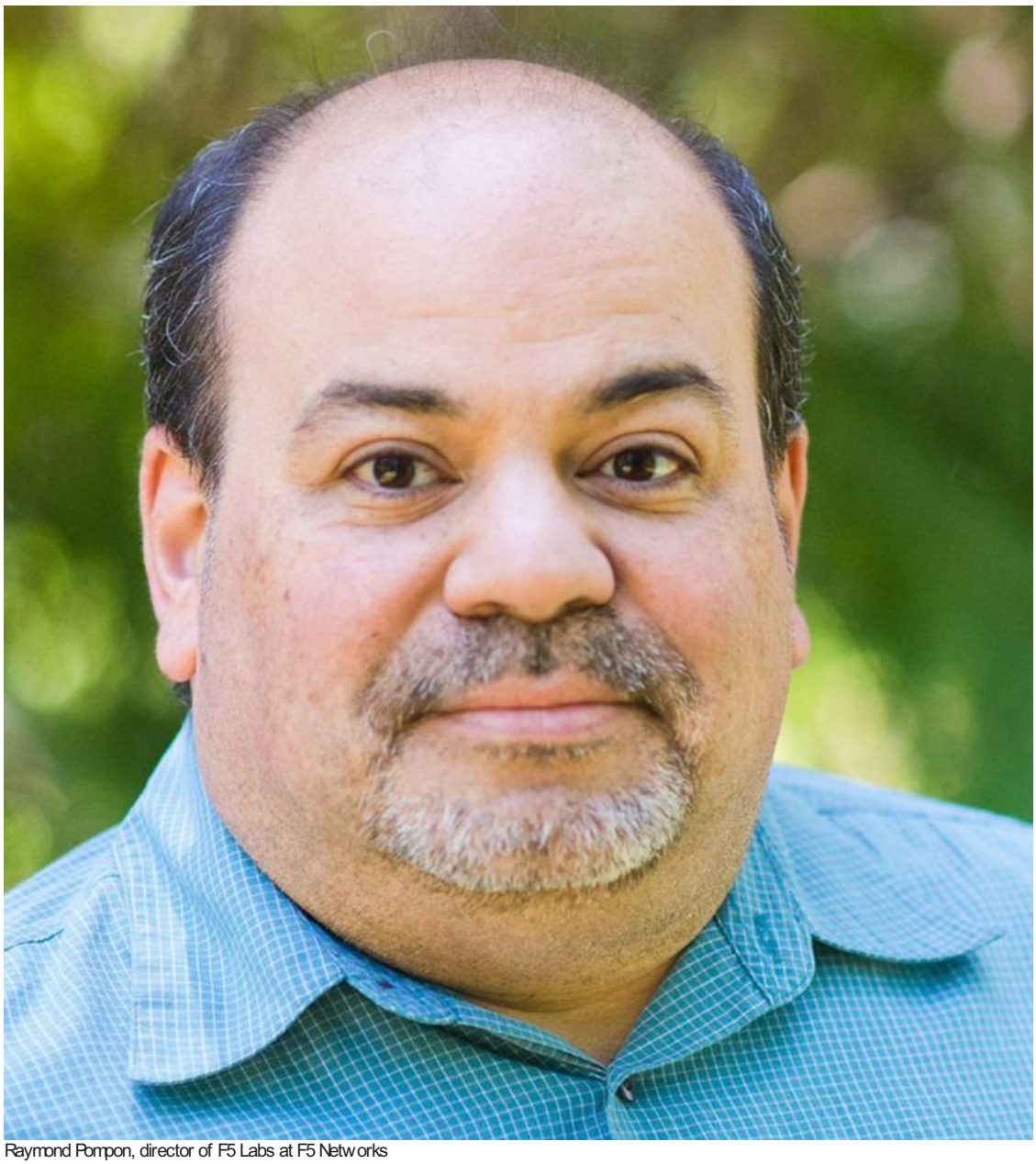
BIZCOMMUNITY

What a pandemic can teach us about cybersecurity

By Raymond Pompon

3 Apr 2020

The Covid-19 pandemic is impacting everyone with travel restrictions, school disruptions, event cancellations, and office closures as we work together to prevent the spread of infection.



Raymond Pompon, director of F5 Labs at F5 Networks

As unprecedented numbers of the global community, including millions of employees, shift rapidly from working onsite to working remotely, organisations around the world must scale capacity to maintain business continuity.

Protecting critical operations is more important than ever. Across the world, cybercriminals are gearing up to prey on fear, uncertainty and an increased reliance on digital tools.

The World Economic Forum has stated that cybersecurity “matters more than ever during the coronavirus pandemic.”

As South Africa comes to terms with its national lockdown – and its associated spike in online activity – it is worth noting that there are strong parallels between managing a pandemic and handling cybersecurity threats. Here’s why:

Containment is never perfect

One of the first moves in pandemic response is to issue a quarantine to contain the spread of the virus. A layperson's concept of quarantine is simple: nothing leaves, and therefore the threat is bottled up.

The reality is that the quarantines will leak, and the virus begins to spread anyway. Containment strategies leak, just like many of our controls in cybersecurity.

It's worth examining what pandemic containment involves. It's really a series of different strategies all applied in diverse ways.

First, there is the isolation of infected individuals, which is like using anti-malware and bot-detection tools to lock down specific machines. There are quarantines applied to geographic areas, which are analogous to how we use network segmentation with firewalls. There is also tracking of person-to-person contact of infected persons, which is akin to how we perform logging and monitoring.

Finally, there are imposed travel restrictions with checkpoints, which are comparable to how we use decryption and traffic inspection to filter out threats.

However, despite all these controls, no one who's worked in the cybersecurity world would expect them to work perfectly.

That doesn't mean we should ditch our firewalls.

Quarantine, especially on a mass scale, isn't expected to stop a pandemic dead in its tracks. Like firewalls, containment controls are about managing and reducing the threat. Managing can mean reducing a flood to a river. It can mean giving us more data about the size, velocity, and nature of the threat.

Most importantly, containment can buy us time so that we can get our other defences ready. Expect containment methods to leak and plan accordingly.

Time is the most precious resource

Whether it's a cyber threat or a pandemic, every second counts. Tools like containment give us more time. But we also need to leverage other options. We need intelligence on what threats are coming, what they look like, and what assets they might be coming after. We need data and thoughtful analysis to optimise our time. We need to plan, prepare, and practice in advance so that we have the right responses and tools ready to go.

Part of that preparation is to make sure the executives are well-briefed on potential threats and consequences. This, too, takes time and, in a crisis, you may not have enough to fully explain, or worse, correct misconceptions. This is especially true with media sometimes polarising individuals into either fear or denial. Neither is helpful. The goal is to help executives

make wise decisions.

While we want people to have the appropriate level of caution regarding the threat, it must match the level of risk. For example, it is problematic to over-emphasise a specific threat, such as advanced attackers and ignore more likely (and possibly overlapping) problems like phishing.

It is vital to paint a realistic picture by quantifying damages and likelihood as clearly as possible. It also helps to speak in terms of the business, not technology. Consider all the other risks and challenges that executives are dealing with, such as competitors, technological changes, recessions, layoffs, regulatory changes. Sometimes getting hacked just isn't a big deal compared to other problems going on.

"Tri" in triage means three

In its most basic form, triage is about making life or death decisions while being pressed for time and resources. When faced with an overwhelming influx of patients, such as in a pandemic, medical professionals are trained to categorise people as follows:

- Those who are likely to live, no matter what we do. These patients can wait.
- Those who are unlikely to live, no matter what we do. We make them as comfortable as we can, but they wait, as well.
- Those for whom immediate care might make a positive difference in the outcome. These we expend resources to treat.

All of these are trade-offs, but the goal is to save as many lives as you can with the resources you've got. It's always better to be proactive. In a pandemic, this can mean hospitalizing the most vulnerable population, the very young or old, as well as asking others self-quarantine unless their symptoms become dire.

In some cybersecurity incidents, we may find ourselves needing to do the same thing. With a good updated inventory, we can prioritise our most important and vulnerable applications. Other lower priority compromised systems may not be worth saving and just rebuilt from bare metal using automation.

Consider the spread of malware or an attacker moving within an organisation. It's better to lose a handful of systems while you put monitoring and remediation in place to harden the rest.

Be a town-planner instead of a firefighter

In summary, it is crucial to be a town-planner instead of a firefighter:

- Use containment to pump the brakes on the spread, but don't assume it will be airtight.
- Have strategies in place to maximise the use of your most precious resource: time. Part of making effective use of time is to provide clear, realistic, and data-driven communication to the key decision-makers.
- Be prepared to proactively make tough decisions about what can be saved and what can be sacrificed with an eye on minimising total damage.

When a big crisis hits, don't expect to have time or resources to think about these tactics at the time.

ABOUT THE AUTHOR

Raymond Pompon, Director of F5 Labs at F5 Networks