CISO to CISO

What Can Pandemics Teach Us About Cyber Security?

Raymond Pompon

Abstract:

How the world responds to Coronavirus can teach cyber-defenders a lot about risk communication, incident response, and how controls work… or don't.

Mobile World Congress: cancelled due to Coronavirus.[i] IBM and others pulled out of the RSA Conference for the same reason.[ii] Supply chains are in jeopardy, since so much technology is manufactured in China.[iii] It seems even we in the tech world can't avoid getting pulled into the Coronavirus gravity well.

While this pandemic isn't hitting most of us yet with deadly force, in time, it could cause some very serious disruptions for many organizations and individuals. Not to downplay the severity of a pandemic, but I think there are some useful parallels to how we manage cyber-threats.

Containment is Never Perfect

One of the first moves in pandemic response is to issue a quarantine to contain the spread of the virus. The People's Republic of China did that with the city of Wuhan on January 23rd. [iv] A layperson's concept of quarantine is simple: nothing leaves, and therefore the threat is bottled up. The reality, as we've seen, is that the quarantines will leak, and the virus begins to spread anyway. We are seeing the same process repeat itself on a small scale with a cruise ship in

Tokyo where passengers were released but found to still be infected.[v] Containment strategies leak, just like many of our controls in cyber-security.

It's worth examining what pandemic containment involves. It's really a series of different strategies all applied in diverse ways. First, there is isolation of infected individuals, which is similar to how we use 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 tracking of the person-to-person contact of infected persons, which is similar to how we do logging and monitoring. And lastly, there are imposed travel restrictions with checkpoints, which are comparable to how we use decryption and traffic inspection to filter out threats. However, given all of these controls, no one who's worked in the cyber security world for any length of time would expect them to work perfectly.

Does this mean we should throw away our firewalls? No. Quarantine, especially on a mass scale, isn't expected to stop a pandemic dead in its tracks. Like firewalls, these containment controls are about managing and reducing the threat. Managing can be 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 defenses ready. We have referred to this concept before as assume breach. Defenders should expect our containment methods to leak and plan accordingly. After all, containing the threat is just one of the tools in our kit.

Time is the Most Precious Resource

In a situation when threats are directly impacting important services and assets, 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 tools. 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 show is how to best use our time. We need to plan, prepare, and practice in advance so that we have the right responses and tools ready to go when everything goes crazy in an incident.

Part of that preparation and making the best use of time is to make sure the executives are well-briefed on the potential threats and the likely consequences. This, too, takes time, and in a crisis, you may not have enough to fully explain, or worse, correct misconceptions. In a pandemic, media stories can sometimes cause reactions that polarize individuals into either fear or denial. Neither is helpful and the truth lies somewhere in between. The goal is to help executives make wise decisions.

Sometimes people are overly afraid of a particular threat. Although total panic is great cardio, it's not very supportive to the overall goal. We need to ensure that people focus their energies on the riskiest issues at hand and not be distracted by dread regarding unlikely scenarios. Taking another lesson from pandemics, consider the message from the World Health Organization: "This is a time for facts, not fear."[vi] We want people to have the appropriate level of caution regarding the threat, but it must match the level of risk. However, some people can get overly fixated on a particular threat, such as advanced attackers, while not looking at more likely (and possibly overlapping) problems like phishing.

Sometimes people aren't worried enough, and we need to give them sufficient reasons to properly prepare for the real threats. This is the most common issue that cyber-security professionals have to grapple with. One key is to make sure you paint a realistic picture by quantifying damages and likelihood as clearly as you can. It also helps to speak in terms of the business, not technology. In the end, executives may still not respond unless the risk to their objectives is high. Consider all the other risks 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.

The "Tri" in Triage Means Three

When the threat really does land home, we need to know how to respond effectively. Medicine has a concept you may have heard of called *triage*. In its most basic form, triage is about making life or death decisions while being pressed for time and resources. The key is that the "tri" in triage means three, just like in triangles and tricycles. So, when faced with an overwhelming influx of patients, such as in a pandemic, medical professionals are trained to categorize people into three buckets:

1. Those who are likely to live, no matter what we do. These patients can wait.
2. Those who are unlikely to live, no matter what we do. We make them as comfortable as we can, but they wait, as well.
3. Those for whom immediate care might make a positive difference in 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 also better to be proactive than reactive. You choose who is going to be saved based on your criteria instead of relying on random chance or personal bias. In a pandemic, this can mean hospitalizing the most vulnerable population, the very young or very old, and asking the healthier to self-quarantine unless their symptoms become dire.[vii]

In some cybersecurity incidents, we may find ourselves needing to do the same thing. With a good updated inventory, we can prioritize 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 organization; it's better to lose a handful of systems while you put monitoring and remediation in place to harden the rest.

Conclusion

There's a lot of attention on pandemics and there are a few key lessons cyber security professionals can draw from how global health professionals are responding. One is use containment to pump the brakes on spread, but don't assume it will be airtight. Second is to have strategies in place to maximize 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. Lastly, be prepared to proactively make tough decisions about what can be saved and what can be sacrificed with an eye on minimizing total damage. Most of all, you

can expect that if a big crisis hits, expect not to have time or resources to think about these things at that time. Put in the plumbing now by preparing and understanding what you need to do.

---

[i] https://www.theverge.com/2020/2/12/21127754/mwc-2020-canceled-coronavirus-trade-show-phone-mobile-world-congress-gsma-statement

[ii] https://www.cnet.com/news/coronavirus-prompts-ibm-rsa-conference-facebook-to-cancel-california-summit/

[iii] https://www.theverge.com/2020/2/18/21141924/coronavirus-tech-industry-impact-report-trendforce

[iv] https://www.nytimes.com/2020/01/22/world/asia/china-coronavirus-travel.html

[v] https://www.axios.com/coronavirus-ship-quarantined-10-infected-japan-2ec35f8c-e340-4c25-8838-32293371da8c.html

[vi] https://news.un.org/en/story/2020/02/1057481

[vii] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1635755/