the Currency, Administrator of National Banks, OCC Bulletin 2001-47 on Third Party Relationships, Nov. 21, 2001 (available at [www.OCC.treas.gov/ftp/bulletin/2001-47.doc](http://www.OCC.treas.gov/ftp/bulletin/2001-47.doc)).
33. *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(1); Mass. Regulations 201 CMR 17.03(f)(1).
34. *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(2); HIPAA Security Regulations, 45 C.F.R. Sections 164.308(b)(1) and 164.314(a)(2); Mass. Regulations 201 CMR 17.03(f)(2).
35. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(3).
36. HIPAA Security Regulations, 45 C.F.R. § 164.306(b)(1).
37. International Organization for Standardization (ISO).
38. HIPAA Security Regulations, 45 C.F.R. § 164.310.
39. *See, e.g.*, ISO 27002, § 9 (“Physical and Environmental Security”) at pp.29–36; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.76–81 (“Physical and Environment Protection”).
40. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; HIPAA Security Regulations, 45 C.F.R. § 164.310(a); Mass. Regulations 201 CMR 17.03(g).
41. Mass. Regulations 201 CMR 17.03(g); Italy Act, Annex B, § 19.4; Poland Ordinance, Attachment A (Basic Security Measures) § I.1; Portugal Act, Article 15(1)(a).
42. Mass. Regulations 201 CMR 17.03(g); Estonia Act, § 19(2); Italy Act, Annex B, § 19.4.
43. HIPAA Security Regulations, 45 C.F.R. Sections 164.310(b) and (c).
44. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C. [technological failures].
45. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.
46. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.
47. Estonia Act, § 19(2); Portugal Act, Article 15(1)(b).
48. *See, e.g.*, ISO 27002, § 10.7 (“Media Handling”) at pp.46–48; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.73–75 (“Media Protection”).
49. Italy Act, Annex B, § 21.
50. HIPAA Security Regulations, 45 C.F.R. § 164.310(d); Mass. Regulations 17.03(c); Poland Ordinance, Attachment Part B (Medium Security Measures), § IX.
51. Poland Ordinance, Attachment A (Basic Security Measures) § VI.
52. HIPAA Security Regulations, 45 C.F.R. § 164.310(d)(2)(i).
53. HIPAA Security Regulations, 45 C.F.R. § 164.310(d)(2)(ii).
54. *See, e.g.*, 16 C.F.R. § 682.3.
55. *See, e.g.*, Italy Act, Annex B, § 22; Poland Ordinance, Attachment A (Basic Security Measures) § VI.
56. *See, e.g.*, ISO 27002, § 11 (“Access Control”) at pp.60–76; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.40–47 (“Access Control”).
57. *See, e.g.*, Mass. Regulations 201 CMR 17.03(c), 17.04(1), (2); Estonia Act, § 19(2)(2); Poland Ordinance, Attachment A (Basic Security Measures) § II.1.
58. HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(3)(ii); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Mass. Regulations 201 CMR 17.03(c), 17.04(1), (2).

59. HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(4) and § 164.312(a).
60. Italy Act, Annex B, § 14.
61. HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(3)(ii)(C); Mass. Regulations 201 CMR 17.04(1), (2).
62. *See, e.g.*, German Federal Data Protection Act, Annex (to the first sentence of § 9 of this Act), § 3; Poland Ordinance, Attachment A (Basic Security Measures) § II.1.
63. *See, e.g.*, German Federal Data Protection Act, Annex (to the first sentence of § 9 of this Act), § 1; Italy Act, § 34(e) and Annex B, §§ 1-13; Portugal Act, Article 15(1)(d).
64. Belgium Act, Art. 16(2)(2); Estonia Act, §§ 19(2)(2) and 19(2)(4); German Federal Data Protection Act, Annex (to the first sentence of § 9 of this Act), § 1; Italy Act, § 34(c) and Annex B, §§ 12 and 13; Poland Ordinance, Section § 5.1; Slovakia Act, § 16(6)(b) and (c); Spain Royal Decree 1720/2007, Article 91 (Basic-level security measures).
65. Mass. Regulations 201 CMR 17.04(4); German Federal Data Protection Act, Annex (to the first sentence of § 9 of this Act), § 2; Italy Act, § 34 and Annex B, §§ 1-13; Portugal Act, Article 15(1)(e); Spain Royal Decree 1720/2007, Article 91 (Basic-level security measures).
66. Spain Royal Decree 1720/2007, Articles 91 and 99 (Basic-level and medium-level security measures).
67. *See, e.g.*, ISO 27002, § 11 (“Access Control”) at pp.60-76; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.65-67 (“Identification and Authentication”).
68. Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(D), and § 301(b)(1) amending 44 U.S.C. § 3542(b)(1) (“‘information security’ means protecting information and information systems from unauthorized access, . . .”).
69. Food and Drug Administration regulations, 21 C.F.R. Part 11.
70. *See, e.g.*, Cal. Civil Code § 1798.81.5(b); Mass. Regulations 201 CMR 17.04(1).
71. *See* FCC Order re Pretexting, 2—In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, Apr. 2, 2007, at ¶¶ 13-25; available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-07-22A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf) (hereinafter FCC Pretexting Order).
72. *See, e.g.*, Italy Act, § 34(a) and (b) and Annex B, §§ 1-13; Poland Ordinance, § 5.2 and Attachment A (Basic Security Measures) § II.2; and Spain Royal Decree 1720/2007, Articles 93 and 98 (Basic-level and medium-level security measures).
73. *Wolfe v. MBNA America Bank*, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007).
74. *See, e.g.*, ISO 27002, § 12 (“Information Systems Acquisition, Development and Maintenance”) at pp.77-89; ISO 27002, § 10.2 (“Third Party Service Delivery Management”) at pp.39-40; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.89-92 (“System and Services Acquisition”).
75. *See, e.g.*, ISO 27002, § 10.1.2 (“Change Management”) at p.37; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.57-59 (“Configuration Management”).
76. Estonia Act, § 19(3).
77. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.
78. Spain Royal Decree 1720/2007, Articles 91, 92, 94, and 101 (Basic-level and high-level security measures).
79. *See, e.g.*, ISO 27002, § 10.4 (“Protection Against Malicious and Mobile Code”) at pp.42-43; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.100-104 (“System and Information Integrity”).
80. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Ziff Davis Assurance of Discontinuance, Para. 25, p.6.
81. *See, e.g.*, US GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; HIPAA Security Regulations, 45 C.F.R. §§ 164.312(c) and (e); Estonia Act, § 19(2)(3); Portugal Act, Article 15(1)(c).
82. Estonia Act, § 19(1); Italy Act, Annex B, § 19.4.
83. Estonia Act, § 19(2)(3).
84. HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(5)(ii)(B); Mass. Regulations 201 CMR 17.04(6), (7).
85. Italy Act, Annex B, § 16; Poland Ordinance, § 5.6 and Attachment A (Basic Security Measures) § III.1.
86. Mass. Regulations 201 CMR 17.04(1)(e); HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(5)(ii)(C).
87. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Ziff Davis Assurance of Discontinuance, ¶ 24(d), p.5 and ¶ 25, p.6.
88. Mass. Regulations 201 CMR 17.04(6); Italy Act, Annex B, §§ 16 and 20.
89. Poland Ordinance, Attachment Part C (High Security Measures), § XII.
90. Mass. Regulations 201 CMR 17.04(1)(e); Spain Royal Decree 1720/2007, Article 98 (Medium-level security measures).
91. *See, e.g.*, ISO 27002, § 10.8 (“Exchange of Information”) at pp.48-52; ISO 27002, § 10.8 (“Electronic Commerce Services”) at pp.53-55; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.93-99 (“System and Communications Protection”).
92. *See, e.g.*, Mass. Regulations 201 CMR 17.03(c).
93. *See, e.g.*, US GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C and HIPAA Security Regulations, 45 C.F.R. §§ 164.312(c) and (e); Estonia Act, § 19(2)(6); Hungary Act, Article 10(2); Ireland Act, § 2-(1)(d); Italy Act, Annex B, § 19.7; Poland Ordinance, Attachment Part C (High Security Measures), § XIII; Portugal Act, Article 15(1)(h); Portugal Act, Article 15(4); Spain Royal Decree 1720/2007, Article 101 (High-level security measures).

94. *See, e.g.*, Mass. Regulations 201 CMR 17.04(3), (5); Nevada Revised Statutes 603A; Poland Ordinance, Attachment A (Basic Security Measures) § V.
95. *See, e.g.*, Maryland and Nevada Social Security Number laws; Mass. Regulations 201 CMR 17.04(3); Portugal Act, Article 15(4) (requiring encryption of the transmission of personal data over a public network where the transmission may jeopardize the fundamental rights, freedoms and guarantees of the data subjects).
96. *See, e.g.*, Spain Royal Decree 1720/2007, Article 92 (Basic-level security measures).
97. Estonia Act, § 19(2)(5); German Federal Data Protection Act, Annex (to the first sentence of § 9 of this Act), § 4; Portugal Act, Article 15(1)(f).
98. *See, e.g.*, ISO 27002, § 12 (“Information Systems Acquisition, Development and Maintenance”) at pp.77-89; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.70-72 (“Maintenance”).
99. Mass. Regulations 201 CMR 17.04(6); Italy Act, Annex B, § 17.
100. Inquiry Regarding the Entry of Verizon-Maine Into The InterLATA Telephone Market Pursuant To Section 271 of Telecommunication Act of 1996, Docket No. 2000-849, Maine Public Utilities Commission, 2003 Me. PUC LEXIS 181, 30 Apr. 2003, available at [www.maine.gov/mpuc/orders/2000/2000-849o.htm](http://www.maine.gov/mpuc/orders/2000/2000-849o.htm).
101. HIPAA Security Regulations, 45 C.F.R. § 164.310(d).
102. Poland Ordinance, Attachment A (Basic Security Measures) § VI.
103. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.312(b); Mass. Regulations 17.03(2)(b), (3); Estonia Act, § 19(2)(3); Poland Ordinance, §§ 7.1-7.3; Spain Royal Decree 1720/2007, Articles 97 and 103 (Medium and high-level security measures).
104. Estonia Act, § 19(2)(3); German Federal Data Protection Act, Annex (to the first sentence of § 9 of this Act), § 5; Portugal Act, Article 15(1)(g).
105. *See, e.g.*, ISO 27002, § 10.10 (“Monitoring”) at pp.55-59; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.50-53 (“Audit and Accountability”).
106. Estonia Act, § 19(2)(3); Spain Royal Decree 1720/2007, Articles 97 and 103 (Medium and high-level security measures).
107. *See, e.g.*, ISO 27002, § 8 (“Human Resources Security”) at pp.23-28; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.84-86 (“Personnel Security”).
108. Greece Act, Article 10(2).
109. Mass. Regulations 201 CMR 17.03(2)(b)(2.); UK, Schedule 1, Part II, Seventh Principle, § 10.
110. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.
111. Spain Royal Decree 1720/2007, Article 89 (Basic-level security measures).
112. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.
113. HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(3)(ii)(A).
114. GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.
115. *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C and HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(1)(ii)(C); Mass. Regulations 201 CMR 17.03(d).
116. HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(3)(ii)(C); Mass. Regulations 201 CMR 17.03(e).
117. *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C and HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(5); Mass. Regulations 201 CMR 17.03(2)(b)(1), 17.04(8); Estonia Act, § 20(3); Ireland Act, § 2C(2); Italy Act, Annex B, §§ 4 and 19.6; Slovakia Act, §§ 17 and 19(3); Spain Royal Decree 1720/2007, Article 89 (Basic-level security measures).
118. *See* 5 C.F.R. Part 930.301, which specifies requirements for an information systems security awareness training program.
119. *See, e.g.*, ISO 27002, § 8.2.2 (“Information Security Awareness, Education and Training”) at p.26; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.48-49 (“Awareness and Training”). Although developed for the US federal government, NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, provides high-level guidelines that can help companies meet their information security awareness and training responsibilities. The publication identifies models for building and maintaining a comprehensive awareness and training program as part of an organization’s information security program. A companion publication, NIST Special Publication 800-16, *Information Technology Security raining Requirements: A Role- and Performance-Based Model*, addresses a more tactical level and discusses the awareness-training-education continuum, role-based training, and course content considerations.
120. Belgium Act, Art 16(2)(3).
121. *See, e.g.*, FISMA, 44 U.S.C. § 3544(b)(4); HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(5)(i); Ziff Davis Assurance of Discontinuance, ¶ 24(d), p. 5.
122. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(7); Italy Act, Annex B, § 19.5; Slovakia Act, Article 16(6); Spain Royal Decree 1720/2007, Article 94 (Basic-level security measures).
123. *See, e.g.*, ISO 27002, § 14 (“Business Continuity Management”) at pp.95-99; ISO 27002, § 10.5 (“Back-up”) at pp.44-45; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Feb. 2005) at pp.60-64 (“Contingency Planning”).
124. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(7); Spain Royal Decree 1720/2007, Article 94 (Basic-level security measures); Italy Act, § 34(f) and Annex B, § 19.5; Poland Ordinance, §§ 5.4 and 5.5 and Attachment A (Basic Security Measures) § IV.3.
125. *See, e.g.*, Spain Royal Decree 1720/2007, Article 102 (High-level security measures); Poland Ordinance, §§ 5.2, and Attachment A (Basic Security Measures) § IV.4.

# Security

---

126. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(7); Italy Act, Annex B, § 18; Poland Ordinance, Attachment A (Basic Security Measures) § IV.4; Spain Royal Decree 1720/2007, Article 94 (Basic-level security measures).
127. *See, e.g.*, Italy Act, Annex B, § 23.
128. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(7); Spain Royal Decree 1720/2007, Article 94 (Basic-level security measures).
129. HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(7).
130. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(6); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Spain Royal Decree 1720/2007, Articles 90 and 100 (Basic and medium-level security measures).
131. Spain Royal Decree 1720/2007, Article 90 (Basic-level security measures).
132. *See, e.g.*, ISO 27002, § 13 (“Information Security Incident Management”) at pp.90-94; NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems (Feb. 2005) at pp.68-69.
133. Mass. Regulations 201 CMR 17.03(j); Spain Royal Decree 1720/2007, Articles 90 and 100 (Basic and medium-level security measures).
134. EU Data Protection Directive, Article 8.
135. Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, 15 Feb. 2007, at pp.19-20, available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp131\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf) (emphasis in original).
136. Italy Act, § 34(h), and Annex B, §§ 19.8 and 24; Portugal Act, Article 15(3); Spain Royal Decree 1720/2007, Article 101 (High-level security measures).
137. Maryland Commercial Code, § 14-3402(a)(4); Nevada Rev. Stat. § 597.970.
138. Available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).
139. Minnesota Plastic Card Security Act, Minn. Stat. Chapter 325E.64; Nevada S.B. 227.

Reprinted from *The Computer & Internet Lawyer*, November 2010, Volume 27, Number 11, pages 1 to 15, with permission from Aspen Publishers, Inc., a Wolters Kluwer business, New York, NY, 1-800-638-8437, [www.aspenpublishers.com](http://www.aspenpublishers.com).