Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Libraries and risk

1.1 The prevalence of risk

Risk pervades life.

Everywhere, and at all times, you live under threat from numerous perils. Fortunately you have the time and opportunity to prepare for whatever might happen, and you possess the intelligence with which to mitigate risk. Working against you, however, is human nature, which includes apathy, stubbornness, irrationality and narrowness of perception: traits that hinder effective disaster planning in any organization.

Librarians are no more inclined than people in other professions to plan for and respond to disasters. Librarians are seldom trained in risk assessment and management, and in many cases have relied on others – police, firefighters, municipal planners, insurers, public health authorities and consultants – to prepare them for and occasionally save them from fire, flooding, severe weather, criminal activities and other negative events. But even when external bodies offer assistance and good advice, many librarians have not availed themselves of these things. There are numerous other tasks to complete. The adult services coordinator and her staff are busy weeding the fiction collection; the children’s librarians are struggling with the summer reading programme; the technical services department has what appears to be an insurmountable cataloguing backlog; the branch clerical staff is having difficulty handling an increase in borrowing and returns; and the head librarian is engaged full time in persuading the city council and library board not to cut the budget. There are few library employees who have time to devote to disaster planning. Moreover, many employees admit that they find planning and any training associated with it to be onerous and dull.

Thus it is no surprise that so many libraries lack effective disaster plans. In fact, library employees at all levels are often oblivious to the most conspicuous threats to their personal safety and operations. The reason is simple. Whereas daily routines involve the frequent repetition of activities, and ordinary problems and their solutions present themselves with dependable regularity, disasters are infrequent. Decades might pass between fires and floods; such disasters might never occur at most sites.

Because risk so infrequently turns into actual threats, you might take your safety and security for granted. The infrequency of emergencies and disasters can lull you into apathy. If deadly pandemics and fires and terrorist attacks are so unlikely and rare, why should you bother to take precautions against them? Are not the chances of such things happening slim? Why waste time, money and other resources to protect yourself from something that will probably never happen?

These are good questions. The answer is twofold. First, if risk never turns into actual threats, and you are never faced with an emergency or disaster, you may celebrate your good luck. At least you have demonstrated good sense and responsible custodianship by preparing for the worst, which is constantly possible. After all, you
are unable to predict the future with absolute certainty, so you were prudent to acknowledge the possibility of nasty surprises.

But, second, if the risk of a fire turns into a real conflagration that engulfs your main branch, then you were equally sensible to have a plan to deal with the loss – temporary or permanent – of that branch building, the loss of the offices, collections, and other assets that it contained, and the displacement of the employees who occupied it. There might be those who criticize you for developing disaster plans, and who suggest that you are ‘alarmist’ or ‘Chicken Little’. You need patience and determination to deal with such criticism as a matter of course, and to proceed with the development of your plan. The first step in the planning process is to identify your library’s risk profile, that is, the spectrum of risks that prevail at your site or sites.

The following sections describe different kinds of risks that all planners must take into account.

# 1.2 Natural risks

‘California means earthquakes’, says a public librarian from Los Angeles. ‘Florida means hurricanes. Anywhere near the Mississippi River means floods. In America, nature is brutal.’

In fact, nature is no gentler anywhere else on earth. A large landmass such as the continental US has a long list of prevailing natural risks, but every square inch of the planet is exposed to a list similar in length, and always has been. There is no point in attempting to find a site that is unaffected by the forces of nature. Rather, it is best to identify whatever natural risks prevail, and to prepare for them accordingly. Among the most common are:

- **Flooding and water ingress.** Any library site near a river, lake, harbour or other natural body of water is at risk from flooding. Even a small local pond can break its banks and flood neighbouring sites. Water ingress – defined as seepage of water into a building – can also occur through an open window, a leaky roof, a clogged drain or a sewer back-up. Some regions have dealt with high levels of precipitation for millennia; others have only recently begun to see it owing to changing weather patterns. There is much anecdotal evidence to indicate that flooding and water ingress cause more damage to libraries than any other risk. ‘Water in the wrong place’ could also be the consequence of technological, proximity and security risks.

- **Fire, smoke and fumes.** Naturally occurring fires threaten any library situated near forests and other wooded areas. Any vegetation – including farmers’ crops, gardens in urban parks and tumbleweed – can burn and lead to damage. Smoke and fumes can pose a serious risk not only to employees but also to fragile IT equipment. Fire, smoke, fumes and explosions could also be consequences of technological, proximity and security risks.

- **Severe weather.** Any weather event that becomes extreme can be defined as severe. Winter storms, thunderstorms, high winds and heatwaves are common examples. Note that natural risks often overlap. Thunderstorms can involve lightning, which can cause fires. Winter storms can cause flooding and water ingress. High winds can damage roofs, and lead to water ingress. Heatwaves can result in fires. You must guard against secondary risks, which can cause more damage than the risks that give rise to them. All natural risks have secondary risks.
• **Earthquakes.** Among the most frightening natural phenomena, earthquakes can occur anywhere on earth, but are far more likely to strike regions identified as seismic zones. These include countries around the Pacific Rim, and particularly China, Japan, Indonesia, Canada, the US, Mexico and Chile. Mediterranean countries such as Italy, Greece and Turkey have a long history of devastating earthquakes. Seismologists cannot predict the occurrence of earthquakes with any accuracy. Library buildings and heavy furniture – including shelving systems – are particularly at risk from earthquakes.

• **Tsunamis.** These earthquake-generated sea waves move at high speed and can destroy coastal cities and their outlying communities. They can cause large numbers of fatalities and enormous property damage. Like earthquakes, tsunamis can wipe out not only a region’s libraries, but its entire information infrastructure, including archives and records centres, schools and post-secondary institutions, and information technology in public and private locations.

• **Landslides and avalanches.** Such natural phenomena occur most often in mountainous regions, although any natural slope – for example, a hillside in an urban park or along a suburban road – can be the site of a landslide or avalanche. Geotechnical engineers note the possibility of different kinds of landslides, including rockslides, landslips, mudslides and debris torrents. These could cut off libraries and their communities from neighbouring areas, and disrupt schedules and routines.

• **Pests.** Some insects and various other kinds of wildlife can become a pest in or around a library. The most common are silverfish, cockroaches and bedbugs; rodents such as rats and mice; and pigeons. These pests can infest and damage library materials. They are also signs of poor sanitation. Bedbugs can bite human beings, and rats can spread disease, but pests are rarely life-threatening unless they take the form of the poisonous snakes that congregated near the entrance of a school library in Kenya, or in the corners of a library parking lot in Arizona. Bears and mountain lions have been sighted near Western Canadian libraries. Cobras and scorpions have ‘made nuisances of themselves near libraries’, according to a rural school librarian in southern India.

Less common but still necessary to note for planning purposes in many libraries are:

• **Pandemics.** The last serious pandemic that caused high levels of fatalities was the Spanish Flu of 1918. Recently, in light of the threat of Avian Influenza and Severe Acute Respiratory Syndrome (SARS), governments worldwide have urged citizens to prepare for an outbreak of influenza that could be equally devastating. High-traffic libraries could face lengthy closures in the event of a pandemic.

• **Drought.** Absence of precipitation and the resulting lack of water for human use can occur not only in countries such as Australia, Ethiopia and Somalia, but also in the Southwestern US and in parts of China. Drought can result in crop failure, famine and the displacement of entire populations.

• **Volcanoes.** Most often, volcanoes are located in seismic zones. Notable examples include Italy’s Mounts Etna and Vesuvius, Washington State’s Mount St Helen and Iceland’s Grimsvötn and Eyjafjallajökull. Volcanic explosions are often accompanied by earthquakes. Aside from damaging any community in their immediate area, volcanoes can also disrupt transportation and communications.

### 1.3 Technological risks

‘Anything that can break down will do so eventually, and with gusto’, says a British university librarian during a risk management seminar in London before the 2012 Summer Olympic Games. ‘You focus on information technology, and worry about
computer crashes, but a power outage could shut us down and cause just as much data
loss. A fire in the toaster in our cafeteria forced us to evacuate for three hours. You
need to consider risks from all of our technology, high and low.’

Among the most common technological risks to libraries are:

- **Power outages and brownouts.** A sudden loss of power can result in darkened stack areas
  and much confusion among employees and patrons. Outages can affect a single building or
  an entire city, and have lasted from a few seconds to several days. They can lead to library
  closures and data loss. A related risk is a power spike or surge, during which electrical
  equipment could be overloaded and burned out or ‘fried’. In such cases, IT failure is com-
  mon. Disruptions in the power supply might also be due to natural, proximity and security
  risks.

- **IT failure.** This risk includes the malfunction of computer hardware and software, often
  resulting in unintended shutdown and data loss. Note that in many instances the mechanical
  cause of IT failure can be difficult to detect. IT failure could be the result of other problems
  including water ingress, fire and severe weather.

- **Data loss.** While data loss can be the result of accidental deletion, power outages and spikes,
  and theft, it can also be due to a deterioration of the media: an aging hard drive or CD, or a
  back-up tape that has been stored in an inappropriate environment.

- **Gas leaks.** Civil authorities will not hesitate to shut down entire neighbourhoods if a gas leak
  occurs, owing to the risk of fire and possible explosions. The length of a shutdown will de-
  pend on how long civil authorities will need to discover the source of the leak, and to repair
  any damage to gas lines. Gas leaks might be the consequence of earthquakes, serious fires or
  sabotage.

- **Toxic spills.** A spill can involve toxic chemicals such as ammonia and chlorine, petroleum
  products, hospital and laboratory waste, and foodstuffs that will deteriorate quickly if ex-
  posed to the elements. Examples of the last include dairy products, meat and fish. Libraries
  situated near lifelines such as major roads and railway lines are particularly at risk from
  toxic spills. Those who assess risks to library sites may refer to toxic spills as proximity and
  security risks.

- **Train derailments.** Derailments can occur on subway and monorail lines that connect urban
  locations as well as on standard gauge railways for long-distance transportation. Occasion-
  ally derailments cause toxic spills, damage to nearby property and the closure of facilities –
  including libraries – in the vicinity. Hence, derailments are often considered to be a form of
  proximity risk.

- **Transportation disruptions.** Motor vehicle accidents, overturned heavy trucks and trailers,
  and damaged roadways can lead to transportation disruptions. More serious disruptions of
  this kind, however, can be the result of natural disasters such as floods, fires, earthquakes
  and severe weather. Accidents that cause road closures can also be considered as a form of
  proximity risk.

- **Telecommunications disruptions.** For communications purposes, modern organizations rely
  on a variety of technologies, a foundation of which is the telephone system. Most disruptions
  in telephone service are due to either overloading or line breakage.

Overloading occurs in the following circumstances:

- A regional disaster such as an earthquake, large fire, flood or windstorm.
- The commencement of severe weather, for example snowfall or high winds, in the general
  area.
– A major disaster with national or international implications, for example 9/11.
– A major political event, for example an election or the resignation of an important government figure.
– A major sporting event held locally.
– Major statutory holidays, for example Christmas and New Year.

Line breakage occurs in the following circumstances:

– A regional disaster, especially involving high winds, winter storms, heavy snowfalls or the ground motion of an earthquake.
– A systems malfunction at the telephone company.
– Shutdowns for emergency repairs or upgrades.
– Sabotage or tampering.

Mobile or cellular networks have been used during landline disruptions, but it is worth noting that in various circumstances these networks could also break down. While telephone companies worldwide are building more redundancy into their networks, there will always be the risk of disruption. Further, an Internet shutdown could affect worldwide communications for extended periods.

Less likely technological risks, but worth noting for the planning purposes of potentially affected libraries, are:

• **Dam failure.** While dam failures pose a flooding risk to communities in their vicinity they could also lead to long-term environmental damage and power supply problems. Dam failure might be due to structural weakness, an earthquake or sabotage.

• **Nuclear power plant failure.** Meltdowns and the unintentional release of radioactive materials are a source of great concern for any organization near a nuclear power plant. Three Mile Island, Chernobyl and Fukushima are examples of plants where events became out of control and had serious long-term effects. Risk from radiation also exists on academic campuses with laboratories that use and store radioactive materials. Librarians on these campuses should take note of any proximity risk from these laboratories.

• **Aircraft accidents.** Fortunately this risk is small. Libraries located near airports would be wise to consider the effects of a crash in their vicinity, but the chances of an aircraft crashing into a library are infinitesimal. Planners might want to include a nearby airport as a proximity risk, not only because of the possibility of a crash but also because of the risk of fire and explosions from airport fuel tanks.

### 1.4 Human-caused risks

Potentially, the most destructive human-caused risk to libraries is war. Library history contains numerous accounts of libraries damaged or destroyed by aerial or artillery bombardment, and of fires set by combatants. Invading armies have threatened library staffs and looted collections. Civil unrest and rioting can be dangerous for libraries, but these are not often as destructive as war. Sadly, libraries can make an easy target for belligerent forces and people on the rampage.

The most common human-caused threats are less dramatic, but in some cases they can cause extensive damage in libraries.
‘One of the more challenging aspects of dealing with customers’, says a retired salesperson from a large American computer manufacturer, ‘is to convince people that one of the biggest risks to any IT system is human carelessness. People delete enormous amounts of data accidentally. They trip over cables and disable entire departments. They leave their laptops and other portable equipment on buses, trains and planes. They leave the server room unlocked. And librarians have made all of these mistakes.’

Such mistakes are so common that it is safe to assume that librarians make them every day. The foundations of such risks would include:

- **Apathy**: ‘I really don’t feel like reviewing this data back-up procedure. Boring! I’ll do it next week, maybe, if I find the time.’
- **Carelessness and clumsiness**: ‘Whoops! I dropped that big old atlas that everyone makes a fuss about, and the binding broke. But I gathered up all of the loose pages, that is except for a few in the middle. I don’t know where they went. Sorry.’
- **Forgetfulness**: ‘I forgot to lock the server room, and now we’re missing the server with all of the borrower data. Sorry.’
- **False assumptions**: ‘I thought that the clericals would bring in those boxes from the loading bay, and they didn’t. Those old books that we acquired at the auction in New York got wet last night when it rained. There were some packages from children’s publishers, too. They got really wet, but they should be fine when you dry them out. Shouldn’t they?’
- **Inattention to detail**: ‘Did I back up all of today’s cataloguing data? Perhaps not. Well, if you lose any, that’s a pity.’
- **Ignorance of internal policies**: ‘Is it okay to show patrons around the rare book vault? Some fellow asked to see our early edition of Joyce’s *Ulysses*, so I showed him where it was in the vault, and he seemed very grateful. He was in there for quite a while. Are you missing that copy of *Ulysses*? No, I haven’t had a chance to read the security manual, but I will, maybe next week.’
- **Inattention to laws and external regulations**: ‘One of our older patrons had a heart attack in the reference area last week, and none of us knew what to do. Somebody should have administered first aid, but nobody on staff had the training. So that unfortunate patron had to wait until an ambulance arrived, and that took quite a while. Our county’s occupational health and safety code demands that we have at least one fully trained first aid attendant on site during business hours, so I guess one of us should take the training. When? Oh, sometime soon.’

Such statements may seem outrageous, but they are reproduced here verbatim from library sources in Canada, the US and the UK. You must never underestimate the likelihood of human-caused risks, which most commonly result in lost data and other valuable assets, damage to collections and facilities, breaches of employee and patron privacy, and loss of the library’s reputation as a responsible custodian.

### 1.5 Proximity risks

Recalling smoke damage to a Midwestern American library branch after fire destroyed a neighbouring building, the local Fire Chief was blunt. ‘I don’t care how well you prepare yourself on your own site’, he said, ‘You have to take a look at what’s next door, and down the block, and even several miles away – anything that could burn or flood you, choke you with smoke or fumes, knock you down with an explosion,
run into you at high speed, fall on you, or rip you off. For your own safety and your library’s, have a look around.’

Library disaster planners should take note of the following:

• **Neighbouring buildings.** Risks at sites and in buildings near a library might include:
  - inadequate fire controls
  - inattention to the requirements of the Fire Code
  - older plumbing and electrical circuitry
  - substandard maintenance
  - older structures unable to withstand earthquake loading
  - inadequate security procedures
  - inadequate sanitation
  - inadequate pest control
  - Criminal activities, for example narcotics distribution.

• **Roadways.** A library might be located near major arteries. Risks arising from its proximity to roadways in the vicinity include:
  - road closures following a motor vehicle accident, or a local emergency such as a fire or gas leak
  - difficulties in entering and leaving the area owing to debris, precipitation and abandoned vehicles in roadways after a storm, fire or earthquake.

• **Retail shopping areas.** Proximity to shopping areas is often related to incidents of robbery, arson and vandalism.

• **Parking lots.** Parking lots can be scenes of muggings, vandalism and assault.

• **Air traffic.** See the above subsection on **Aircraft accidents** (p. 5).

• **Gas (or petrol) stations and fuel tanks.** Fuel spills, fires and explosions can occur on any site that contains fuel tanks. In many cases the cause of these problems is human error.

• **Bodies of water.** See the above subsection on **Flooding and water ingress** (p. 2).

• **Crime hotspots.** In urban areas noted for crime, the most common criminal acts might be vehicle theft and break-ins, mugging and assault, vandalism, shoplifting, and distribution of illicit drugs and stolen goods. See the subsection below on **Security risks.**

### 1.6 Security risks

‘Libraries are truly soft targets’, says a thief who succeeded in stealing hundreds of rare books and manuscripts from North American academic libraries. ‘Librarians are too trusting, and some of them take offence if you tell them that they have security problems. They don’t like to hear it, and often they ignore security risks until a rare book goes missing and all hell breaks loose. But if somebody gets caught stealing in a library, they usually don’t get more than probation or a warning from the cops.’

The following risks are due to a human agent acting intentionally for criminal purposes:

• **Theft.** In most libraries there is a constant risk of theft. Library assets most often stolen are:
  - printed materials of any sort, but particularly rare and valuable materials such as incunabula, early maps and atlases, and noteworthy editions of famous works; also rare ephemera such as concert posters
  - valuable reports, white papers and other grey literature.
• manuscripts, including valuable correspondence, diaries, journals and hand-drawn maps.
• sound recordings of any sort, but most often recordings by popular musicians, orchestras and bands.
• IT equipment, particularly that which is set up in public areas.

Patrons’ items most attractive to thieves include:
• mobile (or cellular) telephones and other handheld technology
• laptop computers
• data sticks
• iPods
• purses and wallets
• keys (especially to cars and homes)
• cameras
• coats, especially leather jackets and woollen topcoats
• jewellery
• expensive pens and other accessories

• Fraud and information theft. Like most organizations, libraries could be defrauded by means of bogus documents, false ID, hacking and computer scams. The confidential information in academic and public libraries – particularly borrowers’ records – could also be stolen and resold to illicit marketing organizations.

Special and corporate libraries hold information that could be considered confidential, and potentially valuable to outside persons and organizations, particularly those in the media. Special librarians often have access to extremely sensitive files. Unfortunately there is a low level of awareness regarding the risk of ‘social engineering’ in most libraries. Social engineering is defined as the use of devious and occasionally criminal methods to obtain sensitive information from unwitting sources.

• Sabotage. A disgruntled employee could sabotage library operations by erasing valuable data, causing a plumbing malfunction or planting a computer virus.
• Arson. Usually the work of a lone miscreant, arson is possible on any site. Parking areas could be the most likely spot for an arson attempt. Arson is a proximity risk for many libraries in urban neighbourhoods. In recent years, arson has become more common during riots and violent protests.

• Bomb threats. Organizations with a moderate to high public profile are targets for bomb threats. These threats are made by pranksters, disgruntled employees, and occasionally by hostile political activists.

• Workplace violence. This is defined as violence or the threat of violence by any one person in a workplace toward any other person. Incidents of workplace violence in libraries can increase during periods of high stress, low morale and economic uncertainty. Most often, cases involve violence by patrons to other patrons or to library employees. Many reports of violence in public and academic libraries note a suspected emotional problem in the offender.

• Hostile intruder. A hostile intrusion is a possible risk. The intruder might have a complaint about library services or operations. There is also the possibility of an intrusion by a ‘street person’, perhaps one under the influence of drugs, or a disgruntled former spouse or partner. The intrusion might occur in employee work areas, or in public areas.

• Malware. Computer viruses, time bombs, Trojan horses, and worms are increasingly sophisticated and common. While many libraries use advanced electronic protection, there is always a risk of a malware attack.
• **Vandalism.** Vandalism at library sites usually has a minimal effect on operations, unless vandals succeed in damaging power lines or computer equipment. At present this risk appears to be minimal. The most common form of vandalism in many neighbourhoods is ‘tagging’, that is spray-painting graffiti on building exteriors.

### 1.7 Enterprise risks

In times of economic uncertainty, enterprise risk management (ERM) can be essential to the continuing operations of libraries. Whereas risk managers and disaster planners usually concentrate on physical risks such as those described above, they are increasingly called upon to consider:

- political risk and hostile legislation
- sudden and deep cuts to operating budgets
- sudden postponements of important projects owing to a lack of funds
- the sudden cancellation of library programmes owing to a lack of funds
- demands from boards and other authorities to cut staff and close branches
- the loss of essential expertise and leadership
- lengthy strike action, and other job actions
- serious morale problems
- crises, for example negative media coverage.

‘You can ward off a lot of enterprise risk if you know how to respond quickly with maximum impact’, says a Canadian academic library director. ‘Budget cuts are never welcome, but there are ways of managing them and their fallout. You have to be a good negotiator to manage enterprise risk. Some librarians are better at negotiating than others.’

Library disaster planners should consider all of the above risks and the likelihood of them leading to actual events. The likelihood of any event is in many cases difficult to determine exactly, but all potential events should be carefully considered in a library’s risk assessment.

### 1.8 References

#### 1.8.1 Interviews

In this chapter I have quoted a public librarian in Los Angeles, a retired salesperson who worked for a large American computer manufacturer, a Midwestern American Fire Chief, a British university librarian, a Canadian academic library director and a school librarian in a rural district of southern India.

I have also quoted a notorious library thief, who, while he has been caught on several occasions in possession of stolen books and manuscripts, has never been charged with an offence.