How Cybercrime Is Evolving

By Gilles Hilary , INSEAD Professor of Accounting and Control, and Christophe Durand, Head of Cyber Strategy, INTERPOL

The anonymous and borderless nature of cybercrime puts every organisation at potential risk.

Once considered an irksome pastime of geeky teens, cybercrime has grown up fast. In 2014 its annual **cost to the global economy** was estimated at US$445 billion. A 2015 Hewlett Packard-sponsored study of large U.S. companies found cyber-attacks growing “**in frequency and severity**” in every sector, at an average yearly cost per company of more than $15 million. Cybercrime’s increasing scale and sophistication have elevated it into a full-fledged illicit industry.

Unlike legitimate businesses, cybercriminals are not constrained by national borders and operate under a cloak of anonymity. This can make it especially difficult for law enforcement agencies, acting on their own within a strict jurisdiction, to catch them and be ready for the next attack. That is why, in 2014, INTERPOL inaugurated the **Global Complex for Innovation** (IGCI) in Singapore, which coordinates anti-cybercrime efforts internationally using a digital ecosystem mostly operated by the private sector, as well as expertise from academia. As this diverse partnership suggests, defeating cybercrime will entail a paradigm shift for public and private organisations alike.

Two types of cybercrime

Broadly speaking, law enforcement divides cybercrime into two categories:

· **Advanced cybercrime** – sophisticated attacks on computer hardware and software;

· **Cyber-enabled crime** – illegal activity that exploits the internet in some way (e.g. terrorism, human trafficking, money laundering)

But the two often blur together nowadays, as when hackers steal databases of customer information from companies and hawk them on “darknet” websites (such as the now-closed **Silk Road**), where other illicit items including drugs and weapons can often also be found.

The online black market gives hackers a quick and easy way to profit from purloined data without putting themselves at further risk, not to mention a strong incentive to continue plying their destructive trade and refining their technique. This is emblematic of a broader trend. Cybercriminals are becoming less and less motivated by anti-establishment ideology and the desire for bragging rights, and more by cold hard cash. Consequently, no organisation should consider itself too small or obscure to merit hackers’ notice.

Ransomware

Case in point: A number of local police departments in the United States have fallen victim to **ransomware** attacks. Outmatched by the perpetrators, officials had no choice but to pay the **relatively modest sums** demanded to regain access to their files. But don’t let the small dollar amounts fool you: Once all the takings are tallied, ransomware attacks are big business. The group behind Cryptowall 3, an especially virulent ransomware campaign from 2015, **reportedly reaped $325 million** in profits from victims.

INTERPOL has helped shutter black-market portals used by cybercriminals to market themselves as ransomware hackers for hire. Anyone with access to the “darknet” could provide a target URL, fill in an online form, and pay a fee (usually in a crypto-currency such as bitcoin) – and without so much as exchanging an email with a cybercriminal, they could then download a kit allowing them to deliver ransomware to their target.

“Zombie army”

Not all collaborations between hackers and the outside world are consensual. Cybercriminals commonly scale up their operations by assembling a network of **malware**-infected computers, also known as botnets or “zombie armies”. Unbeknownst to their owners, bots can be remotely deployed to distribute spam or shut down target websites with a sudden flood of traffic, a/k/a a “distributed denial-of-service (DDoS) attack”.

To evade detection, advanced “bot herders” route infected computers through rendezvous points, rather than issuing marching orders to the network directly. Domain name generation algorithms (DGAs) help conceal the address of the rendezvous point, essentially burying it under a tidal wave of auto-generated domain names (as many as 50,000 per day). The volume can be so great that websites have temporarily shut down as a result of the surge in traffic that occurred when a DGA happened to spit out their domain name.

As authorities caught on to the scheme, hackers developed more complicated DGAs. For example, INTERPOL recently came across one designed to churn out unintelligible domain names based on the most recent foreign exchange rates from the European Central Bank.

INTERPOL has been working with the Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit responsible for overseeing the internet’s domain name structure, to prevent these abuses.

Prevention

Most cyber-attacks begin with a single infected file that ends up on a computer’s hard drive, very often first appearing as an email attachment. Smaller public agencies (police departments, hospitals, etc.) often fall victim due to scant IT and training resources. But even large organisations may not be able to shore up every weak point. A regularly updated, “cold” data backup is your best option to minimize damage in case you get hacked.

Meanwhile, the ICGI continues to be a global hub for the development of more proactive solutions in the fight against cybercrime. It provides a neutral platform for international collaboration among its 190 members. Last year, for example, INTERPOL coordinated joint efforts among police in five countries (among them Russia, the Netherlands and the United States) to take down Simda Botnet, which was thought to have infected over 770,000 computers.

Barclays recently announced it would be **the first financial institution** to have a full-time cybercrime analyst working hand-in-hand with INTERPOL and other IGCI experts. “The scale and complexity of today’s cyberthreat landscape means cooperation across all sectors is vital”, commented IGCI Executive Director Noboru Nakatani.

Greater awareness among the general public is needed too. In the current public mindset, internet-based threats simply don’t loom as large as more tangible concerns. That needs to change, now that global cybercrime syndicates have the ability to do serious damage to the fundamental institutions of our world.

Gilles Hilary *is The Mubdala Chaired Professor of Corporate Governance and Strategy at INSEAD.*

Christophe Durand is INTERPOL’s central point of contact for cyber strategy.

This article is based on ideas shared at the latest ***INSEAD Risk Breakfast*** *.*

Follow INSEAD Knowledge on ***Twitter*** *and* ***Facebook***

3026

Find article at

https://knowledge.insead.edu/operations/how-cybercrime-evolving

About the author(s)

Gilles Hilary Gilles Hilary was a Professor of Accounting and Control at INSEAD and is now a professor at Georgetown.