How Covid-19 is Dramatically Changing Cybersecurity

by **Prashant Deo,** Security Consultant
Geetali Raj, IAM Presales Lead
Ramesh Perumal, Security Solutions Lead

Abstract

The pandemic has created an enormous challenge for businesses worldwide: to continue operating despite massive shutdowns of offices and other facilities. The information technology on which they have long depended – their data centers, cloud systems, departmental servers, and the digital devices their now-remote employees used to stay connected to each other and to the company's data – becomes even more vital. Overnight, the demands placed on the digital infrastructure have skyrocketed.

Such technology also becomes a much bigger and more lucrative target for cybercriminals. Cybersecurity efforts need to be upgraded to prevent a second crisis from emerging: on the digital devices and networks that have become infinitely more vital to companies in recent weeks. In other words, "business continuity" has become a mandate.

In this article, we provide an overview of the heightening technology risks to large companies around the world from cyberattacks, and the factors driving them. We then outline ways to better protect their technology, data and other digital infrastructure in these precarious times.

A Far-More-Connected World

In just a single month, the world became far more digitally connected — and vulnerable — than ever. In March, organizations that had forever required employees to gather at a common physical location were suddenly using the Internet to facilitate remote interaction among a vast constellation of home offices. At-home employees of financial institutions have the regulatory need to ensure communications with each other and with customers about transactions are handled on private, highly secure infrastructure. Businesses are also relying on digital services to maintain the supply chain for essentials, while minimizing social contact.

Officials are depending on digital channels to reassure the public and maintain order. They are communicating rapidly evolving rules, sharing critical physiological and psychological health information, and debunking the onslaught of rumors, fraud and misinformation about bogus remedies. They are using these digital channels to urge employers to pay salaries, and consumers to avoid hoarding food, medical supplies and personal protective equipment.

As Covid-19 tests the strength of healthcare systems around the globe, healthcare providers are turning to chat, phones, email and telemedicine portals for remote counselling and diagnoses. Organizations are using digital infrastructure to procure vital protective supplies for healthcare and hygiene workers, as well as to counsel them on rendering services safely.

Finally, digital channels are providing entertainment for stressed families. They are motivating people under lockdown to make the most of their time and providing the tools to do so. And they are helping to shore up our future by enabling children to learn online while schools remain closed.

An Explosion of Cyber Risks in the Covid-19 Pandemic

The surge in communications and the wholesale shift to operate businesses online have at the same time increased the risk of cyberattacks by an order of magnitude. They have also introduced a wide range of new risks. Organizations' perimeter security is at risk of being breached. They need always-on surveillance and real-time risk analysis for breaches at both physical and digital entry points.

Security and risk management leaders now must safeguard their companies on a massive scale, and quickly. They must ensure that their enterprises' online services and digital platforms are resilient against cyberattacks.

The IT function is under tremendous pressure, too. In some firms, IT professionals must extend remote working capacity to employees who hadn't worked from home in the past. In some cases, this includes their service partners. Many IT departments are in the middle of deploying new types of collaboration software. While that can be crucial to keeping employees synchronized (especially those working in agile teams), such software increases the risk of hacking sensitive data that now resides in less secure remote workplaces.

But it's difficult for IT functions to say no to this. Company leaders, managers and their staffs need access to internal services and applications so they can conduct operations remotely. Since many companies haven't made these applications and data available previously over the Internet or virtual private networks (VPN), security leaders are reluctant to allow access without stringent access mechanisms.

Understandably, very few organizations were prepared for their workforces to be working remotely in mass. They now realize that secure remote-access capacity and protected access to enterprise systems have become a major constraint.

Enforcing enterprise security policies and controls on the remote workforce is a difficult task. Most controls have limited scalability and require considerable time to deploy. We know of some businesses that have had to allow employees to use their personal digital devices to access enterprise applications without any mechanism for enforcing security controls. For most organizations, business continuation plans (BCP) and incident response plans (IRP) are inadequate or even non-existent for dealing with pandemics. Security leaders never anticipated or tested a BCP operation on such a scale.

Fraudsters are well aware that many companies and their employees have opened the door wide to hacking. Cybercriminals are using the heightened digital footprint and traffic to find vulnerabilities, or to siphon off money. They are launching Covid-19-themed attacks in the form of phishing emails with malicious attachments that drop malware to disrupt systems or steal data and credentials. Attackers are creating temporary websites or taking over vulnerable ones to host malicious code. They lure people to these sites and then drop malicious code on their digital devices. Fake websites have also been soliciting donations for daily wage earners through email

links. Some Covid-19 patient count-status apps and links are laden with viruses and identity theft malware. Remote working tools such as videoconferencing systems have been hacked for vulnerabilities; recent examples on Zoom are alarming.

A Robust Cybersecurity Response

In this new environment, cybersecurity professionals must aggressively confront the risks. For starters, they need to quickly make their company's remote workforce aware of scams, and then train them how not to fall victim to them. E-learning or web-based training platforms are valuable here.

But that is only the beginning. Much more needs to be done, as we'll explain. In addition, IT security professionals need to keep an eye on the medium and long term, recognizing that remote work may become the norm for many employees long after the pandemic has ended.

Integral to the success of security efforts will be deploying technologies and solutions that are effective and quick to adopt, such as those that are hosted in the cloud. Cloud-based security and platform services markedly reduce deployment time. They also let companies increase the breadth and depth of security protection rapidly (i.e., referred to as dynamic scalability), depending on the threats of the moment. And cloud-based security also enables IT security professionals to manage all this remotely.

For example, cloud-based secure virtual desktop services give IT professionals remote access to employees' systems, including files and the network. The cloud is also key to security systems. Secure-edge, cloud-based data leakage prevention and threat-protection controls can help safeguard an organization's critical assets. Moreover, cloud-based managed detection and response services can be extended to remote workplaces.

Additionally, companies that use secure remote access technology can give remote employees private access (without a VPN) to enterprise applications and systems. Firms can also use privileged access management (PAM) services to allow special remote access to their IT and application administrators. Multi-factor authentication services including biometric and text based methods, enable stringent risk-based access to internal applications that are opened for remote access.

After Covid-19

It's important to remember that Covid-19 is expected to be temporary, with a time horizon measured in weeks or months. But this will complicate an already-complex landscape for IT and cybersecurity personnel. As they spend, develop and roll out new capabilities during the crisis, they need to bear in mind the aftermath. What must be reversed once the situation is under control? Which new habits or practices will persist? Will IT security pros need to implement new security measures?

There remains a lot of speculation about what happens after the pandemic, but six things appear to be certain:

- **Some organizations will need to move to new operating models.** For these companies, immediately after the crisis, cybersecurity and IT rights will require careful examination and handling. Remote worker monitoring and support will become vital. And for workers who transition from home back to the office, cybersecurity professionals must ensure stringent system and access scrutiny prior to allowing the shifted system to connect back to the network.
- **Companies will need to reset their security systems to ensure there are no outliers.** Both physical and digital systems will need to be restarted, to check for any digital holes in the fence. System and data access rights granted during the pandemic to enable remote work will require auditing to determine whether they should be revoked or updated. IT systems will need to be analyzed for cracks, foul paths or fraudulent identities. The reason is that cybercriminals may have found ways to gain entry into otherwise hardened facilities.
- **New cyber risks that appeared during the pandemic must be understood.** For instance, security experts will need to scrutinize the digital capabilities of critical business functions, making sure they can withstand cyberattacks during a lockdown. They will examine critical supply chains, including digital supply chains, to ensure continuity during a health crisis.
- **Corporate IT security architectures should be reassessed.** This includes access mechanisms, support needs for remote access on a mass scale, and feature risk/context-based security authentication mechanisms.
- **Updates to remote access and bring-your-own-device (BYOD) policies must be made.** They should include cybersecurity hygiene controls.

- **Advanced technology must be deployed.** Threat detection and response capabilities must include advanced capabilities supported by next-generation technologies like big data, artificial intelligence and machine learning. These are needed to detect and respond to adverse behavior at machine speed, without human interventions. Further, organizations will want to explore insurance against losses from cyberattacks incurred during a pandemic scenario.

Security leaders will also need to share the lessons they learned during the crisis. That will help them prepare for any future pandemics. They will need to review current security solutions for scalability, time to provision, cloud-based availability and remote management capability. They should also proactively engage with trusted partners to plan for dynamic scalability and the provision of required services and solutions.

Planning needs to be both creative and comprehensive. IT security leaders should revise their current BCP to include a pandemic-like scenario and perform regular drills. No one will want to be caught without a robust, thoroughly tested backup. The BCP should include a playbook for responding to cybersecurity incidents that emerged during the pandemic.

Leaders face a rising imperative to embrace new approaches and consider new operating technologies. In particular, automation can bring operating efficiencies and reduce dependence on human interventions. Starship Technologies[1], for instance, launched robot food delivery services in the United Kingdom and San Francisco almost two years ago.

With the pandemic in hindsight, companies that suffered delivery problems will need to give serious consideration to such a solution. Overall, new businesses will prosper, and those busy during the lockdown (such as grocery delivery services) will flourish with a new sense of acceptance.

In addition to robots, AI will gain further traction and approval as its contributions during the crisis become better known. AI is being used in drone delivery, chat-based health advisories, mobile geolocation analysis of lockdown perimeters, robotic disinfecting solutions for cities, and even prediction models for staggering the lifting of lockdowns.

1. Starship Technologies, Accessed April 10, 2020. https://www.starship.xyz/business/

A New Era for Cybersecurity

The changes we have laid out won't only affect the IT department. If remote employees demonstrate they work more effectively from home, talent managers will need to review their policies to allow a better work-life balance. Meanwhile, people with critical skills and remote-working demands will need to be quickly onboarded, and effectively.

Additionally, large corporations will face new budgeting constraints. New ways of using funds and investing in the right offerings will emerge. Firms will be stricter about how they allocate resources.

What's more, companies will have the opportunity to revamp the way work is done. New at-home work arrangements developed during the lockdown and that prove to work well should be prioritized. Finally, as people, assets and facilities recover, governments around the world will issue new policies and regulations in light of what was learned during the pandemic.

As they adjust to the new normal post-crisis, organizations will also be forced to optimize costs and accelerate their digital transformations. Security leaders will have to support these initiatives by leveraging digital technology and service models transformed to do more with less. Their BCPs must feature near-zero latency on multiple dimensions: data, provisioning, activation, tracking, network, security, compliance, program management, transition and service-level agreements. These need to be executed in the most cost-effective manner.

The pandemic has ushered in a new era of cyber security. IT security professionals who raise their game and protect their companies' people, technology and data from new or heightened risks of more sophisticated cybercriminals will be crucial players in the economic turnaround.

TATA CONSULTANCY SERVICES

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty.

IT Services
Business Solutions
Consulting

TCS Design Services I M I 04 I 20