Glenny, Misha; Glick, Bryan; Hyppönen. Mikko H.; Wainwright, Robert

Conference Paper

Cybercrime, cybersecurity and the future of the internet

Session Handouts, Global Economic Symposium 2010 (GES), 27-29 September 2010, Istanbul, Turkey

Provided in Cooperation with:
Kiel Institute for the World Economy – Leibniz Center for Research on Global Economic Challenges

Suggested Citation: Glenny, Misha; Glick, Bryan; Hyppönen. Mikko H.; Wainwright, Robert (2010) : Cybercrime, cybersecurity and the future of the internet, Session Handouts, Global Economic Symposium 2010 (GES), 27-29 September 2010, Istanbul, Turkey, Kiel Institute for the World Economy (IfW), Kiel

This Version is available at:
https://hdl.handle.net/10419/79125

Global Economic Symposium

The Global Polity

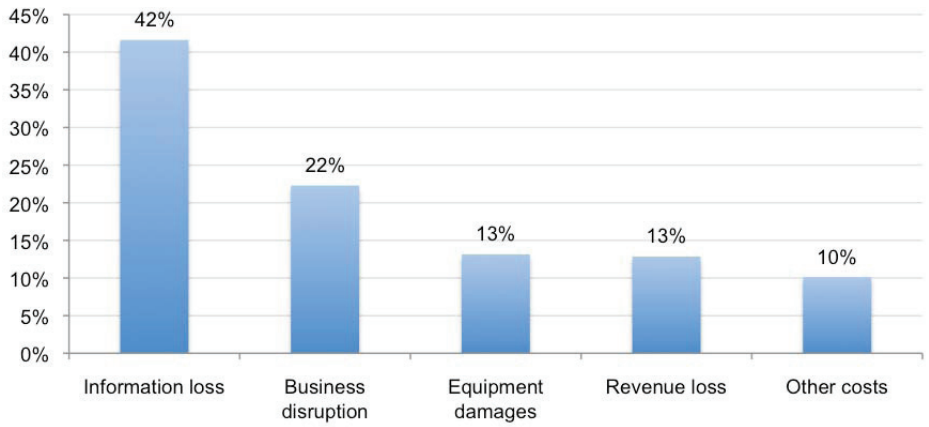
Cybercrime, Cybersecurity and the Future of the Internet

The Challenges

Cybercrime is now the fastest growing sector of cross-border organized crime. In 2009, reported losses in the US stood at $560 million up from US$265 million the previous year. This figure represents the tip of the iceberg for actual global losses, but the rate of increase is consistent in other countries.

According to Verizon, industrial espionage accounts for 35% of malware and hacking activity on the web. The last year has seen a deepening relationship between governments worldwide and companies like Google perceived now as strategic economic and security assets.

On assuming office, President Obama announced cyber security as a strategic priority of his administration. In the United States but increasingly in Europe, too, governments are establishing institutions to deal with critical infrastructure vulnerabilities and programs to engage both business and individual users on the issue. This strategy is in its infancy but attracting ever greater attention and funding. What is the role of the private sector? How can cooperation with major powers such as Russia, India and China on internet administration and on internet security be initiated and pushed forward? How should legislation attempt to adapt to cyber realty? What is the desirable balance between security and questions of civil liberties?



Proposed Solutions

Misha Glenny

Journalist and Author

There are three broad threats to internet security: cyber crime, cyber industrial espionage and cyber warfare. They represent a useful rule of thumb but are not fixed categories—they bleed into one another of necessity.

The one common element that straddles the three threats is that at some point they involve a computer user with advanced hacking ability. Already the role of these people may be quite far removed from the action. This is due to the industrialization of hacking tools which are now easily available: from viruses which buyers may deploy themselves through to operational botnets which can be hired for several hours, days or weeks.

As a consequence, even unskilled computer users are now in a position to mount a cyber attack at relatively little cost. Nonetheless, somebody had to develop these devices in the first place and that requires specialist hacking ability. And just as security tools evolve and adapt to meet the threat, so, too, do the weapons of attack in order to circumvent those security regimes.

Thus will hackers remain the grease that is essential to lubricate all three cyber threats. But despite their established presence, few agencies or academics have shown an inclination to investigate their motivation and their relationship to crime or wider security issues.

It is a controversial issue but I believe it is essential to find ways of identifying potential criminal hackers at an early stage of their career; to develop strategies to divert them into more constructive web-based activities; to study their peculiar social and psychological profiles; and to find ways of using their skills if apprehended rather than locking them up in jail as we in the West do now.

Quite simply, this requires serious research programs that marries computer science with behavioral psychology and criminology. The research capacity exists but there are as yet no programs being developed with this specific discipline in mind.

Bryan Glick

Editor-in-Chief, Computer Weekly

Five concerns and five solutions for cybersecurity

Internet security does not just touch on government, big business and law enforcers. It is an increasingly important concern for the average personal technology user, many of whom have little understanding of the issues and even less knowledge of the technical solutions. They just want to know that if they follow a few simple ground rules, they will be safe.

I would highlight five particular areas of concern that require appropriate solutions.

Data protection and privacy

On the web, personal information can be as valuable a currency as cash. Citizen's attitudes towards the privacy of their personal information are evolving and as a result unwittingly making the challenge greater. Increasingly, the definition of privacy is changing. Where once privacy meant not revealing information unless to a trusted third party, in the social media world information is willingly shared, but privacy concerns relate to how that information is used once shared. Sites like Facebook and Google have fallen foul of users who resent their

data being used in ways they did not anticipate or agree to—but who do not mind the fact that those sites know the information itself.

What is the solution?

Without greater openness and collaboration between major online providers, privacy regulation is likely to follow. At the very least, repositories of personal information need to be proactively open about their policies and show greater respect to their users through clear signposting and feedback.

Better software

Much cybercrime relies on the fact software is bug-ridden or contains flaws in its design. An entire sector of the IT industry has been created off the back of security holes in Microsoft products, for example. There is a clear need and opportunity for greater industry cooperation, standardization and testing of software products to reduce the opportunity for hackers. Too much consumer software is already being produced without consideration for security—the emergence of early viruses based around iPhone apps is a perfect example of this.

What is the solution?

Greater industry cooperation is essential. Various groups already exist, and some suppliers are teaming up to collaborate on software security, but it remains a patchwork of possible solutions. While nobody needs greater layers of bureaucracy, standards bodies should take a greater coordinating role to ensure a common approach across the IT industry.

Rogue states

On the internet, a rogue state is not defined by its weapons or politics but by its laws and regulations. Without a common base level of data protection and computer misuse legislation, there will always be territories that provide a safe haven for cyber criminals and hackers.

What is the solution?

Rogue states must be identified, targeted politically and persuaded to sign up to international norms on cyber crime. Involvement in key global trade bodies should be dependent on an acceptance of such regulation.

Protecting the little guy

Organized cyber criminals have realized that it is easier to steal US$1 from a million people, than to steal $1 million from one person. But in many cases, the response from law enforcement does not reflect the problem. One person complaining to the police about losing $100 through cyber crime, or the theft of personal identity information, is rarely sufficient to elicit a response. In the UK, for example, police have delegated responsibility for small-scale cyber crime reporting to the banks. How well are coordinated attacks spotted? Are trends and patterns sufficiently analyzed? If one person loses $1 million, the police response would be broad and well coordinated. If a cyber crook made a million from a million individuals, would they ever be caught?

What is the solution?

Banks and law enforcers need to coordinate better, and reporting of crimes by individuals affected needs to be simpler and better policed. Too many individuals do not bother because they do not believe they will be helped. Perhaps social media techniques could be used to “crowdsource” reports of theft or fraud? But in general, there needs to be a better relationship between individual and law enforcement to ensure adequate protection and detection of organized, widespread but individually low-level cyber crime.

Mikko H. Hyppönen

Chief Research Officer, F-Secure

What is international crime? Ten years ago it was smuggling, drug trade and money laundering. But over the last ten years, we have seen an explosion of online crime. And online crime is always international because the internet has no borders.

Local law enforcement has limited resources and expertise to investigate online crime. The victims, police, prosecutors and judges rarely uncover the full scope of these crimes. Action against online criminals is too slow, the arrests are few and far between, and too often the penalties are very lenient, especially compared to real-world crimes.

That is why I am calling for the establishment of Internetpol—an online version of Interpol. Internetpol would be an international agency with the enforcement power to really target the organized crime that operates on the web. It would investigate the top of the crime-ware food chain and bring to justice the people who are running the online crime syndicates.

Of course, establishing Internetpol would face a number of challenges. But if we do not take action now, online crime will continue to grow stronger and will end up destroying the current model of internet business, banking and commerce.

Robert Wainwright

Director, Europol

Dealing with cyber crime—Challenges and solutions

The threat from cyber crime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate. Cyber criminal tools pose a direct threat to security and play an increasingly important role in facilitating most forms of organized crime and terrorism.

Challenge 1

There is now a sophisticated and self-sufficient digital underground economy in which data is the illicit commodity. Stolen personal and financial data—used, for example, to gain access to existing bank accounts and credit cards, or to fraudulently establish new lines of credit—has a monetary value. This drives a range of criminal activities, including phishing, pharming, malware distribution and the hacking of corporate databases, and is supported by a fully fledged infrastructure of malicious code writers, specialist web hosts and individuals able to lease networks of many thousands of compromised computers to carry out automated attacks.

Whilst the value of the cyber criminal economy as a whole is not yet known, the most recent estimate of global corporate losses alone stands at approximately €750 billion per year.

Solutions

- Active targeting of underground forums to disrupt the circulation of powerful and easy to use cyber criminal tools, such as malware kits and botnets.
- Disrupt the infrastructure of malicious code writers and specialist web hosts through the active identification of developer groups and a joint action of law enforcement, governments and the ICT industry to dismantle so-called “bullet proof” hosting companies.
- Active targeting of the proceeds of cyber crime (e.g., money mules) in collaboration with the financial sector.
- Continue to develop insight into the behavior of the contemporary cybercriminal by means of intelligence analysis, criminological research and profiling techniques, and based on the

combined law enforcement, IT security industry and academic sources, in order to deploy existing resources more effectively.

Challenge 2

In the last decade advances in communications technologies and the "informatization" of society have converged as never before in human history. This has given rise to the industrialization of a type of crime where the commodity, personal information, moves far too quickly for conventional law enforcement methods to keep pace.

The unprecedented scale of the problem threatens the ability of the authorities to respond—with (according to one estimate) more than 150,000 viruses and other types of malicious code in global circulation, and 148,000 computers compromised per day. At the same time, the authorities have more data on criminal activity at their disposal than ever before, and now have an opportunity to harness this information in ways which make intelligence development and investigation more streamlined and cost effective.

Cyber crime rates continue to increase in line with internet adoption: mobile internet access and the continuing deployment of broadband internet infrastructure throughout the world therefore introduces new levels of vulnerability; with potential victims online for longer periods of time and capable of transmitting much more data than before; the adoption of these internet technologies in developing countries poses a potential external threat to the EU; and the increasing trend for outsourcing data management to third parties presents imminent risks to information security and data protection.

At the same time, the organic development of internet technology has resulted in the existence of myriad actors in the information security field. By way of illustration, the (ENISA) directory of network and information security stakeholders in the EU alone already stretches to over 400 pages.

Solutions

- More must be done to harness the intelligence of network and information security stakeholders, not only to provide a more accurate and comprehensive assessment of cyber criminality, but also to ensure that responses are effective and timely. Active partnerships with ISPs, internet security organizations and online financial services are key. The private sector needs to be assured of a confidential relationship in which information can be exchanged for investigative and intelligence purposes.
- Collaboration, particularly with the private sector, to proactively identify features of future communications technologies liable to criminal exploitation, and to design vulnerabilities out of technologies and environments which are in development. Law enforcement must work in partnership with those who will influence the future business and operating environment, so that all concerned can better anticipate changes in criminal behaviors and technological misuse.

Challenge 3

Cyber crime is a truly global criminal phenomenon which blurs the traditional distinction between threats to internal (criminality and terrorist activity) and external (i.e., military) security and does not respond to single jurisdiction approaches to policing. The liability of networks to exploitation for a number of different ends, and the ease with which individuals may move from one type of illegal activity to another suggests that territorialism in all its forms (both of nations and regions, and specific authorities within nations) hinders efforts to successfully combat the misuse of communications technology.

At present, national authorities are overcoming jurisdictional restrictions by coordinating regionally (as in the EU, ASEAN and AMERIPOL nations) or with agencies with similar levels

of capability/capacity (as in the Virtual Global Taskforce) to better understand and respond to internet-facilitated crime.

Solutions

- More centralized coordination at regional (e.g., EU) and interregional levels, to streamline the fight against cybercrime.
- The establishment of virtual taskforces to target internet-facilitated organized crime. These should be responsive to the evolving criminal environment—e.g., more permanent groups for information sharing, more ad hoc arrangements for specific operations such as dismantling botnets. In all cases the authorities need to have the flexibility to include a variety of stakeholders (law enforcement, military, private sector, academia, user groups) in order to achieve the desired outcome.