Cporative Security in a Connected Digital World: Leveraging Social Media and Emerging Technology in Crisis and Disaster

Wayne P. Bergeron
University of North Alabama, wpbergeron@una.edu

Follow this and additional works at: https://ir.una.edu/pjl

Part of the Law Enforcement and Corrections Commons, and the Political Science Commons

Recommended Citation
We live in an ever connected and digital world which brings great convenience, capability, and comfort to our modern quality of life, but at the same time introduces significant threats and vulnerabilities as well when things fall apart or fail, as they most likely do in crisis and disaster. The purpose of this article is to provide a critical review and state of the current and future security environment related to the various areas of social media and emerging technology that impact policy, preparedness, operations, and response within crisis and disaster situations. Ultimately, we find that some of our biggest opportunities within these areas are also likewise some of the biggest potential challenges and threats we are likely to face going forward within the realm of corporative security. While we may choose to ignore these, or discount their impact in the short term, it is increasingly apparent to the enlightened observer, that they will likely manifest themselves as critical vulnerabilities and potential points of failure in the mid to long term if we do not begin to address them.

#Safety Before Selfie – Please make sure to exit the burning building before texting, tweeting, posting, or live streaming about it.
INTRODUCTION

It is a sad commentary perhaps that in our current modern society that such an emergency warning statement as the one above might actually be necessary as part of the risk communication planning of a corporative security unit, but unfortunately that is in many ways the nature of the current security and emergency management environment that exists both in the public and increasingly in the private sector as well. We currently live in an Über-connected world that allows us access to just about all the knowledge the world has ever produced at the tips of our fingers twenty-four hours a day, seven days a week, and 365 days a year in an easily accessible and on-demand format from just about any place on the face of the earth. Also, if we combine that with the potential ability to be constantly connected with the entirety of people that we have ever met or known (or desire to know) through social media and online communication platforms, it is fairly clear that we are living in a time and age that has largely never existed before and really has no real historical parallel. Of course, if you think about what we actually do with that capability on a day to day basis – the answer may not make you very proud to be a human.

OPPORTUNITIES AND CHALLENGES

As mentioned, given the current environment we potentially have an era in the field of corporative security that should allow us capabilities that far exceed anything that has ever been seen before, with a level of achievability and economic affordability that should make the most miserly, jaded, and cynical executive or manager joyous. However, as with many things, the nature of the truth is much more nuanced and the very capabilities, technologies, and break throughs that provide these advantages also potentially create or expose a set of challenges, vulnerabilities, and liabilities the likes that most of us have likely have not seen before much less have fully considered. This interplay of opportunity and challenge creates a unique security environment and ecosystem that demands a level of understanding and a comprehensive security approach that in many cases is only in its infancy in most organizations for routine operations and conditions and is likely non-existent when it comes to crisis disaster and response situations. Hopefully,
that reality begins to change, and changes quickly given the potential enormity of the consequences.

**SOCIAL MEDIA IN CRISIS AND DISASTER**

Whether we like it or not, social media and the digitally connected world we currently live in have in many ways changed the nature of how we as humans interact and communicate (if you are in doubt of this statement – spend half an hour with any teenager). These changes also have a profound impact on what we currently consider the necessary elements of good living and a reasonable quality of life. So much so, that in many developed countries we are beginning to see internet access and broadband connectivity being increasingly prioritized and regulated as a form of public utility akin to water and electricity versus a mere luxury commodity. Highlighting this was a recent judicial opinion in the United States that saw a judge writing in the majority opinion that “Over the past two decades, this content [internet] has transformed nearly every aspect of our lives, from profound actions like choosing a leader, building a career, and falling in love to more quotidian ones like hailing a cab and watching a movie.” (Kang, 2016) Beyond the domain of individuals, we are also seeing many forward-thinking companies and organizations that are beginning to realize the value of social media technology and are “using social media tools such as wikis, blogs, microblogs and corporate social networks, they are connecting employees globally and are fostering mass collaboration. As a result, these companies are seeing improvements in communication, cross-functional collaboration and creative approaches to problem solving.” (Meister and Willyerd, 2009) The end result of such innovative approaches is that these technologies and approaches are becoming a critical part, and in some cases an existential part of their business model and organizational structure. While many of these approaches are being hard-wired (so to speak) into the organizational structure and culture of these organizations, the security considerations and potential threat and vulnerability impacts are in many cases lagging behind, which creates significant hazard exposure for many organizations. In many instances, the true nature and extent of that risk is largely unknown.
While the individual platforms depicted in figure 1 above may change or increase or decrease in use and popularity, the nature and function of social media in today's society has largely become a constant. Regardless of the platform specifics, the fundamentals of the use of social media are largely universal and organizations, agencies and businesses need to ensure that they consider this in their crisis and disaster planning as well as every day operations both in terms of providing their core services and functions, but also in terms of security for the organization and its employees. When it comes to crisis and disaster situations, social media in many ways provides organizations a robust set of communication tools with some inherently unique capabilities that have largely been unavailable outside the realm of governments. Unlike traditional media which generally only provides one-way information dissemination, social media enables both one-way communication as well as the ability to receive feedback and communication from organizational constituents and can provide that in actual real time in most cases. Beyond just communication capabilities, when combined with aggregation, analytical
tools, and data mining, the use of social media can actually become a valuable source of intelligence information and situational awareness without the need for deployment of sensors or reporting assets. In the wake of disasters, a simple capability such as the geolocation (with some limitations and caveats) can assist in actual search and rescue operations. In the case of geolocated photos, this can also provide real time rapid damage assessment capability that far exceeds traditional damage assessment methods in most cases. Additionally, beyond immediate response and recovery operations, social media platforms can provide the capability for just-in-time training for protective action procedures or video coverage and/or live streaming of events. All of these capabilities when properly integrated, can greatly enhance an organization’s crisis and disaster response capability. (Bergeron, 2016)

**SOCIAL MEDIA MANAGEMENT STRATEGY**

However, when it comes to integrating these capabilities, the challenge for many organizations can be developing a suitable social media strategy that fits their particular organization. The key aspect that is sometimes overlooked is, that although the platforms and the technology may be new, novel, or different, at its very core a social media strategy is still really just a media management strategy and needs to adhere to the basic tenets of the organization’s outcomes and objectives. Some of the key components when it comes to social media in crisis and disaster are: 1) Degraded connectivity and communications capability is a given in crisis and disaster and must be assumed and planned for up front. Graphic rich formats, embedded video, etc, that work well during normal operations will generally become an impediment to effective communication during periods of degraded and limited communication capability. Having a pre-configured plan to switch to alternate lower bandwidth, less graphical, and text-based formats should be considered and planned for up front. 2) A social media and internet communications strategy is more than just a website or Facebook page and must be comprehensive and encompass the breadth and range of platforms that constituents and customers are likely to use on a daily basis and will default to in crisis and disaster.  3) Organizational social media operations must be monitored, updated, and moderated if they have any hope of being effective. There is nothing worse than discovering months old information on a platform when
searching for relevant organizational information during a crisis or disaster. 4) Organizations need to ensure they communicate on multiple platforms, to multiple audiences, utilizing multiple messages and multiple formats appropriate to both the situation and the desired outcome. 5) In terms of management and implementation, even in small organizations social media should not be considered merely an additional duty given to the newest or youngest employee. In a perfect world, the social media management strategy should garner just as much attention as other core operations functions. 6) Finally, social media messaging in crisis and disaster absolutely must be relevant and consistent across platforms and media types and be synched to organizational objectives and desired outcomes. (Bergeron, 2016)

THE GOOD, THE BAD, AND THE UGLY (OF SOCIAL MEDIA)

While for an individual it is very likely in our current “look at me” oriented world, that more comments and online attention contributes to a perception of importance, status, fame, etc. For organizations and many high-profile individuals, more clicks, comments, “likes”, “pokes”, and shares do not necessarily equal overall effectiveness in the social media world. An organization is usually much more likely to have viral content related to lapses, mistakes, indiscretions, and bad behavior of the organization or its employees and associates as it is for outstanding performance activity. Additionally, unlike face to face interaction in most cases, the impersonal and sometimes even anonymous nature of online communications and interactions has a tendency to lead to rude and bad behavior and typically encourages the emotionalization and escalation of events that might otherwise be easily handled if conducted in person. Related to this is the fact that in some cases, “people” online may simply not be who they say they are and in some cases may not even be actual people at all in the case of “botnets” and automated response and “clickbait” server farms.

One of the incredible strengths of social media engagement for organizations can in many cases also be one of the greatest potential weaknesses and vulnerabilities as well. While a robust social media strategy and active engagement allows organizations to “speak” directly to constituents, customers, and stakeholders, in crisis and disaster, many organizations will find that
as the level of engagement and number of followers explodes exponentially, their capability to effectively and efficiently manage those interactions can become incredibly difficult. In such situations, the exponential “blowing up” of social media presence becomes a double-edged sword and can be particularly difficult for small and lean staffed organizations to handle. (Bergeron, 2016)

An additional challenge in the social media world is the increasing propensity for self-selection and filtering of content particularly in normal day to day and pre-crisis and disaster environments. This can also be exacerbated by the algorithmic nature of many social media network operating systems and policies, which will tend to steer their members towards similar sites such as those that they have already shown a propensity to favor. Obviously, this is not as big of a consideration in the immediate aftermath of a crisis and disaster situation as users will tend to search for the relevant content that reaches their perspective needs and is not the case with all social media platforms, additionally this can also be mitigated with multi-platform engagement. Somewhat related to the self-filtering phenomenon, is the fact that the nature of social media interaction with its inherent “trusted relationship” status between social media “friends” and connections in many cases cultivates the perfect environment for the creating, propagating and circulating conspiracy theories. In many ways social media and conspiracy theories are a perfect match and as a result, there are entire organizations, media outlets, and businesses that have been created just to debunk online, internet and social media conspiracy theories. (O’Neill, 2015)

SOCIAL MEDIA “TRUTHS” (IF THERE IS SUCH A THING)

Arguably when it comes to social media and online interaction, the nature of the truth likely changes daily, so to try and enumerate “truths” of the social media world in crisis and disaster is probably a dubious undertaking at best. However, if not immutable truths, there are at least some guiding principals and conventional wisdom that organizations should consider when operating in the social media realm, especially during times of crisis and disaster. The first factor that must be considered is that unlike traditional media sources and outlets such as radio, television, print, etc., social media is largely a “pull” medium and followers and users must specifically seek
out the platforms, channels, and sites specifically. In most cases, the idea of passive exposure to social media content is highly unlikely for most organizations. One caveat to this in crisis and disaster however is the increasing tendency of traditional media outlets (especially broadcast and online) to use social media postings from organizations, agencies, and even individuals as primary sources in emerging crisis and disaster situations. This tendency provides a unique opportunity for an organization to position itself as an early authoritative source to fill the critical information void that will generally always be present in the first minutes and hours after disaster and crisis. The additional advantage here is that the organization can largely communicate directly with the public in an unfiltered manner. A note of caution on that point is in order as this capability can have unintended consequences as has been evidenced by the US White House communications staff having to scramble on a regular basis to counteract some of President Trump’s most “unfiltered” Tweets. (CBS News, 2016)

As mentioned previously, one social media “truth” that is probably the most reliable and durable tenet regardless of platform, organization, or even message, is that followers will increase rapidly both during the run-up to a pending crisis or disaster as well as in its immediate aftermath. In some cases, this can be measured in thousands of new followers per hour which can seriously strain organizational resources dedicated to social media engagement activities. Clearly this is an area that should be accounted for in the organizational social media strategy and contingency planning. Of course, almost as quickly as those followers will be onboarded to social media sites and platforms during crisis and disaster, they will usually begin to separate themselves fairly soon after the immediate aftermath has passed. An innovative organization might plan to try and continue to cultivate and maintain those followers as part of its social media base.

Finally, given the unregulated and free-for-all nature of social media and the online communication environment, organizations should anticipate that they will likely be unable to fully control (or even control at all) the information environment surrounding a crisis and disaster situation. It should be assumed that there will be multiple players and they will all likely have differing agendas, motives, and desired outcomes for their engagement. Not all of them will likely be in the best interest of the impacted organization. Related to this is also the fact that criminals and scammers can and likely
will also occupy the social media space and, in many cases, will compete directly with legitimate organizations and entities. (Bergeron, 2016)

**IMPLICATIONS/OUTLOOK FOR THE FUTURE**

When it comes to social media in crisis and disaster, it is fairly clear that the only real constant is in fact constant change. Even more so than other media environments, the social media environment is dynamic and is in a constant state of flux. Users and followers are also likewise constantly changing their likes, habits, and consumption patterns. For instance, whereas 15 years ago social media largely did not exist, and most people connected to the internet from a dialup landline phone on a desktop computer and mostly viewed static websites. Today’s user and follower likely has no landline phone, connects from a mobile device through a high speed data connection, and may only communicate and interact from within a half dozen-specific applications. That means that organizations must ensure that they tailor their communications to multiple audiences, multiple mediums, and multiple messages. While doing this, it is also imperative that organizational information is planned for in an in-depth and comprehensive manner. Organizations must also remember that in most cases social media should not be relied upon or considered as a replacement for traditional media, but more as a companion or a compliment to it.

There is also another reality that goes beyond social media but is greatly enabled by it and that is the ubiquity of sensors and devices that all possess both a camera with still frame, video, and audio capture capability as well as the capability to instantly upload or broadcast that content onto social media platforms or to share it with traditional media for broadcast as well. As we have seen in many high-profile incidents, this ability has proven critical in defining and in some cases countering the narrative of agencies and organizations. Organizations and agencies must assume that every interaction of its agents and employees can and will be captured, shared, and broadcasted in crisis and disaster situations particularly when they are controversial or show the organization in a bad light. Finally, as stated previously, organizational social media strategy, policy, operations, and management simply cannot be seen as an additional duty or part time job and must be planned
for well before a crisis or disaster occurs and must be carefully managed once it does.

**SOME FINAL THOUGHTS**

Hopefully, as we have seen based on the ideas presented previously in this article, it should be apparent that in the world of corporative security, things are always changing and evolving and when it comes to social media and emerging technology, those items tend to move faster and further than organizations do in anticipating their impact and in reacting to them. This tends to create a natural lag in the ability of organizations to keep pace and a state where organizations and entities are always trying to keep pace with a requisite set of inherent challenges and vulnerabilities as a result. Also, if we consider emerging technology and systems, organizations really need to make sure that embracing these new systems and technologies will actually benefit their mission, goals and objectives, especially when one considers that fact that many of these new additions will come with significant staffing and manpower impacts, maintenance costs, and other possible unseen mandates, liabilities, and lifecycle costs. The key is to make sure that a new capability is truly useful and enhances organizational safety, security, and effectiveness and is not embraced just because it is the newest and greatest thing and since “everyone else is doing it.” It is also important to realize that in many cases the addition of a new technology or capability will also bring increased expectations on the capability of the organization which can be challenging especially in the early stages of adoption since many systems and technologies may come with a significant learning curve and a gap between initial expectations and operational capability. Care must be taken to insure that there is no lapse in organizational effectiveness in such circumstances.

**SOME FINAL, FINAL THOUGHTS**

Finally, given the nature of our ever connected and digital world and the fact that it brings with it great convenience, capability, and comfort to our modern quality of life, we have to remember that at the same time, social media, constant connectivity, and other emerging technologies also can introduce significant threats and vulnerabilities as well when things fall apart or fail, especially in times of crisis and disaster, as they most surely will.
This can and should have a significant impact on the state of the current and future security environment of organizations related to the various areas of social media and emerging technology. As a result, innovative and forward-thinking organizations should not merely wait or simply react to the current ever-changing technology environment, but instead should try to actively manage and shape it by ensuring that their policy, preparedness, operations, and response protocols for crisis and disaster situations are crafted with considerations of the areas previously discussed.

Ultimately, we find that some of our biggest opportunities when it comes to leveraging social media and emerging technology are also likewise some of the biggest potential challenges and threats we are likely to face going forward within the realm of corporative security, and even more so when crisis or disaster strikes. While it may be tempting at times to simply choose to ignore these or give in to the somewhat natural tendency to discount their impact in the short term, it is increasingly apparent to the enlightened observer, that when a crisis or disaster is looming or has occurred, they will likely manifest themselves as critical vulnerabilities and potential points of failure. Finally, this is true both in terms of an immediate situation but is also even more critical in the mid to long term if we do not begin to address them.

REFERENCES


O’Neill, P. (2016). Why it’s impossible to debunk a social-media conspiracy theory. The Daily