Introduction

DEFINING CYBERSECURITY

The Merriam-Webster dictionary defines the term *cybersecurity* as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack." The Oxford English Dictionary (OED) offers a similar definition, describing cybersecurity as "security relating to computer systems or the internet, esp. that intended to protect against viruses or fraud." Those definitions, and particularly the latter, call attention to the complex and multifaceted nature of cybersecurity, which by the third decade of the twenty-first century had come to encompass the protection of computers, mobile devices, networks, websites, cloud services, and other computer and internet-connected technologies from a wide range of cyberattacks.

This volume takes a broad view of the field of cybersecurity, presenting entries that cover not only technologies and practices used to enhance computer security, such as encryption and the zero trust security model, but also the underlying hardware, software, and internet technologies. Additional entries deal with common cyberattacks and cybercrimes, notable computer viruses and hacking incidents, social issues such as doxing and cyberbullying, and geopolitical topics such as cyberwarfare and cyberterrorism. Designed to provide a strong understanding of the importance of cybersecurity in the twenty-first century and the many directions from which security threats can emerge, this volume likewise features several entries on cybersecurity-related professions that will benefit students or adult career-changers interested in entering this rapidly evolving and increasingly critical field.

HISTORY

While Merriam-Webster states that the term cybersecurity dates back to 1989, and the OED dates the term to 1990, the concept of cybersecurity-and the awareness of a need for it-dates back quite a bit farther, having arisen alongside the development of computers. A more commonly used term during the early years of cybersecurity was computer security; beginning in 1972, for instance, the US National Bureau of Standards (later known as the National Institute of Standards and Technology, or NIST) became home to a program dedicated specifically to computer security research.

From the early days of computers, efforts to increase the capabilities of computer technology were often accompanied by corresponding attempts to identify vulnerabilities in computer systems and potentially to exploit them, either for malicious purposes, for comedic purposes, or simply out of curiosity. Over the years, the field of cybersecurity was increasingly complicated by the development of new technologies, including the Advanced Research Projects Agency Network (ARPANET) and, eventually, the publicly accessible internet and World Wide Web. The emergence of the latter technologies enabled everyday people to gain access to the internet and communicate with one another regardless of location. That change resulted in countless positive developments, but it also made cybersecurity a more pressing concern. The internet allowed for the rapid spread of viruses and malware, which could at times be obvious to the user and at other times could infect a computer or system without the user's knowledge. As a result, researchers and technology companies turned their attention toward developing new means of detecting and combating cybersecurity threats, including programs capable of scanning computers for malicious software, firewalls used to filter or block incoming traffic, advanced user-authentication protocols and security models, and many more innovations. Likewise, organizations

increasingly recognized the need to take preventive measures well before a computer system could be compromised. Such measures included penetration testing, a longstanding means of testing computer systems for vulnerabilities, as well as the development of automated systems capable of identifying vulnerabilities to be addressed.

Efforts to monitor and address cybersecurity concerns in a proactive manner proved to be of vital importance by the third decade of the twenty-first century, by which point the number and variety of computerized and network-connected devices in use had increased dramatically. In addition to traditional computers and networks, such devices had come to include tablet computers, mobile devices such as smartphones, wearable devices such as smartwatches, internet-connected appliances, smart speakers, smart thermostats, and a host of other items that had become part of everyday life for many in the United States and elsewhere. While offering a host of benefits in areas such as entertainment and home automation, each category of device offered its own potential vulnerabilities that could be exploited by bad actors, and cybersecurity initiatives were required to expand their reach in order to ensure the security of such devices. The emergence of technologies such as artificial intelligence (AI) and machine learning likewise had implication for cybersecurity during that period. In some cases, such technology was beneficial to the field; AI technology, for example, was being used to develop automated intrusion detection systems and other valuable cybersecurity tools. At the same time, AI technologies also represented potential security risks, as they could possibly be incorporated into malware or otherwise used to violate the security of computers, networks, and devices.

CYBERSECURITY IN BUSINESS

Though applicable to nearly all spheres of twenty-first-century life in the United States, cybersecurity is of particular concern in the business world. Businesses in all industries are at risk of experiencing a cyberattack; according to a worldwide report published by the statistics firm Statista, the industries most plagued by cybercrime incidents between 2021 and 2022 included the public administration, information, finance, professional, healthcare, education, entertainment, and retail industries. In addition to targeting businesses within varied fields, cyberattacks can come in numerous forms. According to Statista, the most common cyberattack US companies experienced during the year 2022 was network intrusion, which represented 45 percent of that year's business-focused cyberattacks. Business email compromise made up 30 percent of the attacks, while other, less-common types of attacks included inadvertent disclosure, intentional disclosure, and account takeover, among others.

Cyberattacks against businesses may be carried out for a variety of purposes. One of those is corporate espionage, in which individuals or groups attempt to access computer systems owned by a company in order to steal trade secrets, access financial data, or otherwise obtain internal information that would give another company a competitive advantage. In other attacks, the true target is not the company itself but the customer or user information that is stored within the company's computer system. In some cases, businesses may store valuable information such as credit card numbers or banking details, which bad actors could go on to exploit or sell to other malicious individuals. A prominent example of such an attack, reported to the public in 2018, was the breach of Marriott International's Starwood database. In that incident, customer information-including credit card numbers—for more than 300 million hotel guests was accessed by hackers, and those guests' identities and financial well-being were thus put at risk. In some cases, cyberattacks against businesses are politically motivated. One such incident took place in 2014, when

A

Aadhaar Hack

ABSTRACT

The Aadhaar hack of 2018 was a cyberattack targeting India's controversial national biometric identification system, Aadhaar. Several major leaks of personal data were reported, though denied by the Indian government. Cybercriminals also created a software patch, sold online, allowing individuals the ability to generate fake Aadhaar profiles.

BACKGROUND

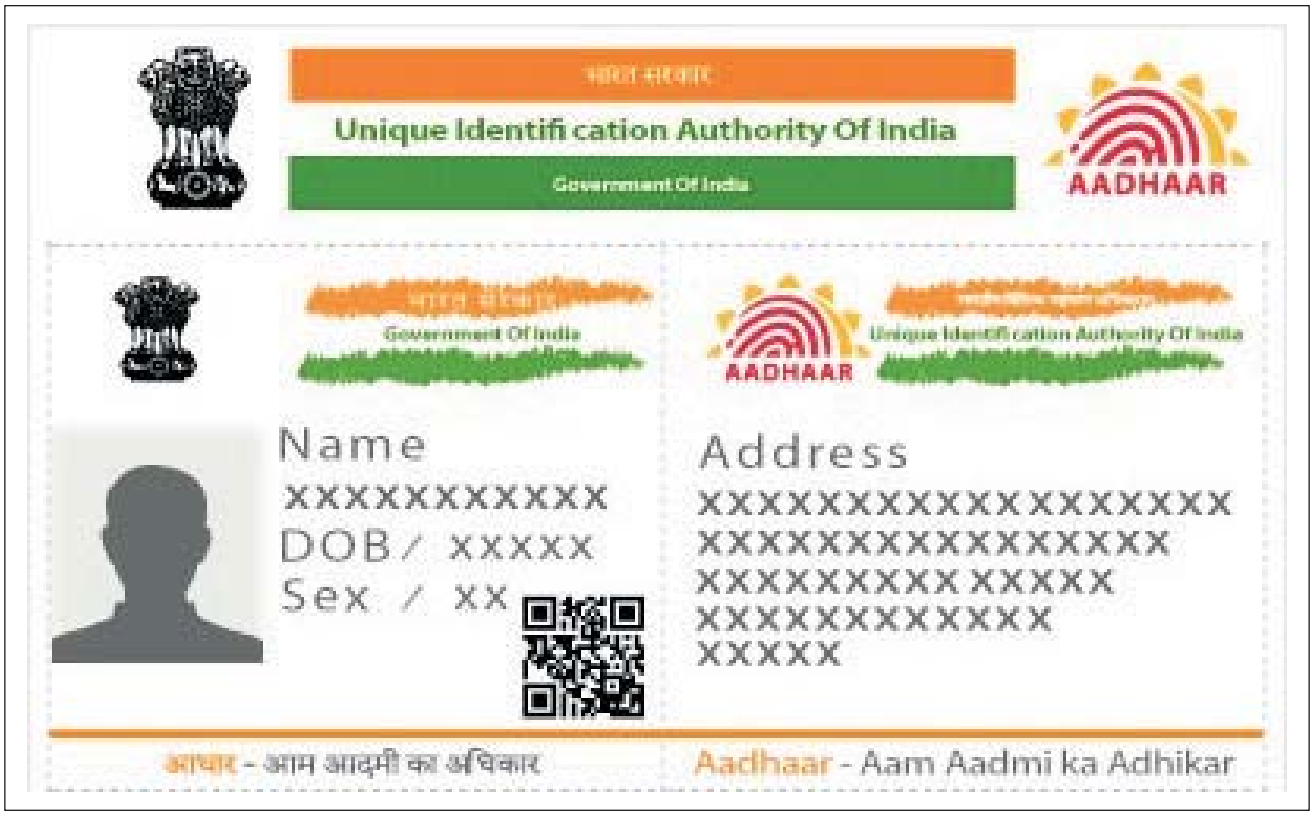
Aadhaar is a biometric identification system introduced by the Indian government in 2009. It provides registered users—who can be any Indian resident—with a unique twelve-digit number linked to the individual's biometric data, including photographs, iris scans, and fingerprints. The system is managed by the Unique Identification Authority of India (UIDAI), which was established specifically for the program.

When first developed, the Aadhaar system was presented as a voluntary service that would enhance security and streamline the process of applying for various consumer and citizen services. The system became controversial with the National Identification Authority of India bill, revealed in 2010, which essentially sought to make registration with Aadhaar necessary to obtain government services. An increasing number of private companies also linked receipt of service to Aadhaar accounts, despite a lack of legal backing for such a requirement. In November 2012 a group of activists filed suit in the Indian Supreme Court challenging the constitutionality of Aadhaar, and subsequent rulings suggested that Aadhaar could not be made mandatory. Despite this, in 2016 a bill providing a legal framework for the system was passed, and government agencies began moving toward requiring Aadhaar registration for things such as scholarships, maternity benefits, and meal programs.

The legal debate over the constitutionality of the Aadhaar project was accompanied by public debate over possible security concerns. Some criticisms took issue with the program as a whole. For example, it was argued that, because biometric data cannot be changed, identity theft through the Aadhaar system could leave victims without any recourse to change the stolen data. Reports also emerged that the program had, in some cases, made it more difficult for those in need to access services due to inflexibility and bureaucratic impediments. Several individuals reportedly died when denied access to food rations, pensions, and hospital treatment because of Aadhaar problems. Meanwhile, complaints of general security flaws and data leaks mounted. Two notable examples came in 2017, when one telecommunications company allegedly leaked Aadhaar data on as many as 120 million customers and another reportedly opened bank accounts for customers without their consent after gathering Aadhaar biometric data to authenticate mobile phone accounts. However, the UIDAI maintained that the system was safe and secure.

OVERVIEW

More security concerns emerged in 2018. That January, an investigative report by journalist Rachna Khaira published in the Indian newspaper the *Tribune* alleged that hackers communicating through



A computer-rendered sample of Aadhaar card. Image by PageImp, via Wikimedia Commons.

the WhatsApp messaging application were selling access to the personal data of all the more than 1 billion registered Aadhaar users for just Rs 500 (less than US$10). Compromised information included names, photographs, addresses, phone numbers, and emails, although not biometric information. The report also found that software could be purchased allowing anyone to print Aadhaar cards. Representatives of the UIDAI and the ruling Bharatiya Janata political party claimed that the *Tribune* report was false and that there had been no unauthorized data breach.

In March 2018 a separate data leak was reported. Due to a lapse in a system run by the state-owned utility company Indane, it was allegedly possible to download private information for Aadhaar users including names, unique twelve-digit identity numbers, and information about services to which an individual was connected. The breach was discovered by security researcher Karan Saini, who warned that anyone registered for the system was vulnerable to having their data stolen. UIDAI again denied the validity of the report and claimed that there had been no data breach, though after media reports circulated, the vulnerable system was taken offline.

Another major hack of the Aadhaar system was reported in September 2018 by Khaira, Aman Sethi, and Gopal Sathe for *HuffPost India*. After a three month-long investigation, the report publicized the existence of a software patch, available for sale through WhatsApp for a price of Rs 2,500 (approximately US$35), that allowed any individual to generate Aadhaar numbers and integrate them into the system. According to the investigation, five security and software analysts confirmed the patch's function and authenticity. The patch allowed individuals to

Further Reading
Cormen, Thomas H. *Algorithms Unlocked*. MIT Press, 2013.
Ferguson, R. Stuart. *Practical Algorithms for 3D Computer Graphics*. 2nd ed., AK Peters/CRC Press, 2013.
Fitter, Hetal N., Akash B. Pandey, Divyang D. Patel, and Jitendra M. Mistry. "A Review on Approaches for Handling Bezier Curves in CAD for Manufacturing." *Procedia Engineering*, vol. 97, 2014, pp. 1155–66.
Kamhoua, Charles A., Christopher D. Kiekintveld, Fei Fang, and Quanyan Zhu, editors. *Game Theory and Machine Learning for Cyber Security*. Wiley, 2021.
MacCormick, John. *Nine Algorithms That Changed the Future: The Ingenious Ideas That Drive Today's Computers*. Princeton UP, 2012.
O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
Parker, Matt. *Things to Make and Do in the Fourth Dimension: A Mathematician's Journey through Narcissistic Numbers, Optimal Dating Algorithms, at Least Two Kinds of Infinity, and More*. Farrar, 2014.
Rychagov, Michael N., Ekaterina V. Tolstaya, and Mikhail Y. Sirotenko, editors. *Smart Algorithms for Multimedia and Imaging*. Springer Cham, 2021.
Sarkar, Jayanta. *Computer Aided Design: A Conceptual Approach*. CRC Press, 2017.
Schapire, Robert E., and Yoav Freund. *Boosting: Foundations and Algorithms*. MIT Press, 2012.
Steiner, Christopher. *Automate This: How Algorithms Came to Rule Our World*. Penguin, 2012.
Valiant, Leslie. *Probably Approximately Correct: Nature's Algorithms for Learning and Prospering in a Complex World*. Basic, 2013.

Android OS

ABSTRACT
Introduced to consumers by the technology company Google, the Android operating system (OS) debuted on the mobile-device market with the release of the T-Mobile G1 (or HTC Dream) smartphone in 2008. The OS quickly became a major competitor in that market and as of 2023 was the dominant mobile OS both in the United States and worldwide.

BACKGROUND
Mobile computing is the fastest-growing segment of the tech market. As pricing has become more affordable, developing nations, particularly in Africa, are the largest growing market for smartphones. With smartphones, users shop, gather information, connect via social media such as X (previously Twitter) and Facebook, and communicate—one of the uses more traditionally associated with phones.

By far the most popular operating system running on mobile phones is Android. Since its launch in 2008, Android has far and away overtaken the competition, which has included popular operating systems such as Apple's iOS. By mid-2023, more than 3 billion Android devices were active worldwide.

OVERVIEW
Android came about amid a transformative moment in mobile technology. Prior to 2007, slide-out keyboards mimicked the typing experience of desktop personal computers (PCs). In June of that year, Apple released its first iPhone, forever altering the landscape of mobile phones. Apple focused on multitouch gestures and touch-screen technology. Nearly concurrent with this, Google's Android released its first application program interface (API).

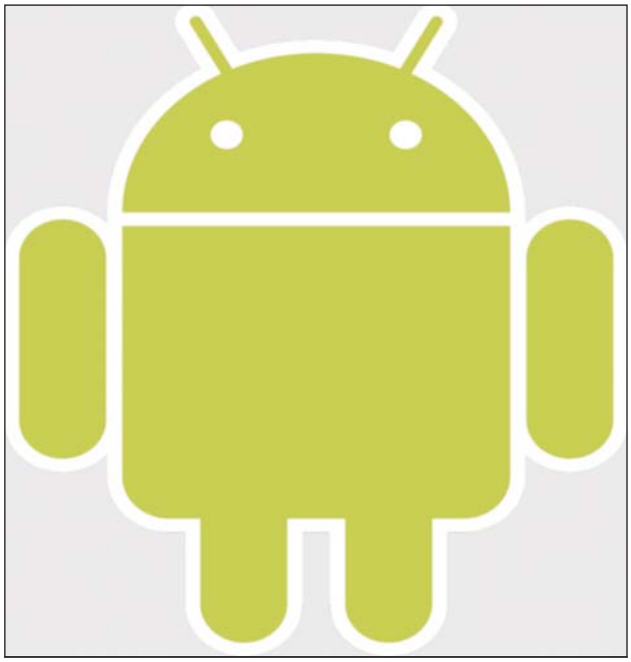
The original API of Google's new OS first appeared in October 2008. The Android OS was first installed on the T-Mobile G1, also known as the HTC Dream. This prototype had a very small set of preinstalled apps, and as it had a slide-out QWERTY keyboard, there were no touch-screen capabilities. It did have native multitasking, which Apple's iOS did not yet have. Still, to compete with Apple, Google was forced to replace physical keyboards and access buttons with virtual onscreen controls. The next iteration of Android shipped with the HTC Magic and was accompanied by a virtual keyboard and a more robust app marketplace. Among the other early features that have stood the

test of time are the pull-down notification list, home-screen widgets, and strong integration with Google's Gmail service.

One later feature, the full-screen immersive mode, became quite popular as it reduces distractions. First released with Android 4.4, "KitKat," in 2013, it hides the navigation and status bars while certain apps are in use. It was retained for the release of Android 5.0, "Lollipop," in 2015, as well as for subsequent releases.

ANDROID CHANGES AND GROWS

Both of Google's operating systems—Android and its cloud-based desktop OS, ChromeOS—are based on the free open-source OS Linux, created by engineer Linus Torvalds and first released in 1991. Open-source software is created using publicly available source code. The open-source development of Android has allowed manufacturers to produce robust, affordable products that contribute to its widespread popularity in emerging and developing markets. This may be one reason why Android has captured many more new users than its closest rival, Apple's iPhone operating system (iOS). This strategy has kept costs down and has also helped build Android's app marketplace, the Google Play Store, which offers millions of apps, many free of charge. As of 2023, Android made up more than 70 percent of the global mobile operating system market.



Android logo. Image by Google Inc., via Wikimedia Commons.

This open-source development of Android has had one adverse effect: the phenomenon known as "forking," which occurs primarily in China. Forking is when a private company takes the OS and creates their own products apart from native Google services such as email. Google seeks to prevent this loss of control (and revenue) by not supporting these companies or including their apps in its marketplace.

Google's business model has always focused on rapid iteration. By contrast, rivals such as Microsoft and Apple have had a far slower, more deliberate pace due to hardware issues. One benefit of Google's faster approach is the ability to address issues and problems in a timely manner. A drawback is the phenomenon known as "cloud rot." As the cloud-based OS grows older, servers that were once devoted to earlier versions are repurposed. Since changes to the OS initially came every few months, apps that worked a month prior would suddenly lose functionality or become completely unusable. Later Android updates have been released on a timescale of six months or more.

Throughout many of Android's first years of existence, new versions of the OS were known by both version numbers and dessert-themed code names, such as Cupcake (version 1.5), Ice Cream Sandwich (version 4.0), and Oreo (versions 8.0 and 8.1). Following the release of Pie (version 9), however, Google moved away from that naming scheme with Android version 10, released in 2019. Android version 11, released as a public beta in June of 2020, was likewise referred to by its version number rather than by a themed nickname. Google

I

Identity Theft

ABSTRACT

Identity theft is among the most frequent consumer complaints reported to the Federal Trade Commission (FTC). Though a relatively new crime, it is often perpetrated through various familiar crimes, such as forgery; counterfeiting; and check, credit, and computer fraud. The National Crime Victimization Survey (NCVS) defines identity theft as (1) unauthorized use or attempted use of an existing account; (2) unauthorized use or attempted use of personal information to open a new account; and (3) misuse of personal information for a fraudulent purpose.

BACKGROUND

The term "identity theft" did not appear in federal laws until 1998. Prior to 1998, crimes related to identity theft were charged under late nineteenth-century false personation statutes. False personation refers to impersonating another individual, such as a police officer or other official, and does not have the financial connotations that the term "identity theft" now carries. The late 1990s saw a staggering increase in reporting on identity theft. TransUnion, one of the three major national credit bureaus, reported that the total number of identity theft inquiries to its fraud department rose from about 35,000 in 1992 to almost 523,000 in 1997. While these numbers did not indicate what percentage of the inquiries were actual identity thefts, they did indicate a growing concern on the part of consumers. In 1998, Congress responded to these growing numbers and passed the Identity Theft and Assumption Deterrence Act, 112 Stat. 3007, making identity theft a federal crime. It expanded 18 U.S.C. § 1028, "Fraud and related activity in connection with identification documents," to make it a federal crime to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

According to the Office for Victims of Crime, the Identity Theft and Assumption Deterrence Act accomplished four things:

1. Identity theft became a separate crime against the person whose identity was stolen. Previously, victims were defined as those who had financial losses, so the emphasis was on banks and other financial institutions rather than on individuals.

Image via iStock/pressureUA. [Used under license.]

N

Network and Computer Systems Administrator

ABSTRACT

Network and computer systems administrators design, build, and maintain computer systems. They work closely with computer security professionals to ensure the security of the computer networks and systems under their purview. Students aspiring to enter the profession should pursue studies in subjects such as computer science and networking.

BACKGROUND

Network and computer systems administrators build, design, and maintain computer systems for businesses and organizations. In addition to constructing local area networks (LANs) and wide area networks (WANs), systems administrators also support and maintain organizational internet systems and related infrastructure. Any computer problems or computer-related questions posed by employees of a company are traditionally handed by system administrators or their staff.

Network and computer systems administrators work closely with computer security professionals and other senior administrative staff to ensure that the computing needs of a business or organization are in place and are functioning properly. They also assist fellow employees with computer-related projects and routine maintenance.

OVERVIEW

Network and computer systems administrators work predominantly in business, administrative, and office settings. They are employed by large companies and often have their own workspaces adjacent to facilities that house computer servers and other hardware relevant to network systems. Network and computer systems administrators are often required to strike a balance between work conducted on their own and collaborative work with other staff members, which can include system maintenance, demonstrations of hardware and software capabilities, or developing and implementing new technologies with fellow staff.

The field of computer administration traditionally attracts professionals with technological skills who have a lengthy history of involvement with and demonstrated passion for computing, be it through academic study, personal interest, or professional development. Most network and computer systems administrators develop an interest in working with and around computers at a young age and are intricately familiar with modern developments in personal and business computing. They may also enter the discipline through previous exposure to programming, software development, or any one of numerous disciplines related to computer science.

DUTIES AND RESPONSIBILITIES

Network and computer systems administrators divide their time between monitoring and maintaining existing computer systems, devising new computer and network technologies with other staff, and assisting different departments and fellow employees with their computing and networking needs through maintenance, troubleshooting, and conducting training seminars.

Network and computer system administrators are traditionally the primary individuals

Y

Y2K Crisis

ABSTRACT

In the years leading up to the year 2000, some computer experts warned that the longtime practice of rendering years in a two-digit format could cause problems within computer systems, prompting global efforts to mitigate the effects of the so-called Y2K bug as well as widespread public concern. Despite predictions of disaster to businesses, governments, and public services, the worldwide transition to the year 2000 caused few problems for computers, thanks to extensive preparations.

BACKGROUND

Across North America and around the world, people waited nervously as midnight approached on December 31, 1999. Many wondered whether predictions of doom about the year 2000 computer transition, popularly called the Y2K (for "year 2000," with *k* representing the Greek *kilo* for "thousand") problem or the millennium bug, would prove correct: would power and water supplies fail, food distribution be disrupted, the economy begin to disintegrate, nuclear missiles launch accidentally, and widespread civil disturbances begin as computers and computer networks failed everywhere? No one was completely sure how to answer these questions, even though massive efforts to avert any possible problems occupied governments and businesses throughout the late 1990s.

A definitive answer was apparent within days after January 1, 2000, came and went: There were no disasters. Some computer problems did occur on New Year's Day and afterward, but they were so few, so inconsequential, and so easily corrected that even the most optimistic experts were surprised.

The story of the Y2K transition problem began with the development of commercial computing. In 1957, Rear Admiral Grace Murray Hopper invented a programming language called FLOW-MATIC, the first to be based on English in order to make computers easier for businesses to use. FLOW-MATIC formed the basis for COBOL, the name of which derived from "common business-oriented language." The principal data storage device of the times was the eighty-column punch card. To conserve space, COBOL used only six digits to represent any given calendar date—two each for the month, the day, and the year, as in "04/15/53" for April 15, 1953. This shortcut dating method saved as much as twenty dollars in the production of a date-sensitive record, so it was an important way of economizing as businesses grew dependent on computers.

Computer scientists, led by Robert Bemer, one of COBOL's developers, warned that using only two digits for each year designation would later cause problems and argued for a four-digit style. However, the desire of businesses to minimize their immediate expenses overwhelmed such objections. When International Business Machines Corporation (IBM) designed its System/360 mainframe computer (marketed in 1964), it incorporated the COBOL two-digit year format. That computer, and its dating style, became the industry standard. Bemer again published warnings about the dating problem in 1971 and 1979, but his protests stirred little interest and no change. To most businesses and government agencies the heart of the danger—the arrival of the

A Best Buy sticker from 1999 recommending that their customers turn off their computers ahead of midnight. Image via Wikimedia Commons. [Public domain.]

year 2000—seemed too far away to worry about at the time.

In 1993, Peter de Jager, a Canadian computer engineer, published an article with the alarming title "Doomsday 2000" in *Computerworld*, a magazine aimed at technology managers. In that article and subsequent lectures, de Jager argued that the Y2K bug could initiate massive disruptions and plunge the economy into a recession. Computers, he pointed out, would read a date such as "01/01/00" as "January 1, 1900," because there was no provision for numbers 2000 and higher in their software, and computer-processed date-sensitive information was fundamental to national infrastructures. There were already signs that he was right: That same year, a US missile warning system malfunctioned when its computer clocks were experimentally turned forward to 01/01/00.

During the next seven years, other glitches turned up sporadically during testing. At the same time, with gathering momentum, attempts were under way to remedy the date problem. In 1996, Senator Daniel Patrick Moynihan of New York held committee hearings on the Y2K bug and directed the Congressional Research Service to study the potential problem. The report produced as a result helped to convince President Bill Clinton to establish the President's Council on Year 2000 Conversion, directed by John A. Koskinen, in 1998. Koskinen oversaw programs to adjust the software used by government agencies. The US government also ordered many organizations essential to the economy, such as stock brokerages, to fix the problem—that is, to "become Y2K compliant"—by August 31, 1999.

Despite initial skepticism about the true seriousness of the Y2K problem, big companies soon undertook remediation efforts of their own. Most employed one or more of three basic methods, termed "windowing," "time shifting," and "encapsulation." Windowing, the most common, entailed