Title [60 characters]: Cybersecurity lessons learned from COVID-19 pandemic

Meta description [max. 156 characters]: What cybersecurity lessons should companies learn from the COVID-19 pandemic? Review them here, and learn how to apply them going forward.

Summary [150-180 characters]: Cybersecurity lessons companies learn from the COVID-19 pandemic include having work-from-home preparations and developing disaster recovery and business continuity plans.

☒ Article Visuals

https://cdn.ttgtmedia.com/rms/onlineimages/business_recovery_and_continuity_bookcover.png
Alt text: Business Recovery and Continuity in a Mega Disaster book cover
Caption: Learn more about *Business Recovery and Continuity in a Mega Disaster: Cybersecurity Lessons Learned from the COVID-19 Pandemic* here.
URL: https://www.routledge.com/Business-Recovery-and-Continuity-in-a-Mega-Disaster-Cybersecurity-Lessons/Das/p/book/9780367685737

Body [?]:

Few companies were prepared for COVID-19 and the disruptions it brought -- especially when it came to cybersecurity. Companies had to quickly adjust to secure a remote workforce, to protect corporate networks being accessed from potentially risky home networks and to address new threats, such as Zoombombing.

A silver lining from the pandemic is companies have a number of lessons to learn from. Author and security researcher Ravi Das wrote Business Recovery and Continuity in a Mega Disaster: Cybersecurity Lessons Learned from the COVID-19 Pandemic *to help organizations do just that.*

Here, Das discusses why he wrote the book, the importance of endpoint security and how to prepare for future pandemics or natural disasters.

Check out an excerpt from Chapter 3 that covers the importance of securing endpoint attack surfaces -- a common target for cyber attackers during a pandemic.

Editor's note: The following interview has been edited for conciseness and clarity.

What was your motivation to write the book?

Ravi Das: In 2019, we saw warning signs of COVID-19 in China. I and many others thought it would stay localized to the Wuhan province; never did we imagine it would spread all over the world. Then, it did. During this time, I saw so many things that went wrong but could have been avoided -- we weren't ready to handle a global pandemic. I wanted to write a book geared toward CISOs that serves as a roadmap of what we learned and what we can do better if another pandemic or incident occurs.

Can you share some of those lessons learned?

Das: The first is there should have been a better transition companywide to work from home. Nobody knew COVID-19 would happen the way it did, but companies should have been worried about natural disasters or weather keeping people from the office. There should be a stack of laptops and wireless devices with the latest security protocols ready to hand out to employees. Everything was done in haste for this pandemic.

Another lesson is to have incident response and business continuity plans in place. Many companies still don't have them; they don't understand the magnitude and importance of having such plans. The plans should be rehearsed quarterly to make sure everyone knows what to do.

A third big lesson is understanding where data sets reside and ensuring they're safeguarded. Part of the challenge is linked to BYOD and the rapid move to work from home. A lot of employees gave up waiting for a company-issued device and began using their own. This created shadow IT with employees using unauthorized apps, which leads to more backdoors for cyber attackers.

COVID-19 was a perfect storm of if anything could go wrong, it went wrong. But things have improved since. Zoom patched its security holes, companies have stocked up on laptops, and networks are better protected as companies figured out how to deploy patches and parents kept their home network isolated from their kids.

How can companies become less reactive and more proactive to prevent the same issues from occurring?

Das: IT can deploy all the major security technologies it wants, but that doesn't mean much if employees aren't learning by example from above. The CISO needs to understand how to lead from the top down so IT managers follow their lead and then employees learn from IT managers. Everyone is demanding employees have good cyber hygiene, but employees need to know those above actually care. One way to do this is to have the CISO record a short webinar about cyber hygiene. This leaves a much stronger impression for employees to follow.

Another way to be proactive is to have the mindset that an attack could really happen, no matter how small it may be. I was talking to a prospect the other day, and they were saying, 'We're just a three-man nonprofit shop.' I told them they were a top target for a cyber attacker because, while they may not have all the valuable data, attackers will still penetrate them and move in a lateral fashion to get at any data they can.

You discuss disaster recovery, incident response and business continuity plans. Is there an order of importance to creating these if an organization has a limited budget?

Das: There shouldn't be a limited time or budget for these documents; they're not that expensive, and they really shouldn't take that long. And, if businesses can't figure out how you do that, they need to consult with an MSP or a cyber consultant that specializes in drafting these plans.

The incident response plan should come first. If you're hitting an issue, you want to mitigate things as soon as possible. Disaster recovery comes second, then business continuity last because it's more of a longer-term goal.

Note, that doesn't include any audits you'll have to do for authorities, especially if the issue was a security incident.

Why does endpoint security often get overlooked in favor of protecting IT infrastructure?

Das: Too many companies still have a reactive mindset -- the focus is often on data in transit, the back-and-forth transmitting of confidential information to sender and receiver. That's a concern, sure, but nobody seems overly concerned about endpoints. And attackers are taking notice. They may not launch threats from endpoints, but they use them as backdoors and stay covertly on devices for months. Then, they move laterally within an IT network infrastructure and figure out where the crown jewels are.

We need to do a better job protecting endpoints. Things have improved -- cloud providers are keeping up with the latest security threats, and some have their own endpoint security platform, such as Microsoft 365 Defender. But there's more to be done.

You recommend different technologies, such as security, orchestration, automation and response, as well as SIEM, in your book. Are there any others you'd suggest adopting in the wake of COVID-19?

Das: I advocate using the least amount of technology overall. Cloud companies provide all the tools and technologies you need, but ultimately, the responsibility is on you to protect your systems and data. Adopting new technology after new technology only increases your attack surface.

Remember that your IT security team has to keep up with each technology and device in the organization. It is going to have to learn about the little nuances of each tool and its log files, which could be a big waste of time.

Use the budget instead to purchase technology and strategically place it where it's needed most. Do a risk assessment, and see where your weak points are, and apply the budget toward those areas. It'll keep your attack surface from expanding and show your C-suite and board of directors that you're frugal with your budget while being strategic and thinking long term.

About the author
Ravi Das is a cybersecurity consultant and business development specialist. He also does cybersecurity consulting through his private practice, RaviDas.Tech Inc. He is also studying for his CompTIA Security+ certification.

Contributor: Kyle Johnson
Contact Editor [?]: Kyle Johnson