Healthcare Providers & COVID-19:

Need for a Plan to Combat Security Threats

Healthcare

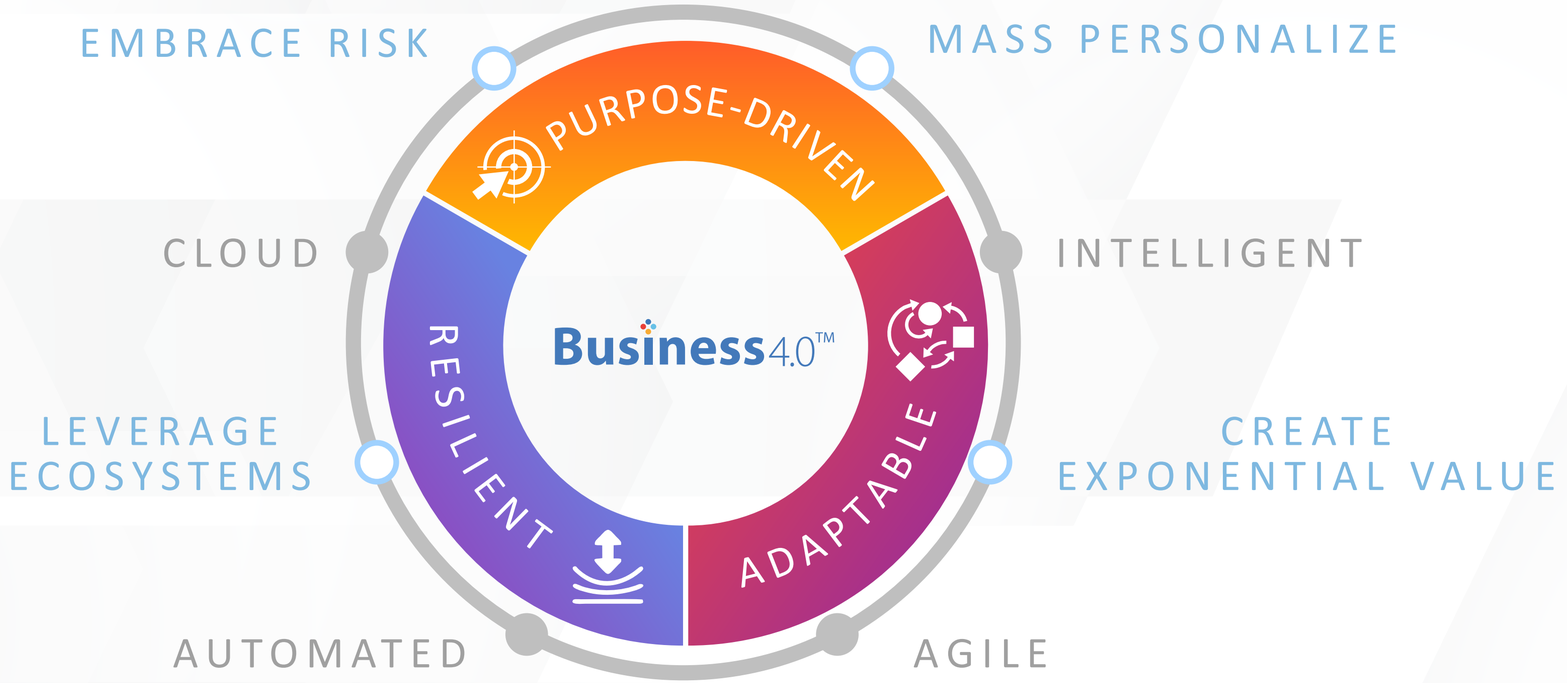
PURPOSE-DRIVEN

RESILIENT

ADAPTABLE

PURPOSE-DRIVEN, RESILIENT & ADAPTABLE

with Business 4.0™;



PURPOSE-DRIVEN

RESILIENT

ADAPTABLE

TATA CONSULTANCY SERVICES

Abstract

The speed with which the COVID-19 pandemic spread across the globe left very little time for healthcare providers to prepare the ground and devise a crisis management plan. Scammers, however, have spotted opportunity in this mayhem, and have launched a series of attacks on healthcare organizations to steal data - compromising sensitive information and causing downtime. This has put additional strain on healthcare IT professionals trying to figure out the best ways to facilitate remote working capabilities for their workforce. Most of the impacted organizations responded to the crisis by fixing some immediate glitches in the system. However, this pandemic has exposed vulnerabilities in the IT infrastructure that call for a complete overhaul. This whitepaper proposes a phased approach in implementing a tailored strategy that suits the security needs of healthcare organizations.

Understanding the gaps in healthcare security infrastructure

As doctors, nurses, emergency responders, and government agencies adopt an all hands on the deck approach to combat the pandemic, hackers are seizing the opportunity to mount the attacks. The scale of impact from these attacks on hospitals can be very damaging. A coordinated attack has the potential to cripple a hospital's infrastructure and its response time, and even cost people's lives.

Before we move on to discussing a crisis management plan, let us take a look at some of these recent cyberattacks.

1. **Data Breaches –** The number of data breaches reported to the Health and Human Services[1] (HHS) for the first quarter of 2020 stand at 122 against 115 cases reported in the last quarter of 2019. About 2.6 million individuals were impacted by the first attack, against 1.5 million people in the last quarter of 2019. This indicates a 70% surge in the number of individuals impacted due to breaches in IT security.

2. **Escalating Ransomware Attacks –** Growing ransomware instances have led to Microsoft[2] issuing a recent warning to healthcare companies and hospitals of human-operated ransomware campaigns that target network devices like gateway and virtual private network infrastructure. These attacks have led to operational downtime and loss of sensitive information.

3. **Email Phishing[3] Attacks –** There has also been an increase in phishing emails targeting users' personal and financial information. Over 1.2 million COVID-19 related phishing emails were circulated in March and April 2020. In fact, FTC has posted advisories to watch out for emails claiming to be from CDC, WHO, and other government agencies offering health advice, treatment, or cure.

4. **Attacks on Remote Working Infrastructure Vulnerabilities –** As healthcare companies open remote working options and adopt work productivity platforms, cybersecurity attackers have crept into organizations' infrastructure and made their way to protected health information.

---

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[2] https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/

[3] https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing

Rising to the challenge

While the focus so far has been on centralized security operations, healthcare providers will now need to adopt an agile and responsive system, irrespective of their maturity level in leveraging cybersecurity services.

Security Operations

Implementing new cybersecurity tools to protect the organization from elevated threat levels will be crucial. While the detection and protection control systems can flag alerts, round-the-clock vigilance of networks and analysis of reports will be able to detect and respond to security threats.

Identity, Access, and Privilege Management

The number of COVID-19 cases is higher in some states than the others. To address this crisis, many states have temporarily lifted licensing restrictions[4], allowing professionals to work across states. Hospitals availing the services of professionals because of these relaxations must deploy physical access controls to combat identity theft. While those who have already implemented the latest cloud-based services can now flex their capacity to a large extent, the providers who rely on multiple services or legacy products will face real challenges. However, they can reach out to third-party partners to set up authentication and identity protocols to combat the crisis.

Patching Operations for Server, Network, and Firewall

Renewed attacks on healthcare providers' VPN infrastructure call for tough infrastructure protocols and upgrading endpoints with most recent patches to prevent any malware attacks. Considering the extensive use of healthcare IT infrastructure and network due to remote working and growing adoption of telehealth options, there is also need to keep the patching at the current level.

[4]https://www.ncsl.org/research/labor-and-employment/covid-19-occupational-licensing-in-public-emergencies.aspx

Evaluating priorities, cybersecurity strategy

In face of the current crisis, organizations need to prioritize long-term investment in risk and governance initiatives instead of looking at these security threats as mere short-term concerns. A checklist can also help organizations gauge their current strength and subsequently assist in preventing and combating a security threat. Some of the key elements of the checklist would include evaluations around:

- If the Business Continuity Plans factor in a pandemic scenario like COVID-19 and were necessary measures in place.
- If remote access has been allowed to internal healthcare applications including the applications holding PHI data and EMR records? If yes, is it allowed over secure VPN or over the internet?
- Remote access allowances for employees' personal devices.
- Ensuring the security of the remote workplace in terms of Anti-virus updates, Security Patches, Access controls, and monitoring security alerts.
- Ensuring backups to maintain continuity in the case of ransomware attacks. Factoring in a mechanism for cloud backup.
- Establishing monitoring and visibility of security controls for remote workplaces as well as satellite care clinics set up for the pandemic.
- With almost 100% IT support staff working remotely, ensuring their privilege access is secured and restricted. Enforcing any stringent authentication and access mechanism for remote privilege workers.
- Ensuring remote workers and front-line staff are not falling prey to the COVID-19 specific phishing email attacks.
- Configuring required data protection, threat protection, and communication security controls to ensure safe and secure use of unified collaboration tools.
- Given the increased adoption of Teleconsulting and Telemedicine, ensuring security and privacy of the patient data accessed by practitioners.
- As the research for antiviral and vaccine is on war footing, a lot of research data is being remotely handled by scientists using cloud-based systems or on-premise systems. Ensuring the security and privacy of data and these systems.
- As clinical trials for the new drugs kick-in, evaluating plans for allowing remote access for online clinical trial management platforms.
- Ensuring the regulatory compliances like HIPPA, HITECH, and other privacy-related requirements in the current borderless working environment.
- With several ancillary industries supplying healthcare products and services (PPEs, Medicines etc.) scrutinizing security for these suppliers.

However, this is in no way a universal checklist for all as the security framework will vary for all organization. Rather, this only serves as a reference for providers to evaluate their position. This checklist, coupled with other tools and techniques, can help organizations arrive at an approach that is in line with the value chain and landscape of the organization.

Cybersecurity approach

Here are the key considerations that can help providers build a foundation for their cybersecurity infrastructure.

Phased Implementation

The firms will need to adopt a phased approach to acquire and build secure defenses around an extended infrastructure perimeter. Immediate fencing needs encompass protection against phishing and other email-based attacks and securing new services, such as teleconsultation and telemedicine from day zero. Providers with legacy infrastructure inherited through mergers & acquisitions will also need to ramp up their patching game to secure endpoints. While these are the immediate needs, there are certain things that can wait a little longer. However, most of the cloud transformation initiatives that are on hold now will need to be prioritized once the situation improves. A secure endpoint and enterprise-risk-simulation service with easy-to-use risk modeling will eliminate the need to create periodic inventory, automating defense mechanisms.

Shared Services

Providers will need to piggyback on capabilities available "as a service" in the market. Not only will this help accelerate setting up of defenses but will also convert Capex investments into consumption-based ones. Managed security operations, enterprise vulnerability management, identity, and access management, governance risk, and compliance can be augmented in shared service and cloud-based models.

More Innovation, Better Protection

In the post-COVID-19 world, the healthcare industry will witness a renewed focus on automation and digitization. Both medical and administrative staff will work remotely, requiring access to the provider's infrastructure as well as devices of patients and care clinics. These devices and data, whether in transit or at rest, will have their own set of vulnerabilities. To cite an example, IoT will require a different set of controls whether built organically or through new partnerships. It will also become important to keep the remote staff updated on the latest information, thereby adhering to government-issued bulletins.

Priorities for Providers (Per impact)

High

	Immediate			Equilibrium				Growth	
Phishing and Ransomware attacks	Cybersecuriy awareness & hygiene	Anti-phishing and email security	Increase capacity on Security monitoring incidence response	Threat Intelligence, anticipation and Detection				Risk simulation	Threat management, Managed detection & Response
R&D and Clinical trials	Access Management, Credentialing		Regulatory Compliance	Data capture, process recording and Encryption	Multi-factor Authentication	Privilege Access Management		Risk simulation	Data Privacy, Subject rights management & Cyber-vigilance
Remote workplace security	Secure Remote access	Access Control, Re-certification	Identity and Access Management protocols	Risk based Access	Multi-factor Authentication	Data Encryption & Separation of duties	Secure BYOD controls	Frequent review of Identities, Access Management, privileges	End point protection, Vulnerability Management
New Care Models-Teleconsult ation/medicine	Secure Architecture, DevOps	Regulatory Compliance	Access Management, Credentialing	Data Encryption	Multi-factor Authentication	Secure BYOD controls		Frequent review of Access Management, privileges	Call monitoring for patient and data privacy
AR/VR Home care, Digital Surveillance	Secure Architecture, DevOps	Regulatory Compliance	Certification of devices and infrastructure	Data Encryption	Environment vulnerability Management	Secure Access Control		Threat Intelligence, frequent review of Access controls	Monitoring privacy, data protection and end point controls
Securing the supply chain	Secure Remote access	Access Control, Re-certification	Identity and Access Management protocols	Risk based Access	Multi-factor Authentication	Data Encryption & Separation of duties	Secure BYOD controls	Frequent review of Identities, Access Management, privileges	End point protection, Vulnerability Management
Automation of hospital processes	Recertification of software		Regulatory Compliance	Digitization and automation systems security				Threat intelligence for operations	Data Privacy, Connected Medical Devices Security
Advisories/bulletins in conjunction with govt.	Authenticating media & Access Management, Credentialing			Website/Channel threat mgmt., External Risk Management				Web crawling for fake-fraudulent websites and social platform messages pretending to be from government sources	
Training of healthcare staff and carers	Securing channels of enablement			Access control and monitoring of information usage				Content filtering and encryption for personal devices	

Low

Strategy (Incremental strengthening of Cybersecurity)

Figure 1 Cybersecurity strategy for Providers

Conclusion

A tailored cybersecurity strategy, coupled with a strong organizational foundation, can help providers launch a post-COVID-19 security plan. In the immediate term healthcare providers need to focus on critical processes and cybersecurity controls to defend the perimeter of the extended organization. Once the immediate cybersecurity controls are established, healthcare providers can focus on implementing robust and enhanced controls to meet current and future business demands. As organizations embrace and adapt to the changed social and business environment, additional protocols like secure remote access, cyber vigilance, and risk simulations will need to be implemented to turn the security posturing from a reactive to a more proactive model.

About the Authors

Geetali Raj
Solutions Consultant,
Cyber Security

Muthuselvan Nallamuthu
Business Manager,
Healthcare

Prashant Deo
Domain Consultant,
Cyber Security

Geetali Raj is part of Cyber Security unit at TCS. With 16 years in IT industry she has worked across various roles and streams such as Enterprise Integration, SOA, RFID, Business Process Management, Automation and AI. She has spoken at multiple events and has publications under her name. She has done her Master's in marketing and holds a Bachelors in Engineering degree in Information Technology from Mumbai university.

Muthuselvan Nallamuthu is Business Manager within Healthcare Major Markets Unit responsible for new customer relationships in US west and mid-west geographies. He has spent over 17+ years in the industry partnering with Healthcare Payers and providers in their transformation journey. He is passionate about technology led innovations to enable accessible, cost effective, high quality healthcare and deliver positive health outcomes. He has done his MBA from IIM Ahmedabad and Bachelors in Engineering from College of Engineering Guindy, Chennai.

Prashant Deo is an IT professional with 15 + years of experience across industry verticals in Information security & Risk Management, Information Security Services, IT Compliance Management, IT-enabled business transformation and IT Infrastructure Management. He has a degree in electronics & telecommunication engineering, certificate program in business management and additional industry standard certifications in the area of Information Security Specialties - Information Security Management, Risk Management, Information Security Services, Security Audits & Operations, IT Compliance Management, Intellectual Property Management, IT led business transformation.

Contact

For more information on TCS' Healthcare solutions and services, please visit https://www.tcs.com/life-sciences-healthcare

Email: healthcare.solutions@tcs.com

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**

Corporate Marketing | Design Services | M | 06 | 20

PURPOSE-DRIVEN

RESILIENT

ADAPTABLE