The Dark Side of Technology

Chris Wellisz

The benefits of the digital age are tempered by the risks

DIGITAL technology has given us comforts and conveniences that could scarcely be imagined even a generation ago. The Internet saves students and scholars hours of tedious research in libraries and enables instantaneous visual, oral, and written communication at virtually no cost. Anyone with a smartphone can use GPS to avoid getting lost in an unfamiliar city or find the nearest Starbucks. There's online shopping and banking for consumers and computer-aided diagnostics for doctors. Such are the wonders of the digital era that scholars Erik Brynjolfsson and Andrew McAfee have dubbed it "The Second Machine Age," declaring that computers are doing for our mental capacity what the steam engine did for muscle power.

But there are drawbacks to progress. Some critics of the digital era lament the power of a few giant social media outlets to shape public opinion. Others raise serious concerns about pathologies such as cyberbullying and Internet pornography. And there are those who worry about the potential loss of privacy, and the danger to civil liberties, at a time when practically every movement, phone call, and email message leaves a digital trail that can be exploited by a nosy neighbor or an intrusive government.

While these are all legitimate concerns, they are impossible to quantify. Yet some aspects of digital technology do impose measurable costs on companies and economies that offset at least part of the efficiency offered by the second machine age.

Hackers can take control of cars or shut down an electric grid. Cyberthieves steal personal information and use it to drain bank accounts or make fraudulent online credit card purchases. Email, mobile phones, and social media, while revolutionizing communication, take a toll on the productivity of office workers mesmerized by their Twitter feeds or addicted to instant messaging.

Cybersecurity Risks

When a group of former officers from Unit 8200, Israel's signals intelligence corps, set out to start a private cybersecurity business, they agreed that Internet-connected cars were the next big thing.

"They just looked at what was going on in the markets and they thought, OK, there are going to be millions of connected cars on the road quite soon," said Yoni Heilbronn, vice president for marketing at Argus Cyber Security Ltd.

Three years later, Tel Aviv–based Argus has added offices in Germany, Japan, and the United States. The company is flourishing as stories about hackers taking control of cars—not to mention accidents, though not hacking, linked to the autopilot feature of Tesla Motors vehicles—focus public attention on the need to improve automotive cybersecurity.

Welcome to the Internet of Things—objects connected to a network that allows them to send and receive data—which is expanding to include devices ranging from diagnostic equipment in hospitals to coffeemakers and other home appliances. This year, the number of Internet-enabled devices will expand 30 percent to 6.4 billion, predicts Gartner Inc., a leading information technology research and advisory firm. Worldwide spending on security for the Internet of Things will jump 24 percent to $348 million.

A connected world offers new opportunities for cybercriminals to gather personal information that can be used for fraudulent transactions or for ransomware—malicious software that can immobilize devices or encrypt data and demand money in return for a decryption key.

"It's a new point of access for the fraudsters," says Bradley J. Wiskirchen, chief executive officer of Kount, an Internet security firm based in Boise, Idaho. "They don't necessarily have to hack into my computer if they can hack into my printer or refrigerator and collect data on me."

Hacking into Internet-enabled household devices is often easy for the simple reason that they have little, if any, built-in security. Companies like Palo Alto, California–based Nest Labs, a maker of smart appliances with sophisticated security features, are the exception.

"A lot of the others, they get some open-source software and they bolt it onto a device, and that's it—there's not really a lot of thought for security," says Chris King, a vulnerability analyst at CERT Coordination Center, part of Carnegie Mellon University's Software Engineering Institute. Even toys like the Wi-Fi–enabled Hello Barbie doll can be hacked.

The list of vulnerable devices is growing as the wired world expands. Hackers have shut down hospital diagnostic systems to extract ransom, King says. In western Ukraine last year, hackers took down a power grid, leaving more than 200,000 people without electricity. Cybervandals in Germany targeted a steel mill, causing massive damage to a foundry.

Cybercriminals gather personal information for fraudulent transactions or ransomware.

The specter of hackable cars is particularly scary because of the potential for deadly accidents. By 2020, about 250 million cars worldwide will have some form of onboard wireless connectivity, Gartner estimates.

Just about everything in a modern car—brakes, steering, tire pressure, lighting—is mediated by computerized controllers, which are connected to each other via a communication system, or "bus," that was invented 30 years ago, before the Internet age. The bus itself is inherently insecure, as are many of a car's other devices.

"A system that was never designed to be on the Internet is now connected, and suddenly it's vulnerable to all of these things the designers never thought of," says King.

Makers of automobiles and parts are taking the threat seriously and stepping up security measures after a pair of high-profile break-ins.

At Argus, researchers hacked into a device called Zubie, which monitors a car's performance and wirelessly delivers real-time data to the driver's smartphone via the cloud, along with maintenance alerts and tips on improving driving habits. The researchers were then able to control the car's steering, brakes, and engine. Argus informed Zubie of the vulnerability, which the company said it has since fixed.

Last year, Fiat Chrysler Automobiles announced a recall of 1.4 million vehicles after *Wired* magazine reported that researchers had used a laptop computer to seize control of a Jeep Cherokee via its dashboard computer.

"When you have cars that are connected, they will have to be protected," says Heilbronn at Argus. ■

Cybertheft

Magnus Carlsson was in his eighth-floor office overlooking a busy street in Bethesda, Maryland, when an email popped up on his computer. His boss, chief executive of the Association for Financial Professionals, needed help making a funds transfer.

But when Carlsson hit the reply button, an unfamiliar address appeared in his Outlook window. "I knew from the start it was a textbook scam," said Carlsson. He should know: part of his job as manager for treasury and payments at the global industry group representing finance executives is to warn members around the world of sources of financial fraud, including Internet scams.

The tactic he described, known as "business email compromise," is fast gaining favor among cybercriminals as

Cybertheft *(continued)*

a way to get company employees to make wire transfers to bogus suppliers or creditors, usually by mimicking an emailed order from a superior. In a survey of the association's members, 64 percent reported having been exposed to compromised business email.

Cybercriminals bent on causing mayhem could bring down the entire global financial system.

It's just one strand of an expanding global web of cyberfraud that includes tactics and tools with fanciful, if sinister-sounding, names—ransomware, spear phishing, Trojan horses. Cybercriminals are growing more sophisticated, active, and audacious by the day, going after high-profile game, including JPMorgan Chase & Co., British Airways, the Philippines' Commission on Elections, and the U.S. Internal Revenue Service, then moving down the corporate food chain to easier prey when the biggest organizations devote more resources to cybersecurity.

Cybercrime "is growing because it's so easy, and as more countries and companies come online, with just initial approaches to cybersecurity, they're easy targets," says James Andrew Lewis, a senior vice president at the Center for Strategic & International Studies in Washington, D.C., who has written extensively about cyberfraud. "Law enforcement is fabulously uneven across the planet. So if you're a smart hacker, you live in a country that's not going to enforce its laws."

Lewis estimates the global damage wrought by cybercrime at more than $500 billion a year—exceeding the gross domestic product of Sweden. That figure includes the value of stolen cash and intellectual property, the cost of repairing breaches, and the toll cybercrime takes on innovation, trade, and economic growth.

Financial firms offer a particularly tempting target, as the theft of $81 million from the central bank of Bangladesh this year showed. In that attack, hackers used the credentials of a bank employee to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York.

The financial loss was huge for a country like Bangladesh, but regulators worry about a far more serious risk: cybercriminals bent on causing mayhem could bring down the entire global financial system, triggering an economic meltdown to rival the crisis of 2007–08.

"It's about potentially denying market participants access to key parts of the plumbing of our markets," said Greg Medcraft, chairman of the Australian Securities and Investments Commission. "Cyberattacks are probably the next black swan event in the world."

A survey on threats to global financial stability, conducted by the Depository Trust & Clearing Corporation, showed that a plurality of respondents, 25 percent, put cybercrime at the top of the list. That figure is down from 46 percent last year, in part because financial institutions are investing in protective measures and also because other risks—such as a slowdown in Asia—have gained prominence.

Still, regulators aren't taking any chances. Payment and trade settlement systems, key components of the global financial system, should adopt plans to defend against and react to cyberintrusions and appoint an executive to oversee those plans, according to guidelines issued in June by the Bank for International Settlements and the International Organization of Securities Commissions.

Cybercrime is the second most common type of business crime after asset misappropriation, according to a PwC survey. But while 61 percent of CEOs said they were concerned about cybersecurity, only 37 percent of organizations reported having a response plan.

Internet crime falls into two broad categories. The first is monetizable break-ins, such as identity and payment card theft. The second is cyberespionage: theft of trade secrets, negotiating strategies, and product information.

The number of exposed identities jumped 23 percent last year to 429 million, according to Symantec Corporation's annual "Internet Security Threat Report." The actual number probably exceeded 500 million because many companies don't report breaches.

Following massive data breaches at companies such as health insurer Anthem Inc. and digital marketplace eBay Inc., just about every identity in the United States has been exposed, reckons Bradley J. Wiskirchen, chief executive officer of Kount, a leading provider of digital risk-management solutions based in Boise, Idaho.

"Virtually everyone has been compromised," Wiskirchen says. Stolen identities are traded on a burgeoning electronic black market, where sophisticated international merchants sell their wares on websites to rival the world's best retailers, complete with money-back guarantees, bulk discounts, and tutorials.

The average cost of a data breach has risen to $4 million from $3.79 million, according to a recent survey of 383 companies in 12 countries by IBM and the Ponemon Institute. Breaches were most likely to occur in Brazil and South Africa, least likely in Australia and Germany.

The 2014 attack on New York-based JPMorgan Chase & Co. exposed 83 million customer records, including names, email and postal addresses, and phone numbers. It was the largest attack on a financial institution in U.S. history, and while the bank didn't say how much the breach cost, it announced plans to spend an additional $250 million a year on security measures.

The cost of intellectual property theft is harder to estimate, but the economic toll may be larger. Theft of intellectual property ranging from paint formulas to rockets reduces the profits to be made from innovation, says Lewis at the Center for Strategic & International Studies. "People are incentivized by financial return to invent new things, and if they don't get that financial return, they'll do something else," Lewis says.

The result: underinvestment in new technology and the loss of jobs and economic growth. Even the countries that benefit lose out in the long run because relying on stolen technologies prevents them from learning how to develop their own. "The whole world grows more slowly because of this," Lewis says.

Lewis's estimate of the overall cost of cybercrime, including intellectual property theft, is an average of 0.5 percent of GDP globally. In high-income countries, where innovation plays a bigger economic role, the loss may be as high as 0.9 percent of GDP. For developing economies it's closer to 0.2 percent. All this is driving dramatic growth in demand for cybersecurity services, which will expand to $170 billion in 2020 from $75 billion last year, according to a forecast by Cybersecurity Ventures, a research and market-intelligence firm.

Kount's annual increase in transaction volume is in the triple digits, "and we have barely scratched the surface of the potential opportunities," Wiskirchen says. "Unfortunately, I'm in a very big growth industry." ■

Digital Distraction

Laurie Voss recalls the time when, as a young Silicon Valley programmer, he was given a month to complete an exceptionally dull and unrewarding project. "It was a thankless task," Voss recalls. "I spent a lot of time on Twitter that month."

To Voss, who is now chief technology officer at his own start-up, NPM, tweeting on the job is the 21st century version of a phenomenon as old as the Dead Sea scrolls: procrastination.

Digital distraction and its cousin, information overload, are taking a growing toll on productivity.

The latest apps and gadgets certainly offer new and irresistible ways to waste time. In cubicles the world over, office workers are bombarded by a relentless stream of blinks and beeps from mobile phones, computers, and tablets. Digital distraction and its cousin, information overload, are taking a growing toll on productivity as new technologies spread across the globe and the knowledge economy expands.

Three in four U.S. employers say that two or more hours a day are wasted because employees are distracted, according to a survey released in June by CareerBuilder, a human resources consulting company based in Chicago.

Employers cited mobile phone use and texting as the biggest time killers, followed by the Internet, office gossip, and social media. Consequences include lower-quality work, reduced morale among workers who must pick up the slack for distracted colleagues, and missed deadlines.

Nathan Zeldes, a Jerusalem-based organizational consultant, identifies email as the biggest waste of time, and he blames employers for failing to limit its use. An office worker can expect to get between 50 and 300 job-related messages a day, he says.

"There's no way you can read or process that intelligently," Zeldes says. "And it keeps coming in."

Useless email and unnecessary interruptions cost the average knowledge worker one day a week in lost productivity, Zeldes says, citing a study he conducted in 2006 while working as an engineer for computer chip maker Intel Corporation. That comes to about $1 billion a year for a company with 50,000 workers.

Email is difficult to resist, Zeldes says. Employees feel compelled to read and respond to messages at any time of the day or night for fear of missing out on important communications or out of a desire to impress coworkers or the boss.

"I liken it to the prisoner's dilemma," he says. "Everybody would love to send less email and go home early. But nobody dares to be the first to cut back."

Gloria Mark, a PhD psychologist who teaches at the Department of Informatics at the University of California, Irvine, uses a gambling analogy to describe how people are conditioned to use email.

"I call it the Las Vegas phenomenon," she says. A slot machine player is rewarded at random intervals by an occasional payout. The prospect of another payout is enough to keep the player pulling the handle.

"Randomly reinforced behavior is the hardest behavior to extinguish," Mark says.

In a 2012 study, Mark found that workers can concentrate on a computer screen only for an average of 75.5 seconds before switching tasks. By last year, that number was down to 47 seconds.

Workers and their bosses have deployed a variety of strategies to combat distraction and overload. Many set aside specific chunks of time to deal with email and ignore their inboxes the rest of the day.

"I spend a lot of time optimizing my email life," says Voss at NPM. His solution is to "ruthlessly filter" out any message "that's repetitive, anything that's routine, anything that I don't need to know about or deal with."

"Turn off all notifications. Don't let things pop up in your face," counsels Cliff Williams, senior designer for Nextdoor, a San Francisco–based company that calls itself a "private social network for your neighborhood."

Still, Williams concedes that avoiding distractions is a "constant struggle."

"It's kind of like losing weight," he says. "You lose some and you gain some back." ■

Chris Wellisz is a financial journalist based in Washington, D.C.