Introduction

Andrea M. Matwyshyn

In July 2005, a hacker sitting in the parking lot of a Marshalls store in Minnesota used a laptop and a telescope-shaped antenna to steal at least 45.7 million credit and debit card numbers from a TJX Companies Inc. database.[1] When the breach came to light in 2007, TJX Companies estimated that it would cost more than $150 million to correct its security problems and settle with consumers affected by the breach.[2] In addition to TJX's direct losses from this incident, which are estimated to be between $1.35 billion[3] and $4.5 billion,[4] the company also faces losses from settlement payouts[5] and, potentially, court-awarded damages.[6]

Perhaps the most troubling part of this information crime was its avoidability: TJX, a retailer worth approximately $17.4 billion had simply neglected its information security and was using a form of encryption on its wireless network that was widely known for years to be obsolete.[7] The network through which the hacker accessed the database had less security on it than many people have on their home wireless networks.[8] In other words, TJX made itself an easy mark for hackers.

TJX is not alone in its information security mistakes. Reviewing newspaper headlines on any given day is likely to yield an article about a corporate data breach. Otherwise sophisticated business entities are regularly failing to secure key information assets. Although the details of particular incidents and the reasons behind them vary, a common theme emerges: corporations are struggling with incorporating information security practices into their operations.

This book explores some of the dynamics behind this corporate struggle with information security.

The Social Ecology of Corporate Information Security

The year 2007 was a record year for data compromise, and the trend continued upward in 2008. Estimates of the number of personally identifiable consumer records exposed run as high as 162 million for 2007 alone.[9] For example, approximately one in seven adult Social Security numbers has already been compromised as a result of data breaches.[10] Corporate data losses in particular are staggering: according to estimates, the value of each corporate record lost was approximately $197 in 2007,[11] and consequently, in 2007 U.S. corporations may have lost as much as $32 billion owing to information security breaches. Despite increasing media and consumer attention, corporate data leakage continues unabated. Why?

The reasons for the continuing escalation in data vulnerability are complex and include dynamics on three levels: the macro or societal level; the meso or group level; and the micro or individual level.

Macro Level—Networked Data, Information Crime, And Law

On the macro level, corporate hoarding of networked, aggregated consumer data, the expansion of information criminality, and the arrival of information security regulation have all affected the ecology of corporate information security.

Corporate Hoarding of Networked, Aggregated Consumer Data Over the past decade, the internet became a regular part of consumer economic behaviors, and a new economic environment emerged. A defining characteristic of this new commercial environment is widespread corporate collection, aggregation, and leveraging of personally identifiable consumer data. Consumers increasingly venture online to engage in information-sensitive activities, such as checking bank balances or transmitting credit card information in connection with purchases,[12] and for many consumers the purchasing of goods through the internet is a routine part of life.[13] In the course of engaging in this routine, they leave a trail of information behind them.

Corporate entities began to see commercial opportunities in the wealth of readily available, personally identifiable data. Companies began to horde data; they started to collect as much information as possible about their customers in order to target products more effectively and to generate secondary streams of revenue by licensing their databases of consumer information.[14] Because the internet allows large amounts of data to be exchanged by remote parties, internet data brokers emerged and further invigorated the market for collecting and reselling consumer data. They began to place a premium on consumer information databases and to change the way consumer data were valued in corporate acquisitions.[15]

In the broader business context, the business environment in our society has been dramatically altered by the integration of information technology into corporate governance and operations over the last two decades.[16] Businesses have become progressively more technology-centric and, consequently, organized in large part around their unifying computer systems. Centralization arose because businesses sought to solve communication problems between parts of the company, and for many, overcoming these communication obstacles across machines became a corporate priority.[17] The goal was to allow all parts of the organization to effectively interact with each other and communicate internal data.[18] Business communications progressively shifted from real space to virtual space,[19] and entirely new technology-contingent information businesses have arisen, such as eBay and Google.[20] Even the most traditional of companies began to experiment with internet sales through company websites. Increasing computerization and automation of businesses generated enterprise-wide computing and management ripe for data hoarding and leveraging.

Progressively, these new databases of both corporate proprietary information and personally identifiable consumer information became networked with each other and the outside world.[21] Because these internet-mediated databases frequently operated in the context of a highly centralized corporate technology environment, a large "attack surface" for information theft was created. Preexisting centralization of computer systems made attacks on key targets easier: access into the system at any one of multiple points gives an attacker an avenue to compromise the targeted databases. In other words, the ease of sharing databases inadvertently resulted in the ease of attacking them.

Expansion in Information Crime These trends of corporate data hoarding and centralization did not go unnoticed by information criminals. As corporate databases of personally identifiable information became larger, they became progressively more useful for identity theft and extortion operations. The more sensitive the information contained in corporate databases, the more attractive the target.[22]

Information thievery is highly lucrative.[23] By some estimates, the information crime economy is as lucrative as the drug economy for its participants, or even more so.[24] In particular, the involvement of organized crime in identity theft has brought an additional level of professionalization to these criminal enterprises. Information criminals are frequently highly technologically proficient and in some cases represent the "bleeding edge" of technology research and development. Although they innovate in a socially detrimental manner, they are unquestionably entrepreneurial;[25] information criminals adjust their behavior over time in response to industry anti-crime efforts. The competition between information criminals and information security professional is an arms race of sorts.

According to the Federal Trade Commission (FTC), the total economic costs of reported incidents of identity theft amount to approximately $50 billion per year to consumers and corporations.[26] As this statistic implies, information crime does not affect only consumers; it affects businesses as well. Information criminals harm business entities in the process of victimizing consumers. For example, "phishing" fraud losses alone measured between $500 million and $2.4 billion annually in the early 2000s.[27] Phishing presents a severe threat to corporate goodwill as well as to information security. The goal of phishing is to leverage the goodwill of a trusted services provider,[28] and through an email trick consumers into revealing personal financial information, usernames, passwords, Social Security numbers and the like.[29] Phishing attacks frequently include registered domain names that appear to be associated with the targeted company and otherwise infringe on the intellectual property of the targeted company. During a phishing attack, an assailant simultaneously victimizes both entities and their consumers with "spoofing"[30] emails to deceive recipients into believing that the email originated from a credible source with which the consumer may possess a trusted commercial relationship, such as a financial services provider.[31] In some instances, information criminals will pretend to act on behalf of a company and use information stolen from that company to send out more effective phishing attacks directly to consumers.[32] Because the consumer has a preexisting relationship with the company, the consumer is likely to be more easily victimized by this type of falsified communication. Similarly, legitimate email communications from business entities may be ignored by cautious consumers who mistake a legitimate communication for a phishing attack.[33] Consumers victimized by phishing attacks are frequently aware that the company whose email is spoofed is not directly responsible for the phishing attack. Nevertheless, such consumers may develop a negative view of the company, particularly if the victimized company does not aggressively and publicly pursue the attacker.

For example, Monster.com was recently compromised by hackers using stolen credentials to harvest data from the Monster job-seeker database. The harvested data were then used, among other things, for sending targeted messages to job seekers purported to be from Monster.com. These messages contained a malicious attachment,[34] a Trojan called Infostealer.Monstres, which uploaded more than 1.6 million pieces of personal data belonging to several hundred thousand people to a remote server.[35] The likely goal behind this attack on Monster.com was to facilitate the criminals' subsequent phishing attacks on consumers. The criminals obtained information from Monster.com that was potentially directly useful for identity theft. But it was also useful for sending phishing emails that appeared to be highly credible and from an allegedly trusted source—Monster.com. As such, the information criminals not only compromised Monster.com's databases, but also leveraged Monster's name in their criminal phishing enterprise in order to compromise users' machines.

The criminals who illegally accessed Monster's records sought to compromise as many job seekers' machines as possible not only for identity theft purposes but also for zombie drones.[36] The end-product of these types of phishing attacks is frequently the creation of zombie drone armies or botnets[37]—coordinated groups of security-compromised consumer and corporate machines remotely controlled by criminals. Approximately 250,000 new zombies are identified per day[38] with approximately 100 million total zombies currently in operation, by some expert estimates.[39] Botnets are a significant threat to corporations. Organized crime syndicates have begun launching extortion rackets against businesses, threatening them with attacks from zombie drones in botnets.[40] Depending on the size of the army of zombie drones, such an attack could cripple a business, disrupting operations for an extended period of time. The attack may target a company directly, or the attacker may disrupt the infrastructure upon which the company relies. For example, according to the CIA, power outages in multiple cities have been traced to these types of cyberattacks.[41] As such, national security interests are also clearly implicated.

Rise of Information Security Regulation Legally speaking, the field of information security regulation is in its infancy; it is a little over a decade old. In 1996, three years after the Mosaic browser was launched,[42] questions of data security and privacy began to gain momentum within the United States, partially as a result of international influences. In 1995 the European Union passed the EU "Data Directive."[43] The Data Directive took effect in November 1998,[44] and multinational business interests in the United States were concerned; they were beginning to increase investment in internet operations, and many had already established websites.[45] The Data Directive contains provisions that prohibit transfer of the data of any European person outside the European Union without consent, and they require contractual imposition of a minimum level of care in handling on any third parties receiving the data.[46] However, despite the EU's aggressive stance toward data protection,[47] the United States did not have any consumer information security legislation[48] in effect until April 2000.[49]

At this writing in early 2009, the information security legal regime adopted in the United States is a patchwork of state and federal laws. On the federal level, health data, financial data, and children's data are statutorily regulated, through the Health Insurance Portability and Accountability Act,[50] the Gramm-Leach-Bliley Act,[51] and the Children's Online Privacy Protection Act,[52] respectively. In addition to enforcing these statutory regimes, the Federal Trade Commission has instituted a number of prosecutions for inadequate security practices under unfair trade practices regulation.[53] On the state level, state data breach notification laws have been passed in over 80 percent of states since 2003.[54]

However, much of information crime involves data not necessarily deemed particularly "sensitive" by federal statutes at present, and many entities that aggregate large amounts of information do not fall into any of the legal categories of restricted data set forth in the previous section. Therefore, not all business entities are currently proactively regulated by information security statutes. At most, state data breach notification statutes impose on them a duty to disclose the existence of a breach. Specifically, the biggest economic losses are not the result of illegal leveraging of the statutorily protected categories of data; rather, losses result from stolen personally identifiable information, such as Social Security numbers and credit card information, as was the case in the TJX breach.

Meso—Transitive Information Risks of Data and Reputation

On the mesosystem/interpersonal level, information vulnerability erodes commercial trust and imposes costs on third parties. Part of the reason for this erosion and cost transference arises from the nature of information risk. The impact of information risk is inherently transitive: a fundamental tenet of security is that a system is only as strong as its weakest links, not its strongest points.[55] This transitivity means that risk follows the information itself, and the security of the whole system depends on the lowest common denominator—the security of the least secure trusted party. Therefore, a company's information security is only as good as the information security of its least secure business partner. If a company shares sensitive corporate information with a business partner and that partner experiences a data leak, the negative effects to the shared data are similar to those that would have occurred if the first company had been breached itself. Stated another way, each time a company shares data, it acquires dependency on another company. Companies suffer economic harms and reputational damage as a consequence of both their own suboptimal security practices and their business partners' inadequate security practices.[56]

For example, in the TJX breach detailed at the beginning of this chapter, TJX, the company that suffered the breach, was not the only affected business entity. Banks that had issued the compromised credit card numbers had to reissue those cards and blamed TJX for the cost of doing so. Not surprisingly, TJX found itself a defendant in several class-action suits as a consequence of its data breach. Litigants pursuing TJX for damages included not only consumers, but also a group of banking associations from Massachusetts, Connecticut, and Maine that included over 300 banks whose customers were implicated in the breach. In April 2007, these associations sued TJX, seeking to recover the "dramatic costs" that they absorbed to protect their cardholders from identity theft risks resulting from the TJX breach.[57] The banks argued that as corporate data breaches such as the TJX breach become more frequent and larger in scale, banks cannot continue to absorb the downstream costs of other companies' information security mistakes.[58] As the TJX suits demonstrate, data breaches never occur in a corporate vacuum.

Micro—Recognizing Internal Corporate Deficits

Individual companies frequently ignore information security or believe the return on investment in information security to be inadequate. These suboptimal approaches result from, first, a failure to recognize the losses caused by weak information security, and second, an absence of thorough risk management planning.

Recognizing Asset Value Diminution and Resource Usurpation as a Consequence of Security Breaches Many companies do not yet recognize that security breaches cause losses: they diminish the value of corporate assets and usurp resources. Confidentiality, integrity, and the availability of corporate assets are all negatively affected by corporate information vulnerability and information crime. In fact, certain corporate assets, such as databases of customer information and preferences, are valuable only because they are confidential.[59] Similarly, corporate proprietary information protected solely by trade secret law could, in effect, lose all of its value in an information crime incident because the information's status as a trade secret is entirely contingent on its confidentiality.[60] Ignoring information security can quickly become more expensive than investing in it. One data breach can greatly diminish the value of such an intangible asset.[61] For example, the damage that a corporate insider can generate in one episode of information theft has been, in at least one instance, approximated to be between $50 million and $100 million.[62]

Suboptimal security also jeopardizes the integrity of corporate systems. By some estimates, corporations sustained more than $1.5 trillion in losses in 2000 owing to security breaches, such as computer viruses.[63] In 2007 the average cost of a data breach rose to $6.3 million from $4.8 million in 2006.[64] Corporate integrity is further affected by a parallel diminution in brand value and corporate goodwill. A company considered to be vulnerable usually suffers bad press and a corresponding decrease in the value of its investments in brand identity building. A brand can become damaged in the minds of business partners and consumers if it is associated with lax information security.[65] Finally, some integrity losses are related to opportunity costs. Occasionally, certain types of vulnerabilities, such as name-your-own-price vulnerabilities, deprive a company of revenue it would otherwise have received.[66]

The availability of other corporate assets also becomes limited when security issues arise. During an attempt to compromise a company's network, a remote attacker may usurp technological resources such as bandwidth and employee time. Employee time devoted to responding to an incident does not diminish or end when the attack ends; numerous hours are subsequently logged performing forensic examinations, writing incident reports, and fulfilling other recordkeeping obligations. Finally, if a security incident results in a violation of consumer data privacy, the availability of capital is further diminished by expenses for fines, court costs, attorneys' fees, settlement costs, the bureaucratic costs of setting up compliance mechanisms required by consent decrees, settlement agreements, and court decisions.

Changing Risk Management Planning For many companies struggling to implement information security throughout their organizations, building security into a legacy environment unfamiliar with information security principles is a challenge. Frequently, proponents of stronger security face internal corporate resistance to setting new security-related corporate priorities and investment levels.[67] In part because of such tensions in risk management planning, certain types of information security mistakes recur. The five most common information security errors visible today in corporate information security risk management include a lack of planning, nonresponsiveness to external reports of breaches, letting criminals in, theft by rogue employees, and a failure to update existing security.

Lack of Planning For the reasons elaborated in the preceding pages, there is a lack of adequate information security risk management in business worldwide. According to the fifth annual Global State of Information Security Survey conducted in 2007, a worldwide study by *CIO* magazine, *CSO* magazine, and PricewaterhouseCoopers of 7,200 information technology (IT), security, and business executives in more than 119 countries in all industries, companies are slow to make improvements in corporate information security.[68] Perhaps the most disturbing finding of the study was that only 33 percent of the responding executives stated that their companies keep an accurate inventory of user data or the locations and jurisdictions where data is stored, and only 24 percent keep an inventory of all third parties using their customer data.[69] Although data breaches are driving privacy concerns, encryption of data at rest, for example, remains a low priority despite its being the source of many data leakage issues.[70] Only 60 percent of the organizations surveyed have a chief security officer or chief information security officer in place. Similarly, 36 percent stated that their organizations do not audit or monitor user compliance with security policies, and only 48 percent measured and reviewed the effectiveness of security policies annually.[71] Most companies responding to the study also indicated that their organizations do not document enforcement procedures in their information security policies, and only 28 percent of policies include collection of security metrics.[72]

Ignoring External Reports One of the most easily avoidable information security mistakes is not taking external reports of problems seriously. Companies, and individual employees within companies, sometimes believe that quashing an external report of a vulnerability or breach will make the problem go away. For example, in November 2002, a security hole in the Victoria's Secret website allowed a customer to access over 500 customers' names, addresses, and orders. The customer who discovered the hole contacted Victoria's Secret directly and advised Victoria's Secret of the problem. Despite promises of data security in their website privacy policy, Victoria's Secret employees informed the customer that nothing could be done. In anger, he contacted the press and the New York

State attorney general. Victoria's Secret was subsequently prosecuted by the New York State attorney general and ultimately entered into a settlement that included a $50,000 penalty.[73]

Letting Criminals In Sometimes companies let hackers into their own databases because of inadequate monitoring practices. For instance, in February 2005, ChoicePoint, Inc., a data aggregator, revealed that it had sold data about more than 145,000 consumers to information criminals. According to the FTC complaint that resulted from this breach, ChoicePoint had prior knowledge of the inadequacy of its customer screening process and ignored law enforcement warnings of fraudulent activity in 2001. It willingly sold data to companies without a legitimate business need for consumer information, even in circumstances where these purchasers looked suspicious. According to the Federal Trade Commission at least 800 consumers became victims of identity theft as a result of this breach. Ultimately, ChoicePoint entered into a settlement agreement with the FTC, agreeing to pay a fine of $15 million.[74]

Theft by Rogue Employees Companies frequently forget about internal threats to their security. The greatest threats to corporate intangible assets frequently arise from rogue employees. Limiting access by employees to sensitive information on a "least privilege" / need-to-know basis can be a critical step in avoiding information theft. For example, on June 23, 2004, a former AOL employee was charged with stealing the provider's entire subscriber list of 37 million consumers (over 90 million screen names, credit card information, telephone numbers, and zip codes) and selling it to a spammer who leveraged and resold the information.[75] The software engineer who stole the data did not have immediate access to the information himself, but he was able to obtain it by impersonating another employee. Although the initial sale price of the list on the black market is unknown, the spammer paid $100,000 for a second sale of updated information with 18 million additional screen names. The list was then resold to a second spammer for $32,000 and leveraged by the first spammer in his internet gambling business and mass-marketing emails to AOL members about herbal penile enlargement pills.[76]

Failure to Update Existing Security Revisiting the TJX data breach once more, the importance of viewing security as an ongoing process becomes apparent. Security cannot be viewed as an off-the-shelf product; vigilance and constant updating of security measures are mandatory. The encryption protocol that TJX used, WEP, was widely known to be broken for four years before the TJX breach.[77] It was common knowledge in the information security community at the time of the breach that WEP could be easily compromised in one minute by a skilled attacker.[78] Companies must constantly reevaluate their information security measures in order to respond to changing criminal knowledge.

The Future of Corporate Information Security Policy

In the chapters that follow, this book engages in a bottom-up, multidisciplinary analysis of some of the changing corporate information security dynamics introduced to this point. As the previous sections have made clear, an analysis of corporate information security policy requires adopting an evolutionary approach that recognizes the emergent nature of information threats.

Chapter 1, "Computer Science as a Social Science: Applications to Computer Security," argues the importance of adopting this multidisciplinary lens in analyzing information security. Jon Pincus, Sarah Blankinship, and Thomas Ostwald write that developing the best information security practices requires broadening the scope of our current perspectives on information security: "Computer security has historically been regarded primarily as a technical problem: if systems are correctly architected, designed, and implemented—and rely on provably strong foundations such as cryptography—they will be 'secure' in the face of various attackers. In this view, today's endemic security problems can be reduced to limitations in the underlying theory and failures of those who construct and use computer systems to choose appropriate methods." Although computer science is not traditionally viewed as a social science, problems in its domain are inherently social in nature, relating to people and their interactions. Pincus, Blankinship, and Ostwald argue that applying social science perspectives to the field of computer security not only helps explain current limitations and highlights emerging trends, but also points the way toward a radical rethinking of how to make progress on this vital issue.

Chapters 2 and 3 present two perspectives on the public-facing aspects of corporate information security. Chapter 2, "Compromising Positions: Organizational and Hacker Responsibility for Exposed Digital Records," by Kris Erickson and Philip Howard, sets forth an analysis of the empirical extent of known corporate information security compromise. Erickson and Howard analyze over 200 incidents of compromised data between 1995 and 2007. They find that more than 1.75 billion records have been exposed, either through hacker intrusions or poor corporate management, and that in the United States there have been eight records compromised for every adult. They conclude that businesses were the primary sources of these incidents.

In Chapter 3, "A Reporter's View: Corporate Information Security and the Impact of Data Breach Notification Laws," Kim Zetter presents an insider's view of how information about corporate information security breaches reaches the public. She says that "[d]espite the passage of state-level data security breach notification legislation in many states, journalists still often have to rely on sources other than the companies and organizations that experience a breach for information about a breach—either because the breach is not considered newsworthy or because the data that are stolen do not fall into the category of data covered by notification laws." Journalists learn about breaches from a number of sources. Rarely, though, are companies or organizations that experienced the breach the first to reveal it. Zetter describes some of the practical limitations of data breach notification laws with regard to public disclosure of corporate security breaches. She says that companies fear that disclosing such information would place them at a disadvantage with competitors and make them vulnerable to lawsuits from customers as well as to other potential intruders.

In contrast to Chapters 2 and 3, Chapters 4 and 5 present two sets of internal corporate information security concerns relating to protecting intellectual property assets. In Chapter 4, "Embedding Thickets in Information Security? Cryptography Patenting and Strategic Implications for Information Technology," Greg Vetter discusses the strategic concerns companies face in deciding whether to patent information security methods. Vetter argues that the full promise of cryptography for information security is unrealized. Companies are increasingly patenting security technologies in an effort to expand their portfolios and better protect corporate intangible assets. Cryptographic methods can enable authentication in an electronic environment and help secure information storage, communications, and transactions. Patenting in the field has expanded aggressively, and greater patent density, sometimes described as a "thicket," affects both developers and users and brings with it the potential to chill innovation. This greater patent density, argues Vetter, suggests the need for countermeasures such as patent pooling, patent-aware standard setting by firms and the government, and portfolio management of patents.

Chapter 5, "Dangers from the Inside: Employees as Threats to Trade Secrets," by Elizabeth Rowe, discusses the risks that rogue insiders present to corporate information security, particularly with regard to trade secrets. Says

Rowe, "The loss of a trade secret is particularly devastating to a company because a trade secret once lost is lost forever. The widespread availability and use of computers, together with an overall decline in employee loyalty, provides fertile ground for the dissemination of trade secrets." Rowe argues that the biggest computer security threats and accompanying threats to a company's trade secrets originate with the company's own employees. Put in criminal law terms, employees often have the motive and the opportunity that outsiders lack. Employees usually have legal access to the trade secret information by virtue of their employment relationship and can use that access to misappropriate trade secrets. "Examples abound of employees who have either stolen trade secrets for their own or a new employer's benefit, or have destroyed them completely by disclosing them over the internet. Recent statistics indicate that the large majority of computer crimes are committed by employees." Rowe provides background on trade secret law, presents examples of disclosures that have occurred using computers, and ends with some lessons for trade secret owners.

Chapters 6, 7, and 8 consider information security in connection with the three categories of statutorily protected data: health data, financial data, and children's data. Chapter 6, "Electronic Health Information Security and Privacy," by Sharona Hoffman and Andy Podgurski, addresses the regulatory, policy, and social impacts of electronic health data security vulnerabilities and the mechanisms that have been implemented to address them. The electronic processing of health information provides considerable benefits to patients and health care providers, but at the same time, argue Hoffman and Podgurski, it creates material risks to the confidentiality, integrity, and availability of the information. The internet creates a means for rapid dispersion and trafficking of illegally obtained private health information. The authors describe the wide-ranging threats to health information security and the harms that security breaches can produce: "Some of the threats are internal, such as irresponsible or malicious employees, while other threats are external, such as hackers and data miners. The harms associated with improper disclosure of private medical data can include medical identity theft, blackmail, public humiliation, medical mistakes, discrimination, and loss of financial, employment, and other opportunities." In order to address security risks related to electronic health data, the U.S. Department of Health and Human Services enacted the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, part of the more general HIPAA Privacy Rule. The Security Rule requires the implementation of administrative, physical, and technical safeguards for the storage and transmission of electronic health information. Hoffman and Podgurski present a critique of the Security Rule from both legal and technical perspectives. They argue that the rule suffers from several defects, including its narrow definition of "covered entities," the limited scope of information it allows data subjects to obtain about their health information, vague and incomplete standards and implementation specifications, and lack of a private cause of action. They offer detailed recommendations for improving safeguards for electronically processed health records.

Chapter 7, "Quasi Secrets: The Nature of Financial information and Its Implications for Data Security," by Cem Paya, presents a technical critique challenging the most basic premises underlying the Gramm-Leach-Bliley Act—that "financial data" refers to data held by financial institutions. Instead, Paya argues that a better analysis starts with looking to the data, not the holder. He points out that financial information appears to be the type of data most frequently targeted by malicious actors. After providing a primer on the basics of information security engineering, he asks whether there is something inherent in the nature of financial information that makes it a challenge for information security and any regulatory framework. Analyzing the two most common forms of financial information—credit card numbers and Social Security numbers—Paya concludes that although the credit card industry appears to successfully mitigate risks of disclosure, the use of Social Security numbers as a financial identifier is inherently problematic and should be eliminated.

In Chapter 8, "From 'Ego' to 'Social Comparison'—Cultural Transmission and Child Data Protection Policies and Laws in a Digital Age," Diana Slaughter-Defoe and Zhenlin Wang discuss the evolution of child protection and information security online. In the past quarter-century, child development scholars have embraced ecological paradigms that expand the identified cultural transmitters beyond parents to include the broader cultural context. All forms of mass media, including the internet, form part of children's cultural context. The Children's Online Privacy Protection Act and other internet child protection legislation were enacted in order to create a safe internet space in which children can interact with commercial enterprises and other users. Defoe and Wang believe that current laws addressing internet child protection are ineffective. They assert that "future legislation should take into account children's developmental attributes" and emphasize empowering parents in guiding their children's development and securing their children's information.

Chapters 9 and 10 present international perspectives on two challenges to the evolution of information security best business practices: changing contract norms and new business models. In Chapter 9, "Contracting Insecurity: Software Terms That Undermine Information Security," Jennifer Chandler argues that contract law provides one of the most effective means by which companies can impose obligations of data security on others. However, contract law can simultaneously provide a means for companies to shirk their information security obligations. This chapter highlights a selection of terms and practices that arguably undermine information security. One series of clauses undermines information security by suppressing public knowledge about software security vulnerabilities. Such clauses frequently prevent research by barring reverse-engineering clauses or anti-benchmarking clauses and suppressing the public disclosure of information about security flaws. Other practices that undermine information security according to Chandler are those where "consent" to the practices is obtained through the license and the software is difficult to uninstall, abuses the software update system for non-security-related purposes, or obtains user consent for practices that expose third parties to possible harm.

In Chapter 10, "Data Control and Social Networking: Irreconcilable Ideas?," Lilian Edwards and Ian Brown present the challenges to information security from social networking websites and the new business models they represent. The success of this new generation of data-intensive virtual-space enterprises raises heightened concerns about information security. It is already known that identity thieves are making extensive use of personal information disclosed in such virtual spaces to commit fraud, while unaccredited writers of subapplications for these spaces can also gain access and evade security around vast amounts of valuable data. Edwards and Brown argue that although the law may provide some data control protections, aspects of the code itself provide equally important means of achieving a delicate balance between users' expectations of data security and privacy and their desire to share information.

Finally, the Conclusion reiterates the four major themes of the preceding chapters—first, a need to focus on the human elements in information security; second, a need to recognize the emergent nature of information security threats; third, a need to consider the multiple simultaneous contexts of information risk; and, fourth, a need for immediate improvements in corporate self-governance. In the short term, companies must put in place rigorous codes of information security conduct and exercise vigilant enforcement. In the long term, companies must learn to build cultures of information security and develop a sense of collective corporate responsibility for information security, regardless of whether regulation requires them to do so. Meaningful improvements in information security require a commitment to security as an ongoing, collaborative process.