Cyberattacks can trigger societal crises, scientists warn

Cyberattacks threaten the technical systems they target and also spark extensive social media discussions that can escalate into broader community crises.

SHARJAH, EMIRATE OF SHARJAH, UNITED ARAB EMIRATES, January 19, 2026 /EINPresswire.com/ --

Cyberattacks can wreak havoc on the systems they target, yet their impact often spreads far beyond technical failures, potentially triggering crises that engulf entire communities, a new study argues.

When hackers strike “critical infrastructure,” they “pose serious risks to societal resilience,” the study notes, adding that public responses can be intense and wide-ranging, shifting from denial and humor to anger, bargaining, depression, and acceptance.

The study, published in the journal Engineering, Construction and Architectural Management, explores public responses to the 2021 cyberattack on a Florida water treatment plant by examining social media conversations and their role in shaping cybersecurity strategies. (https://doi.org/10.1108/ECAM-02-2025-0213)

In February 2021, an intruder gained remote access to the control system of a water plant in Oldsmar, Florida, and attempted to dramatically increase levels of sodium hydroxide (lye), a chemical used in small amounts to treat water.

The hacker initially succeeded in altering the settings and increasing the level of the chemical in treated water, which could have posed serious health risks if left uncorrected. A plant operator spotted the unauthorized changes in real time and quickly reversed them, preventing harm.

“This research examined how people react when a cyberattack targets critical infrastructure, using the 2021 Florida water treatment plant hack as a real-world case,” said Dr. Bharadwaj R. K. Mantha, an assistant professor at the University of Sharjah’s College of Engineering. “Rather than focusing only on technical failures, the study looks at public reactions expressed on social media (e.g., X, formerly Twitter, in the context of this study) and treats them as an important part of the crisis itself.”

Public reaction to Florida water plant hack

To explore public perceptions of the Florida cyberattack, the researchers conducted a qualitative data analysis of online narratives surrounding the incident. They collected social media posts from X (formerly Twitter) during the first week following the hack. They compiled conversations on the incident from February 8 to February 15, 2021.

"These tweets provided a diverse range of public reactions, including expressions of disbelief, humor, fear, critiques of systemic vulnerabilities, and calls for accountability," the authors explain. "This dataset, as naturally occurring data without the intervention of the researchers, offered valuable insights into how the public processes and responds to cybersecurity incidents in real time."

To reinforce their findings, the researchers also carried out a critical review of existing literature on cybersecurity vulnerabilities in infrastructure systems and on cyberattacks as sociotechnical crises. Their review systematically explores the complex landscape of cybersecurity challenges and their varied implications, draws parallels from previous studies on how cyberattacks can be considered sociotechnical crises, and then identifies key research gaps and positions.

The authors frame their analysis using the Kübler-Ross model, a well-known psychological framework introduced by the psychiatrist Elisabeth Kübler-Ross in 1969 to describe emotional responses to death and dying. Although originally developed for end-of-life contexts, the five-stage model—denial, anger, bargaining, depression, and acceptance—has since been widely applied to explain how individuals respond to loss, crises, and major disruptions.

In the context of the study, the authors use the Kübler-Ross model to shed light on the model's stages and how they unfold when the public is confronted with serious cyber threats to "assist facility managers, government agencies, and municipalities to better understand how the public perceives cyber incidents on critical infrastructure," Dr. Mantha emphasized.

Public emotions and perceptions

Analyzing social media conversations surrounding the attempted hack of Oldsmar's water system, the study finds that public reactions "followed a structured emotional progression, from denial and humor to anger, bargaining, depression, and acceptance.

"Social media discourse revealed concerns over systemic vulnerabilities, accountability demands and calls for cybersecurity reform. These insights emphasize the importance of transparent crisis communication, proactive risk management and public engagement in strengthening cybersecurity resilience."

Dr. Mantha, a co-author of the study, emphasized that cyberattacks affect far more than infrastructure and digital systems. "Public reactions follow recognizable patterns, from disbelief

and humor to fear, anger, and eventual acceptance."

He added that social media functions as a real-time "public sector," exposing underlying anxieties, mistrust, and expectations. "Ignoring public sentiment during cyber crises undermines trust and slows recovery. Online discussions rapidly highlighted systemic weaknesses—such as outdated software—and sharply criticized perceived lapses in cybersecurity practices."

While public perceptions may not always reflect actual reality, Dr. Mantha notes that they remain critical for policymakers and crisis managers. "Our findings show that these perceptions are a key part of the landscape and must be addressed appropriately by the responsible authorities. There was sustained public demand for accountability, transparency, and reform. Importantly, the discourse often included technically informed suggestions—not just emotional reactions."

Implications for cyber crisis communication

The authors argue that their findings carry far-reaching implications, particularly for improving crisis communication strategies during cyber incidents. Dr. Johan Ninan, the study's lead author and an assistant professor at Delft University of Technology in the Netherlands, said, "Our study on the Florida water plant hack shows that in building cybersecurity for critical infrastructure, public trust and communication are as vital as firewalls and software."

They further contend that the research demonstrates how social media can function as a valuable feedback mechanism for strengthening cybersecurity planning and management, supporting a shift from purely technical cybersecurity approaches to more human-centered models.

Balaji Kesavan, a US-based independent researcher and co-author, added, "Our study paves the way for using large language models to analyze social media sentiment in near real time. This enables municipalities to better understand and proactively react to public reactions during critical infrastructure cyber incidents."

Expanding on the potential industry implications of their work, the authors explain that their findings "offer actionable insights for the public, media, private sector, and government agencies into crisis response planning, fostering trust and resilience in digital infrastructure security by integrating public feedback into cybersecurity planning through structured social media analysis and iterative learning practices."

LEON BARKHO
University Of Sharjah
+971 50 165 4376
email us here