Pandemic Parallels: What Can Cybersecurity Learn From COVID-19?

Steven Furnell, University of Nottingham

Julie Haney and Mary Theofanos, National Institute of Standards and Technology

While the threats may appear to be vastly different, further investigation reveals that the cybersecurity community can learn much from the COVID-19 messaging response.

COVID-19 impacts may be more extreme than those of cybersecurity, this article explores the similarities, especially the challenges inherent in how people manage risk and respond to these threats. A better understanding of the parallels can inform our future approach to tackling the promotion of cybersecurity and response to cybersecurity threats.

The COVID-19 pandemic has demonstrated society's dependence on information technology, including the need for adequate cybersecurity to protect the remote workforce and the technologies we are using. Beyond this direct linkage, there are further parallels that can be drawn between COVID-19 and cybersecurity threats. While acknowledging that COVID-19 and cybersecurity threats share characteristics that make them challenging to communicate and mitigate. We also acknowledge that there are differences between the two threats.

COMPARING COVID-19 AND CYBERSECURITY THREATS

The nature of the threat

COVID-19 is a new strain of the coronavirus and may mutate over time, with symptoms varying from one person to another. Similarly, cybersecurity threats can take many forms and change over time. Despite the evolving nature

Digital Object Identifier 10.1109/MC.2020.3046888
Date of current version: 12 March 2021

EDITOR **JAMES BRET MICHAEL**
IEEE Senior Member; bmichael@nps.edu

of both, there are still safeguarding behaviors that mitigate the risk, at least to some degree. With COVID-19, mitigations include handwashing, social distancing, face coverings, and disinfecting surfaces. These, in turn, affect our interactions in numerous contexts. Similarly, basic cybersecurity safeguards (for example, using antivirus software and strong passwords and not clicking on suspicious attachments) apply across numerous systems and services but also vary depending on the context (for example, work versus home).

Another striking similarity in both COVID-19 and cybersecurity is that affected parties can be asymptomatic. Just as those showing no signs of a COVID-19 infection may inadvertently pass it on, the same may be true of our connected but infected systems. Just because systems are not showing signs of being breached does not mean they haven't actually been compromised. While some might dismiss this as a fear-based argument, there is much evidence of this being the case with malware infections, advanced persistent threats, and other vulnerability exploitations.

For both COVID-19 and cybersecurity, the consequences of infection and transmission may not be easily observed, may be delayed, or may vary in intensity. Without a tangible, immediate impact, the connection between actions and negative consequences can be hard to spot. In the case of asymptomatic individuals with COVID-19, without robust contact tracing, we may have no way of knowing how many others they might have infected. There is also variability in the time between infection and onset of symptoms and intensity, ranging from severe and debilitating to mild (or no) symptoms. As in COVID-19, the short-term consequences of cybersecurity errors may be severe (for example, a financial loss or major disruption to critical infrastructure) or milder and more easily recoverable (for example, a password reset on a personal email account). In addition, there may be long-term effects of both threats. With COVID-19, there may be permanent organ damage,[1] while in cybersecurity, a system may never be able to fully recover from an attack.

Measures of effectiveness (MOEs) for safeguards are another basis for comparison. The cybersecurity community may have a difficult time determining cause and effect because MOEs may be less defined and influenced by confounding variables. For example, are the number of attacks down because of implemented countermeasures, or have the attack vectors or targets changed? Or is it actually because the capability to effectively monitor and identify threats is inadequate? In contrast, COVID-19 MOEs can be scientifically captured to some degree (for example, positivity rates, medical trials, and transmission simulations), even given the unknowns on long-term effectiveness. However, similar to cybersecurity, it can be difficult to establish a causal relationship between COVID-19 countermeasures and trends, given other influencing factors.

Attitudes and behaviors

There are also parallels between the two threats in terms of people's attitudes and behaviors. Both tend to disrupt normal behavior and demand actions that most people would not otherwise take. Therefore, these protective actions may be perceived as being anywhere from mildly inconvenient to significantly disruptive. Over time, fatigue, frustration, and eventual noncompliance may result, even when initial motivation was strong.[2,3]

Another shared factor is the contested nature of the actions required to defend against the threat. There are those who don't use the accepted safeguards in both contexts, and, although best practices exist, there can often be disagreement about the best course of action. With COVID-19, there is still uncertainty about the efficacy of certain countermeasures or treatments, while in cybersecurity, some still insist that safeguards, such as antivirus software, do more to degrade the system performance than they do to protect. We also find people contesting the fundamental nature of the threat itself. COVID-19 has been met with differing views of the severity of the threat. With cybersecurity threats, there are still those choosing to dismiss threats—it is not difficult to find rumors that the industry itself has created malware to sell products.[4]

Both contexts include groups that think they are less susceptible or unlikely to become a victim. With COVID-19, this is exemplified by children and adolescents, who generally experience less severe symptoms.[1] In cybersecurity, we have a parallel with Mac users' frequent belief that they are safe from malware.[5] Unlike the pandemic, cybersecurity breaches are the result of deliberate, targeted actions by active adversaries, so people may not expect to be targeted and don't see themselves as potential victims. However, in both cases, the reality is that they are not immune—they may be less likely to be adversely affected but may still be impacted and ultimately impact others.

Social influence and peer pressure play a role in risk-related behaviors.[6] Adolescents and young adults might not wear face masks to protect against COVID-19 due to social or peer pressure.[7] The social norms of family and friends and workplace culture can affect cybersecurity decisions,[8] for example, adolescents sharing passwords with friends as a display of trust.

Additional risk arises if people simply don't understand what needs to be done, for instance, when rules

are fundamentally unclear or because people cannot relate to them. This is common in cybersecurity, where many don't have the skills or knowledge to implement certain countermeasures. As such, it is important to consider how successfully the threats and mitigations have been framed for their target audiences.

Mastering the messaging

Despite some pushback, one success in dealing with COVID-19 has been the ability to quickly get messages to a wide population. Consider the United Kingdom, where the initial lockdown period was accompanied by clear messaging appearing everywhere across broadcast, print, and online media: "Stay home, Protect the NHS, Save lives." These three brief statements conveyed what people had to do (stay home) and why they had to do it (to protect others and the National Health Service). A later iteration, "Hands. Face. Space."[9] [accompanied by icon-style imagery (Figure 1)] arguably provided the simplest and most directly instructive slogan.

By contrast, cybersecurity risk communication lags behind and cannot claim to have a similarly widespread or effective campaign behind it. The long-standing Stay Safe Online message of "Stop. Think. Connect."[10] clearly has a similar punchy style but is arguably less successful in encapsulating both the "what" and "why" aspects into the guidance. Cybersecurity guidance may feel less tangible than health advice, consisting of more abstract concepts not easily understood by the general public and more diversity of countermeasures depending on the specific threat. Although there are medical complexities with COVID-19, most people tend to understand the basics of infectious disease and are accustomed to frequently washing their hands, staying home when sick, and taking preventative measures such as getting an annual flu shot.

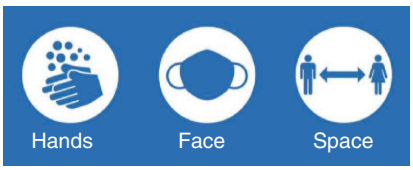

FIGURE 1. The U.K.'s COVID-19 messaging.

Both contexts still face the challenge that, as the threat evolves, so too does the messaging about what to do about it. For example, in the lockdown stages of the pandemic, the messaging was clear—stay home and don't socialize. This is straightforward to follow. In the cybersecurity context, it equates to policies such as banning personal devices in the workplace or not connecting certain systems to the Internet. However, as soon as you relax beyond the extreme position, there are shades of gray and the potential for confusion. If you start to allow people to go out and socialize, where can they go, and how many people can they see at a time? If you allow personal devices in the workplace, what are the bounds of permitted use?

The challenge of keeping track of changing guidance as threats evolve or become better understood plagues both contexts. By the time baseline advice becomes widely known, the situation has often changed to the point where additional or amended advice is required to ensure sufficient protection. For example, people in both the United States and the United Kingdom were originally told that face masks weren't effective, but the advice changed as new information came to light.

The same challenge also applies to cybersecurity, albeit with less rapid change, for example, the changing nature of password guidance, where, for many years, the standard advice was to include a mixture of character types. This requirement was set aside in the National Institute of Standards and Technology's 2017 Digital Identity Guidelines,[11] which were based on the recognition that it doesn't usefully contribute toward preventing password breaches but certainly hampers usability. Nonetheless, several years later, there is still much password guidance (and enforcement) related to character complexity. Unfortunately, in both the COVID-19 and cybersecurity contexts, the change of guidance causes some people to question the validity of the advice and credibility of the source and use the fact that the guidance changes as a justification for not following it at all.

Individual benefit versus public good

We also observe parallel tensions between individuals and the public good. With COVID-19, individual rights are often cited by those refusing to wear masks. Proposed contact tracing via mobile phone apps was met with concern about the potential for privacy violations. Cybersecurity is also often viewed as being at odds with privacy, with an emphasis on one seen as detrimental to the other.

Decisions to adopt protections are motivated by different drivers: the desire to protect oneself or the hope of protecting others. The former is obvious with COVID-19, especially among those considered to be high risk. The latter is explicitly headlined in terms of the use of face coverings. The concern for others is perhaps less pronounced but no less applicable to cybersecurity. The Mac community again provides a good example. How many use antivirus software with the aim of blocking Windows malware that, while harmless to them, could affect others if passed on? The answer is likely very few.

Another scenario is when vulnerable home systems, including the Internet of Things (IoT) devices, are co-opted into botnets and used to launch attacks against others. The users whose systems have been compromised may not experience any direct negative consequences, but their security failure becomes the basis for harming someone else. Both examples illustrate that, when compared to the general willingness to take steps to contain a virus like COVID-19, a clear sense of community protection in the cybersecurity realm is lacking. This is not surprising given the difficulty for many to conceptualize how cybersecurity relates to them personally, let alone how their behaviors might affect others.

WHAT CAN WE LEARN?

By observing the parallels and differences, we identify several lessons from the COVID-19 response applicable to cybersecurity.

Carefully craft the message

In general, COVID-19 messaging has been clear, actionable, and successful in bringing widescale awareness. As learned in the early days of COVID-19, guidance should be consistent and accurate to establish credibility and trust in the message and its source. Studying the United Kingdom's "Hands. Face. Space." message, a similar trio of cybersecurity reminders for the general public could be something such as "Device. Identity. Data." (DID) (Figure 2). This highlights three components that people should recognize need safeguarding, and it even offers the potential for developing slogans (for example, "Cybersecurity? I DID it!"). Cybersecurity can also learn from COVID-19 messaging emphasizing community protection since this concept is difficult for most to conceptualize with cybersecurity.

Realize it's more than the messaging

Other significant influences (for example, biases and social pressures) may be difficult for simple messaging to overcome. The pandemic has demonstrated that messaging should be part of a framework of protections. However, that wider framework must be ready to handle the result of effective messaging. For example, with COVID-19, the messaging that people should get tested if they experience symptoms was frequently undermined by confusion about how and where to get tested; people became aware of a safeguard they subsequently couldn't access. In cybersecurity, there are similar examples. There's no point in having a "report phishing" campaign if an organization isn't prepared to handle the reports that it subsequently receives.

Implement tiered defenses

In both health and cybersecurity, campaigns that depend solely on the actions of the general public are seldom 100% successful. New habits take time to form and can be hampered by multiple factors, including the evolving understanding of the threat and best practices. Practices may also be overly burdensome, resulting in fatigue, noncompliance, or slipups. This fatigue is especially evident with COVID-19; people are asked to modify their "normal" behavior, compliance can be isolating and stressful, and its effectiveness may be unclear if infection numbers fail to drop. While there is hope that the effects of the pandemic will be temporary, cybersecurity is for a lifetime. Unfortunately, placing an undue burden on users who do not have a strong grasp of security has been a fundamental problem for decades.

COVID-19 has shown that a tiered system of defenses can be effective. Consider, for example, local and national guidelines governing the safe operation of businesses in addition to what individuals can do. The same layering can be applied to cybersecurity. The efficacy of utilizing strong authentication and wariness of suspicious emails on an individual level is limited if the underlying authentication structure is vulnerable or the email provider doesn't filter out known-bad or suspicious content. Whereas many regions of the world implemented mandatory border restrictions or stay-at-home orders to combat the spread of COVID-19, there is also a need to better understand the potential role of mandatory cybersecurity policies in certain circumstances, for both the good of the individual and society.

FIGURE 2. Cybersecurity reminders.

Given the parallels, cybersecurity can learn valuable lessons from the COVID-19 messaging response. One could argue that we've seen more effective large-scale messaging and enforcement of safeguards with COVID-19 precisely because it poses a greater risk. However, while cybersecurity threats have not yet had the same urgency or widespread impact, there is the potential of life-impacting consequences, for example, if connected health devices or safety-related IoT devices are hacked. The public awareness of cybersecurity is lagging behind relative to the time it has been with us but must catch up before there's a more serious cybersecurity event on a global scale.

DISCLAIMER

These opinions, recommendations, findings, and conclusions do not necessarily reflect the views or policies of the National Institute for Standards and Technology or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for government purposes, notwithstanding any copyright annotations thereon.

REFERENCES

1. "Coronavirus (COVID-19)," Centers for Disease Control and Prevention, Atlanta, GA, 2020. [Online]. Available https://www.cdc.gov/coronavirus/2019-ncov
2. S. Furnell and K. Thomson, "Recognising and addressing 'security fatigue'," *Comput. Fraud Secur.*, vol. 2009, no. 11, pp. 7–11, 2009. doi: 10.1016/S1361-3723(09)70139-3.
3. B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman, "Security fatigue," *IT Prof.*, vol. 18, no. 5, pp. 26–32, 2016. doi: 10.1109/MITP.2016.84.
4. N. Lopez. "Kaspersky Antivirus accused of creating fake malware for over 10 years." The Next Web. https://thenextweb.com/insider/2015/08/14/kaspersky-antivirus-accused-of-creating-malware-for-over-10-years/ (accessed Dec. 7, 2020).
5. A. Hope. "Macs are no longer safe: Report shows macs' malware threats outpace windows by 2:1." CPO Magazine. https://www.cpomagazine.com/cybersecurity-security/

macs-are-no-longer-safe-report-shows-macs-malware-threats-outpace-windows-by-21/ (accessed Dec. 7, 2020).
6. M. Gardner and L. Steinberg, "Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: An experimental study," *Develop. Psychol.*, vol. 41, no. 4, p. 625, 2005. doi: 10.1037/0012-1649.41.4.625.
7. R. F. Wilson, "Factors influencing risk for COVID-19 exposure among young adults aged 18–23 years—Winnebago County, Wisconsin, March–July 2020," *Morbidity Mortality Weekly Rep.*, vol. 69, no. 41, pp. 1497–1502, 2020.
8. L. Coventry, P. Briggs, J. Blythe, and M. Tran, "Using behavioural insights to improve the public's use of cyber security best practices," Government Office for Science, London, 2014. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf
9. "New campaign to prevent spread of coronavirus indoors this winter," Department of Health and Social Care, London, 2020. [Online]. Available: https://www.gov.uk/government/news/new-campaign-to-prevent-spread-of-coronavirus-indoors-this-winter
10. "STOP. THINK. CONNECT." National Cybersecurity Security Alliance. https://staysafeonline.org/stop-think-connect/ (accessed Oct. 13, 2020).
11. P. A. Grassi et al., "Digital identity guidelines: Authentication and lifecycle management," National Inst. of Standards and Technol., Gaithersburg, MD, NIST Special Publication 800-63B, 2017. [Online] Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

STEVEN FURNELL is a professor of cybersecurity at the University of Nottingham, Nottingham, NG8 1BB, U.K. Contact him at steven.furnell@nottingham.ac.uk.

JULIE HANEY is a computer scientist at the National Institute of Standards and Technology, Gaithersburg, Maryland, 20899, USA. Contact her at julie.haney@nist.gov.

MARY THEOFANOS is a computer scientist at the National Institute of Standards and Technology, Gaithersburg, Maryland, 20899, USA. Contact her at marytheo@nist.gov.

Digital Object Identifier 10.1109/MC.2021.3059058