BIZCOMMUNITY

# The race for trust, treasure and time in the cybersecurity war

By Trevor Coetzee

26 Jan 2017

In the conventional economy, money is the only currency. But we are increasingly inhabiting a world comprised of the cloud, mobility, the Internet of Things and an infinite number of goods and services that are exchanged online.



In this so-called Second Economy, money isn't the only currency. In this technological and social realm, trust, time and treasure are the new currencies – and one of them is worth a lot more to cybercriminals than money.

## Trust

The Second Economy is built on the psychological currency of trust. When we transact online, we trust that the company we're dealing with will protect our information.

But trust is under relentless attack and is the prime casualty of cyber conflict. Hacktivists aren't after money. Rather, they want to embarrass their targets and reduce their brand value by sowing mistrust. Each attack serves to erode the trust of customers in a company's ability to withstand future breaches and protect their interests. And when trust is lost, it can do as much damage as lost funds, if not more.

A cyber defence focused primarily on protecting financial assets is therefore insufficient. The problem, however, is that public concern about personal data loss is falling despite a rise in data thefts. Also, breach victims are not typically penalised, even when their own negligence contributes, which suggests that breach costs should be evaluated in the Second Economy.

## Time

In the Second Economy, time matters more than money.

On the one hand, cybercriminals, or black hats, have time on their side. They design their attacks at leisure, crafting carefully thought out and executed strategies that can sometimes go undetected within a network for months, even years.

They also use time to their advantage in ransomware attacks by attaching deadlines to ransom pay-outs for the safe return of data. Under such immense time pressures, victims are more likely to respond impulsively and pay the ransom.

On the other hand, victims, or white hats, are in a constant race against time and are always reacting under pressure. When a breach occurs, time is the ultimate weapon – detecting and remediating threats as quickly as possible becomes the goal in a race where every second counts and time most certainly is money.

The time it takes an organisation to respond to breaches depends on the tools, policies and political structures that are in place before the notion of a threat is even recognised.

But the status quo in most organisations is that separate divisions have separate security policies, which slows down their response times. An IT strategy that allows for new technology to be rapidly on-boarded will ensure that new software releases will not hinder productivity and that software updates are not time-consuming.

## Treasure

In the Second Economy, money – or profit – is not the only treasure that black hats are after. When it comes to sowing mistrust, cybercriminals could be motivated by principle – as it often seen in attacks by 'hacktivist' group, Anonymous – while nation-states identify targets to expand their province.

Whatever their treasure, black hats have clear incentives motivating their next move, and with each attack, the trust economy is ultimately corroded. These fast-moving, fast-adapting black hats govern the terms of cyber conflict and control the pace of innovation and the nature and timing of assaults. Organisations play a perpetual game of catch-up, yet they consistently ignore or rationalise the risk.

This must change.

## Gaining the upper hand

Individual users cannot shirk responsibility for helping safeguard the Second Economy and, at the strategic level, today's siloed, reactive, barely collaborative defence posture must yield to a new white hat paradigm that is adaptive, aggressive, proactive, newly generous on information-sharing and unpredictable.

If we are to secure the now indispensable, interned-based Second Economy, we have to reject conventional defence paradigms in favour of radical new thinking. Where we have relied on old playbooks, we must be newly unpredictable; where we have hoarded information, we must become collaborative; where we have undervalued cyber defence, we must prioritise it.

A good start is at the organisational IT level through adopting technology platforms that accept new security software

quickly and result in a better-aligned ecosystem. We need to develop a whole spectrum of response plays and not simply plan for an unlikely worst-case scenario.

No single solution can eradicate all threats. We need a superior platform that allows for swift on-boarding of new technologies, over an architecture backed by common tools and workflows, along with automation and orchestration capabilities – one that doesn't multiply operational complexity for already overburdened staff. An integrated platform also offers the benefit of tapping into aggregate innovative capabilities of hundreds of potential players, all connected over the same infrastructure. This gives white hats a fighting chance at making time their ally.

Cyber security professionals with a more simplified back office infrastructure, as provided by fewer vendors in their environment, report experiencing fewer threats, better detection times and more confidence in their security posture than those with a more fragmented, multi-vendor approach.

There also needs to be organisational change. CEOs must advocate for more strategic, proactive defence while end-users must develop better security consciousness.

Finally, we need bold information sharing. By hoarding information, we make the Second Economy more vulnerable. Better defence depends on better sharing impulses. Bold, perhaps altruistic information sharing gestures by cyber defence organisations can change the culture.

Our economy is no longer a physical one but one of connected networks and systems where cybercriminals have put us on the defensive. We now live in a world where more than money is at stake and where we're fighting against time and working to justify trust.

If we're going to win the race, we need to abandon old security playbooks to become more unpredictable and collaborative and make cyber defence a priority.

## ABOUT THE AUTHOR

Trevor Coetzee, regional director, South Africa and sub-Saharan Africa, Intel Security