The ongoing war against cybercrime

March 24 2015, by Nicholas Gilmour

The challenge is to keep the cyber criminals locked out of systems. Credit: Flickr/Yuri Samoilov, CC BY

Cybercrime is estimated to cost the global economy upwards of US$400 billion a year, and these costs are expected to continue to rise.

At greatest risk is the financial industry as its assets are the easiest to monetise. These globally connected financial institutions have committed huge resources to hardening their information infrastructures that includes personnel, security services and mechanisms, and physical

controls.

A recent survey of IT professionals working in the financial sector found that "only 16% felt very prepared to fend off intrusions aimed at financial accounts".

Despite their best efforts, banking operations around the world have recently been breached by a single organised cybercrime operation for a reported US$1 billion.

So despite vast resources committed to preventing breaches, why do they continue to occur?

The weakest link: people

In today's highly integrated, digitally dependent enterprise, a single digital path into an organisation willingly opened creates an opportunity for anyone who is both aggressive and entrepreneurial enough to commit cybercrime.

It does not matter how secure an organisation thinks its systems are against cyber attacks, all it needs is the action of a single staff member – either accidentally or intentionally – to breach that security.

Access by staff to email, the web and teleworking systems open the door to malicious code that then provides outsiders with internal access.

Even something as simple as a memory stick or thumb drive found in the parking lot can be the carrier of sophisticated root kits and remote administration tools (RAT) that can be used to gain remote access and hide malicious code.

This lets the attacker own the system that can be used to gain access.

From there it's a simple task to monitor internal activities using insiders' credentials until enough process knowledge is gained.

Cyber criminals can then begin transferring key records, whole databases, and even transfers of account balances. This is simplified even further when key employees are assigned the access and a usage right to carry out certain transactions and it is these credentials that have been hijacked.

Cybercrime knows no boundaries and wears no face

The very nature of the internet as a global network allows international communications connecting people and supply chains almost anywhere in the world.

This allows criminals to access company systems from nearly any jurisdiction. Because law enforcement is a sovereign-based endeavour, multijurisdictional investigations require nations to collaborate.

Despite international agreements on cybercrime cooperation such as the Council of Europe's Convention on Cybercrime the mobile nature of cyber-attacks requires specialised skill sets, fast response times and people resources in order to track and apprehend suspects.

When these resources come together, the anonymity and concealment the internet provides makes it difficult to prove that a given individual indeed used a given system to break the law.

Risk versus rewards with nominal costs

The existence of hacking tools and exploits has been around for decades.However, the significant financial benefits of cybercrime have

spawned a supporting service: malware for hire.

Crime is profitable and for a relatively modest sum, do-it-yourself toolkits and customisation services – available through the internet – can generate significant financial rewards. In other words, these services can create made-to-order malware for whatever purpose required.

The cost-benefit analysis to making money becomes easy when combined with a well-planned delivery approach and financial laundering scheme.

With the advent of digital currencies such as Bitcoin, stolen cash can easily be converted and transferred anywhere in the world.

Organised crime

Cybercrime has become big business. Driven by profit, organised crime has clearly extended its know-how to ensure widespread exploitation of open and hidden networks.

Utilising the skills of others and having an ability to control those master minding cybercrime endeavours, organised crime has confidently enlarged its entrepreneurial behaviour mimicking legitimate business practices to secure financial profit through strategic alignment of resources.

Whereas safe havens, weak states and outdated legislation once provided the necessary sanctuary for cybercrime, today anonymisation and encryption protect such activities.

Features such as these have altered the organisational structure of organised crime. Relationships have moved away from recognisable heirarchial structures to transient and transactional motivated criminal

enterprises.

Improved cybercrime opportunities have also facilitated the laundering of illicit funds. As organised crime has become richer and more powerful, the concealed cyber facilitated criminal process has helped cyber criminals launder illicitly derived funds away from the oversight and regulation of the legitimate economy.

Thoughts for the future

Disabling cybercrime is possible, but like so many modern day harms, there is no simple solution. It is apparent that what we are doing to tackle cybercrime is not working.

Hence, future responses must be universal, and while enhanced communication and international commitment exist – it must remain resolute.

The components of cybercrime are diverse, encompassing victims on an international scale.

While practices do exist to counter the many facets of cyber crime, success is slight. Evidence of what works and what doesn't would certainly support preventative activities.

By creating a comprehensive picture of cybercrime, it could then be possible to generate timely and accurate ground level assessments – helping to align transnational debate.

Then, and only then, can we begin to think outside the box, conjuring up new ideas on real world cyber related criminally driven problems to help the development of a new anti-cybercrime campaign.

Source: The Conversation