Introduction

Computer security is a technical and social problem. It is just as much about social relationships as it is about computers as tools. Internet security professionals are as concerned with how people use information as they are with how machines manipulate and process that information. This book is a case study of how the knowledge systems articulated by computer antivirus industry professionals affect technological security. It analyzes the tensions and political dilemmas at the heart of the interrelationships among science, technology, and society.

All technologies involve 'scripts'. A computer virus is a metaphor that generates images of global viral epidemics and outbreaks, of infectious code reeking havoc on personal computers and global information networks, and of machines that no longer respond to or are under our control. The reality of infected computers generates an entire industry seemingly dedicated to protecting computers and their users from infection, and disinfecting those that succumb. Indeed, those who work within the antivirus industry perpetuate this scripted imagery, and consider themselves part of a security force that polices the 'dark alleys' of the 'information superhighway'.

Based on qualitative interviews over six years with various professionals within the antivirus industry, this book explores changing definitions of security and technological threats to corporate communications within the global marketplace. Grounded in these professionals' own words and attitudes, it highlights the complexity of the issues surrounding the antivirus industry's perspectives of virus writers and spammers, its negotiations with transnational corporations within a techno-capitalist economy, and its interactions with global corporations as end users.

This book also provides a theoretical reflection on the development of technological artifacts. Grounded in the science and technology studies paradigm, it examines how these antivirus professionals' interpretations, economic interests, and disciplinary conflicts affect the production of computer security technology. The competing and cooperating social groups within the industry attempt to achieve industry consensus and technological stabilization, endeavoring to 'black box' or frame certain aspects of antivirus software as transparent, unambiguous, and thus not needing further analysis (Latour 1999). The negotiations, persuasions, and even the disciplinary actions for those who deviate from industry protocols have real-world effects on this technological product. Therefore this book is also about how technology can never be 'black–boxed'. At the beginning of the twenty-first century's culture of fear, antivirus technologies have increasingly become sites of negotiations as industry workers battle over various definitions of threat and disparate interpretations of computer security.

This book examines the history of the antivirus industry and its intersection with the advance of information capitalism. The antivirus industry's foundation is in the mythical beginnings of the open source movement, where computer experts freely distributed their knowledge and worked cooperatively on solving technical problems and threats to the internet, above and outside the pressures of the marketplace. However, antivirus software today is also a consumer product bought and sold in the global marketplace. Industry experts compete in how to best protect information and corporate money in the growth of the high-tech transnational economic system. While industry professionals articulate the empowering processes of openness and collectivity, they also must negotiate their professional lives shaped by their immersion within global capital flows.

Tension arises from the industry professionals' negotiations between generating profit and protecting the internet. They must address the changing 'discourses of danger' in response to transformations of both technologies and escalating world crises. The compromises around these negotiations inform the professionals working within this industry by providing a vocabulary of motives, a sense of identity, values and prevailing concepts of organizational work and worth, and an industry logic. These compromises, however, are addressed differently between the various segments of the industry, and as such are continually contested.

This book is therefore also about the constant shifting between technological objects that appear as neutral—networks, computer code, e-mail programs, and the internet—and the social and ethical values embedded in these objects by the various industry segments. These antivirus industry professionals battle in the global marketplace over malware exploits, transformations of technology, and definitions of 'security'. By documenting these struggles, this book brings alive both the human and the technological and illuminates the seemingly invisible values and ideals networked into the lines of code within antivirus products.

Hackers

I wish to make it clear that this book does not purport to be a depiction of the hacking culture. It is written as a contribution to ongoing analysis of the information age and its institutions of social control and definitions of deviance. Other writers have provided detailed descriptions of the origins and social organization of hackers. This book, while being grateful for such efforts, is written with a different aim. While drawing upon and using their analyses of hackers, this book is about the antivirus industry and its perspective of the world, which includes the industry's stigmatization of, negotiations with, and dependency on these malware writers and the code they write.

The industry's construction of virus writers is not simple or one-sided. Definitions of crime and deviance reflect and influence transformations of social structures. Over the course of the interviews, the antivirus industry's stigmatization of virus writers ranged from juvenile delinquents to 'script-kiddies', to the Russian mafia, and to multimillionaire spammers. These changing definitions arose in relation to geopolitical transformations and advancing technologies, and the interrelated issues of ideological control over those technologies. "[T]he struggle around the definition of crime and deviance is located within the field of action that is constituted by plural and even conflicting efforts at producing control" (Melossi 1994, 205). The effort at securing technological control over the flow of global information is at the heart of the antivirus industry.

There is a growing body of literature about hackers, virus writers, and various aspects of cyber crime. Pekka Himanen (2001) in *The Hacker Ethic: A Radical Approach to the Philosophy of Business* corrects the misperception that 'hackers' are merely teenage misfits glued to their computers. He explains how the background philosophy and positive definition of hackers as 'passionate programmers' originated in the early 1960s. This definition suggests hackers are those people who, regardless of the field in which they work, do what they do for personal satisfaction and the altruism of furthering their area of interest. The other significant element of the hacker ethic that Himanen identifies is the duty to share discoveries and interesting information with like-minded people, and the accompanying peer recognition from that sharing. Hackers enter into this information creation and exchange motivated by enthusiasm, joy, and passion, not just money. Central to the hacker ethic is this task-centric orientation that Himanen contrasts to the time-centric, external reward, and motivation approach of the Protestant work ethic. Generally, the hacker ethic is not motivated by external hierarchies or rules from above, and according to Himanen, it is the 'creative spirit' and driving force of individuals in the information age. Himanen identifies the 'cracker' as the exploitive and malevolent offshoot of the hacker. While Himanen specifies the differences between these two labels, cracker as a deviant label never 'catches on' or reaches cultural iconic status, but instead is almost invisible in popular jargon. Negative computer exploits become attached to the term 'hackers'.

In many ways, Himanen's positive review of the hacker ethic describes the work ethic of antivirus industry professionals. They, too, articulate a task-centric approach to their jobs, and are motivated by the joy, passion, and enthusiasm of problem solving. They are 'on call 24/7', dedicating themselves to solving the latest malware exploit. However, in comparison to Himanen's hacker work ethic, similarities stop there. This enthusiasm and dedication for problem solving articulated by antivirus industry professionals are in support of and funded by large amounts of corporate money. While sharing Himanen's hacker work ethic, antivirus professionals exist to protect corporate information, and to stop, contain, or reverse damage to information caused by the release of malware. This (dis)similarity is at the core of the antivirus industry. The hacker ethic of information sharing, a non-monetary orientation, and a task-centric focus all become points of tension and conflict as these antivirus industry professionals attempt to negotiate the competing logics. This book is an examination of those contestations and their effect on antivirus technological innovation.

The Hacker Manifesto by McKensie Wark (2004) also offers a Marxist framework for understanding the emergence of a 'hacker class'. He also examines institutional forces that are generated to resist it. Wark theorizes that the hacker class is needed by the 'vectorialist class' (informational entrepreneurs) to do their actual work. The inventors, the imaginaries, and the visionaries of technology's potential all belong to Wark's hacker class. They remain free, outside the bounds of financial influences, and cannot be completely controlled. *The Hacker Manifesto* identifies many of the tensions articulated by antivirus professionals as central to their industry. The mythical beginnings of the internet and many of Wark's critical aphorisms, such as "information wants to be free but is everywhere in chains," are supported by the antivirus professional's own ideological position (Wark 2004, 135).

Indeed, antivirus professionals support many of Wark's assumptions. They suggest that their industry and hackers operate within a similar technological and information-saturated world. Verifying Wark's oppositional structures, antivirus industry professionals suggest that the information society is affected by a strategic dance between the 'white hat' and the 'black hat' technologists. Antivirus professionals, as 'white hats', both work for and within the system. They must negotiate with the state, with transnational corporations, and with the media to protect corporate financial flows. Yet, their professional identities and the logic of the industry are dependent upon the 'black hat' hackers they demonize. The tensions and double-speak that arise out of the similar technological movements within this strategic dance are fascinating.

A researcher who has interviewed and researched the philosophies, ethical positions, and mind-sets of 'black hat' virus writers is Sarah Gordon. Gordon challenged the idea of virus writers as a monolithic group, and has documented the multiple world views of many malware writers. In 1994, she compared various virus writer groupings—adolescents, university students, adults, and ex-virus writers—and evaluated their stated rationales for writing viruses. All except the 'adults' were judged to be normal on the Kohlberg scale of age-related ethical development (Gordon 1994). They wrote viruses for various reasons, but the majority could not be conceptualized as unethical for their developmental level.

Douglas Thomas and Brian Loader (2000) in *Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age* also identify several motives of computer virus writers. Through case studies and critical analysis of hacker discourse, they also highlight the range of malware writers' intention such as experimentation or political activism. In 2000, these authors suggested that most hackers engaged in a cooperative spirit of inquiry and investigation and were more interested in finding, sharing, and discussing software loopholes in order to understand and improve technology, rather than exploiting those loopholes for selfish or unethical purposes.

From the many books and articles published before 2000, hackers and computer virus writers had been seen by many as, if not heroes challenging technological code as a form of social control, then merely misguided delinquents needing education about the real-world consequences of their actions. Acknowledging the research into and with these virus writers, this book documents the antivirus industry's evolution in correspondence with the continual transformation of internet crimes. The further development and evolution of the internet and the Web since 2000 has created a more efficient means for people to gather and sort information and make online purchases 24/7. These same technologies have also ushered in new waves of criminal activity. Interviews for this book began in 2000, when the security industry was targeting 'script-kiddies' and the virus writers who were just experimenting. By 2006, however, the image of these writers changed. Malware writers were organized into high-tech forms of criminal behavior, stealing identities and targeting global systems for profit. Today, their mafia-like organizations around the world have also become global and informational, reflecting the flows of global commerce. While spam was once a mere annoyance, today it is used by organized crime networks with botnets seeding infected machines with adware and hosting fraudulent e-commerce or banking Web sites. These transformations of the 'dark alleys' of the information superhighway both influence and reflect the antivirus industry technology, as it attempts "plural and conflicting efforts at producing control" (Melossi 1994).

Theoretical Groundings

The term 'computer virus' is a metaphor that combines the biological imagery of viral epidemics and outbreaks with high-tech global informatics. Many authors have commented upon this coupling. Deborah Lupton suggested in 1994 that the metaphor of a computer virus reveals our ambivalent attitude toward new technologies. She suggested that computer viruses refer to the "computer technology's parasitical potential to invade and take control from within" (Lupton 1994, 566). Stefan Helmreich (2000) drew on David Harvey (1990) and Emily Martin (1994) to characterize computer viruses as "employing language reminiscent of that used to describe 'bodies' of nation-states under military threat from without and within" (Helmreich 2000, 473). In 2005, Jussi Parikka, citing Humberto Maturana, stated, "During the past few decades, biological creatures like viruses, worms, bugs, and bacteria seem to have migrated from the natural habitats to ecologies of silicone [sic] and electricity" (Parikka 2005, 1). The hybridity at the core of the computer virus metaphor serves as a ripe field for academic analysis.

This book, however, complicates this theoretical orientation. It focuses on those whose daily enterprise seeks to, if not destroy, at least contain the effects of this coupling. The antivirus industry works within and against the narratives of a body/machine metaphor as industry workers research, develop, and use antivirus products. At its most basic, the antivirus product is computer code designed to contain other strings of self-replicating computer code. The antivirus product then is the culmination of scientific research, industry negotiations, and the application of marketing in an economy based on both the fear of invasions and faith in technological progress. As such, it is a prime object for science and technology studies.

Researchers in the field of science and technology studies have produced a great deal of scholarship that documents and analyzes the social shaping of technology (MacKenzie and Wajcman 1985; Bijker

1995). An important area of this scholarship is the Social Construction of Technology (SCOT), which explores the various human processes that affect the discovery, design, development, and use of technological artifacts. This field of research challenges the idea of technological determinism, which neutralizes or renders invisible the material conditions of development and technological practices, and the social environments within and through which technologies originate and operate. These researchers do not conceptualize IT artifacts as stable, discrete, independent, or fixed (Orlikowski and Lacono 2001).

Instead, researchers in this field focus on how technological design is an open process that can produce different outcomes depending on the social circumstances of development. Using rich case studies of technological invention and development, social constructivist research examines how interpretations, social interests, and disciplinary conflicts shape the production of a technology by framing its cultural meanings and the social interactions among relevant social groups (Orlikowski and Lacono 2001). No one person or group creates a technological artifact. Negotiations and various knowledges, observations, and goals allow for multiple paths toward that development. Technological artifacts are in this sense 'under determined' and are the product of flexible interpretations and power relationships.

These contestations and negotiations between social groups and their effects on the technological artifact are relevant areas of study in the antivirus industry. Various social groups, with different rankings and statuses, and with different invested positions and interpretations labor to see their vision of antivirus software realized. The cultural contexts of those groups, their taken-for-granted assumptions, and their social situation within the larger sociocultural environment all come to affect the technological artifact. Who is included and who is excluded, who has what access to what information, what barriers are crossed or raised and by whom, what compromises are brokered, what is left silenced and unspoken, or not even conceptualized because of variations in such factors as gender, race, or class backgrounds—all these variables come to affect the technological artifact. For the antivirus industry, power, contestation, inequality, and hierarchy inscribe the industry and shape the production of antivirus software. This book reveals how these intervening mechanisms, having little to do with the antivirus technology per se, (re)shape the software product.

Another key point of SCOT analysis is that artifact development is ‘finished’ only when the various groups reach a consensus. “Design ceases not because the artifact works in some objective sense but because the set of relevant social groups accepts that it works for them” (Bijker 1995, 270). This acceptance leads to a sense of ‘closure’ and ‘stabilization’ with no further implementation or further design modifications. If there are any lingering problems, they are redefined as insignificant.

However, recent scholarship questions the definitions and perceptions of ‘closure’ and technological ‘stabilization’. IT artifacts are not static and unchanging. They are dynamic because “new materials are invented, different features are developed, existing functions fail and are corrected, new standards are set, and users adapt the artifact for new and different uses” (Orlikowski and Barley 2001). Technological artifacts in this sense are never stable or closed. Within the antivirus industry, the antivirus product is constantly being modified and adapted to changing technological transformations and to evolving corporate needs. Corporate end users engage in the co-construction of their technologies as vendors form end user focus groups to help inform their researchers, as product-developers reach out to consumers to understand their preferences, and as corporate end users retool their antivirus products to fit their corporate needs. Science and Technology Studies researchers increasingly identify this type of ambiguity between producers’ open-ended artifacts and users’ sanctioned and unsanctioned modifications as important areas of current research.

Technological artifacts are, in this sense, open and evolving. They are also granted power. Similar to the microbes in Bruno Latour’s (1988) analysis of the “Pasteurization of France,” computer code can destroy or protect. Latour’s actor–network theory (ANT) suggests that the human and the nonhuman are entwined and inseparable, a concept of interconnectedness that is usually overlooked in both academic analysis and our daily interactions. Drawing on actor–network theory, computer code is rearticulated as actively intervening, both positively and negatively, in our economy, in our faith in technology, and in our relationships. Antivirus experts are authorized and empowered by the behavior of computer code. Indeed, the antivirus industry conceptualizes itself as the necessary gatekeepers watching and protecting the global economy against the actions of computer code. The actions of computer code are important as antivirus industry professionals respond to outbreaks and dedicate their professional lives to eradicating the effects of malware. Latour's ANT helps bring this interaction between industry professionals and the actions of the computer code into the foreground.

The other foundational theorist for this book is Michel Foucault. Much of the exploration of the power relationships within the antivirus industry draws upon Foucualt's (1972) analysis of the power/knowledge nexus. Foucault sees power as strategies and influences running through networks; these strategies and influences are seemingly invisible and taken for granted as 'natural' and inevitable. One of the central concerns of Foucault's work is to dispel these seeming self-evidences. His work illuminates how even familiar and taken-for-granted assumptions of authority and common sense are not 'natural' or part of a naturally existing order. Through a number of different examples from hospitals to prisons, Foucault has shown how what counts as truth and knowledge depends on, or is determined by, the conceptual system in operation (Casey 1995).

Within the antivirus industry, there are two conflicting conceptual systems in operation. One is a technical hierarchy, based on a faith in the technological knowledge and research proficiency of the antivirus expert. Reflecting cyberspace generally, at the top of the cultural construct that led to the creation of the internet is the techno-meritocratic culture of scientific and technological excellence, emerging essentially from big science and the academic world (Castells 2001). This conceptual system is based on sharing research, open discussions, and academic debates, and is even foundational to the positive elements of the hacker work ethic discussed earlier. Both the hackers' and the antivirus industry's status as technological experts and their recognition through their community of peers, is enmeshed within and is a part of this culture of techno-meritocracy. However, the antivirus industry is a for-profit endeavor. And the conceptual orientation of the corporate business system is closed and competitive, where research results are guarded secrets. Corporate research and development, the results from R&D, are valuable, profitable, and protected as such. Within the antivirus industry, research and development merges with bottom-line profits and industry rankings. This conflict between cooperative and competitive systems, between scientific and corporate research ideals, generates various definitions of, knowledge about, and expertise in computer code, security threats, and end users' needs.

Information Capitalism

The internet evolved from merely a complex communication system into a major new arena for capital accumulation and the operations of global capital (Sassen 2002; Castells 1996). The power relations of the older manufacturing capitalism have been reconfigured on a global scale around information-driven systems. This brand of information capitalism is profoundly different from its historical predecessors. According to Manuel Castells (1996), information capitalism has three fundamentally distinctive features: it is global and instantaneous; it is structured to a large extent around a network of information flows; and capital is realized, invested, and accumulated mainly in these spheres of circulation. Access to these networks of information flows then becomes vitally important. Indeed, Castells suggests that ownership and property relations have been replaced in the information age by the ability to access information and generate intellectual capital. Access to technological know-how is at the root of productivity and competitiveness. Consequently, new patterns of inequality emerge on the basis of reduced access to information. New concentrations of 'information wealth', global elites, and the 'informational bourgeoisie' dominate the arenas of this information society.

Access and intellectual capital are key concepts for understanding the antivirus industry. As the gatekeepers of information flows, as the digital fingers on the pulse/flow of information, as the security point/node in the flow of information on the internet, industry professionals monitor these flows for threats. Through their products, they assure the continued 'frictionless' circulation of these flows. Based on their knowledge and technical expertise, these industry professionals turn their information into capital as they transform their knowledge and computer code into products that protect threatened circulation flows. Because of this position in the information age, they profit financially, both as individuals and as businesses, as long as the threats persist.

While working to secure the information society, eruptions occur inside the industry as different segments of the industry also vie for the power to control the security surrounding information capital. Through erecting knowledge monopolies and disciplinary exclusions, their various knowledges become a powerful form of intellectual property. These various industry segments simultaneously produce, reproduce, and are victimized by the ability to channel the circulation of information flows. This book is a structural and systemic analysis of how antivirus technologies are embedded in these complex interdependent networks, and how they are shaped by these broader social, economic, and political institutional influences.

Method

I am an outsider to the antivirus industry. My background is in anthropology and culture studies with a theoretical interest in the social conditions structuring technology. Having attended several of the Virus Bulletin International Conferences, going to the sessions and listening to questions after the sessions, as well as the conversations over breakfasts, lunches, dinners, . . . and drinks, I began sensing a subtly shifting power dynamic within, what I had thought to be, a relatively stable set of associations. As industry professionals attempted to respond to the changes in technology, in personnel, and in the definitions of threats and security, I began to see symbolic and some not so symbolic challenges to previously revered authorities and industry groups. Antivirus professionals were re-defining themselves and their industry within what they portrayed as an increasingly technocratic and insecure global economy. This book is one perspective of these changing social relations as the antivirus industry negotiated issues of security and profit in an increasingly technologically vulnerable world.

Of the multiple divergent perspectives that began to emerge in the conferences' end-of-session questions and in personal conversations with both presenters and attendees, the most obvious and seemingly most misunderstood issues were grounded in the conflicting interests, attitudes, and perspectives held between antivirus developers and IT administrators as the developers' corporate customers. The diversity was articulated in their contradictory goals, directions, and the services generally expected of and provided by the industry. However, in listening to these divergent worldviews being expressed by variously-situated individuals, I realized that each took for granted that their perspective was universally understood and absorbed. Each assumed the other was and should be operating within the same reference points.

In order to investigate this seeming discrepancy, I scheduled interviews with several IT administrators of the biggest corporate representatives at these conferences and many of the product managers of the largest antivirus developers. I conducted many of these interviews at the Virus Bulletin International Conference in Orlando, Florida, and at the Association of Antivirus Asian Researchers Conference in Tokyo, Japan—both in 2000. I also interviewed IT administrators of large corporations outside the Virus Bulletin conference world, specifically targeting those who had never attended an antivirus conference. I conducted follow-up interviews over the next six years as personnel changed, as new threats emerged, and as the industry adapted.

Originally I had not conceptualized antivirus researchers as related to the divergent perspectives between IT administrators and antivirus product managers. I saw antivirus researchers as an economically integrated, intimate part of the developers' market orientation, and consequently not central to my sense of the conflicting points of view articulated between corporate customers and the antivirus product developers. But the more I talked with the product developers, the more they recommended I needed to include the antivirus researchers as men who have the power to guide and influence both the direction and the products of the entire industry.[1] I listened to these managers as 'native' experts and expanded the parameters of my research to include the technological researchers and their perspective of their industry. Consequently, I have interviewed thirty-three individuals within the antivirus industry distributed across corporate IT administrators in charge of computer security, antivirus product managers and vendors, and antivirus researchers.

The three categories of workers within the antivirus industry, the corporate IT managers, the vendors, and the researchers, do not exist independently of each other. In fact it was often the moments when

[1] While 'men' is used here, six women within the various levels of the antivirus industry granted me the privilege of interviewing them and allowed me to record their insights into their world. Gender is a significant factor that needs to be addressed within the antivirus industry and is discussed in the final chapter, "Situated Exclusions and Reinforced Power." To protect the women's anonymity, all respondents are identified as male.

the boundaries between these categories blurred, such as when a virus outbreak occurred, that led to questions about who had the appropriate knowledge and information to protect the internet. Was it the frontline IT manager who first gathered the information about the virus attacking his network? Or was it the vendor who had multiple IT managers' reports of the virus attacking the network? Or was it the researcher who analyzed the computer code in order to provide a solution? Discussion about these socially-situated knowledge sites highlighted the tensions of the knowledge/power nexus. It was this blurring or leakage between competing definitions and categories that enabled dominant, commonsense notions of security to become problematic as these workers discussed their perspectives, their roles, and their sense of their socially-situated exclusive knowledges.

Throughout the six years of interviewing, changes in broader social and cultural structures affected the industry. Security issues exploded around 9/11 and the U.S. government's war on terror, Microsoft changed from being the target of virus writers' exploits to a supplier of antivirus products for the home market, and several new technologies came to market while others became outdated. Individually, some of the original participants changed jobs, some quit the industry, and new recruits joined the industry. Indeed, each participant's engagements with the industry is experienced differently and has changed and shifted in multiple and various ways over the years.

There is a need to highlight the partiality and constructed nature of any research project because of all these changes and transformations, and these multiple voices and shifting subject positions (Lather 2004; Fine 1994). The antivirus industry was and continues to be adapting and transforming. The voices and analysis gathered here are limited by the specific people who agreed to be interviewed, the historical changes, and the erratic features of a globalized high-tech economy. The conclusions then are also partial and based on the perspectives given at the time, and over time, from a self-selected group of people in an industry coping with turn-of-the-century fractures, ruptures, and continuities.

My interviews and analysis are based on a post-positivist theoretical orientation that questions the universality of facts and truths. In broad contrast to the neutral, objectivist stance of the positivist, a post-positivist employing qualitative research methods asserts her subjectivity and the partialness of her research (Lather 2004; Fine 1994). All research settings are permeated with inequalities and power relations that ultimately resolve themselves in favor of the researcher (Bloom 1996). I acknowledge the ways that both researcher and researched actively construct the stories and interpretations on which this final research text is based. However, I also accept responsibility for the production of the final text and my authoritative claim to knowledge about this industry (Harrison, MacGibbon, and Morton 2001).

All informants' names have been changed and identifying characteristics have been eliminated. All interviews were taped with the permission of the respondents and were transcribed. The interview questions were loosely structured to cover the interviewees' backgrounds and experiences in the antivirus industry, a description of their jobs, its challenges and rewards, and their definitions and attitudes toward other job categories within the industry. Questions also focused on the variously occurring current world and industry events and corresponding (re)definitions of threat and security that accompanied them.

All interviews were analyzed applying the principles of grounded theory such as familiarization, data exploration, reflection and data sense making, and linking of emerging patterns (Easterby-Smith, Thorpe, and Lowe 1991). Using the above typology, the processes, the common as well as differing practices, and espoused industry values were identified.

The stories I have chosen to use to illustrate my analysis represent some moments in an evolving engagement with individuals negotiating changes in their working lives on the high-tech edge of a continually transforming information economy. Their ongoing negotiations are always contextual and contingent, and a major aim of this book is to explore some of that complexity in relation to computer security at the turn of the twenty-first century. Of course the researcher has the ultimate control and authority over the text she produces; it is her interpretations, her choices of material, and her representations of others' stories that prevail in any written work she produces. What follows, then, is my representation of the research stories I collected during the six years of contact with the antivirus industry.