British Actuarial Journal (2024), Vol. **29**, e21, pp. 1–12
doi:10.1017/S1357321724000278

Institute and Faculty of Actuaries

SESSIONAL MEETING DISCUSSION

Infrastructure: managing resilience and adaptation

[Institute and Faculty of Actuaries, Sessional Webinar, Thursday 25 January 2024].

The Moderator (Mr N. Aspinall): Welcome, everybody. I am delighted that you can join us for the "Infrastructure: Managing Resilience and Adaptation" paper presented by the Infrastructure Working Party. Today, we will be discussing that paper with the four authors.

Chris Lewin is an actuary and former CEO of several of the largest pension funds in the UK and was a public member of Network Rail. He is the lead of the Infrastructure Working Party. Evangelia Soultani is a life assurance actuary with experience in regulatory frameworks and financial modelling. Currently, she is working on measuring cybersecurity risks, including using quantitative models. Monica Rossi is an investment professional with over 10 years of experience in investment product development and portfolio management in emerging markets. Kumar Sudheer Raj is an Assistant Professor in Actuarial Science at the Institute of Insurance and Risk Management, promoted by the Insurance Regulatory and Development Authority of India. Welcome to all of you and thank you for attending today.

Our first speaker is Chris (Lewin), who is going to give a summary of the paper.

Mr C. G. Lewin, F.I.A.: Good afternoon, everybody. I hope you will find the meeting very stimulating and that it will lead your thoughts in some new directions.

Resilience refers to the ability of the service provided by infrastructure to continue at an acceptable standard, even when things go wrong. What constitutes an acceptable standard is a very important and debatable question. It may change from time to time. It depends on what users, government and commentators think is necessary. Then when things go so badly wrong that the service is lost all together, the ability to recover that service quickly is important. The question of what we mean by "quickly" depends on the perceptions of the users. They will be inclined to be, perhaps, more tolerant if they understand the reason for the failure and they think the service is being restored within a reasonable time.

Resilience also takes account of the ability to adapt the infrastructure if things are continuing to go wrong on a regular basis and the service is getting worse. This may require some very big changes to the service or to the way it is provided, to get back to a standard of ongoing resilience, and this can be complex.

Events that can lead to a lack of resilience are natural catastrophes, such as storms, hurricanes, landslides and floods. There are a number of external bodies that have worked on resilience ideas such as the United Nations and the Institution of Civil Engineers. The United Nations has given some pointers to how buildings should be designed:

- Resistance to heat waves in urban areas.
- Resilience against drought.
- Coastal communities perhaps considering new ways of building.
- Giving protection from strong winds with strong connections for the roof.

- Resistance to cold with thick walls and what are known as "water walls", which absorb heat during the day and radiate it at night, and installing insulation and painting external surfaces in dark colours.

The Institution of Civil Engineers has laid down some general principles for infrastructure, which they say should:

- Be able to adaptively transform.
- Be able to adapt beyond its primary purpose.
- Be able to fail safely and operate even if there is unforeseen human intervention.
- Be able to handle the variability of a changing environment.
- Be environmentally integrated and recognise the importance of the natural environment and not mitigate against climate change in a way that causes further damage.
- Importantly, have design principles, which lead to thinking about the hazards that can befall the infrastructure.

The guidelines for good practice include the following:

- Project teams must consider not just natural disasters but events like pandemics, terrorism, cyberattacks, etc.
- Critical components should be stronger than the basic requirements. There should be safeguards against cascading failure.
- Resilient infrastructure must boost people's awareness of how best to use it in challenging situations.
- There has to be clear communication between asset managers and users about upcoming disruptions.
- By giving communities a sense of ownership of the infrastructure, we can reduce vandalism that might take it out of service at a critical time.

The National Infrastructure Commission in the UK has made some suggestions such as:

- The UK Government should set national resilience standards every 5 years for the key industries of energy, water, digital and transport services.
- Regulators should have more power over investment plans.
- Regular stress testing of infrastructure systems should be undertaken and supervised by regulators.
- Engineering standards for new infrastructure should take account of future climate change.

The government has responded that there should be a whole-of-society approach, better assessment of cross-cutting and complex risks and better management of emergencies. They have introduced a Resilience Directorate in the Cabinet Office to take account of climate risk assessments.

We now come to the resilience framework we ourselves have suggested. There are four key aspects:

- Envisaging adverse events and scenarios.
- Planning in advance for mitigation to be put in place when serious events occur.
- Aiming to continue a standard of service that is acceptable to users, which means understanding what standard of service is acceptable in different circumstances.
- Establishing a long-term plan to monitor performance with trigger points for action. That should include performance due to failures or climate change but also include performance due to other factors that might cause the infrastructure to deteriorate. For example, thefts of cable on a railway line. There should be a performance measurement plan that says, "If

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

performance deteriorates beyond a certain point, you have a trigger point for action that is already planned in". Those trigger points can vary, of course, as society's expectations change.

There are some important aspects to mention about recovery plans:

- Obviously, having well-tested crisis management plans includes panels of people who can be called up quickly to manage a situation. One way of preparing for an inevitable cyber crisis is to keep manual operating systems and old equipment in reserve and to train staff in advance to use them. For example, in the case of the British Library, which is still recovering from a massive cyberattack, they have gone back to using paper and pen for ordering books instead of using computers.
- Knowing how to get spare parts quickly, as opposed to scrambling for them when the crisis happens, could mean storing supplies in external locations away from main operations.
- Being prepared to advise users about their own alternative options, which entail not using your infrastructure, but using another kind of infrastructure.
- Having backup communication systems.

There are a number of questions around acceptable performance:

- What minimum standard of performance would be acceptable?
- In planning, should one pay more for a higher performance standard? In other words, should one be aiming for perfection, or should one just be aiming for an acceptable standard throughout?
- Assessing what constitutes acceptable performance has subjective elements. It will be judged comparatively by looking at what kind of performance is being achieved for other kinds of infrastructure. Lower standards of performance, if they do arise, may still be acceptable temporarily, if communication with users is good.

Some of the measures of performance are:

- Percentage of time when the service fails or is late.
- Length of time before a failed service is restored.
- Causes of failures and deterioration.
- Numbers of people affected.
- Extent of any pollution caused.
- Size of carbon emissions.

We now come to the impact of climate on new projects and Figure 1 is quite thought-provoking in this regard.

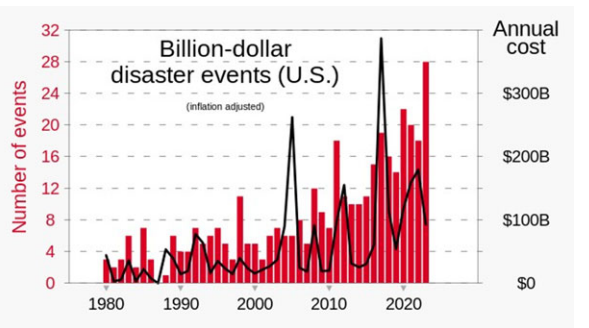

Figure 1. Billon-dollar disaster events in the USA from 1980 to 2020.

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

The number of events exceeding a billion dollars is 28 in the most recent year compared with less than 10 in the 1980s. The figures are inflation adjusted and hence are comparable.

A key question is whether one should be planning for worst-case scenarios, or should one take a more measured approach and perhaps plan for a reasonable minimum degree of protection initially, obviously at lower cost, with the ability to increase protection later? Perhaps one could make new builds more flexible. Then when evaluating future options related to climate change, you could perhaps use actuarial techniques, such as discounted cash flow techniques taking account of the time value of money. These are techniques that actuaries have used for many years in insurance and pensions.

We now come to issues around interdependence:

- Interdependence arises when one piece of infrastructure is highly dependent on another piece of infrastructure for inputs and for its ability to operate. An example that demonstrates interdependence is a waste collection system that needs unblocked roads, fuel for lorries, a supply of electricity and water and staff at work.
- The various types of interdependency could be physical, geographical or digital. There are questions about whether a number of pieces of infrastructure all may be affected by the same external event. For example, they might all go down together in a volcanic eruption or an earthquake. Chains of resilience are not immediately obvious. They have to be sought out via intellectual effort and stress testing to find weaknesses and to change things so that, as far as possible, if one element goes down it does not affect all other elements. Electricity is a key element for many infrastructure systems, but that is fairly obvious and already gets lots of attention and mitigation.
- Mitigation measures for interdependent systems include holding higher buffer stocks and finding new sources of supply. It can be beneficial to change the location of, perhaps, the key control centre in a piece of infrastructure, so it is not next to a control centre for a piece of infrastructure on which it is dependent. It is also useful to have discussions between the managements of dependent pieces of infrastructure to formulate joint emergency plans.

A lot of information is needed to make resilience possible:

- Knowledge of past events and what worked in response to them will help in devising mitigation options. Having teased out the existing chains of resilience, this will enable priorities to be identified for recovering different systems if any widespread failure occurs. If, shall we say, a whole city goes down, we might want to have a pre-determined particular order in which to recover the various infrastructure systems.
- Information flows to the users of the services are important so that they can be personally resilient. The more information they have, the better they can manage independently, such as changing their journeys, altering where they get food, etc.

Financial resilience is very important. Operators must be able to meet the maintenance costs of the structure. Otherwise, that could, over a period of years, lead to failure. There must be sufficient funds to stop the continual degradation of the service and to provide for enhancements from time to time and to meet major recovery costs, if necessary, either from insurance or from the government.

Stakeholders such as government and private investors have important roles. The government needs to "think big" about the future and give leads on the approaches to infrastructure that may be needed, such as:

- Building underground.
- Building only for a limited life.

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

- Building flexibly.
- Regulating new infrastructure to accommodate climate change
- Introducing revised infrastructure standards on sustainability, fire safety, etc.
- Providing leadership on the resilience of key industries, including food supply.
- Identifying chains of resilience and encouraging action to reduce weaknesses.
- Getting public support for allocating more finance to infrastructure resilience.

Then there is the role of private investors who often own infrastructure. If their infrastructure fails, it will not only affect their profits, but it will also affect other pieces of infrastructure, perhaps run by the state or other investors. It is much more important than it may appear at first sight for investors to finance resilience improvements, beginning with their existing assets, but also for ones they may acquire in the future. Property surveys, for the purposes of buying a new building, should consider resilience. Investors could, perhaps, insist that there is a disaster plan that is rehearsed every 2 years, and they should get a continuous data flow on performance so they can see when resilience is starting to deteriorate.

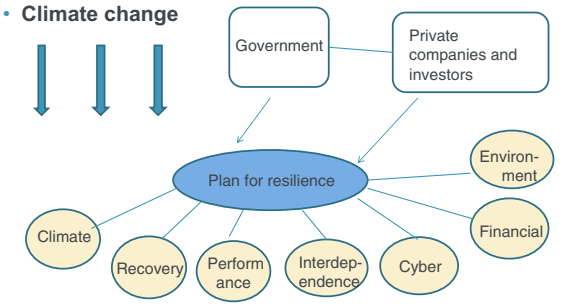

Figure 2. Knitting the framework together.

As Figure 2 shows, there are a lot of different but interrelated strands here, all impacting on resilience. There is climate change, which has the capacity to affect everything. The parties involved in infrastructure, each with their own objectives, include the government, regulators, private companies and investors. Users must make their own resilience plans. There is the question of having sufficient finances available, which affects all these areas; and there is the concern about the environment, making sure that environmental performance is maintained, and perhaps strengthened, as society's requirements for a good environment increase.

Much more needs to be done by all concerned. Climate change creates new risks, with unknown timings. Are climate change and its impacts accelerating exponentially or steadily? There is, therefore, a need for resilience planning, looking at various future scenarios and incorporating the time dimension. A very good long-term plan has been prepared for the City of London, for example. There is a lot more scope for actuaries to be involved in the future, to apply actuarial techniques and to provide advice, including advice on the various interdependencies that are critical and need to be better understood. Finally, resilience will cost more, but it may save money eventually. It will have the effect of making people happier.

Moderator: I am now going to hand over to Evangelia Soultani, who is going to respond and focus on more of the details.

Ms E. Soultani: Chris (Lewin) has very clearly referenced the many different risks that could challenge the resilience of infrastructure. Climate change is one major risk that results in natural catastrophes. It is an evident risk for infrastructure assets and a challenge for resilience. Cyber resilience, on the other hand, is much more silent and insidious. However, as the catastrophic

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

effects of cyberattacks become much more evident and frequent, the need for a sound and comprehensive cybersecurity strategy, improving resilience and security, is no longer an afterthought.

For infrastructure such as roads, bridges and facilities like having trash collected from our buildings, what is the connection with cyber threats? The reality is that we are living in cities that are becoming smart cities and the processes that are involved in running such a city are also becoming smart processes. So, for example, trash collection is following a smart waste management process controlled through cyber-physical systems (CPS). CPS provide an opportunity to positively improve the quality of life in many domains, including transportation, healthcare, energy, farming, manufacturing, smart grids and everyday living. There are many areas and many industries. According to studies, the references to which are within our article, the global smart building market is forecast to grow by approximately USD127 billion by 2027, at a combined annual rate of 12.5%. As a result, the dependency on the internet, and internet of things (IoT) technology, will increase, and so will the risk for attacks. Some interesting numbers are that 57% of IoT devices are vulnerable to medium and high-severity attacks. 72% of healthcare networks mix IoT and IT devices, allowing malware to spread from individual to vulnerable IoT devices within the same network. 98% of all IoT device traffic is unencrypted, exposing personal and confidential data on the network.

Cyber risk is any risk that emanates from the use of electronic data and its transmission, including technology tools, internet and telecom networks. Cyber risk can affect the confidentiality, integrity and availability of data and systems; this is sometimes known as the "CIA triad". It can impact the reputation, the compliance and financial stability of an organisation. This makes it a business risk.

Sources of cyber risk are malware and ransomware, phishing and social engineering, third-party vendors, insider threats, natural disasters and human errors. Every digital asset has a physical reference and presence somewhere, so this needs to be protected. Therefore, when it comes to infrastructure projects, the term information technology is no longer sufficient to cover the range of technologies that are used to deliver the financial service or product. Information technology (IT), the technology backbone of any organisation, is necessary to monitor, manage and secure core functions, mainly finance, human resource, etc. They are usually connected, standardised and replaceable. Operational technology (OT) is for connecting, monitoring, managing and securing an organisation's industrial operations. Businesses engage in activities such as manufacturing, mining, oil and gas extraction, etc. These are heavily related to operational technologies and the relevant systems are usually isolated. They are specialised and durable. The key difference between information technology and OT is that IT is centred on an organisation's front end, and OT is focused on its back-end production.

The term cyber-physical systems (CPS) was coined more than 15 years ago but is now in the mainstream as digital transformation intensifies and OT environments become increasingly interconnected with IT systems and internet of things devices. An example of CPS is virtual power plants and Internet of things implementations that are used to coordinate distributed power sources, such as solar, wind and hydrogen power generation sites. Other examples of CPS are found in utilities where smart grids collect data across regions to derive insights into power consumption patterns and enable predictive maintenance. This allows energy companies to enhance demand response efforts and avoid blackouts. In healthcare, institutions apply AI to analyse massive data sets and improve disease diagnosis as well as to deliver personalised treatment recommendations. In conclusion, CPS integrate computational components with physical processes, which interact through a network.

We next present some famous attacks that indicate not a lack of preventative measures, but how infrastructure and business continuity operations can be affected and also how organisations can recover from attacks. The most recent one is the attack on the British Library in October 2023, where all the libraries, their electronic catalogues and essential digital services, including the

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

website, were unavailable. The library is still in the process of restoring its digital services and it may take some time to fully recover. However, it is one of the priorities to restore accessibility to the online library, from the current use of paper and pencil to access the catalogue. The library was prepared for such events and, despite the disruption that was created, it is still able to provide the service. It was able to continue to provide service, and even in the week of the cyberattack, they were able to successfully host a 5-day event on artificial intelligence. So, their existing mitigation plan worked. They continued their services and reduced the effects of the attack. More details about the attack on the British Library are shown in Figure 3.

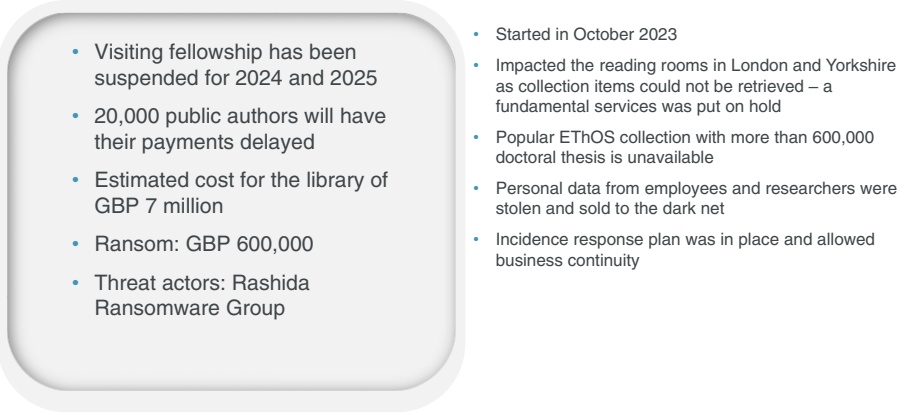

Figure 3. Details on the British Library attack.

The WannaCry event in 2017 was a famous one that affected the National Health Service (NHS). It affected computers worldwide by exploiting a vulnerability in Microsoft software. More than 19,000 NHS appointments had to be cancelled, which cost approximately £92 million. A simple update of the operating system could have prevented the WannaCry attack as, ironically, the necessary patch was available 1 month before the attack. Awareness about potential malicious action and social engineering is also important, to prevent opening and downloading links and attachments from sources that are not secure. More details about the WannaCry attack are shown in Figure 4.

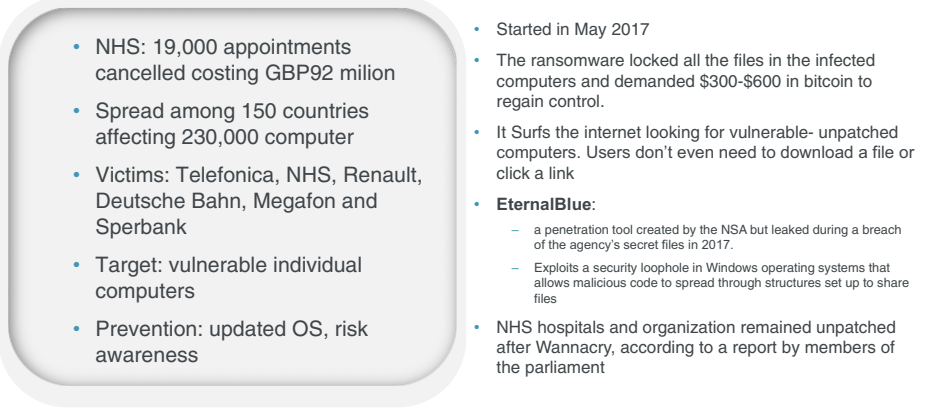

Figure 4. Details on the NHS WannaCry attack.

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

NotPetya is another famous attack, with the initial target being the state of Ukraine. Although the attack was in 2017, 1 month after the WannaCry attack, it exploited the same vulnerability as the WannaCry virus. Still, thousands of computers were infected worldwide, and the overall cost was more than USD10 billion. It could have been prevented in the same way as the WannaCry virus, as it exploited the same vulnerability. Research shows it was developed in France. The EternalBlue vulnerability allowed the malware to run malicious instructions using administrator access gained through the Mimikatz research tool. The way to protect against this and similar attacks was to update the operational systems. More details about the NotPetya attack are shown in Figure 5.

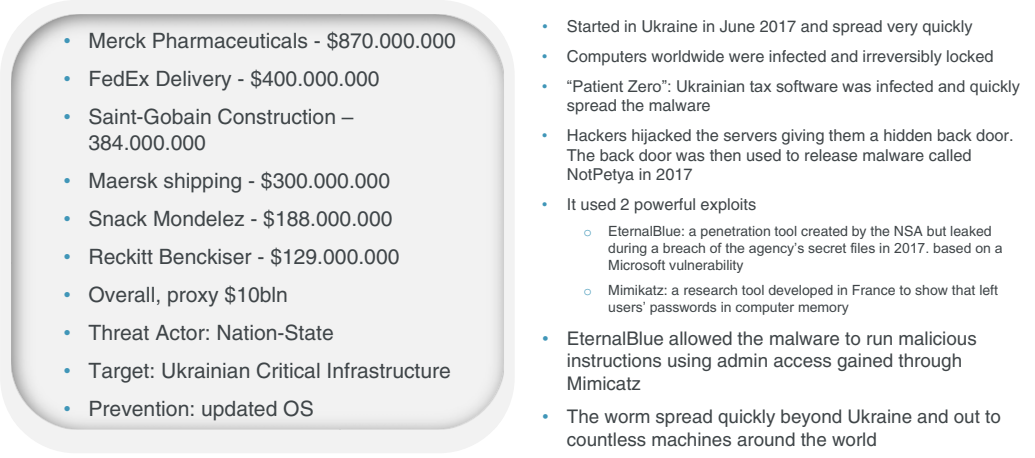

Figure 5. Detail on the NotPetya attack.

Last, but not least, the first cyber weapon, Stuxnet, which attacked the nuclear facilities of Iran, was in development since 2005 or 2006. It was finally deployed in 2010 and successfully targeted each of the three layers of a CPS. It used cyberware to distribute the malware and identify its targets. It used the control system layer to control physical processes and it affected the physical layer, causing physical damage. More details about the Stuxnet weapon are shown in Figure 6.

Figure 6. Stuxnet – the first true cyber-kinetic weapon.

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

We can respond to risk in four ways: retaining it, removing it, reducing it or transferring it; and we now focus on how we can reduce exposure. To manage cyber risk effectively, we need to follow a systematic process that can identify, assess, prioritise and mitigate potential threats and vulnerabilities that affect an organisation. Additionally, it is very important to educate and train staff on cybersecurity best practices. Although regulations and standards exist providing principles and models, it is important for each company to tailor those models and methods to address the risks that arise from the implementation of a business strategy.

Moving from theory to practice, what are the best strategies, keeping in mind that we are talking about infrastructure or critical infrastructure? Network segmentation, that is, to divide a computer network into smaller parts, improves network performance and its security. Another way is to introduce multi-factor authentication, a security method that requires users to provide two or more ways to prove their identification. A third way is the zero-trust protocol, which is a security model that assumes no network or user is trustworthy by default. It requires continuous verification of identity to access rights for all different data and different systems, ensuring that unnecessary services are disabled and the threat landscape is reduced. It is very important to provide cybersecurity training to all operations, administrators and all employees.

A vital consideration is how we bring together cybersecurity across all these different types of systems: information, operation and the hybrid cyber-physical. Especially when it comes to OT, it is good to remember that it involves durable systems, which means that these are often legacy systems that could be more than 30 years old, with all the associated vulnerabilities and limited security controls. It is a challenge to update those, given the limited ability to implement security controls on legacy OT systems that were supplied before cybersecurity became an issue.

Third-party remote connections to IT devices are a challenge and so too is unclear ownership between OT and IT. The shortage of combined cybersecurity and automation skills with the required cybersecurity and automation control system-specific experiences is a problem for IT teams. For example, having an expert on IT in OT cybersecurity, but lacking automation and process expertise, presents a problem. Some principles to remember are to always establish content prior to a design and ensure that it may make compromise difficult for threat actors and make disruption difficult and detection easier through the virus systems and solutions used.

Moderator: How can actuarial techniques help planners of new infrastructure on deciding what level of protection and climate resilience should be built in?

Mr K. Sudheer Raj: I would like to answer your question through a hypothetical case, which we have done in our paper.

Proposal - To built a new Hospital at capital cost of £500 million.

Location - The Hospital is situated where severe storms would take place (1 in 100 years)

Additional Cost – £200 million at outset for roof-top and structural cost , £25 million for hospital makeover.

Benefits – An amount of £100 million pa is set towards community well-being provided by the hospital.

Assumptions – Discounted cashflow technique , 4% interest rate, No Inflation

A three Climate scenario analysis is performed under four options.

Scenario a : No Climate change, probability of storm = 1% pa, Repair Cost - £20 million per storm

Scenario b : Climate worsens gradually in 20 years, probability of storm is 1 % pa increasing to 20 % pa by year 20, Repair Cost - £20 million per storm increasing to £ 80m by year 20 and remain same thereafter.

Scenario c : Same as scenario b, Climate worsens further after year 20. A total climate protection is carried with the cost of £255 million (£25 million at the outset and £230 million at year 20)

Figure 7. A hypothetical hospital case study for adaptive pathway.

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

In Figure 7, we show figures relating to a proposal for a new hospital at a capital cost of £500 million. We say that the hospital is in a place where there is a 1% annual chance of a severe storm or 1 storm expected in 100 years. There is an additional cost of £200 million at the outset for rooftop and structural costs and £25 million for hospital makeover. In the beginning, there are costs and there are benefits associated with the hospital, considering the community well-being that will be provided by the hospital. For calculation purposes, we have to discount these cash flows, and we use a 4% interest rate, and we assume there is no inflation. We run a three-climate scenario. In the first scenario, there is no climate change and the probability of a storm happening is 1% per annum and has a repair cost of £20 million per storm. In scenario B, the climate worsens gradually, and the probability of the storm keeps on rising, until it becomes 20% after 20 years, increasing our cost from £20 million per storm. It increases to £80 million by year 20 and remains at that value after that point. In scenario C, we assume the situation worsens further. A total climate protection is carried out with a cost of £255 million: £25 million at the outset and £230 million at year 20.

-A discounted cashflow analysis is conducted under four options.

Results-

- ❑ Option (1) is the best option in scenario A and B and worst in scenario C.
- ❑ Option (3) is the best option in Scenario C.
- ❑ Option (4) is not the best option under any scenarios.
- ❑ In all options under various scenarios the benefits are worth more than the costs.

	Amount in £ million			
Scenarios	Option(1)	Option(2)	Option(3)	Option(4)
A	4.95	4.72	3.95	3.57
B	3.86	3.72	3.64	3.57
C	2.44	2.34	3.64	3.57

Fig: Benefit cost ratio (Benefits/Total Costs)

To know about types of options please see the Appendix of the paper- https://doi.org/10.1080/23789689.2023.2241728

Note – All Figures are shown only for illustration purpose.

Figure 8. Benefit-cost ratio.

The four options are illustrated in Figure 8. We made sure that under all options for the various scenarios, the benefits should be worth more than the cost. We found from our data that option 1 is the best option in scenarios A and B and the worst in scenario C. More details on this can be found in our paper.

Moderator: Can you explain how the modular approach to buildings in designing infrastructure projects helps to improve their resilience?

Miss M. Rossi: Flexibility in infrastructure design is a key enabler of resilience. It allows systems to adapt to changing conditions or respond swiftly to disasters to absorb shocks or dissipate future challenges. Modular buildings specifically offer several advantages for enabling resilience in infrastructure projects. They can make it easier to plan for adapted pathways as well. For the example of planning a new hospital, as outlined by my colleague Kumar (Sudheer Raj), should we consider that the project be modularised? The decision to spend that additional £200 million at the outset of the project can be deferred until, say, updated climate event forecasts become available or new materials and technology become accessible. Since modular buildings can be disassembled and relocated, or refurbished, if necessary, in this case, portions of the hospital can continue to

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

serve the community whilst other parts are being upgraded offsite. This means that the project can start delivering positive cash flows before being 100% complete. This approach will minimise the cost of temporary partial closure whilst any new flood protection, for example, is being installed. Another benefit of constructing the hospital in a modular way is that it lets management test demand and revenue forecast assumptions before the project is complete so that changes can still be made. The management will not have any redundant capacity that goes unused or perhaps, if demand has been underestimated, then the project plans can still be amended to allow for that additional capacity to be built. In addition to planning flexibility, a modular construction approach also minimises field construction labour and therefore it is a means to mitigate danger risk on site. Hence, it reduces the worker injury liability exposure. In addition, you have less material wastage, less air and sound pollution and lower carbon dioxide emissions on site.

This is also a way that some construction risk can be transferred to your contractors. Construction can continue, irrespective of, say, weather delays or even pending permit application approvals. In addition, the ability to reuse materials, which is a popular trend now in the infrastructure space, promotes a more sustainable approach to construction. The flexibility a modular construction approach introduces to a project can be very valuable over time.

Moderator: Building resilience costs money, and so there is a trade-off between short-term cost and longer-term resilience. Do you, in general, see a difference between publicly funded and privately funded projects?

Mr Lewin: There is, first, the question of whether one should be spending much additional money now, which is where the kind of discounted cashflow analysis Kumar (Sudheer Raj) presented is useful. It does not follow that we should necessarily make everything fully resilient straight away. On the question of where the funding should be coming from, undoubtedly some of it will have to come from government sources. For large pieces of infrastructure, the cost is so immense that only the government can provide extra money. When it comes to infrastructure that is privately owned, for example by insurance companies and pension funds, those organisations will need to consider putting up some extra money to get an asset that is much more future proof than would otherwise be the case. Those institutions will increasingly have to consider community aspects, such as, questions of environment and environmental resilience, as well as anything else. Funding will have to be both from the public sector and the private sector.

Moderator: To what extent can the insurance industry be pulled into resilience planning and resilience protection?

Mr Lewin: It is already happening to a limited extent in the UK through flood programmes where insurance companies will, in effect, make flood insurance available at comparatively low cost in areas that are liable to flooding. That is one way in which insurance can help.

Mr Sudheer Raj: The other way would be through the role of private investors. Insurance and pension funds can look to build resilience for the future as investors. A relevant example is provided by the hospital case study. Insurance companies and pension funds can invest in that kind of building in an area that is in a coastal place, for example, in the southern part of America or maybe in the southern part of Africa, thus building resilience for the future.

Moderator: There is offsetting between the short-term costs and the long-term benefits. Should the government be using more actuaries to help understand that? How can actuaries do more in this field?

Mr Lewin: I think a lot of organisations will not want to employ actuaries full time. A government might, and in the UK, we have the Government Actuaries Department, which can certainly get involved in this area. But I think to a considerable extent it will be firms of actuarial consultants

https://doi.org/10.1017/S1357321724000278 Published online by Cambridge University Press

who will be employed to do particular jobs, perhaps to join project development teams and so on. I would expect that this will increase more and more as people realise the benefits of actuarial advice. Even though the advice can be expensive, it can provide benefits that are worth very much more than the cost.

Moderator: We have, in the last 4 years, been through an incredible test of all our disaster recovery systems through the pandemic and exposure to viruses. How has that real-world experience informed your thinking about resilience? To offer one example, I have started to think about the length of time that solutions might take compared to the length of time I might have envisaged before those solutions were needed. I have found that to be quite a helpful prioritisation technique. If it took me a month to put in place a solution to something from which I was unlikely to suffer within 6 months, then that might be a lower priority than developing a solution taking one day to a problem from which I might suffer in the next hour. I just offer that into the resilience conversation. I wonder if the panellists have an experience from the last 4 years that has come into this work and into your thinking on resilience?

Mr Lewin: We all admire the resilience of individuals who lost family members or who themselves have gone through severe bouts of Covid and so on. That has brought home to me that individual resilience is something that should be encouraged in many different ways. Not just thinking about health but thinking about one's own personal precautions around the house and so on, against flooding or other perils. It is happening to a limited extent, but I think it could happen more widely.

Miss Rossi: It made me appreciate the importance of collaboration across cross-functional expertise and cross-functional disciplines. It is the actuaries coming together with the engineers, the consumers, the business and government officials. You want a collaborative solution. I do not think that anyone can do it alone, so that for me really became apparent.

Moderator: We all suddenly relied on our computer systems and working from home a lot more than we did in February 2020. Were you aware of cyber risk going up a lot and thoughts of cyber resilience coming to the fore?

Ms Soultani: The rate of attacks increased during the pandemic period and there have been costs from that. Cyber insurance premiums have risen a lot. Unfortunately, the costs were very high for insurance. This made insurers rethink the way they react and respond to cyber risk. The price managers also stopped selling cyber insurance after writing losses. The pandemic was a shock in all areas of life both professionally and individually. We had to work and live in a different way. Companies responded remarkably quickly and successfully. This has allowed for a better transition from the normal way to a new normal. I believe that we are still in a transition phase where we are rethinking the way that we react to changes and in our lives in general.

Mr Sudheer Raj: Climate change is here, so we were not resilient 20 years ago. As the times change, human beings also need to be resilient against these adverse changes.

Moderator: Thank you.

Cite this article: Infrastructure: managing resilience and adaptation. *British Actuarial Journal*. https://doi.org/10.1017/S1357321724000278