- PDF
- Send to a friend

# Cybercrime - and what we will have to do if we want to get it under control

Essay by Michael Barrett, July 18, 2008 in response to What Would a More Secure Future Look Like?

*A version of this piece was* published *on Reuter's* "The Great Debate" on February 4, 2009.

As I write this, in the spring of 2008, we have recently passed a milestone - on April 22nd, 1993, Mosaic 1.0 was released by the National Center for Supercomputing Applications (NCSA) . This was the first web browser used by the general public, making the World Wide Web more than just a tool for academics.

How many Internet users are there today? Conservative estimates exceed one billion people. In a decade and a half we have gone from minimal Internet usage to approximately 20% of the world's population now being online. Moreover, the bulk of that growth has occurred since the year 2000.

In this essay, I will explore two themes: first, how societies adopt new technologies and second, how governance and regulation may co-evolve with new technologies. I'll use two historical examples – the road system and airplanes – to ask what lessons they may provide for the Internet.

In addition to being the 15th anniversary of Mosaic, 2008 is also the 100th anniversary of the introduction of the Ford Model T. There had certainly been other motor cars available prior to 1908, but the Model T revolutionized how Americans viewed cars and dramatically increased the number of cars on the road, necessitating a new approach to regulation. Pre-Model T regulation can be described as quirky: men walking in front of cars with red flags, 20 MPH speed limits, and so on. However, shortly after 1908, regulation began to change rapidly. For example, in 1918 New York introduced three color traffic lights. A year later, the League of Nations established a committee to harmonize aspects of road system regulation, and its recommendations were accepted and implemented by a number of countries.

New York's original traffic lights were based on the earlier signaling used on railroads, which were themselves based on maritime signaling. In other words, there's an established history of stealing good ideas for safety equipment, and re-applying it to a new niche. There's also a long history of mandating safety equipment via regulation.

Aviation also teaches us useful lessons. The Wright Flyer of 1903 had the same impact on aviation that the Model T had on automobiles. The US Government established the National Advisory Committee for Aeronautics in 1915 ; the Airmail Act was passed in 1925, and the Air Commerce Act was passed in 1926. Less than 25 years after the first flight, there was an extensive regulatory infrastructure in place. Still, contemporary debate centered around a general distrust of regulation, and a sense that the government wouldn't be able to deal effectively with new technology. But the pressure for regulation was sufficiently strong: accidents were commonplace and the public regarded aviation as novel, fascinating and unsafe.

The other lesson to be learned from aviation is that while each country manages its own

process, there is considerable standardization. This is at least in part due to ICAO (the International Civil Aviation Organization). ICAO was formed in 1948 under the auspices of the United Nations. The rationale for such harmonization is obvious – if an airplane is going to fly from one continent to another, the equipment in question needs to be deemed safe in both the origin and destination; the licenses and certifications of the pilots need to be accepted universally, and so on. Commercial aviation has implemented more standardization than many other areas of global commerce.

In the cases of both automobiles and aviation, accidents were the primary force behind regulation. While private industry certainly played a very significant part, it's no exaggeration that the road and air transportation networks that we take for granted would never have existed without government regulation, and could not exist without it. Can we expect the Internet to be different?

Internet regulation over the past fifteen years has been minimal. I'd argue that there's a single reason for this: the forcing function that accidents represented for road and air transportation has not existed for the Internet. I'd further argue that e-crime will play this role.

I have been working in Information technology for years and I can vividly remember when the first viruses were written, often by security researchers. Security technology failures have gone through a rather predictable sequence: initial discovery by security professionals, followed by wide scale abuse by teenage vandals, and finally appropriation by wholly criminal enterprises. Now that the teenage vandals have largely dropped away, we are left with attacks motivated solely by money.

This phenomenon has only been a feature of the information security landscape since about 2004. In less than five years, e-crime has changed from an anomaly into an industry. A recent Gartner report suggested that the global "take" from just one form of e-crime, phishing, was $3.2 billion in 2007 (and this may be an underestimate). This is impressive for an industry created less than five years ago. Worse, there is no reason to believe that e-crime is under any effective control. This is not due to inertia or lack of interest. Companies such as my own employer, PayPal, invest substantially in the security of our own applications and infrastructure; we have state of the art fraud management systems; we work with law enforcement to catch, prosecute, and convict criminals whenever possible.

The problem, however, is that there is a huge asymmetry at work. In many jurisdictions, there is no chance of e-criminals being detected, arrested, indicted, convicted, or punished.

Nonetheless, we are cautiously optimistic that phishing can be controlled. If other companies adopt the same strategies we have at PayPal, we're confident that phishing will become substantially more difficult and less financially rewarding. Unfortunately, there's also strong evidence that criminals will simply switch from phishing to malware.

I have spent the last three years looking for a clear answer to a very simple question – "How many PCs globally are infected by malware?" Perhaps surprisingly, it's very difficult to get an answer to this from commercial sources. However, the topic has become interesting to academics, and their conclusions are downright frightening – 12%.

Worse, 12% refers to an average of PCs owned by both consumers and businesses. Because businesses employ people (like me) to ensure the security of their computers, infection by malware is particularly disturbing. By contrast, consumers are on their own when it comes to PC security: most of them purchased a machine that appears to be capable of magic, and they have no clue as to what represents safe vs. unsafe behavior. We exhort them to "buy a firewall", "turn on auto-updates", "buy an anti-virus package" and so on, but there are no apparent consequences if they do not. Further, there's direct evidence that consumers think they know

how to protect themselves – but don't, as evidenced by a common belief that phishing e-mails can be spotted by their poor quality graphics, and abysmal grammar and spelling. This is why data from ISPs suggests that anywhere from 25% to 30% of consumer PCs have been compromised.

By now, I may have convinced the reader that I am of the Chicken Little mentality. But my fear may be warranted: it's pretty clear that the criminals are only just starting to flex their muscles – the monetization of e-crime is so new that they've only been plying their trade for a very short time. If we collectively take no action, then we have perhaps five to ten years before criminal greed literally takes the Internet away from us. If e-crime continues its rise, consumer confidence will be eroded, possibly leading to popular abandonment of the Internet and e-commerce.

However, if things start getting bad enough, society will demand change and, as the histories of other industries teach us, legislators and regulators will step in and mandate change. The obvious question is what that change should look like.

I believe that a very good case can be made for using the road system as an analogy for the Internet. The question we need to ask ourselves is: "Who's responsible for making the roads safe?"

Drivers are responsible for:
- Being appropriately trained and licensed to operate a vehicle;
- Ensuring that the vehicle is properly licensed, safe to operate, and insured;
- Following all appropriate regulations about safe driving.

Private industry is responsible for:
- Offering safe vehicles for sale;
- Providing safe road equipment to government agencies;
- Building roads to specifications provided by government agencies;
- Offering affordable vehicle insurance to drivers.

Governments are responsible for ensuring that:
- Roads are designed to be safe, and are maintained to ensure safety;
- Equipment used in the road system is safe (have you ever noticed that traffic lights don't fail with all directions showing green?);
- Drivers are trained and tested to meet standards of safe driving;
- Unsafe drivers are targeted by law enforcement officials;
- There is a minimum level of safety equipment built into personal vehicles;
- There is a robust market for affordable & effective vehicle insurance.

The analogous question is: "Who's responsible for making the Internet safe?" I'd argue that there should be a shared responsibility among government, private industry and consumers. However, almost none of these regulatory elements are in place today. We need to develop a model framework for Internet governance, and we need to do it soon.

If you are driving a car on the public roads, an entirely different set of standards apply than if you are driving "off road." Similarly, if you connect your PC to the Internet, it should be appropriately protected by either a hardware or software firewall and an anti-virus product. If you connect an unprotected device to the Internet, you should be liable for any financial losses that you might incur from e-crime, as well as for possible damages that your PC might cause to others. This is regulation at the individual level.

At the level of private industry, ISPs could be responsible for determining whether the PCs of their customers have been compromised, and if they have, refusing to connect them to the

Internet. Such determination could be made directly by the ISP concerned, as there are now tools that enable this, or by reports from reliable organizations. Additionally, website hosts and operators should be liable for damages their sites may inflict (even unintentionally) on visiting PCs.

Finally, it's clear that governments need to act:

We need a globally harmonized framework of legislation against e-crime. Governments need to agree on the definitions of e-crime and of phishing so that attackers from all jurisdictions can be aggressively pursued in the criminal justice system. In order to achieve this, it's quite possible that a new global governance organization is needed.

Governments need to substantially increase their investment in e-crime law enforcement. The Internet is a global entity. Either we need to find a way to enable global law enforcement teams to cooperate effectively, or we should give up on attempting to police the Internet locally, and establish the "InterNetPol."

Action is needed and we must act soon. I don't want to minimize the sheer difficulty of what we're facing. But, I do know this: we must change the way we work before e-criminals take away this shining thing we call the Internet.

Michael Barrett *is the chief information security officer at* PayPal*, where he oversees the information systems and services that protect the integrity and confidentiality of customer and employee information . Previously, he has served as vice president of security and utility strategy at American Express, and president of the Liberty Alliance, where he co-chaired the Identity Theft Prevention Working Group. He has twice been named one of the 50 most powerful people in networking by Network World magazine and was recently listed as one of* ITSecurity.com*'s 59 top influencers in the security industry. He is also an advisor to the Berkman Center's* StopBadWare *project.*

All Essays

View all thematic areas »

**Source URL:**
http://publius.cc/cybercrime_and_what_we_will_have_do_if_we_want_get_it_under_control#comment-0