strategy+business

A Better Way to Battle Malware

Emulating the methods used to transform production quality could clean up the Internet — and might even pay for itself.

BY TIM LASETER AND ERIC JOHNSON

pwc | strategy&
Formerly Booz & Company

A Better Way to Battle Malware

Emulating the methods used to transform production quality could clean up the Internet — and might even pay for itself.

by Tim Laseter and Eric Johnson

Pundits proclaim the miraculous power of the Internet. It ushered in a "New Economy" and created a "flat world." We even refer to our progeny as members of the "Net generation." More than 5 billion devices are now connected to the Internet, accessing or serving up 500 billion gigabytes of information and transmitting 2 trillion e-mails per day. The decentralized structure of the Internet has ushered in a new level of worldwide connectivity, enabling product development teams to collaborate across the globe, banks to reach people in the developing world, and middle-aged divorcees to find their high school sweethearts.

But this increasing connectivity has a dark side. Although spam recently dropped to its lowest levels in years, it still accounts for fully 75 percent of global e-mail traffic, 1.5 trillion messages per day. Every minute produces 42 new strains of malware — short for *malicious software* — including viruses, worms, and Trojans. An average of 8,600 new websites with malicious code are created each day, and 50 percent of results for the top 100 daily search terms lead to malicious sites. Until last year, 4.5 million computers were under the control of a single botnet that used these computers for nefarious means and disguised the malware presence by minimizing its impact on the computer's performance and by eliminating other malware attempting to attack its network of computers. It was malware with its own antivirus software.

How then can we improve the safety and reliability of the Internet, an increasingly critical, shared global resource? As business leaders, managers, and individuals, we place our trust in the technical wizards in the back room who run the servers and write the code. We install antivirus software as directed and update other programs when told (at least when we have time to restart our computers). But the results suggest this isn't enough.

The best way to drive the kind of improvement in information security that would really clean up the Internet, we believe, is for corporate leaders and computer security professionals to reflect on the lessons of the manufacturing quality movement of the late 20th century. The methods employed by quality professionals — Six Sigma is an example — raised the visibility of the "cost of quality" and triggered a fundamental change in the philosophy of error prevention. Similarly, information security needs to be raised to the boardroom level, and the computer experts need to come out of the back rooms to engage all users to address the challenge. By doing this, we could collectively reduce malware to a level that does not put Internet-enabled advances at risk.

A Short History of Malware

The origins of security concerns and computer malware are as old as the computer itself. In the earliest days, when computers were *wired* rather than *programmed,* companies generally secured these physical (albeit not virtual) behemoths in locked offices and buildings to prevent unauthorized access.

In 1949, even before computers evolved to clearly separate

hardware and software, the leading theoretician of computing, John von Neumann, delivered a lecture on the "theory and organization of complicated automata," which laid the foundation for both positive and negative impacts of software. His *Theory of Self-Reproducing Automata* (University of Illinois Press), published posthumously in 1966, explicitly addressed the idea of self-replicating code. In fact, in 1980, Arpanet, the U.S. Department of Defense–sponsored predecessor of the Internet, shut down thanks to an accidentally propagated status message. In 1983, Fred Cohen intentionally developed a program that could "'infect' other programs by modifying them to include a possibly evolved copy of itself," as he put it in his thesis, on the then-popular VAX family of minicomputers, which preceded the advent of personal computers. Drawing upon a biological analogy, he called the new program a *virus*.

Taking a step beyond viruses, *worms* — the now-common term coined by John Brunner in his 1975 novel, *The Shockwave Rider* (Harper & Row) — began wriggling into the security landscape in the late 1980s. Whereas viruses simply infect a computer program (or files), worms go further by copying themselves between systems. Using security flaws known as back doors, worms propagate without the help of a careless user. The 1988 Morris worm penetrated and expanded on both DEC and Sun machines and infected about 6,000 of the 60,000 hosts on the nascent Arpanet. (Robert Morris, the worm's creator, was the first person to be prosecuted and convicted under the 1986 Computer Fraud and Abuse Act.)

A critical point in the evolution of the Internet — and the rising risk of information security — came with e-mail, the first sanctioned commercial use of the Internet. History credits Ray Tomlinson with inventing e-mail for Arpanet in 1971, but CompuServe, MCI Mail, and OnTyme first offered interconnected e-mail services to the masses in 1989. That same year marked the introduction of hypertext and the World Wide Web. Suddenly, the increasingly ubiquitous personal computers could share information through simple dialup services. By 1991, the number of host sites on the Internet stood at 600,000 — 10 times the number in existence three years before, when the Morris worm had wreaked its havoc. A year later, hosts passed the 1 million mark, and the number began doubling every three months.

Over the following decade, distributed computing contributed to massive increases in productivity but also introduced a cybersecurity arms race. Empowered users added devices to the network while IT professionals sought to add firewalls and other forms of protection to block increasingly clever and malicious hackers. Today, corporate IT executives shop the aisles of the annual RSA conference in San Francisco for literally thousands of security solutions. But individually, each solution provides little real security.

Similarly, individual users suffer productivity losses ranging from the minor intrusion of spam to the catastrophic malware-driven computer crash. Headlines make users increasingly wary of privacy risks as diverse as the relatively benign intrusion of cookies that track user behavior and the fear of identity theft through corporate hacking, such as the 46 million customer records breached in a 2007 incident involving retailer T.J. Maxx.

Despite spending money on increasingly sophisticated tools, CIOs often feel like the Dutch boy

Corporate IT executives shop for literally thousands of security solutions. But individually, each provides little security.

plugging the hole in the dike with his finger. Other senior executives rarely appreciate the magnitude of the risk or the amount of backroom work required to minimize that risk. Mostly, the CEO sees an ever-growing IT budget for a wide array of tools and patches, but no comprehensive solution. To change that dynamic, executives should reflect on the lessons of the quality revolution. While computer scientists were envisioning the opportunities of the Internet and the pending risks, quality professionals managed to recruit the executive suite and the masses to produce a sea change in attitudes about the importance of, and expectations for, product quality.

Learning from Quality
Preventing the spread of malware presents a challenge similar to the elimination of errors in the opera-

tions realm, and we propose that the evolution of thinking about product quality offers managers useful lessons about how to eliminate malware. Expectations about product quality have shifted dramatically over the past 40 years. In the 1970s, consumers had become accustomed to buying new products, whether toasters or automobiles, that had been designed, built, and shipped with inherent flaws, and companies commonly sorted through supplier shipments to ensure an "acceptable quality level" (often 95 to 99 percent), which was deemed good enough for the captive consumers of that time. Today, consumers expect new products to work flawlessly from the moment they buy them. Companies no longer inspect incoming goods but hold suppliers accountable to delivering "Six Sigma quality" measured in parts per million, with single-digit targets.

The quality transition did not happen overnight, however. The first evolutionary stage occurred with the introduction of statistical process control and the accompanying

Tim Laseter
lasetert@darden.virginia.edu
holds teaching appointments at an evolving mix of leading business schools, including the Darden School at the University of Virginia. He is the author or coauthor of four books, including *Internet Retail Operations* (Taylor & Francis, 2011) and *The Portable MBA* (Wiley, 2010). Formerly a partner with Booz & Company, he has more than 25 years of operations strategy experience.

Eric Johnson
m.eric.johnson@tuck.dartmouth.edu
is professor of operations management at the Tuck School at Dartmouth College and director of its Glassmeyer/McNamee Center for Digital Strategies. He focuses on the impact of information technology on supply chain management and has published recent articles in the *Financial Times, Sloan Management Review, Harvard Business Review,* and *CIO* magazine.

shift from *inspection* to *prevention.* Although initially ignored in the United States, W. Edwards Deming, a statistician who became a noted management guru, introduced his philosophy in Japan during the military-led nation building after World War II. Managers from leading companies such as Toyota, Canon, and Sony eagerly applied the new tools to control quality at the source — and in the process transformed the image of Japan from a producer of cheap knockoffs in the 1960s to the gold standard of manufacturing prowess and product quality by the mid-1980s.

The shift to prevention also led to a focus on root-cause analysis and problem solving. Statistical quality control charts separated normal, random variation from "special cause" variation. But that was just the starting point. Knowing that a spike in a chart isn't random doesn't tell you what caused the spike. Engineers and quality specialists needed tools to determine the root cause of problems in order to fix them.

Two engineers-turned-consultants, Genichi Taguchi and Dorian Shainin, proved instrumental in translating the statistical concepts into practical tools during the 1950s and '60s. Employed at Nippon Telegraph and Telephone during the period when Japanese companies were aggressively adopting Deming's philosophy, Taguchi developed a methodology for finding root causes. The Taguchi method built upon classic experimental design methods developed by R.A. Fisher before World War I, but offered a more user-friendly package. Although some questioned the rigor of Taguchi's methods, he was able to make accessible the testing of multivariate hypotheses, which armed a host of

engineers with a practical problem-solving technique.

Shainin pushed practicality even further by famously exclaiming, "Talk to the parts; they are smarter than the engineers." Rather than hypothesize potential causes and then design an experiment to test them, Shainin encouraged hands-on problem solving. He employed a method of paired swaps between a faulty and functional product to identify the "red X," the one part most likely to be causing the problem. He appreciated that statistical methods could tease out subtle relationships and interaction effects, but his pragmatic problem solving focused on identifying and fixing the biggest issues rapidly.

Philip Crosby helped ignite the modern quality movement by framing the problem in managerial terms with his 1979 book, *Quality Is Free: The Art of Making Quality Certain* (McGraw-Hill). Crosby challenged senior managers to quantify the true cost of quality, using a framework developed by Armand Feigenbaum that deconstructed both the cost of ensuring good quality and the cost of poor quality into four categories: *prevention, appraisal, internal failure,* and *external failure.* Crosby asserted that the total cost of these four categories could easily add up to more then 30 percent of a company's revenues, but most senior managers missed this problem, focusing instead on balancing the money spent on appraisal versus the cost of external failure. Thus, by Crosby's calculations, better quality was "free" because investments in prevention could be funded by reducing the vast amount of money spent reworking internal failures and fixing or replacing defective products. Although Crosby did not

push the science of quality forward, he accelerated the application by articulating the dynamics in bottom-line terms, thus elevating the issue into the executive suite.

However, initial efforts toward a quality revolution in Western economies struggled to take hold during the 1980s. Many companies misattributed Japan's success to the use of quality circles, where small groups of frontline employees worked to drive continuous improvement through incremental change. Western managers falsely assumed they

nalism, he preached his 14 points of management and maintained a travel schedule beyond the limits of many people half his age until his death at 93.

Over time, management provided the needed training and the empowering environment to allow employees to address quality issues through small incremental improvements and simple tools such as *Ishikawa* (or "fishbone") diagrams to identify possible root causes and Pareto charts to focus on the critical few. But as Deming had predicted,

raised the bar of expectations for quality performance and made it everyone's job. The language of "acceptable levels" of poor quality had been permanently erased from the business lexicon. The philosophic mantra of "zero defects" was replaced by the goal of Six Sigma quality, precisely defined as defects of less than 3.4 parts per million. And building on the Japanese notions of quality circles and continuous improvement, Six Sigma engaged the entire organization. Problem-solving black belts led the way, but a host of green belts, from frontline employees to senior managers, also participated.

Today, consumers expect new products to work flawlessly from the moment they buy them.

could simply create teams and empower employees to reduce quality errors. However, without the proper support, these early efforts evolved into sloganeering with posters admonishing employees to "Do it right the first time!" while management washed its hands of responsibility.

Fortunately, Deming's 1986 book, *Out of the Crisis* (MIT, Center for Advanced Engineering Study), spoke to the real management task at hand, on the basis of his experience in Japan: "Long-term commitment to new learning and new philosophy is required of any management that seeks transformation. The timid and the fainthearted, and the people that expect quick results, are doomed to disappointment." An octogenarian at the time, Deming admonished managers and corporate leaders to accept responsibility for creating an environment that encouraged poor quality. With a subtle mix of humor and pedantic pater-

many leading companies eventually concluded that simple tools and frontline employees were insufficient to the task.

To push for step-function rather than incremental improvement, in the mid-1980s Motorola developed Six Sigma and trained a set of technical experts, known as black belts, to apply more sophisticated problem-solving tools. General Electric CEO Jack Welch learned of the power of the methods from Larry Bossidy, CEO of Allied-Signal (now Honeywell) in the early 1990s and helped popularize the Six Sigma approach by training thousands of GE managers as certified black belts. Although most of the tools had existed in previous quality system manifestations, Six Sigma added a clear focus on quantifying the benefits of solving problems and investing critical time in getting stakeholder buy-in to implement proposed solutions.

Most importantly, Six Sigma

Quality and Information Security
If today's managers adopted the approach taken by the quality movement toward product flaws, they could revolutionize how we tackle online security problems. The goals of information security are simple but daunting: ensure the confidentiality, integrity, and availability of information. Unpacking those three words reveals that we want information to be limited to the owners and to those they grant access. We don't want the information to be changed without the owner's permission, and we want to be able to access our information anytime we want.

Achieving these goals requires maintaining control over both logical systems and their physical environment. We are all familiar with physical security. At home, we install strong doors that we lock, giving keys only to our family and friends. We install intrusion alarms that monitor doors, windows, or movement in the house. We examine travelers' identities and use metal detectors and body scanners at airport entries to watch for terrorists. We install surveillance cameras to

watch for suspicious behavior.

Many of these analogies carry over to the digital world. Firewalls limit access through specific doors, called ports. As e-mail passes into a corporate network and then a user's machine, it is examined to see if it contains malware. Besides watching the doors, antivirus software continues to monitor suspicious files and activity. Identity management and access control systems require users to identify themselves and ensure users see only information they are entitled to see. Intrusion detection systems watch for hackers who have found a way into the network. And encryption is used for both data at rest (in storage on a hard drive) and data that is moving on a network to make it impossible to read without the appropriate keys in case it is stolen or lost.

The history of information security offers some interesting parallels to the evolution of quality thinking, but also some critical differences. Both the similarities and differences provide insight in thinking about the growing challenge of Internet malware. As was the case with the quality revolution, the early practitioners of information security were technical experts, laboring in obscurity even as they battled the enemy. The quality statisticians, however, waged war against innate waste and error to reduce unintentional variation; the infotech security wizards have been fighting in an escalating and increasingly nasty war against an enemy with destructive intent. Early viruses generally reflected benign, often humorous attempts to demonstrate the fallibility of both humans and computers. Later, more malicious efforts appeared as a way to demonstrate technical superiority in a game of one-upmanship. Increasingly, malware reflects clear goals such as financial gain or social protest. The intentionality of malware provides a clear distinction between the two movements, but the lessons of the quality revolution remain relevant to malware nonetheless.

Crosby's notions of cost map well onto security. Firms invest both in negative effects of excessive controls. Tight policies limiting use of new devices or unapproved applications offer greater security, but they also stifle innovation — something hard to quantify.

After quantifying the full costs of information security, companies need to focus on the root causes. Although "denial of service" attacks

To date, no one has made a compelling case to assert that "information security is free," but that may, in fact, be correct.

prevention (education) and ongoing appraisal (penetration testing). Likewise, security failures lead to both internal costs (lost productivity) and external costs (fines and damaged reputations). To date, no one has made a compelling case comparable to Crosby's to assert that "information security is free," but that may, in fact, be correct. Understanding all of these costs offers an important step toward improving security; however, in this case, the objective is not hard quantification but a change in executive and organizational mind-sets.

To move from the back room to the boardroom, information security specialists should employ a common, rigorous framework for quantifying the bottom-line impact of security breaches. Too frequently, senior executives are aware only of the cost side of the equation. They see growing investments in software tools designed to catch problems but rarely see hard quantification of the benefits of these controls. Even more unusual is a quantification of the

and botnets grab the headlines, the root causes of many security breaches include both benign and malicious insiders with access to sensitive information. So, just as retail stores check departing employees for stolen merchandise, data loss prevention systems watch for data moving on a corporate network. If an employee deliberately (or accidentally) tries to e-mail a spreadsheet of credit card numbers or product release plans, the system bars the door. Related monitoring tools scrutinize employees' use of company data, watching for suspicious frequency, unexplained volume, or a particular combination of data. Other security tools help users make good security decisions, such as warning them if a hyperlink in an e-mail message appears fraudulent.

In the words of Dorian Shainin, IT security experts need to "talk to the parts" rather than stay in the back room running system diagnostics. Users — the parts in information networks — rarely understand the true vulnerability inherent in

the connectivity of the Internet. Rather than keeping users in the dark and assuming that malware protection programs such as Norton and McAfee have everything under control, we need to educate frontline employees. Following the lesson of Taguchi, companies must empower employees with user-friendly malware protection tools. Information security cannot be the sole domain of the technical team. Users need to understand the real threats, and technicians need to appreciate the loss of benefits that results from overly restrictive controls. Taking a lesson from Six Sigma, security specialists need to focus on stakeholder buy-in, and to recruit advocates in the user community. Cybersecurity is everyone's job, not just that of the CIO or security specialist.

The increased visibility for management as well as users should be accompanied by higher expectations. Just as the quality movement led managers and employees to expect Six Sigma performance — and led consumers to expect that products would work right the first time and every time — so too must our society admit that current levels of cybersecurity are unacceptable. Do we really believe that an e-mail network consisting of three-quarters spam is acceptable? If we fully understood the untold costs of both lost productivity and needless investment in storage and bandwidth, we would also come to the conclusion that security is free. Once we — as a society composed of individuals, institutions, businesses, and government — accept the challenge, then we can truly move down the road toward an open, but safe, global community. ✚

pwc | **strategy&**
Formerly Booz & Company