**Int. J. Sci. R. Tech., 2025 2(10)**
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

*Original Article*

# Cybersecurity in the Era of the COVID-19 Pandemic

**Gauri Sethi***

*Asian International University, Imphal, west Manipur*

**ABSTRACT**

The COVID-19 pandemic (beginning early 2020) triggered a rapid and unprecedented global shift to remote work, telehealth, online education, and digital commerce. This shift expanded the attack surface for cybercriminals, accelerated adoption of cloud and collaboration tools, and exposed gaps in organizational preparedness. This paper synthesizes empirical reports and peer-reviewed literature to describe the major cyber threats observed during the pandemic, their impacts (with emphasis on healthcare and critical infrastructure), and effective technical, organizational, and policy mitigations.

**Keywords:** COVID-themed phishing and fraud surged, ransomware attacks increased sharply and targeted healthcare and supply-chain organizations, videoconferencing and telehealth platforms exposed privacy/security weaknesses, and threat actors exploited human factors amid crisis. We conclude with actionable recommendations for resilient cyber posture during prolonged crises and future pandemics

## INTRODUCTION

The COVID-19 pandemic forced near-instantaneous operational changes across governments, businesses, schools, and healthcare providers. In many regions, large portions of the workforce shifted to remote setups and institutions adopted or scaled digital services (telehealth, remote learning, cloud collaboration) in a matter of days. While these changes preserved continuity of operations, they also created a fertile environment for malicious actors to exploit fear, uncertainty, and rapid technology adoption. This paper examines the threat landscape that emerged, quantifies impacts using authoritative reports, and proposes mitigations for organizations and policymakers.

## 2. Background & Context

On March 13, 2020, key national cyber agencies publicly urged organizations to adopt a heightened state of cybersecurity as telework options were rapidly deployed; multiple governments and security organizations released telework and pandemic-specific guidance throughout 2020–2021. These advisories recognized that rushed deployments, broadly distributed endpoints, and overwhelmed security staff increase risk.

Early monitoring in 2020 recorded large volumes of COVID-themed malicious content: spam, malware, phishing, and malicious URLs tied to pandemic topics. INTERPOL's analysis and public summaries reported hundreds of thousands of COVID-related spam messages and tens of thousands of malicious URLs in early 2020, illustrating how threat actors weaponized pandemic information.

## 3. Major Threats Observed During the Pandemic

### 3.1 COVID-themed Phishing, Scams, and Fraud

Phishing remained a dominant vector: attackers used COVID-related themes (vaccine news, travel restrictions, financial relief, PPE offers) to harvest credentials, deliver malware, or defraud victims. Malicious domains and impersonation campaigns were widespread and highly effective because recipients expected legitimate pandemic communications. INTERPOL's aggregated data highlighted phishing/scam as a major proportion of pandemic threats.

### 3.2 Ransomware and Targeted Disruption

Ransomware grew in frequency and impact during 2020–2021. Several intelligence and industry reports showed a marked increase in ransomware incidents,

**Relevant conflicts of interest/financial disclosures**: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

with attackers focusing on organizations that could least afford downtime — healthcare, logistics, and manufacturing. IBM X-Force and related analyses noted that attacks on industries supporting the COVID-19 response doubled in 2020 relative to prior periods and that ransomware became a top attack category.

### 3.3 Vulnerabilities in Videoconferencing and Collaboration Tools

The mass adoption of videoconferencing and collaboration platforms (e.g., Zoom, Teams) created new privacy and security challenges. “Zoombombing” and misconfigured meeting defaults led to high-visibility disruptions; researchers and security teams documented encryption and configuration weaknesses that were exploited early in the pandemic. These incidents illustrated how default settings, user behavior (publicly posted meeting links), and rapid scaling can combine to produce serious risks.

### 3.4 Telehealth & Remote Care Risks

Healthcare systems rapidly pivoted to telehealth, introducing new privacy and security requirements. Studies and systematic reviews found that telehealth implementations often faced insufficient privacy protections, insecure platforms, and incomplete compliance with health data regulations — all while healthcare staff were stretched thin. These weaknesses made telehealth an attractive target for data theft and operational disruption.

### 3.5 Supply-chain & Critical Infrastructure Exposure

Critical infrastructure and supply chains were targeted because disruption would produce cascading effects during the pandemic. Increased remote access to industrial control systems (often via hastily deployed VPNs or remote desktop solutions) and third-party dependencies raised systemic risk. Reports emphasized the need to prioritize defenses for supply-chain and medically critical operations.

## 4. Impacts: Quantitative & Qualitative Evidence

- INTERPOL and private sector partners documented hundreds of thousands of pandemic-related spam messages and tens of thousands of malicious URLs in early phases of COVID-19, demonstrating scale.
- IBM’s reporting indicated that attacks on healthcare and sectors supporting pandemic response approximately doubled in 2020 vs prior periods; ransomware became a leading threat that increased both frequency and financial impact.

Qualitatively, the pandemic exposed how organizational dependency on digital services — when combined with constrained budgets and stretched human resources — amplified consequences of breaches: patient care interruptions, supply chain delays, privacy breaches, and trust erosion.

## 5. Why the Pandemic Changed the Attack Surface (Analysis)

Key structural drivers:

1. Rapid Adoption of Remote Work & Tools. Instantaneous scaling of VPNs, remote access, and cloud collaboration increased the number of publicly reachable endpoints and created configuration errors.
2. Human Factors Under Stress. Fear, information overload, and remote social isolation increased the effectiveness of social engineering.
3. Criticality of Targets. Attackers rationally prioritized targets (hospitals, manufacturers, logistics) where disruption would create leverage for extortion.
4. Third-party & Supply-chain Dependencies. Accelerated reliance on cloud providers and third-party services propagated risks beyond organizational perimeters.

## 6. Case Studies

### 6.1 INTERPOL: Pandemic-Themed Cybercrime Metrics (Early 2020)

INTERPOL’s August 2020 analysis catalogued the rapid emergence of COVID-themed cybercrime — from fraudulent online sales of PPE to large volumes of COVID-related spam and malicious URLs. These real-time metrics were critical to law enforcement and public awareness efforts.

### 6.2 Zoom & Videoconferencing Security

Zoom's explosive growth (from ~10 million daily meeting participants in late 2019 to hundreds of millions in early 2020) created an environment where default configuration weaknesses were consequential. Reports and academic analysis documented the technical and human causes of "Zoombombing" and how vendor-led fixes and user education mitigated but did not eliminate risk.

### 6.3 Ransomware Targeting Healthcare (IBM X-Force)

IBM X-Force observed that groups opportunistically targeted healthcare and related sectors during 2020, leveraging ransomware and data-exfiltration extortion schemes; the industry reported increases in both number and severity of incidents. These events highlighted the ethical and operational dilemmas in paying ransoms and the systemic consequences of encrypted clinical systems.

## 7. Mitigation Strategies: Technical, Organizational & Policy

### 7.1 Technical Controls

- Zero Trust & Least Privilege. Apply Zero Trust principles: verify every access request regardless of network location, enforce least privilege, and use strong multi-factor authentication (MFA).
- Hardened Remote Access. Replace legacy RDP exposed to the internet with VPNs/secure gateways, segmented access, and jump hosts; ensure MFA and session logging.
- Improve Patch Management. Prioritize patching of internet-facing systems and known exploited vulnerabilities; monitor vendor advisories.
- Endpoint Detection & Response (EDR). Deploy EDR and centralized logging to detect anomalies across distributed endpoints.
- Secure Collaboration Defaults. Configure videoconferencing tools with waiting rooms, meeting passcodes, screen-sharing restrictions, and restricted recording. (Vendor guidance evolved rapidly during 2020.)

### 7.2 Organizational & Human Measures

- Targeted Training & Phishing Exercises. Use realistic, pandemic-context training; simulate phishing that mirrors the themes attackers used.
- Incident Response Planning for Remote Contexts. Update playbooks to include remote forensic collection, legal/regulatory notification for cross-jurisdiction incidents, and continuity of care for healthcare providers.
- Third-party Risk Management. Inventory third-party services, require minimum security baselines, and monitor vendor posture continuously.
- Business Continuity & Prioritization. Identify critical services and create prioritized recovery objectives, especially for healthcare and supply-chain systems.

### 7.3 Policy & Public Sector Actions

- Coordinated Advisories & Information Sharing. Governments and CERTs should issue timely, pragmatic guidance for telework, telehealth, and vendor configuration best practices; public-private information sharing (e.g.,Indicators, TTPs) is essential. CISA's telework guidance and pandemic advisories are examples of such public action.
- Support for Smaller Entities. Small healthcare providers and SMEs often lack security resources; policy should enable subsidized access to secure telehealth platforms, training, and cyber insurance models that incentivize good hygiene.
- Law Enforcement & International Cooperation. Cross-border crime requires collaboration between agencies (INTERPOL operations and information sharing were notable early responses).

## DISCUSSION

### Lessons Learned & Long-term Implications

COVID-19 demonstrated that cyber risk is fundamentally socio-technical: technology changes quickly, but human workflows, incentives, and institutional readiness often lag. Key lessons:

- Resilience over Perfection. Organizations should aim for resilient operations: assume breaches will happen and ensure rapid detection and recovery.
- Design for Rapid Scale. Security controls and default configurations must be designed to remain effective under sudden, large-scale adoption. Vendors have a role to play in safe defaults.

- Healthcare as Priority. Protecting health systems during a public health emergency is both an ethical imperative and a national security priority; cybersecurity investment must reflect that.
- Policy & Funding. Governments should support cyber capacity building for critical sectors and small organizations that cannot self-fund rapid modernization.

### 9. Recommendations (Actionable Checklist)

**For leadership:**

- Adopt a documented Zero Trust roadmap and enforce MFA broadly.
- Prioritize critical services (healthcare, supply chain) for enhanced monitoring and backups.

**For security teams:**

- Run pandemic-themed phishing simulations quarterly and tailor training.
- Harden videoconferencing and telehealth platform configurations; require vendor security attestations.

**For policymakers:**

- Provide targeted funding or tax incentives to strengthen security in small healthcare providers and schools.
- Facilitate cross-sector threat intelligence sharing and public advisories during crises.

**For vendors:**

- Ship secure-by-default settings and clear, simple configuration guidance for rapid onboarding.
- Offer tiered solutions that enable resource-constrained customers to maintain secure operations without extensive engineering.

## CONCLUSION

The COVID-19 pandemic was a stress test for global cybersecurity. While threat actors actively exploited the situation—using phishing, ransomware, and platform weaknesses—the crisis also catalyzed important improvements: increased awareness, faster vendor hardening, and stronger cooperation among public and private actors. Future pandemics or global disruptions will be met first in the digital domain; the lessons from COVID-19 must be institutionalized so that resiliency, secure defaults, and preparedness are permanent features of organizational and public policy design.

## REFERENCE

1. CISA. Telework Guidance and Resources; Coronavirus guidance and advisories (telework guidance and advice released March 2020 and subsequently updated).
2. INTERPOL. COVID-19 Cybercrime Analysis Report (Aug 2020) — documented large volumes of COVID-themed spam, malware incidents, and malicious URLs.
3. IBM X-Force / IBM Security reporting. Attacks on industries supporting COVID-19 response doubled; ransomware trends during 2020–2021.
4. He, Y. et al. (2021). Health Care Cybersecurity Challenges and Solutions (review on healthcare cybersecurity during COVID-19). PMC/NCBI.
5. Houser, S.H., et al. (2023). Privacy and Security Risk Factors Related to Telehealth during COVID-19 — systematic review of telehealth privacy/security challenges. PMC/NCBI.

HOW TO CITE: Gauri Sethi*, Cybersecurity in the Era of the COVID-19 Pandemic, Int. J. Sci. R. Tech., 2025, 2 (10), 90-93. https://doi.org/10.5281/zenodo.17292829