The cost of inaction on cybercrime in the Middle East

Simone Vernacchia, Senior Director and Cybersecurity and Infrastructure Lead at PwC, talks to Arabian Business about cybercrime.

Tackling online fraud will require governments to look at the origins of attacks as well as the technologies to combat them.

While the global digital revolution has transformed culture and commerce, it has also engendered new means of crime and conflict.

Despite broad global economic optimism, PwC's Global CEO Survey of over 1,000 CEOs released in January at Davos shows that 40 percent of business leaders are now "extremely concerned" about cyber threats – a level on a par with geopolitical uncertainty (40 percent) and terrorism (41 percent).

Their fears are very well-founded.

In 2016, Cybersecurity Ventures, a US research firm, predicted that cybercrime will cost the world $6tr annually by 2021 – with the average cost to an organisation of a data breach running to $3.6m.

In 2017, the global cost of damage caused by ransomware attacks, such as the one which brought the UK's health service to a standstill, are expected to exceed $5bn. According to our Global Analysis of Economic Crime Report, cyberattacks are now the second most reported economic felony, affecting more than 32 percent of organisations worldwide.

Despite increasing awareness of the threat by companies in the Middle East and the early adoption of effective cybercrime legislation in countries such as the UAE, a critical challenge facing all businesses around the world is to accurately identify not only how they are being attacked but also, most importantly, who is attacking them and why they are doing so.

To date, most assessments focus on the targets of attacks and the way they are carried out; with very little analysis conducted on the perpetrators and their motivations – largely because it is easier to observe the consequences of cyberattacks than to attribute the sources and reasons behind them.

The problem with such an approach is that it only provides part of the overall threat picture and this fact, in combination with how rapidly cyber attackers' techniques are evolving and changing, too often affords incomplete information from which to determine an effective and appropriate response to threats.

New crimes, old methods

The ability of governments and organisations to bring cyberattacks under control will increasingly require a comprehensive analysis of actors as well as their actions. The challenge, however, is that effectively tracking the origins of attacks, and then attributing them to a specific actor is far from simple.

In order to correctly track down the origin of a cybersecurity related event, attacks need to be analysed from a number of viewpoints.

These include the following considerations: motivation – for example, whether or not a possible incentive exists for an actor to perform the attack; technical origin – such as information about the location of devices deployed or the channels required for paying a ransom; information obtained from malware – through which it may be possible to identify the coder; and an analysis of operating hours, language and tactics – which again might provide clues as to both location and identity.

From these initial assessments, the next step is to categorise the attack as accurately as possible – for example, crime, warfare or activist related – and from this knowledge attempt to establish responsibility using all the clues available.

The problem, however, is that attackers do their best to hide their true identity. In the event of a criminal attack, the perpetrator wants to protect himself or herself from law enforcement and prosecution. Should the attack be politically motivated, the actor would want a shield from catastrophic retribution, which could even include military action.

Given this fact, actors often leave trails of fake information in order to redirect retaliation elsewhere or to cover their tracks. Adding to the complexity is the recent development of a cyber black market. Here, disparate hackers sell services or software tools, including corporate emails, credentials, credit cards, exploits, zero-day vulnerabilities, malware and phishing kits. These can provide all that is required for a cyberattack and will leave only dead-end clues as to ultimate responsibility.

Seeking a remedy

Considering the complexity surrounding tracing attacks and accurately attributing them to specific actors, retaliatory options become difficult and potentially dangerous – especially when it

The cost of inaction on cybercrime in the Middle East

Simone Vernacchia, Senior Director and Cybersecurity and Infrastructure Lead at PwC, talks to Arabian Business about cybercrime.

comes to involving nation states. As a result, an ongoing effort by the public and private sectors to develop accurate techniques that provide as full a picture as possible is vital.

Such tools may not, as yet, follow the tenets of traditional criminal justice and investigatory processes, given that cyberattacks and digital attribution are only in their infancy compared with physical crimes. However, systems for cyber attribution are slowly developing, albeit understandably based around degrees of certainty rather than absolute levels.

Given the pace of change and complexity of subject matter, cyberattacks can often seem like a theoretical danger, but the reality is that they either have or will affect all of us.

That is why we are committed to working with both public and private partners across the region to make information on these threats accessible, and prevent what can be truly disastrous impacts.

This article first appeared in Arabian Business in March 2018.