



REVIEW OF RESEARCH

ISSN: 2249-894X

IMPACT FACTOR : 5.7631 (UIF)

VOLUME - 11 | ISSUE - 12 | SEPTEMBER - 2022



THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGY ,PRIVACY ISSUES AND CYBER THREATS ON THE DIGITAL BATTLEFIELD IN THE EMERGENCY PERIOD OF Y2K

Prof. Asharani Jogdankar

DCE.(Civil.) B.Tech. (Civil Engineerig), & B.Tech.Hons. (Environment Engineering.)

Certificates in Software:- Auto CAD, Revit, Staad Pro. & BEC.

Lecturer in Department of Civil Engineering.

**Shri Siddheshwar Women's Polytechnic College Solapur.
Maharashtra.**

ABSTRACTS

Y2K bug, also called Year 2000 bug or Millennium Bug, was an issue in the coding of electronics that was foreseen to make devastation in PCs and Laptops around the world over close to the beginning of the year 2000 (in metric estimations, k means to 1,000). After a period of widespread alert, hot game plans, and programming alterations, barely any noteworthy frustrations occurred in the advancement from December 31, 1999, to January 1, 2000.

The Y2K bug was a specific issues recognized in the late 1990s from a date progress in PC structures from the year 1999 to 2000 at the turn of the thousand years. The change was required to chop down PC structures establishment, for instance, those for banking and power plants. The Y2K Scare was a problem at the turn of the 21st century where PC customers and programming engineers expected that PCs would stop going after December 31, 1999. ... A lot of brain stroming went into preparing for the millennium Bug. Right when complex PC programs were first composed during the 1960s, engineers used a two-digit code for the year, disregarding the "19." As the year 2000 moved nearer, many acknowledged that the systems would not translate the "00" adequately, consequently causing a critical glitch in the system.



KEY WORDS : plans and programming alterations, ICT, Y2K, Cyber Threat

INTRODUCTION

The Y2K issue was not confined to PCs running customary programming, in any case. Various contraptions containing PC chips, reaching out from lifts to temperature-control systems in business structures to clinical equipment, were acknowledged to be in harm's way, which required the checking of these "embedded structures" for affectability to plan dates. The Y2K bug was a PC deformity, or bug, that may have caused issues when overseeing dates past December 31, 1999. The blemish, looked by programming architects and customers wherever all through the world on January 1, 2000, is in any case called the "thousand years bug." (The letter K, which speaks to Thousand (a unit of 1000), is typically used to address the number 1,000. Along these lines, Y2K speaks to Year 2000.) Many skeptics trust it was hardly an issue in any way shape or form. Exactly when confounded PC programs were

being made during the 1960s through the 1980s, PC engineers used a two-digit code for the year. The "19" was disregarded. Instead of a date examining 1970, it read 70. Planners condensed the date since data storing in PCs was costly and consumed a huge amount of room.

THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGY

Information and correspondence developments (ICTs) accept a fundamental activity in arranging crisis response between pre-center organizations and emergency divisions of clinical facilities. Notwithstanding the advances in these advances, there remain a collection of challenges to their use during a crisis. To recognize these troubles, we coordinated focus gathering interviews with emergency division (ED) and emergency clinical organizations (EMS) staff. We found that ED and EMS staff have commonly fluctuating acknowledgments about the supportiveness and comfort of information gadgets and particular instruments used in crisis the board. We analyze the importance of joining correspondence and information contraptions into consolidated frameworks of ICTs for incredible crisis response. We furthermore include design features of ICTs which can reinforce predictable and convincing correspondence and coordination among ED and EMS gatherings.

Starting late, there has been a push towards association of information and correspondence propels (ICTs) for emergency crisis response¹. It is ordinary that such developments will improve information sharing, resource assignment, correspondence, and participation among emergency clinical organizations (EMS) and emergency workplaces (EDs) of hospitals². In any case, since an extensive part of the progressions proposed are new, there is minimal verification to enable that they to will undoubtedly be viable in the field.

Care providers' perspective on the points of interest, ease of use, and handiness of information structures sway the successful execution and choice of these systems in healthcare³. Along these lines, in order to support ED and EMS workforce through emergency response progresses, we first need to appreciate their attitudes towards these advances. We ought to in like manner appreciate their wants for the focal points and challenges of ICT use during crisis response.

They drove an abstract report with therapeutic administrations providers related with the pre-crisis facility organizations and ED of Hershey Medical Center (HMC), a huge indicating center in Pennsylvania with raised degrees of ICT use. Their examination targets were two-overlay. In any case, They were enthusiastic about taking a gander at EMS and ED work power's perspective on the normal employment, handiness, and ease of use of ICTs during a mass misfortune scene (MCI). Second, investigating how current ICTs used by these thought providers support the leading body of a potential MCI.

The assessment revealed that ED and EMS bunches shift on their viewpoints towards the activity and handiness of ICTs for crisis response. This results in inconsistencies in information the administrators practices between these gatherings. In like manner, there is a qualification in how these thought providers see and use information development (IT, for instance, PC based systems, and correspondence progresses (CT, for instance, telephones and pagers. These revelations propose the need to design especially consolidated frameworks of ICTs and train customers about the benefits of these headways

PRIVACY ISSUES

Recall Y2K? In the decently early significant lots of PC programming, various systems were planned to organize dates by the last two digits of a year, dismissing the "19" close to the start of the number to save memory space. That may have made PCs work even more profitably, yet it made an issue: What may happen when that date diverted over from 1999 to the year 2000—or "00"? Some focused on that PCs wouldn't understand how to translate an unfilled motivation for a year, and would scrutinize these dates as invalid, causing glitches around the world. PC composes being utilized any place from the area McDonald's to nuclear munitions stores were possibly running with a comparative shortcoming.

That was the prophetically disastrous speculation behind the Y2K caution: The inevitable PC unsettling influence that should incapacitate banks and governments when the clock struck 12 PM on January 1, 2000. We know since mankind came out of Y2K respectably strong, resulting to spending a normal \$300 billion to \$600 billion to fix likely issues in the years before the thousand years. However simultaneously, a few issues sprang up—some caused a certified cerebral agony, while others gave to some degree a laugh. Here are a few occasions of the issues the Y2K bug truly caused.

A variety of issues including banks, crisis centers, travel masters, and various associations occurred, yet most were just passing inconveniences that were hardly prominent enough to make the close by news. Taking everything into account, Hotmail demonstrating the year as "3900" for several hours isn't in reality enough to get people revolting in the roads.

While the Y2K alert as of now is for the most part thought of as an overcompensation, the nonappearance of any principle issues may have been a consequence of the a huge number of dollars filled the fixes in the years ahead of time. In a gathering on CNN, Bill Gates said that Y2K "ended up being a really minor issue since people genuinely coordinated. If people had ignored the thing, by then we would be seeing the certifiable impact."

Y2K Changed the Field of Cybersecurity Technology

When looking at the computerized development feature throughout ongoing years, it is evident that the catalyst for computerized headway was Y2K. Before the Y2K furor, "cybersecurity" was hidden in the structures planning limit, and outside risks involved software engineers wanting to utilize free figuring capacities with close to no consideration on information/data access or framework pummeling. Malware existed, anyway it was a more prominent measure of a bother than a strategy for system deal. Remediation focused basically on growing check capacities and included multifaceted approval, improved mystery express methodologies and encryption as affiliations attempted to shield their system from being oversubscribed. Things changed when the Y2K issue got self-evident.

According to a Department of Commerce measure, the nation's private and open division affiliations consumed \$100 billion to address the issues with Y2K. Y2K plans focused on the openness of structures, ensuring mis-coded applications didn't make the force miss the mark or money related adjusts to disappear. The improvement of new gadgets and progressions organized expressly for cybersecurity purposes hit the market during this time, giving a rundown of abilities expected to a solid security exercises program.

Y2K in like manner helped shape the Security Information and Event Management (SIEM) exhibit as traders made and sell applications that assembled and gathered events over all structures in a framework. Furthermore, it conveyed firewalls and antagonistic to disease programming to the front line as affiliations intended to thwart the predicted spread of malware across what was required to be basically weak systems. Finally, the way of believing was to give a shield of confirmation to keep the difficulty producers outside the framework "dividers."

After Y2K voyaged all over, security programs ended up being less locked in. Each vertical began looking at attributes that spoke to the most genuine risk or had the most conceivable impact on their specific industry, and consistence rules followed intently following this example. In the business and therapeutic administrations world, the consideration was on protection as seen by the establishment of the Payment Card Industry Data Security Standard (PCI DSS) and the continued with revolve around the Health Insurance Portability and Accountability Act (HIPAA). Stressed over decency, the cash related portion organized the Sarbanes–Oxley Act while the organization, hindrance and essential structure affiliations fundamentally based on availability. This all achieved the market segregating their framework and structure resources and applying fluctuating degrees of control to each. As far as possible was renamed, almost separated, with advancements being consigned to particular structures rather than affiliation wide.

As the risk condition advanced, so too did security specialists, getting logically create in their strategies and toolboxes. New advances hit the scene to help manage malware solidly without being passed on every IP-engaged contraption. The introduction and advancement of security testing and

weakness the board mechanical assemblies similarly ended up being progressively overwhelming. All the while, affiliations associated with moral developers to receive a proactive methodology to understanding their vulnerabilities. By merging invasion testing into their security programs, affiliations benefitted by a sweeping see potential ambush vectors and peril circumstances influencing their IT environmental factors.

Directly, affiliations are stood up to with the unusualness and arranged assortment of mobile phones and applications that must interface with the framework. The Internet of Things (IoT) is for sure renaming the cybersecurity feature and the limits that affiliations must secure. With very various endpoints to try to ensure about at the device level, affiliations are moving towards an information driven approach to manage security. Fixing and concentrated on shortcoming remediation is being enhanced with an accentuation on looking at the colossal proportions of data that is ingested by computerized gadgets and progressions (for instance gigantic data examination). The goal of gigantic data assessment is to get examples and guides to reveal greater threats to corporate data including the insider peril. This advancement will in like manner achieve additional particular responses to perceive and ease perils at the data and application layer. Fundamentally, it will progress new courses of action that map the data traffic stream and others that will fill in as a security orchestrator – blocking perils and ambushes extensively instead of focusing on solitary events. The new widely inclusive security game plans will change what was a thought all things considered 15 years earlier into a without a doubt differentiator for affiliations. Cybersecurity is going to help the business as opposed to oblige it.

CONCLUSION

The headway of cybersecurity advancements and approaches has gained extensive ground since Y2K. In that time, cybersecurity has created from a major structures association ability to maybe the greatest division in IT. In all honesty, an April 2014 MarketsandMarkets research report evaluated the overall cybersecurity market will be worth \$155.74 billion by 2019. The cybersecurity requirements to address the challenges related with the IoT simply help the continued with improvement of the market piece and the availability of new and rising gadgets and headways. It will be a charming ride.

REFERENCES

1. Bruce Caldwell; Andy Patrizio (1997-09-15). "Testing for 2000". *InformationWeek*
2. Leap Day Tuesday Last Y2K Worry". *Wired*. 2000-02-25.
3. Carrington, Damian (2000-01-04). "Was Y2K bug a boost?". *BBC News*. Archived from the original on 2004-04-22
4. ^ Eric Andrew-Gee (2019-12-28). "Y2K: The strange, true history of how Canada prepared for an apocalypse that never happened, but changed us all". *The Globe and Mail*.
5. Cory Johnson (1999-12-29). "Y2K Crier's Crisis". *TheStreet*.
6. Barnaby J. Feder (1998-10-11). "The Town Crier for the Year 2000". *The New York Times*.
7. Bolles, Spencer (1985-01-19).
8. "2000". *Newsgroup: net.bugs*. Usenet: 820@reed.UUCP. Retrieved 2019-08-15.
9. American RadioWorks Y2K Notebook Problems – *The Surprising Legacy of Y2K*.
10. Rose, Ted (1999-12-22). "Who invented Y2K and why did it become so universally popular?".
11. A web search on images for "computer memory ads 1975" returns advertisements showing pricing for 8K of memory at \$990 and 64K of memory at \$1495.



Prof. Asharani Jogdankar
DCE.(Civil.) B.Tech. (Civil Engineerig),
& B.Tech.Hons. (Environment Engineering.)
Certificates in Software:- Auto CAD, Revit, Staad Pro. & BEC.
Lecturer in Department of Civil Engineering.
Shri Siddheshwar Women's Polytechnic College Solapur.
Maharashtra.