Accessing Data and Maintaining Privacy Before, During and After Catastrophic Events

The basic precepts of privacy do not change in the face of catastrophes, but the type and amount of personally identifiable information (PII) used and generated and the need for legitimate access to those data increase substantially. There are different requirements for data collection, storage, access and disposal for a range of catastrophic events. It is important to understand how those data might best be protected throughout their life cycles to ensure the privacy rights of individuals and still provide what is needed for first responders and assistance agencies. It is also important to discuss the continuity and restoration of IT systems and business processes and the recovery of data and access affected by catastrophes.

There are substantial differences between regular contingency planning—business continuity planning (BCP) and disaster recovery planning (DRP)—and catastrophe contingency planning (CCP).[1] These differences make for increased difficulty and complexity in recovering both systems and the sensitive data that they contain and ensuring that only authorized and authenticated users have access.

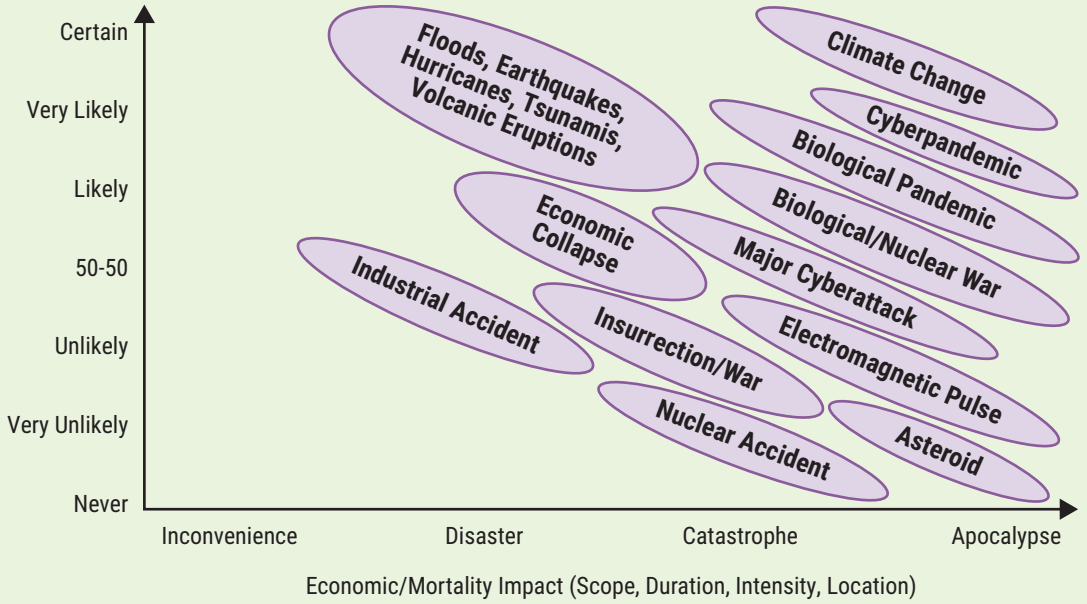
Types of Catastrophic Events

The terms disaster, catastrophe and apocalypse are used to describe increasingly destructive, high-impact events. **Figure 1** shows examples of such events, with impact plotted against likelihood. The diagram is illustrative rather than definitive. The placement and magnitude of the incidents are based on estimates by the World Economic Forum, the Global Challenges Foundation and the other subject matter expert opinions.

In **figure 1**, the orientation of the ovals implies that less impactful events are more common than those of greater impact. For example, less powerful earthquakes occur more frequently[2] compared to those that are devastating, such as the 2010 earthquake that destroyed Port-au-Prince, Haiti, leaving an estimated 250,000 dead, 300,000 injured and 1.5 million homeless. Not only are such events damaging in and of themselves, but relationships between and among events in **figure 1** must be considered. These relationships include causation and intensity. For example, a pandemic might lead to economic crises and political upheavals. Such combined events exacerbate privacy risk because they cut across multiple data silos. For example, the health records of those affected by a pandemic need to be shared with others, such as contact

C. Warren Axelrod, Ph.D., CISM, CISSP
Is the research director for financial services at the US Cyber Consequences Unit. Previously, he was the business information security officer and chief privacy officer at US Trust. Axelrod was a cofounder and board member of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and represented the banking and finance sector in Washington DC, USA, during the Y2K date rollover. In 2001, he testified on cybersecurity before the US Congress. He received ISACA's Michael P. Cangemi Best Book/Article Award in 2009. The most recent of his five books is *Engineering Safe and Secure Software Systems*. His current research interests include the behavioral aspects of cybersecurity risk management.

Figure 1—Catastrophic Events by Likelihood and Impact



tracers, but sharing systems and communications could have been destroyed by a flood or wildfire, so it may be necessary to provide greater access to sensitive personal information to overcome adverse circumstances. There are also surges in unauthorized access to troves of personal data facilitated by these disruptions. Hurricane Katrina in the United States spawned a rash of identity theft and egregious fraud, as hackers were able to pose as victims.[3]

Although each category of catastrophe is different, they all have certain aspects in common from a data security and privacy perspective. Examining the risk by type of catastrophe can help in understanding how to mitigate the risk.

Figure 2 illustrates the nature and characteristics of the catastrophic events illustrated in **figure 1**. The impact depends very much on the geography and reach of catastrophes. Preparation is shown to be quite low in many cases. If there was greater preparation, responses would not be so dramatic. However, human biases tend to lead people to be underprepared.

Anticipating Catastrophic Events

Nicholas Taleb popularized the concept of "black swans," meaning high-impact, low-probability events.[4] However, Taleb himself argued against the COVID-19 pandemic being a black swan.[5] Instead, he categorized the pandemic as "a portent of a more fragile global system."

Some suggest that a better way to anticipate the future than "simplistic extrapolations" is to combine "scenario planning" (or thought experiments) and "probabilistic forecasting." Advocates of scenario planning consider plausibility over probability, whereas forecasters believe in calculating the odds of possible outcomes and then quantifying risk.[6]

Although some believe that specific catastrophes are almost impossible to predict realistically in scope, timing and location, published predictions are always discovered after the fact.[7] It can be argued that catastrophes will occur over a period of time, but it is usually not known what the category of catastrophe will be and when and where it might happen. As a result, some level of preparation is needed. This may include food and water storage, availability of hospital ships, compatible communications or training, and equipping first responders.[8] When it comes to privacy in highly disruptive times, it makes sense to secure personal data in various forms (e.g., paper, electronic storage) and at locations that are likely to survive and be accessible under a range of catastrophic conditions.

Figure 2—The Nature and Characteristics of Catastrophes

Type of Catastrophe	Geography	Impact	Preparation	Level of Response
Hurricane	Local Regional	Disastrous Catastrophic	Moderate High	High Very high
Snowstorm	Local Regional	Disastrous Catastrophic	Moderate High	Usually moderate to high High
Tsunami	Local Regional	Disastrous Catastrophic	Minimal Moderate	Very high Extremely high
Wildfire	Local Regional	Disastrous Catastrophic	Moderate Moderate	High Very high
Health pandemic	Global	Catastrophic	Minimal	Moderate to high depending on country
Climate change	Global Regional	Catastrophic Apocalyptic	Minimal Minimal	Minimal Minimal
Cyberpandemic	Regional Global	Catastrophic Apocalyptic	None None	Minimal Extremely high
Supervolcano	Global	Catastrophic	None	Extremely high
Large asteroid	Global	Apocalyptic	None	None
Electromagnetic pulse	Regional Global	Catastrophic Apocalyptic	None Minimal	Extremely high None
Nuclear war	Global	Apocalyptic	Moderate	Extremely high
Cyberwar	Regional Global	Disastrous Catastrophic	Minimal Minimal	High Extremely high
Insurrection Conventional war	Regional Global	Catastrophic Apocalyptic	Moderate High	High Extremely high
Nuclear/industrial accident	Local Regional	Disastrous Catastrophic	Minimal Moderate	Very high Extremely high
Financial crisis or collapse	Regional Global	Disastrous Catastrophic	Minimal Minimal	Moderate Extremely high

Preparation and Mitigation Strategies

Although many catastrophes cannot be readily anticipated or avoided, there are actions that can be taken to reduce the impact on privacy for individuals and organizations, and potentially speed the recovery and restoration of personal, government and organizational, secret, and other critical records. **Figure 3** shows suggested privacy preparation and mitigation activities and the type of response appropriate for each catastrophe.

Addressing Risk Perception

Behavioral scientists argue that there are a number of significant biases that arise when it comes to preparing for catastrophes.[9] Preparedness errors can be traced to the harmful effects of six systematic biases:[10]

1. **Myopia bias**—A tendency to focus on overly short time horizons
2. **Amnesia bias**—A tendency to forget too quickly the lessons of past disasters
3. **Optimism bias**—A tendency to underestimate the likelihood of losses from future hazards
4. **Inertia bias**—A tendency to maintain the *status quo* or adopt a default option
5. **Simplification bias**—A tendency to selectively tend to a subset of the relevant factors
6. **Herding bias**—A tendency to base choices on observed actions of others

There are also a number of other biases such as:[11]

- **Availability bias**—The tendency to estimate the likelihood of specific events occurring based on one's own experience

Enjoying this article?

- Read *Conducting an IT Security Risk Assessment. www.isaca.org/conducting-an-IT-security-incident-assessment*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 3—Data Preparation and Mitigation and Responses for Disasters and Catastrophes

Disaster or Catastrophe	Responses for Consideration	Personal Data Preparation and Mitigation of Losses		
		Individuals	Government	Businesses
Hurricane	• Evacuate within hours or days of notification and seek a safe location.	• Identify and list personal information documents.[a] • Collect documents and electronic devices in storage for quick access. • Scan documents and load the information onto a Universal Serial Bus (USB) drive. • Download the latest online documents to a USB drive. • Upload the latest documents to cloud storage if secure.[b]	• Collect individuals' data in advance to facilitate response, recovery and rebuilding. • Provide access to personal information to data owners and authorized personnel during and after the event.	• Assist employees, customers, partners and first responders in getting access to personal data on an as-needed basis. • Protect intellectual property and trade secrets from leaking to competitors.
Earthquake, tsunami	• For a large earthquake, immediately exit from buildings and evacuate affected areas for safer place. • Upon tsunami alert, evacuate coastal areas and seek high ground.	• Same as hurricanes, except there may be no time to access documents. • Have document scans and electronic data reside in the cloud with access given to trusted friends, relatives or custodians.	• Same as hurricanes, except area offices may not be operational. • Personal and agency-sensitive data may not be accessible out-of-area if not stored in other location(s).	• Same as hurricanes, except businesses may not be operational. • Personal and organization-sensitive data may not be accessible out-of-area if not stored in other location(s).
Flash flood, ocean surge, mudslide, tornado, wildfire	• Evacuate within seconds or minutes. • For expected floods, go to upper floors (not attic) with easy access and exit. • For tornadoes, go to internal rooms, bathtubs or basements.	• Similar to hurricanes or earthquakes, where warnings and alerts might be given sufficiently in advance, allowing personal information to be gathered and transported elsewhere.	• Similar to hurricanes or earthquakes where there might be sufficient time to gather and take critical documents.	• Similar to hurricanes or earthquakes where there might be sufficient time to gather and take critical documents.
Climate change	Short term: • Same as hurricanes Medium term: • Raise buildings. • Build sea walls. Longer term: • Move away from vulnerable coasts, flood plains and fire-prone areas.	• Follow privacy practices for high-category hurricanes, which are arguably influenced by climate change. Climate change is likely to play out over a prolonged period, which allows time for non-emergent planning and consideration of plan execution.	• Follow privacy practices for high-category hurricanes, which are arguably influenced by climate change. Climate change is likely to play out over a prolonged period, which allows time for non-emergent planning and consideration of plan execution.	• Follow privacy practices for high-category hurricanes, which are arguably influenced by climate change. Climate change is likely to play out over a prolonged period, which allows time for non-emergent planning and consideration of plan execution.
Industrial explosion or nuclear accident	• Evacuate the area upon notification. • Activate first responders.	• Similar to earthquakes	• Similar to earthquakes	• Similar to earthquakes
Insurrection and wars (including cyberwars)	• Go to a safe/secure area if possible. • Go to refugee camps. • Emigrate if possible. • Await instructions from leaders.	• Gather personal documents and take them with you if possible.	• Depends on the nature of the war or insurrection.	• Depends on the nature of the war or insurrection.
Cyberpandemic, Electromagnetic Pulse (EMP)	• Stay in place unless the current location is no longer viable. • Try to determine the extent of outage and how to recover.	• Maintain hard copies of crucial documents. • Store documents in a safe place that does not require electronic access.	• Maintain hard copies of crucial documents. • Store documents in a safe place that does not require electronic access.	• Maintain hard copies of crucial documents. • Store documents in a safe place that does not require electronic access.

Figure 3—Data Preparation and Mitigation and Responses for Disasters and Catastrophes *(cont.)*

Disaster or Catastrophe	Responses for Consideration	Personal Data Preparation and Mitigation of Losses		
		Individuals	Government	Businesses
Disease pandemic	• Follow public health advice and mandates. • Stay home unless work is qualified as essential. • Leave home only for health reasons and essential activities.	• Follow the advice for hurricanes, without having to evacuate the premises or to relocate. • Ensure that others can access wills and healthcare proxies in hard copy.	• Greater need to protect personal information due to agencies being overwhelmed with cases, deaths and consequent services. • Need to protect against fraud.[c]	• Google/Apple and others developed apps for contact tracing.[d]
Cyberattack	• Attempt to avoid or minimize damage from an attack. • Stay in place unless the cyberattack makes the location unsafe. • Engage experts to assist with recovery and repair.	• Keep separate offline copies of sensitive personal information. • Do not respond to suspicious requests for personal information. • Report attacks to appropriate agencies.	• Maintain public-facing websites to facilitate the reporting of data/privacy breaches. • Enforce existing laws regarding personal data breaches.	• Build privacy into software. • Report weaknesses. • Provide patches and fixes on a timely basis.
Economic collapse	• Apply for financial and other aid as available.	• Follow the advice for hurricanes, with the likelihood of having to relocate or find jobs. • Be cognizant of increases in attempts at identity theft and fraud.	• Monitor relief services for identity theft and fraud. • Protect the personal data of those seeking support.	• Keep access management systems up to date during periods of high turnover.[e]
Asteroid collision	• Response varies with asteroid's size and consequences of impact.	• For lesser impact, follow advice for earthquakes, hurricanes and tsunamis.	• For lesser impact, follow advice for earthquakes, hurricanes and tsunamis.	• For lesser impact, follow advice for earthquakes, hurricanes and tsunamis.

(a.) Includes, but is not limited to, driver's licenses, passports, birth certificates, marriage licenses, wills (including health care proxies), medical records, lists of medications, property deeds, credit cards, payment schedules, bank checks, cash, usernames and passwords, insurance documents, bank statements, brokerage account statements, loan and mortgage documents, tax forms and payments and other financial records. (b.) There have been several recent high-profile revelations of security vulnerabilities due to misconfigured security buckets on Amazon Web Services (AWS) and Google. It is not known whether these vulnerabilities have been exploited by attackers. However, caution has been advised by victim organizations. (c.) Zamost, S.; K. Tausche; K. Hernandez; "Criminals Launder Coronavirus Relief Money, Exploit Victims through Popular Apps," CNBC, 18 November 2020, *www.cnbc.com/2020/11/18/criminals-launder-coronavirus-relief-money-exploit-victims-through-popular-apps.html*. (d.) Cranor, L. F.; "Privacy: Digital Contact Tracing May Protect Privacy, But It Is Unlikely to Stop the Pandemic," Communications of the ACM, vol. 63, iss. 11, November 2020, p. 22–24, *https://cacm.acm.org/magazines/2020/11/248196-digital-contact-tracing-may-protect-privacy-but-it-is-unlikely-to-stop-the-pandemic/fulltext*. (e.) Sharman, R.; *Digital Identity and Access Management: Technologies and Framework*, IGI Global, USA, 2012

- **Compounding bias**—The tendency to focus on the low probability of an adverse event in the immediate future rather than on the relatively higher probability of the event occurring over a longer period
- **Anchoring bias**—The tendency to be overly influenced by short-term considerations that come easily to mind

Privacy, Restrictiveness and Convenience in Times of Disaster

It is interesting to what extent computer users are willing to trade privacy for convenience or, conversely, give up convenience for privacy. Early studies showed how little enticement people need to give up private personal information. In one experiment, students were willing to give up their passwords for a piece of candy.[12] When confronted with having to click "I Agree" in order to access certain online services, many people do not even read the agreement as to whether the organization on the other side can share information about them and their use of services, purchases and preferences. There is an ongoing fight as to whether one should be allowed to opt in or opt out, where the former benefits the individual and the latter is greatly preferred by marketers. In the United States, the opt-out option is preferred, whereas the EU lawmakers favor opting in. Regardless, there is an implicit tradeoff even when options are limited or difficult to operate, and giving away privacy for well below the value of the data is common.

There are also decisions to be made about the balance between privacy and convenience, secrecy and useability, and security and utility/productivity. **Figure 4** shows some suggested considerations

with respect to tradeoffs among all of these factors. The designation as to whether these tradeoffs are common or frequent or occasional or rare are subjective based upon the general emphasis in research publications and news articles. However, it is important to note that in turbulent times, it is often necessary to give up sensitive personal information, such as health conditions, in order to be helped by first responders and frontline workers.

These considerations are greatly affected by context and the relative power of users and application owners/vendors. They play an important role when it comes to catastrophe contingency planning and operations since the tradeoffs become very different. During catastrophes, decisions lean toward utility and productivity, while convenience and usability, though important, tend to take a back seat.

There are a number of convenience-privacy trade-offs that can be considered. **Figures 5, 6** and **7** are illustrative and not based on empirical evidence.[13] In **figure 5**, the combination of usefulness and privacy is greatest when the restrictions are at a minimum. The least value is when there is a compromise and moderate restrictions are applied. Simply changing the value curves in **figure 6** shows that the maximum value is attained at the highest level of restrictiveness—quite the opposite of the previous example. Therefore, one should be very guarded when deciding how restrictive security measures should be because the decision is so dependent on the shape of the value curves.

The determination of relationships among these various factors is difficult at the best of times, much more so in the midst of an upheaval. For purposes of illustration, **figures 5, 6** and **7** show how the different shapes of the curves representing privacy and convenience (and other factors) can affect decisions as to level of restrictiveness from lowest to highest to somewhere in between.

Although it may be possible to estimate various relationships among privacy and convenience

Figure 4—Considerations Regarding the Protection-Restrictiveness Tradeoff

Means of Protecting Information Assets	Restrictiveness		
	Convenience	Usability	Utility/Productivity
Privacy	Common	Occasional	Rare
Secrecy	Rare	Rare	Common
Security	Common	Common	Common

Figure 5—Maximum Value of Convenience and Privacy at Lowest Level of Restrictiveness

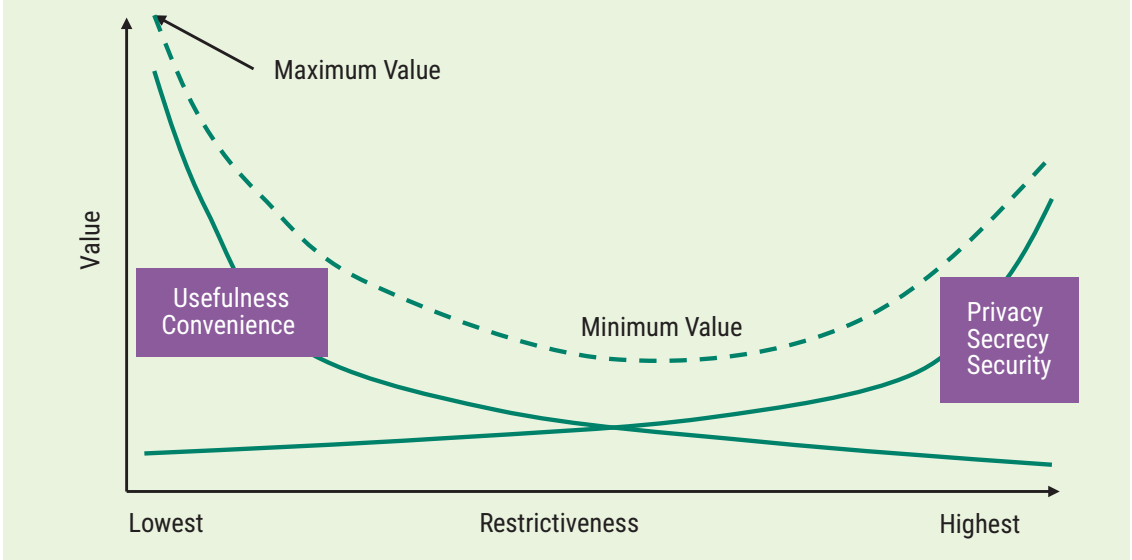


Figure 6—Maximum Value of Convenience and Privacy at Highest Level of Restrictiveness

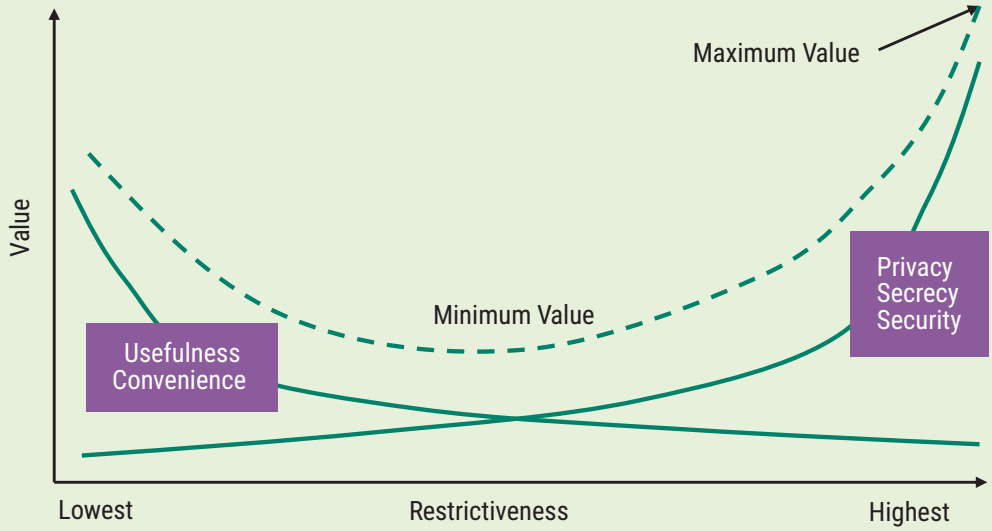
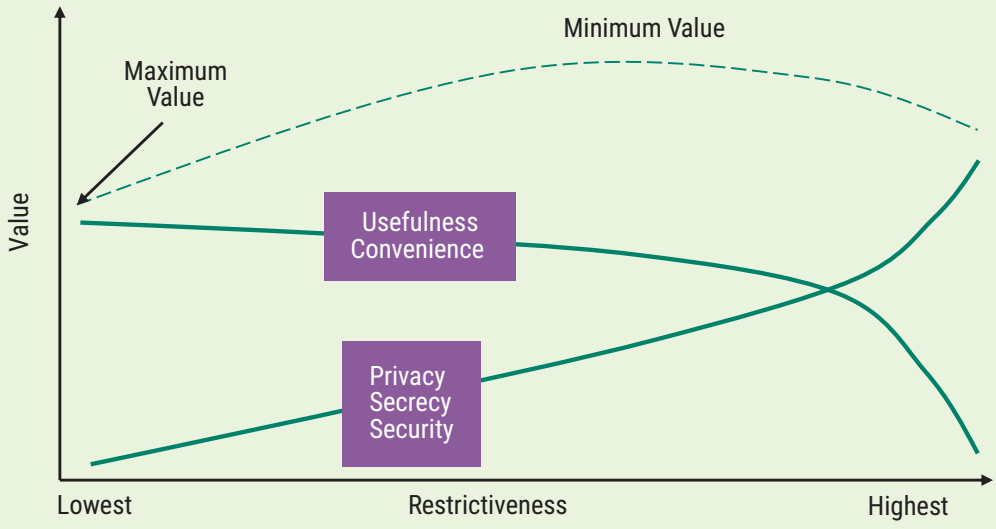


Figure 7—Maximum Value of Convenience and Privacy at Moderate Level of Restrictiveness



during regular times, the curves are likely to change considerably during a catastrophe. For example, it might become much more important to share certain personal information, such as health records showing medications and allergies, following an earthquake when individuals may have had to evacuate a building without their life-preserving medications, or they may be unconscious and not able to tell medical staff whether they are allergic to medications such as penicillin.

Recognizing the difficulties and limitations of ascertaining relationships between privacy and convenience and the other factors by surveying contingency planners, incident responders, individuals, emergency product and service vendors, and software and communication developers is extremely important and may well serve to avoid, or at least reduce, serious mistakes by those tasked with assigning access to personal data.

The collection, accessibility and storage of some nonpublic personal information is paramount. Privacy is brought up as a concern, but tends to take second place to utility.[14] Furthermore, although physical security professionals are frequently included in contingency planning—they have to be because the plans often require moving operations to other facilities—information security support may be an afterthought, if considered at all. In any event, the development and testing of contingency plans requires the collection and publication of substantial amounts of confidential personal and business information for both the organization and third parties, which needs to be updated regularly. Such information would be extremely valuable to competitors and potential attackers were it to be hacked. Consideration for securing such personal and sensitive business information is crucial.

Business continuity and disaster recovery planning shifts the curves in **figures 5, 6** and **7** to suggest relaxing restrictiveness and increasing access and availability to systems and data. Therefore, **figure 5** will likely be more representative for contingency situations than **figure 6**. The combined graph, showing a maximum value at moderate restrictiveness, would likely shift to the left.

Figure 8 shows what the privacy and security are for different situations and how the benefits and threats differ under those situations.

Data Retention and Disposal

A major, justifiable concern with respect to privacy emanates from a fear that personal and other sensitive data collected during catastrophes for good reason by applications (apps) that were used to gather and process the data that are retained by government are also retained by influential organizations such as Facebook and Google. Although many agree to having such sensitive data, such as tracking data, to help facilitate recovery from catastrophes, such agreement does not necessarily cover retention of the data and apps once the disaster or catastrophe has passed and the need for the data and apps no longer exists.

It is easy to see how both public and private sector organizations might try to justify holding on to contingency data and keeping the computer systems and command and control centers active beyond an actual or potential catastrophe.[15] There are certainly situations when it makes good sense to retain data, software, media and equipment, in which case these resources should be well secured

Figure 8—Privacy and Security Issues, Benefits and Threats by Situation

Situation	Privacy Issues	Security Issues	Benefits	Threats[a]
Regular business	• Identity theft • Fraudulent use • Information leakage	• Access (identity and access management) • Data protection (encryption) • Data management (creation, use, storage, disposal)	• Marketing • Ease of use	• Data breaches • Denial of service • Ransomware
Contingency planning, business continuity and disaster recovery	• Names, telephone numbers, email and physical addresses of contacts	Same as above plus: • Locations • Systems • Personnel	• Rapid response • Quicker recovery	Same as above plus: • Spoofing (masquerading) • Physical theft, loss, damage, manipulation
Catastrophe planning, recovery and restoration	• Names, telephone numbers, email and physical addresses of contacts	Same as above	Same as above	Same as above

(a) European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2020—List of Top 15 Threats," 20 October 2020, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats*

and only available to authorized personnel, where the authorizing entity is apolitical and trusted.

If the data and media are to be disposed of, there are many ways it can be done.[16] The key is to have the disposal process overseen and audited to ensure compliance with the rules of data disposal and media destruction.

It is imperative to be continuously aware of the danger that contingency data and collection capabilities might be used to monitor and control the population when the event is over (as currently exists in China), despite not having been given explicit approval.[17] This could lead to uses that violate basic personal rights.

> "IN PREPARING CONTINGENCY PLANS FOR POSSIBLE CATASTROPHIC EVENTS, PLANNERS MAY NEGLECT SERIOUS ISSUES RELATING TO PRIVACY AND SECRECY."

Conclusion

In preparing contingency plans for possible catastrophic events, planners may neglect serious issues relating to privacy and secrecy. While physical safety and survival are rightly the major concerns during catastrophes, pulling together personal records, if they have been lost due to events such as fire, floods or earthquakes, can be a daunting task if certain preparations to facilitate authorized access have not been made in advance. There are a variety of preparatory and mitigation measures that can be taken in advance of catastrophes to preserve and make available critical, governmental and organizational data during and following incidents. Any progress made in this effort of ensuring, protecting and preserving privacy will most likely pay substantial dividends should unpredicted and unimagined events occur.

Endnotes

1 Gupta, M.; R. Sharman; *Social and Organizational Liabilities in Information Security*, IGI Global, USA, 2008, p. 1–22

2 United States Geological Survey (USGS), "Why Are We Having So Many Earthquakes? Has Naturally Occurring Earthquake Activity Been Increasing? Does This Mean a Big One Is Going to Hit? Or We Haven't Had Any Earthquakes in a Long Time; Does This Mean That the Pressure Is Building Up for a Big One?" *https://www.usgs.gov/faqs/why-are-we-having-so-many-earthquakes-has-naturally-occurring-earthquake-activity-been?qt-news_science_products=0#qt-news_science_products*

3 United States Federal Bureau of Investigation (FBI), "More Than 900 Defendants Charged With Disaster-Related Fraud by Hurricane Katrina Fraud Task Force During Three Years of Operation," 1 October 2008, *https://archives.fbi.gov/archives/news/pressrel/press-releases/more-than-900-defendants-charged-with-disaster-related-fraud-by-hurricane-katrina-fraud-task-force-during-three-years-in-operation*

4 Taleb, N. N.; *The Black Swan, Second Edition: The Impact of the Highly Improbable*, Random House, USA, 2010

5 Avishai, B.: "The Pandemic Isn't a Black Swan, but a Portent of a More Fragile Global System," *The New Yorker*, 21 April 2020, *www.newyorker.com/news/daily-comment/the-pandemic-isnt-a-black-swan-but-a-portent-of-a-more-fragile-global-system*

6 Scoblic, J. P.; P. E. Tetlock; "A Better Crystal Ball: The Right Way to Think About the Future," *Foreign Affairs*, vol. 99, iss. 6, November/December 2020, p. 10–18, *https://www.foreignaffairs.com/articles/united-states/2020-10-13/better-crystal-ball*

7 Since those professing to predict the future commonly cover a wide range of outcomes, some forecasters will likely be correct and others (often the majority) will be wrong, as seen with the financial crisis of 2008–2009, for example.

8 *Op cit* Gupta and Sharman

9 Slovic, P.; E. U. Weber; *Perception of Risk Posed by Extreme Events*, Risk Management Strategies in an Uncertain World Conference, Palisades, New York, USA, 12–13 April 2002, *www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/slovic_wp.pdf*

10 Meyer, R.; H. Kunreuther; *The Ostrich Paradox: Why We Underprepare for Disasters*, Wharton School Press, USA, 2017

11 *Ibid.*

12 Vaughan-Nichols, S. J.; "Would You Sell Your Password for Chocolate?" *Computerworld*, 1 May 2008, *https://www.computerworld.com/article/2478374/would-you-sell-your-password-for-chocolate-.html*

13 It would be an interesting and valuable research project to determine the shapes and magnitudes of the curves in **figures 5**, **6** and **7**, as well as other possibilities.

14 There is at least one case where an organization posted its contingency plan containing names, addresses and telephone numbers of key personnel, thereby making the data available to anyone with Internet access. The report had "Confidential" printed all over it.

15 The author participated in the joint public-private National Information Center setup for Y2K command and control. He believed and stated that the command center and the software supporting it (and some low number of maintenance staff) should be retained to facilitate the handling of future disastrous situations. The center was summarily dismantled following Y2K, much to the detriment of readiness for managing future events. The Y2K command center did not use personal information as such, although some of the information collected could have threatened the national security of the United States and other countries had it been released.

16 Financial Services Roundtable, BITS Key Considerations for Securing Data in Storage and Transport, BITS Security and Risk Assessment Working Group, 2006, *https://silo.tips/download/bits-key-considerations-for-securing-data-securing-physical-media-in-storage-tra*

17 *Op cit* Abrich and Chan