Seven Cybersecurity Lessons the Coronavirus Can Teach the Armed Forces (and Us All)

Dr. Mike Lloyd
Ray Rothrock

If we have learned anything from the COVID-19 pandemic, it is that very bad things can happen very quickly, especially if we are not sufficiently prepared. It turns out that everything we have been told about the pandemic is also relevant for cybersecurity; as such, the pandemic is an exceptional learning tool for cyber professionals.

Cyberattacks are like biological viruses in several ways: they can spread incredibly fast, their consequences can wreak huge economic damage, and the destruction they cause can be very difficult from which to recover. Viruses spread through human social networks and cyber-attacks exploit our online networks of trust.

Viruses and cybercrime are conceptual and invisible, which can make it challenging to understand how they propagate and how they can be stopped. Analogies can be helpful, and there is a strong connection between COVID-19 and cybersecurity that can increase our understanding. We have been forced to learn what it takes to stop a virus; those lessons are helpful here.

Security leaders have long predicted that a major cyberattack was right around the corner and that it would fundamentally alter society as we know it. In 2013, Secretary of Homeland Security Janet Napolitano predicted, "Our country will, at some point, face a major cyber event that will have a serious effect on our lives, our economy and the everyday functioning of our society."

COVID-19 proves that the world is truly at great risk of disruption. It should lead those of us in cybersecurity to think of what a COVID-like cyber event might look like: no clear attacker, no clear symptoms, a lot of doubt about who or what has been infected, who is carrying the disease and who is not, a lot of disturbance–and the need to break out of the normal ways of doing things.

Dr. Mike Lloyd is an epidemiologist-turned-chief technology officer of RedSeal, a cloud security company. He holds 21 patents earned over more than 25 years of modeling and controlling fast-moving, complex security and network systems. His leadership as CTO has propelled RedSeal and its technology to win nearly 30 awards for excellence since 2018.

To prepare for this kind of event–one that will spread fast and far and will have an equal or greater economic impact–here are seven lessons security teams can glean from the pandemic.

#1: Understand Lateral Movement

Our lives are globally interconnected, and we spread disease as we connect with each other. The fact is that this pandemic started in one country and spread to even small, remote island communities is the first example in our lifetime that makes this point on a global scale.

Similarly, digital attackers need to only breach one target to start their infiltration. However, despite security teams' best efforts, it is impossible to protect all our networks down to every endpoint all the time.

Once an attacker finds an "in" to the network, it usually takes just a few lateral moves to get from one place to anywhere else on the network. Unfortunately, there are still organizations where, once the intruder gets inside their network, it is too easy to move around. An attacker can stay hidden and move with impunity.

The analogies are so close that it is difficult to distinguish when we are talking about lateral movement of a disease and when we are talking about lateral movement of cyber attackers. They really do behave in similar ways.

In this analogy, air travel and super-spreader events are opportunities for real-world bugs. When we wear masks, wash hands and practice social distancing, we greatly reduce the virus' opportunity for lateral movement. Likewise, digital defenders need to break up lateral movement across their complex networks–essentially social distancing for the network brought about by reducing access to critical assets.

Ray Rothrock is executive chair of RedSeal, and the author of *Digital Resilience: Is Your Company Ready for the Next Cyber Threat?*, one of the Top 10 must-reads on information security. He has three decades of investing in, advising and leading many of the tech and cyber companies that form the fabric of today's networks, and is a member of the Nuclear Threat Institute's Board of Directors and its Science and Technology Advisory Group.

#2: Identify Problem Areas

Some countries–and even cities–have better success in fighting coronavirus because they can quickly identify where the disease really is, and focus efforts to stop its progress. This is why testing is so important and why communities that use contact tracing to identify carriers and their contacts, test them promptly, and quarantine as necessary make strong progress in reducing infection rates.

Digital security is the same. Teams work to know where their network is infected, and then response teams scramble to quarantine or block the intruders. When they are able to know quickly where the problem is, they can respond more effectively and efficiently to prevent its spread.

Unfortunately, the cyber version of contact tracing is much harder because computers communicate across a network in many different and shifting directions. The equivalent would be if contract tracers had to deal with every person on earth flying to at least one new country every day.

The best course of action is to map out a network well ahead of an attack and understand where one's critical assets are. Security teams need to understand all the access pathways and normal information flows for the organization ahead of time. Thankfully, automation products exist to help network managers keep track of all the detail and the constant changes.

#3: Slow the Spread

By sheltering in place and not coming in contact with other people, we impede the coronavirus' ability to spread among the population. As a result, this global effort to stay home and "flatten the curve" reduces strain on our taxed medical systems.

Similarly, when digital defenders wall data and network communications into distinct areas, they can make it harder for attackers to expand their intrusion. We cannot stop every determined attacker or nation-state, but we can slow it down. Ultimately, slowing attackers down buys time to detect them so one can effectively respond by blocking or quarantining them.

#4: Practice Good Hygiene

Basic hygiene is the main way we have to combat the spread of COVID-19. Our first line of defense in this unprecedented pandemic is everyone's consistent use of basic hygiene: hand washing, not touching faces, and using face masks 100% of the time when in public. People not practicing basic hygiene eventually endanger us all by increasing the probability of a viral transfer.

Similarly, not practicing basic cyber hygiene endangers organizations. Poor or inconsistent cyber hygiene includes failing to change passwords regularly, randomly clicking on inter-network links, or neglecting to enable all available security features on devices, such as firewalls and antimalware.

The good news is that it is possible for people to improve their hygiene habits. The pandemic showed us that hundreds of millions of people can change their behavior if they think they or their loved ones are at risk.

Basic cyber hygiene depends on applying current security advice, not just in one or two places, but consistently across one's entire organization, network, and its component parts. This means the organization will be less likely to battle common cybersecurity issues.

Device hardening, dual-factor authentication, and other practices are critical to tamping down the threats and reducing the attack surface. These may be even more important than the best technological defense.

One must know what devices are on the network; one also wants to make sure those devices are securely configured. One needs to confirm the network is set up as intended, and, when something changes, one needs confirmation that the network's security is up to the challenge. Cyber wargaming plays an important role here. Cyber terrain modeling can automatically map networks and identify defensive weaknesses.

Real-world networks are riddled with unintentional hygiene failures. As with fighting this pandemic, even 95 percent compliance with basic hygiene standards is not enough. It takes only one unintentional exposure for COVID-19 to spread, and it is the same for cyber as well. That is why it is imperative to perform the basics well, everywhere, all the time.

#5: Adapt and Evolve

Humans are the most successful animals on the planet because of their adaptability.

Network defenders need to adapt and evolve, too. What was considered decent security yesterday is routinely out of date today. Tactics keep shifting, new vulnerabilities are continually

discovered, and the rules for defense never settle down. We can continue to get better at blocking certain kinds of cyberthreats, but as soon as we do, the attackers will find a way around. This means our countermeasures must keep changing.

When battling real viruses, we cannot win with rigidity. The only long-term advantage is to maintain adaptability. In cyber, we must be flexible, and we can do that only by modelling and understanding—in effect, to do the equivalent of war games against our networks.

Security teams should plan to become adept at the sort of penetration-testing exercises that the average company currently does only once a year or so. Cyber threats and coronaviruses continually evolve and adapt. One needs to do the same, because every day will present a new and different set of challenges.

#6: Social Distance the Network

Modern computing allows software to run with wild abandon, sharing virtual machines and containers on limited physical resources. At first, this was a great advantage, because we could make one computer do the job of several and we could reallocate inefficiently used resources to where they could make a difference.

However, in the face of the ever-shifting cyber landscape, one of network security teams' greatest challenges is getting overwhelmed. To avoid this, they need to adopt and apply new strategies and ideas. In this case, social distancing is one of the most important lessons to carry from the pandemic into online security.

Security personnel must think like public health professionals: We know interactions—between people and networks—are necessary. As a result, there will always be the risk of something nasty getting inside. Perfect prevention is not an option.

Consequently, we manage the risk of a dangerous world by asking for reasonable accommodations. This compromise results in social distancing for people or, its online equivalent, network segmentation.

While social distancing helps, it does not guarantee perfect protection. Similarly, we must address cybersecurity on the assumption that someone will infiltrate the network. Of course, completely disconnecting from the outside world is not the answer in either case. Networks across all industries—from banking and finance to military, healthcare, and industrial operations—need to connect to perform their functions, deliver value, and provide efficiencies. Creating controls in the network increases the barriers between systems and intentionally keeps separate things separate.

#7: Embrace Resilience

The COVID-19 pandemic is ongoing. Prevention measures like hand washing, social distancing and wearing masks (particularly in enclosed public spaces) are essential but are not always foolproof.

Similarly, to counter cyberattacks, the primary strategy to-date has been prevention. Prevention however, in the form of traditional firewalls and antivirus systems, is falling short. Cyberattacks are now so advanced that, should a hacker's attention turn to one's organization, the attack will almost certainly succeed. Consider this one startling fact: Despite rising cybersecurity budgets that now reach billions of dollars annually, cyber losses continue to outpace cyber investments dramatically.

Clearly, we need more than prevention. We need resilience. For people, that means staying healthy, eating a balanced diet, getting sufficient rest, exercising regularly, keeping stress levels low, etc.

For cybersecurity, the best defense is also to be resilient. Resilience is the ability to take a punch and then continue to function, keep the lights on, and stay productive even while fending off or countering a cyberattack. Resilience means showing one's leaders not just how one intends to protect everything, but also explaining how the organization can quickly recover when the inevitable attacks occur.

CONCLUSION

There are important security lessons we can take from the current pandemic to make modern networks stronger and more resilient. This article has highlighted seven characteristics of the COVID-19 pandemic that have direct parallels with cyber attackers and our network security measures. Whatever the world looks like after this pandemic passes, viruses, hackers, and cyber criminals will continue to develop new ways of attacking their targets. Furthermore, the first and strongest line of defense is, and will always be, basic hygiene.