Fighting cybercrime

The Global Cybersecurity Agenda

Viewpoint | Hamadoun I. Touré, ITU secretary-general

Everything is connected, including crime

With more than one billion Internet users in the world today, the number of crimes committed in cyberspace has increased exponentially. The loss is estimated to run to several billion dollars, both from fraud on the Internet and from the costs of rebuilding networks that have suffered cyberattacks, and we know these figures are low because many financial institutions don't report how often they have been attacked or how much they have lost. To illustrate the magnitude of the problem, a major United States retail giant recently admitted the loss of 45 million credit cards and debit due to hackers exploiting a flaw in its network, making it one of the biggest data breaches in history.

Financial theft, fraud and network security are only a few of the many cyberthreats these days: others range from the costly annoyance of spam to personal identity theft to the proliferation of child pornography to cleanup costs after computer viruses. With schools, hospitals and government organizations moving more and more of their services online, the vulnerability of the system and everyone connected to it becomes frighteningly apparent.

For example, just one word change on a patient's medical file in a hospital could kill that patient, and hackers who can thwart sophisticated banking systems have no trouble breaking into a hospital's network. Children, students and senior citizens communicating by Internet or mobile phone are equally exposed; someone of malicious mind could acquire personal data or even track an individual's exact location. This is becoming a major concern for public authorities all over the world.

For all these reasons, when the World Summit on the Information Society met in Tunisia in November 2005, it asked ITU to coordinate a mechanism for building confidence and security in the use of information and communication technologies. WSIS turned to ITU because of its leadership in this area. What is needed is a global perspective, and ITU is ideally suited for the task because it combines public and private interests, with 191 countries and 700 ICT-related companies and organizations as members and associates. In addition, since its inception in 1865, ITU has established a track record of leveling the playing field and brokering agreements involving governments and industry alike.

There is no simple definition for cybersecurity, but the magnitude of the issue calls for a coordinated global response. It is important to foster a common understanding of the importance of cybersecurity and it is equally important that all stakeholders (governments, intergovernmental organizations, the private sector and civil society) come together and agree on how to deal with cybercrime because criminals use weaknesses wherever they can be found. While there are a number of existing frameworks, they are enforceable within geographical boundaries that are either national or regional, thus leaving room for criminals to use loopholes to their advantage and in almost total impunity as they shift their operations to countries where appropriate and enforceable laws are not yet in place. Unless there is close international cooperation, even countries with strong cybersecurity measures in place will be at risk because they will not be able to prosecute criminals outside their national jurisdictions.

NICK KOUDIS / GETTY IMAGES.

In cybersecurity, digital networks are only as secure as the weakest link.

This is why, on May 17, I am launching an important initiative called the Global Cybersecurity Agenda, intended to create a platform where governments, including law enforcement authorities, the private sector, international organizations and civil society, can work together to defeat cybercrime. The Agenda will have a two-year timetable to bring all countries up to speed and come to an agreement on the five pillars of this international effort, namely, 1) finding workable technical solutions for every environment; 2) developing interoperable legislative frameworks; 3) implementing capacity-building schemes; 4) setting up appropriate organizational structures; and 5) adopting effective international cooperation mechanisms.

A major first step will be for every country to have a national cybersecurity policy and response team. Most industrialized countries do, but because cybercrime is not limited by geographic boundaries, enforcement of laws elsewhere will be difficult unless every country is engaged. Initially, we will focus our efforts on the 50 least developed countries in the world because they are the most vulnerable. We will steadily move to other developing countries until we have covered all the ground, because when a cyberattack occurs in one country, it can have devastating effects in other connected countries.

'ITU will focus on the 50 least developed countries, as they are the most vulnerable'

In cybersecurity, we are only as secure as the weakest link. We must therefore increase the level of awareness and build human and institutional capacities in every corner of the globe; we need enforceable national laws that are interoperable worldwide so that there can be no safe havens for cybercriminals; we need to assess vulnerabilities and threats and anticipate dangers collectively to adapt our strategies and solutions at all levels and, to this end, we must put in place organizational structures that can monitor, identify and respond to cyberthreats. And we need technical measures not only at the application level but also at every point of the infrastructure if we are to secure networks. This is why we need the Global Cybersecurity Agenda.

The aim of the multistakeholder approach to tackling cybersecurity is not to add layers to what is already being done. Rather, ITU will act as a catalyst and facilitator, bringing public and private partners together to share experiences and best practices, both online and in physical meetings, and to fast-track a global response to cybercrime. Legislators can work out interoperable legal frameworks to put an end to safe havens. Policymakers can develop the right international cooperation mechanisms, and the private sector can help find technical solutions that are applicable worldwide. We will provide the tools and appropriate environment to ensure that all elements are linked in order to enhance security and confidence in cyberspace. ■

ITU / JEAN-MARC FERRÉ.

ITU Secretary-General Hamadoun I. Touré is launching the Global Cybersecurity Agenda on May 17.

International level | Fighting cybercrime

The global cybersecurity threat demands a global solution

Twenty years ago, PCs around the world began spontaneously flashing an advertisement for an obscure Pakistani computer shop. By today's standards, that first global PC virus — apparently a botched attempt by two brothers to stop piracy of their own firm's software — seems very tame indeed. Cybercrime has rapidly grown into a billion-dollar business spanning identity theft, resource hijacking, phishing, denial-of-service attacks, child pornography and more, controlled by highly organized international gangs intent on exploiting the frailty of networks and the humans who use them.

The vast majority of modern viruses are not designed to cause system havoc, but rather to secretly install themselves on the PCs of unsuspecting users for various nefarious purposes, such as retrieving personal information or co-opting machines into a vast global pool of spam "zombies." While security solutions do exist, at best they represent an isolated response to a particular threat or cover a specific jurisdiction, with scant acknowledgement of the dynamic realities of modern cyberspace — fluid technologies, evolving hacker skills, shifting targets, the exploitation of loopholes in a borderless new realm and the rapidly mutating nature of threats and risks.

As the UN specialized agency for telecommunications and information and communication technologies, the International Telecommunication Union believes a coordinated global approach to cybersecurity is the only effective weapon against a global evil that, if not halted, threatens to compromise the enormous potential of the Internet for economic development, particularly in poorer nations that lack access to sophisticated technological fixes.

"Privacy issues, public safety, national security, the protection of minors — cybersecurity now touches every element of society," says Alex Ntoko, ITU's strategy and policy adviser. "Countries cannot shut their borders to incoming cyberthreats, and modern cybercriminals need never be present at the scene of the crime. That's why attempts to solve these issues at a national or regional level are no longer workable — a concerted global approach is the only answer."

Ntoko says an internationally coordinated approach will need to focus on developing new harmonized frameworks to address complex technical and legal issues, along with internationally agreed organizational strategies and capacity-building and awareness-raising programs targeting the developing world, where cybercriminals have been quick to exploit legislative loopholes and poor infrastructure protection.

"In the Information Age, governments not only need to ensure the absolute integrity of their own data, but have a responsibility to demand compliance with minimum security standards and to strengthen law enforcement when it comes to cybercrime. But the private sector, with its unrivaled technical expertise, must also play a key role. We need a new, multistakeholder approach that recognizes and harnesses the essential contribution of every player," Ntoko says.

'Cybercrime has become a billion dollar business'

As more than one billion people are already online, ITU is pushing for fast action in the form of a new Global Cybersecurity Agenda designed to build consensus among the global community on what cybersecurity is and why an international cybersecurity framework is important. The Agenda also encompasses provisions for an internationally coordinated security response, so that when a cyberattack occurs in one country, other nations can be rapidly forewarned, limiting damage and severely curtailing any financial benefit to the criminals concerned. "If, through a collaborative international approach, we can do our best to ensure cybercrime no longer pays, it will go a long way to reduce cybercrime," says Ntoko. ■

The Australian experience

Australia's Spam Act 2003, one of the world's first pieces of antispam legislation to really get tough with spammers, has quickly become a benchmark for antispam initiatives worldwide.

The act makes it illegal to send, or cause to be sent, unsolicited commercial electronic messages that either originate in Australia or are sent to an address accessed in Australia. It also allows the Australian Communications and Media Authority to take direct action against spammers and protects Internet service providers who take steps to eradicate spam from their networks.

Penalties of $1.1 million a day, actively enforced, have seen Australia drop from 10th to 23rd on the global list of spamming nations.

Identity theft | A global approach

Setting standards to protect electronic identity

The first concrete steps toward a harmonized global approach to electronic identity management (IdM) are at last being taken, through an international Focus Group led by the International Telecommunication Union, the United Nations agency responsible for telecommunications and information and communication technology, based in Geneva.

The group, which comprises developers, software vendors, standards development organizations, equipment manufacturers, telcos and researchers, met in Geneva in February and April to work on a new global technical framework for IdM that would ensure interoperability between existing systems and pave the way for simpler, more secure interaction between consumers, e-commerce services and online communication resources.

Now a rapidly growing problem worldwide, identity theft poses a serious threat to the Internet's ongoing viability as a commercial platform. In the United States alone, the Federal Trade Commission estimates that around 10 million consumers a year fall victim to some form of identity theft, with ID-related problems now accounting for around 37 percent of all FTC consumer complaints.

If that weren't bad enough, the scale of the problem is moving beyond the merely personal, as networks begin to integrate "intelligent" objects like Auto-ID tags, sensors and software agents that can act independently of human intervention.

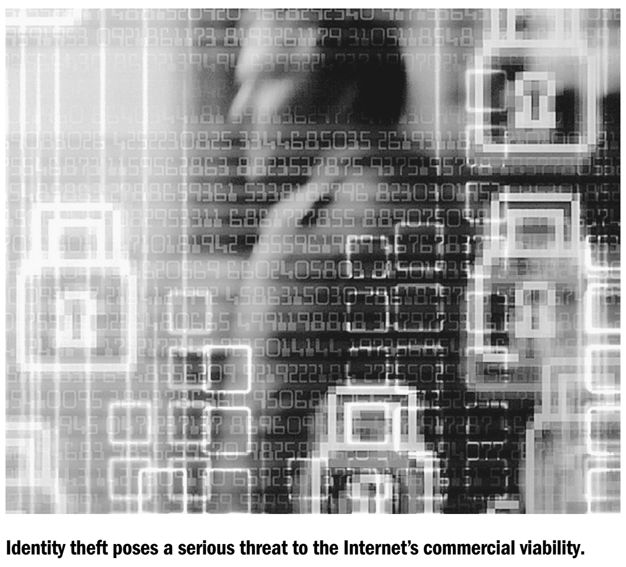
"Identity management is growing to encompass many different uses of communications networks, as well as every kind of entity on those networks, including objects that communicate between themselves," says Tony Rutkowski, vice president of regulatory affairs with Verisign, who works with ITU expert groups in the area of identity and radio-frequency identity technologies. "If you overlay rapidly scaling cybercrime, the challenges are already clearly apparent — and are likely to worsen significantly as more powerful technologies come online."

'Nobody can go it alone in this space'

The work being done under the auspices of ITU's Focus Group on Identity Management aims to produce deliverables that include a global assessment of IdM requirements and capabilities, along with a gap analysis to identify where new global standards are needed.

International consensus on a global platform for effective IdM promises to greatly diminish the potential for identity theft and fraud, reducing the need for multiple user names and passwords for different services, and creating a recognized "trustmetric" that would be interchangeable across different electronic security systems. "An IdM system must have global acceptance; nobody can go it alone in this space," notes Focus Group Chairman Abbie Barbir, senior adviser in the strategic standards group of Nortel.

ITU already boasts a long and successful history in the field of ICT security standards, with ITU-T Recommendation X.509 now serving as the primary "public key" mechanism that ensures communications security across the world's vast ICT infrastructures. ■


ITU / JEAN-MARC FERRÉ.

Identity theft poses a serious threat to the Internet's commercial viability.

Security snapshots around the world

- **In 2006, Japan's security agency, IPA, detected almost 45,000 different viruses on the Internet worldwide.**
- **Experts estimate there are now over 100,000 different types of spyware programs on the Internet, with more than 80 percent of all business computers estimated to be infected with one or more programs.**
- **The global watchdog Spamhaus now blocks more than 50 billion e-mail spam messages every day. Spam accounts for around three-quarters of all e-mail traffic, with health- and product-related sales pitches accounting for over 80 percent of all messages.**
- **Up to 50 new bots are now detected every day. Around 95 percent of all spam is sent by zombie PCs — with up to one million new machines infected each day.**
- **The cost of spam in 2007 is estimated to reach $100 billion worldwide — double that of just two years ago.**
- **ITU Cybersecurity Gateway is the world's most comprehensive pool of global information resources, with links to the world's leading cybersecurity agencies and initiatives. See www.itu.int/cybersecurity.**

Fighting cybercrime: The Global Cybersecurity Agenda did not involve the reporting or editorial departments of the IHT. It was sponsored by the International Telecommunication Union, which provided the text.

For information on the IHT Advertising Supplements program: supplements@iht.com

Spam | A level playing field

Countering spam by enforcing legislation worldwide

Once it was just plain irritating. But today's spam is taking on an increasingly sinister cast, with gangs of organized criminals unleashing subtle viruses designed to turn ordinary Internet-connected PCs into zombies working in vast "botnets" — usually unbeknown to their users — sending out millions of unsolicited direct marketing pitches and even fraudulent messages designed to dupe unsuspecting recipients into revealing their credit card or bank account details.

Spamhaus, the international nonprofit organization that runs the Internet's largest spam-blocking system, says it now blocks more than 50 billion spams every day. "Around 95 percent of spam is now being sent from hijacked 'zombie' computers," says Steve Linford, Spamhaus CEO. "There are already more than 150 million infected PCs worldwide, with 500,000 to 1,000,000 new machines infected every day,"

The volume of spam continues to grow at exponential rates for one simple reason: it's a very profitable business. As long as consumers continue to buy from spammers, spam will continue to invade our mailboxes. And while all Internet service providers publicly claim to be antispam, some of the world's largest and best-known do virtually nothing to deter spammers, with some even cynically factoring revenues from spam hosting into their bottom line.

For the moment, at least, technical fixes have failed to solve the problem; spammers simply find a workaround that exploits computer systems' difficulty in differentiating good e-mail from bad. Better results, it seems, could be achieved by the right kind of legislation — combined, of course, with the political will to enforce it.

"Legislation really can work — but it can't just sit on the shelf, it needs to be aggressively enforced worldwide," says Susan Schorr, ITU regulatory specialist. "Australia and the Netherlands are two countries that have succeeded in dramatically reducing spam at a national level."

Another problem, she says, it that not all members of the e-mail ecosystem have an incentive to stamp spam out. "Many ISPs do spend huge sums on filters and spam monitoring — but not all," says Schorr. "And as soon as you get one who fails to do its part, everyone on the Internet is at risk. That's why ITU has proposed an enforceable Code of Conduct for ISPs designed to level the playing field by ensuring everyone plays by the same rules."

According to Robert Shaw, ITU's head of ICT applications and cybersecurity, "The transborder nature of spam also means purely national solutions can't entirely solve the problem — one reason why we are well-placed to serve as an impartial international forum promoting cooperation between anti-spam authorities." ITU is backing a comprehensive approach that spans policy, technical, commercial and consumer awareness elements, Shaw says, "but stemming the global tide of spam will ultimately depend on everyone playing an active role."

Besides developing policy initiatives like the Code of Conduct, ITU is very active in antispam activities, convening high-level seminars and workshops, conducting a survey targeting governments worldwide, promoting information sharing and exchange with other United Nations agencies and nongovernmental organizations through a vast Web site of antispam resources, and serving as a founding member of StopSpamAlliance.org, with the organization for Asia-Pacific Economic Cooperation, the European Union's Contact Network of Spam Authorities, the London Action Plan, the Organization for Economic Cooperation and Development and the Seoul-Melbourne Anti-Spam group. ■