Organisational Resilience at the University of Northampton: Growing Immunity to a Full Spectrum of Threats

Dr Mils Hills and Mr Nick Allen: The University of Northampton, Park Campus, Boughton Green Road, Northampton, UK.

Dr Mils Hills is Associate Professor of Risk and Resilience at the University of Northampton. He draws on twenty years of experience developing tools and techniques to enhance the ability of decision-makers and supporting processes to be immune to distraction and deception in both defence and civilian contexts. He has worked in the Cabinet Office, consultancy and led a national capability for the Ministry of Defence's research laboratory. Mils has a PhD and an MA in Social Anthropology from the University of St Andrews and was the first social anthropologist to work for the UK Government.

Mr Nick Allen is an experienced University administrator with extensive experience gained in his career, which includes working at the Open University and the University of Northampton. Over the recent years, Nick has increasingly led and collaborated with academics in both bidding for and executing research and strategic consultancy. Currently based in the Office of the Vice Chancellor, he also sits on many committees and teams which have planned the development of a brand new campus to which the University moves in summer 2018.

Abstract: This paper introduces the concepts of immunity and full spectrum threats in the context of business continuity and resilience planning at a UK higher education institution. It also describes the approach taken by the University of Northampton to build a reliable response capability through behavioural change at strategic and operational levels. It is hoped that the experience and processes presented will enable readers to complement their thinking, planning and exercising.

Introduction

This paper describes the authors' involvement in a series of iterative processes to review current arrangements for a reliable business continuity and crisis management capability to address health, security, criminal, cyber and other scenarios. As the University planned a move to a new campus in an urban location from two leafy, suburban ones and also took into account national guidance from government and law enforcement professionals about threats to all significant organisations with crowded places, open campuses and student bodies, it was recognised at the highest level that significant enhancements to processes and preparedness were needed.

The paper will begin by outlining some of the specific challenges faced by higher education institutions (colleges and universities) in the UK. It will then introduce what organisational resilience means for the modern, digital dependent university. The concepts of immunity and full spectrum threat are then introduced. The term immunity is useful as it reminds us that organisations, their people and processes being able to prevent and respond to risk is an emergent capability built up from active learning, proactive health and constant challenge. The notion of full spectrum threat is most commonly recognised at the moment in relation to hybrid warfare, but means that there are a wide range of risks (some of which may blend) that any organisation needs to anticipate and have the capacity to manage the consequences of. In summary, this is about developing the confidence and competence of teams to be agile and adaptive to a dynamic threat environment. The final sections of the paper describe how the authors worked with the senior and operational management of the university to assess current capability and extend it in terms of breadth and depth. These processes embedded the above concepts and understandings, drew on some proprietary techniques and leveraged specialist external insight where necessary.

The Specific Challenges of UK Higher Education Institutions

A university or college (a Higher Education Institution or HEI) is no different to any other organisation in that it could easily be the target of attack in any form. Indeed, given the fundamentally open nature of, especially, university campuses (parkland or city-centre) and the fact that there are thousands of individuals studying, working and living in close proximity, to some degree they offer a very soft target for conventional criminal exploitation or terrorist attack. In the former case, students and staff could be the victims of mugging or theft, in the latter as 'crowded places' in UK government nomenclature they could be targeted for a wide range of terrorist attack methodology. A student body is also a customer base for those pursuing fraud, selling illegal drugs and other nefarious activities.

Beyond these facts, the modern university is a digital university, as dependent on Internet access, data confidentiality, integrity and availability as any FTSE 100 business. Teaching, learning, grading, the efficient management of the institution and the holding of intellectual property (IP) is all enabled by digital systems. Without these, business continuity is immediately impacted. If compromised, significant investment as well as stakeholder trust and confidence are lost. The potential value of IP that is lost could be significant and as universities seek to diversity their income streams through spin-offs, undertaking consultancy and contract research and so on: massive harm could be done to the financial viability of an HEI.

In addition, any event that occurs at or near a college or university campus will inevitably generate reputational consequences. Even routine occurrences attract a quantity of scrutiny and attention which may be undeserved but would be impossible to prevent. The importance of detecting potential threats and risks generated from within the institution is therefore high. The ability to quickly spot a developing situation with reputational consequences and intervene effectively is critical.

Organisational Resilience

We understand organisational resilience to be the inherent capability of an organisation to ensure that it minimises incurred costs and reputational damage by maintaining the delivery of business critical services. There are many definitions of resilience – but the authors believe that it is critical that rather than just thinking about the ability to *respond and recover* (as the UK Cabinet Office summarises it), we should be relentlessly focussed on resilience being about certainty in the ability to continue to meet expectations of customers and others under challenging circumstances, most importantly, as well as being able to respond and recover when there is no choice but to accept the suspension of normal levels of customer service. Ideally, all eventualities would be detected or managed in a way which meant that customers need not be aware that there had been a need to initiate resilience arrangements. In addition, we believe that resilience arises from sound planning, action and corporate culture and not just from specific business continuity, crisis and risk management activities.

Immunity

The immune system is a powerful analogy. Frequently used by marketing gurus to spin the provision of slightly adaptive software solutions, the immune system is much more useful as a means of both conceptualising what's needed to handle a wide range of threats and events and achieving buy-in with boards and others as a communications tool. Hills has [insert references, Vancouver style] (and is) exploring how the analogy can be employed in practical terms. In summary, the simple reality that an immune system is made up of passive and active components is incredibly useful. The skin or shell of an organism, for example, is a protective barrier which prevents the intrusion of pathogens and shields from at least some damage. As well as a physical structure, the skin has management systems which ensure that it is maintained in the best condition possible as well as at the correct level of acidity / alkalinity to make it a hostile environment for fungi or bacteria which might otherwise colonise it and then cause harm to it or invade were the integrity of the skin to be broken.

These aspects of the passive immune system alone offer a rich source of ideas for how an organisation might protect its attack surfaces (personnel, physical, cyber, reputational, etc.) from harm and kept in the best condition possible and where any weakening is detected.

The active immune system is made up of complex cells and mechanisms which recognise invading or home-grown (e.g. tumour cells) threats as unwanted and act instantly to engage, contain and destroy them. Other cells and systems identify novel threats and develop means to prevent them from propagating in the system. Supportive reactions are initiated to make the organism a less benign environment for an invader (e.g. raising the temperature through initiating a fever response) or signalling for the mass production of cells and attraction of helper cells.

The parallels are immediate and obvious if we transpose how the biological organism's immune system works and how we would want the corporate body to function: reactively and pro-actively. The vision which the University of Northampton has developed is one where security and other staff (and eventually all employees and students) are sensors: *agents of immunity*. Here, those charged with security, health and safety, wellbeing and related functions form a protective capability. They work to identify problems or potential problems in ways that embody the ethos and values of the organisation. The senior management team and the operational leads are responsible for setting expectations of others as well as in their own actions working in the interests of developing and maintaining immunity.

Full Spectrum Threat

The experience of many involved in business continuity, crisis management and other activities is one where both emergencies and routine disruptions create consequences where the precise cause of the emergency or event may not be immediately obvious and sometimes may never be understood. For the former case, imagine a scenario where fire alarms sound and planned and chaotic evacuations are unfolding from many buildings – but it transpires that the initial triggering of a fire alarm was because an individual feeling under threat from individuals had no other means of attracting attention. In the case of causations which may never be understood, mass hysteria and failure in cyber systems could be mentioned. Hills has worked with many orgaisations whose databases and other systems have failed, but because they have eventually re-started and investigation would be complex and expensive, no formal diagnosis takes place. Embedded risks and vulnerabilities therefore remain.

Any organisation, HEI or otherwise, therefore has to be prepared to handle and intervene effectively against situations which may not be as they seem. In addition, it may be very difficult to manage such an eventuality because the systems needed to undertake strategic leadership and operational control are part of (or are) the target. In the event of the failure of communications media – how would the responding mult-layered team work to achieve situational awareness, make decisions, communicate decisions and monitor the effectiveness of those decisions. We assume that email, mobile telephony etc. will persist: but instead perhaps a graceful degradation to reliance on cheap handheld two-way radios would be sensible. And, of course, all involved would have to rehearse working in these conditions on a regular basis.

The term full spectrum threats is unashamedly borrowed from cutting-edge thinking by scholars of military conduct. For example, Jonsson and Seely have lobbied for the West to more usefully think about the complex, unrestricted nature of the strategy and tactics of the Russian Federation as being open to all of the various ways in which power can be projected: "kinetic violence, information, economic and energy, and political influence operations".[i] By encouraging a focus on *consequences* rather than *causes* we bypass the restrictions that are presented to us by being obsessed by history or the latest near miss or incident that has befallen an unfortunate other. If the ambition of an adversary is to impose costs on their targets, defence strategists need to be aware that these costs may be served in any domain. Similarly, planned attacks or natural disasters can challenge the sustainability and even survival of businesses even though, with hindsight, it is totally clear that, say, an embedded risk could have been surfaced and resolved or that a combination of continuity and emergency planners have, in the past, largely been involved in the drafting of plans for specific threats or eventualities. The endless generation and prioritisation of lists of potential doom-laden occurrences and amending of plans to make them specific to certain circumstances has been largely nugatory (especially when in our experience these plans are unlikely to be able to work even in the expected scenarios).

By thinking of the full spectrum of threats which create a consequence (just think of the variety of ways in which a building and anything contained in it could be made off-limits: fire, flood, crime scene, collision by a vehicle, contamination, sinkholes, infestation of vermin, loss of power, incapacitation of control systems through cyber attack etc.) – we begin to realise that we need to invest in human capacity (and the technology and knowledge needed to enable it) to adapt and extend to cope with an unknowably large set of threats which create a more knowable but unpredictable series of consequences. Plans will not suffice, narrow exercises will not assure the ability to cope with and tame significant challenges which will no doubt co-occur with other events, develop in unusual ways and so on. Full spectrum threats will overlap with one another and require close collaboration and co-ordination between experienced people, reinforced by those learning from their exposure to real world challenges and all supported by technological and other resources which enable decision-makers to understand a developing, dynamic, difficult situation and intervene effectively in it.

The University of Northampton Experience

Understanding the need for senior management and other decision-makers to be able to manage a wide range of potential scenarios of a range of durations, the University of Northampton undertook a systematic review of its arrangements for crisis and related situations. As part of this process, the authors of this paper became a core team. Uniting an academic-practitioner (Hills) with an administrator-practitioner (Allen) turned out to be one of the most helpful ideas we could have had. This cocktail of talents meant that we were able to leverage Hills' experience and research portfolio with the pragmatic insight and bureaucratic nous of Allen.

Hills was able to convince Allen of the merits of adopting and adapting an approach that he had developed in the UK Cabinet Office's Civil Contingencies Secretariat (CCS) and used in consultancy since. Scenario-Driven Exercises (SDEs), described in the open literature for the first time by Hills in 2015,[ii] are a fast-to-develop, cheap and high impact way of both testing existing plans, processes and capabilities and designing enhancements 'on the fly'. The authors worked together to deliver such exercises – once for the senior management team and another for the operational team. The first was to embed the concepts introduced above, the second to translate the ethos captured from the SMT and embed it into their plans for operational health, safety and security.

Both events were highly collegiate, convivial and focused on outcomes which would benefit the organisation and those charged with supporting actions in the event of either a crisis or notification that a crisis may occur. We were also able to capture key learning points from participants at the SMT drawn from their experience at other institutions handling very challenging events and who could also inject caution to those that were new to such roles and responsibilities about, for example, the amount of actual support from stakeholders and first responders versus what they had hoped for.

The SMT were also able to benefit from our invitation for a recently retired member of the UK special forces community to undertake some targeted training. The focus of this, which reinforced emerging lessons from the Scenario-Driven Exercise (SDE), was on the demands of performance under pressure. The trainer was able to work with the SMT to explain how the individual body and mind and teams could be prepared to cope better with the stress and uncertainty of crises by drawing on several models of special forces thinking.

Work with the operational team involved being able to provide a confidential space and neutral facilitation to draw up an approach which would enable them to align development and investment with SMT requirements **and also** address necessary changes and long-desired outcomes that they held dear. Again, there was substantial value added to the work of colleagues as benefit was provided by trusted and approachable individuals motivated by an aspiration to ensure that inherent human capability at all levels was enhanced for the move to the new campus in a time where, regionally and nationally, the threat posed by conventional criminality and terrorism is growing.

Associated work also drew on the specialist insights of law enforcement and other personnel – some on the staff of the university, some part of our extended network of friends, some specially commissioned – to ensure that the university's plans knitted into and were cognisant of the response plans of the emergency services and others. Beyond that, the authors were able to bid for Home Office funding essentially to extend the line of attack in this project at the sector-wide organisation level in the Higher Education Institution space, leading to an extension of value from the University to the colleges and universities nationwide.

Conclusion

This paper has described an extensive, but rapid, approach taken by the University of Northampton to increase its immunity to a full spectrum of threats which the authors led. The overall ambition of the work undertaken by the University was to achieve what the former head of the US Cyber Command described as a high-reliability organisation which relentlessly seeks to reduce exposure to risk and simultaneously increase capacity to stretch to deliver core business despite threats materialising. As he put it, to achieve this, one has to realise more than just technology is needed: "It's about ethos. It's about culture. [It's about] how you man, train, and equip your organization, how you structure it, the operational concepts that you apply."

This paper has detailed the ethos of the institution, the recognition of the need for behavioural (culture) change and the implications for the selection of individuals to undertake certain roles, an example of training undertaken and hinted at the ways in which investments in equipment have been underpinned by insights gained from the work of the authors. It is hoped that a short insight into the concepts which have driven our approach will inspire readers to extend and replace these with their own. Finally, we are delighted to work with others in developing these ideas and welcome correspondence.

References

[i] Oscar Jonsson & Robert Seely (2015) Russian Full-Spectrum Conflict: An Appraisal After Ukraine, The Journal of Slavic Military Studies, 28:1, 1-22, DOI: 10.1080/13518046.2015.998118 (pages 7-8).

[ii] Mils Hills (2015) "Assuring organisational resilience with lean scenario-driven exercises", International Journal of Emergency Services, Vol. 4 Issue: 1, pp.37-49, https://doi.org/10.1108/IJES-09-2014-0019