Bell

Managing and supporting pandemic response: A long-term perspective

White paper
October 2009

By Tyson Macaulay, CISA, CISSP, Hon BA
Security Liaison Officer, Bell

Summary

Introduction

Based on reports from the 2009 winter season in the southern hemisphere, the pandemic threat has moved from speculation to reality. While organizations are indeed aware of the issue, many of the response strategies they intend to deploy are not entirely in line with their critical infrastructure needs. Many assumptions are being made about ICT infrastructures that simply will not hold true when a pandemic strikes.

When it comes to pandemic response, most organizations have a limited picture of how a sudden shift to telework will affect their infrastructures, More importantly, they do not have the processes in place to manage this change.

While they do have a grasp of the immediate impacts, organizations are less aware of the cascading effect of a pandemic on partners, suppliers, clients and regulators. In many cases, these after-effects are beyond the event horizon of most pandemic response planners.

Teleworking is at the core of pandemic response and risk management strategies for many organizations. A sudden surge in telework requirements, however, can place an unprecedented strain on an organization’s information and communication technology (ICT) infrastructure. The onus is on enterprises to ensure that in the event of a pandemic, there is no degradation in help desk service, voice messaging, telephony services, Internet services and information assets.

This paper outlines the potential impacts that may occur once a pandemic response has been activated. It will also provide an overview of the management, operational and technical controls that can be employed to mitigate the risk to ICT and information assets.

Objectives

This paper has two objectives. The first is to provide insights into the technological threats to an effective pandemic response and the resulting organizational risks. These threats are considered in the context of telework as a central mitigation strategy for many organizations seeking to maintain operations. To clarify our intent, we do not consider telework itself a threat. However, a sudden or rapid migration to teleworking by a substantial proportion of the workforce will have significant effects and need to be anticipated and planned for.

The second goal is to present a variety of sample controls and safeguards which can lessen the technological threats and risks to pandemic response. These controls and safeguards have been designed to allow for rapid deployment, either proactively or reactively, within days of a crisis.

Pandemic response and ICT

The ability of support staff and industries to remain functional during pandemic response is directly proportional to the effectiveness of their ICT strategies, plans and infrastructures that support teleworking. By way of illustration, let us look at a typical ICT reference infrastructure from a telework perspective. We will then outline a likely series of cascading impact stages which will affect an organization that is under-prepared.

Enterprise ICT under normal conditions

Integration communications technologies (ICTs) in typical organizations are designed and maintained to support normal operating conditions, not crisis conditions. Where organizations have designed their ICT infrastructures for crisis conditions, the focus tends to be on rapidly deploying ICT services to alternate locations in order to support normal demands. However, pandemic response is as much about addressing abnormal demands as it is about normal demands. Provisioning for this sort of crisis essentially requires investments that go beyond supporting classic business continuity (e.g. failover to alternate sites) to include an additional form of preparedness that is rarely undertaken.

Figure 1 shows the primary ICT interfaces to a sample organization. These include a telephony interface supporting voice and modem traffic and an Internet connection. These shared interfaces serve a range of users, such as employees, contractors, partners, equity owners, sister organizations, clients, suppliers, regulators and/or government agencies. This diagram also shows a simple security zone architecture where Internet-facing resources are placed within a demilitarized zone (DMZ). Applications are placed in a zone for services available from the Internet and internally. And finally, an internal zone is deployed for users and higher security applications. A help desk is also indicated.

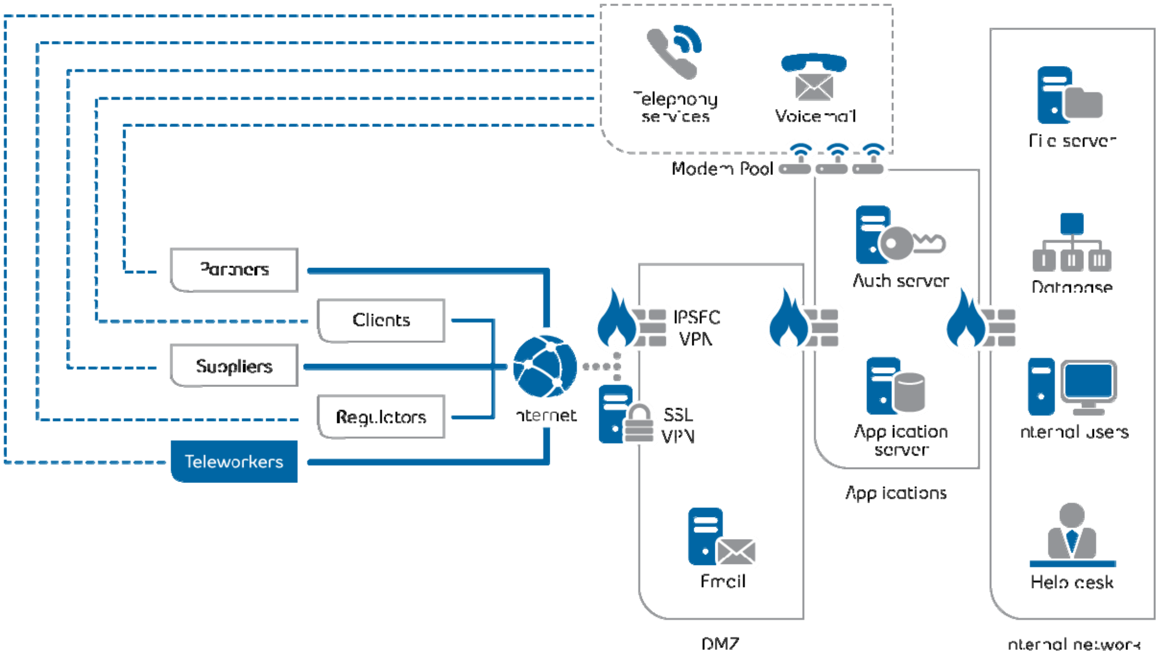

Figure 1: Sample teleworking reference architecture

Pandemic scenario – pandemic ICT impact stages

Drawing upon available information on infection, reporting, mortality/morbidity and absenteeism rates, the following scenario outlines the potential cascading ICT impacts that may occur where a highly contagious viral infection, such as swine flu, is approaching emergency proportions. (Public authorities are projecting H1N1 infections rates of 20% to 40% of the population over two years.)[i]

These will not necessarily occur in the same sequence in all organizations, nor do they include all the potential impacts. This scenario focuses specifically on the ICT infrastructure used by first-responders, their support staff and other critical infrastructure entities.

Stage 1: Help desk and voice mail degradation

The transition from normal conditions to stage one impacts occurs at the onset of pandemic response and the implementation of telework strategies for as many staff as possible. This can be initiated at the point where absenteeism rapidly increases as workers become sick, are afraid to come into work or must stay home to care for family members.

Figure 2 illustrates the first ICT impacts to be felt once a typical pandemic telework response strategy is enacted. While many users may be capable of teleworking, many will not have enrolled for remote access to telework resources, or will encounter technical difficulties with the installation or configuration of software elements.

Studies have shown that in Canada, a normal organization will have 4% of its workforce employing remote access resources on a daily basis.[ii] When there is a sudden surge in demand, and 20% and 60% of the workforce are seeking around the clock access to ICT resources, help desks can become quickly overwhelmed and unable to support users. At the same time, absenteeism will also be affecting the number of available help desk workers.

The help desk crisis will immediately be apparent and simultaneously lead to a greater reliance on voice mail messaging to maintain communications with co-workers. However, default configurations from a leading voice mail system maker have limited capacity (e.g. seven minutes of messages per mailbox).[iii] Under pandemic response conditions where 20% to 60% of the workforce is trying to maintain communications with each other, voice mail systems will be severely under-provisioned both in terms of the message storage capacity and their ability to support concurrent users.

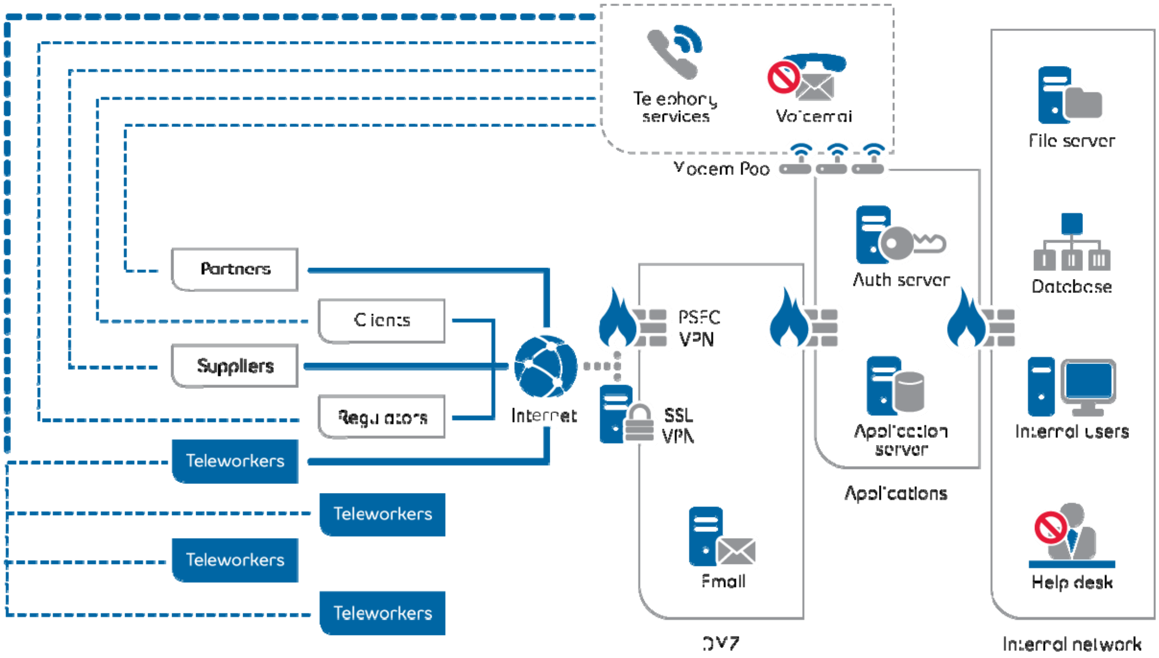

Figure 2: Stage 1 -Help desk and voice mail degradation

Stage 2: Internet degradation

In stage 1, an organization has a seriously degraded or disabled help desk and voice mail system. Between 20% and 60% of staff are absent from work and a significant proportion of these are trying to engage in teleworking in order to maintain service delivery or production. Figure 3 illustrates the next cascading ICT impact to be felt once a typical pandemic response strategy based upon teleworking is enacted.

Despite the fact that the help desk has degraded capabilities, remote access for users will continue to be a primary area of support focus for organizations. At this stage, all available users are accessing telework resources on a constant basis, logging in and holding applications and accounts open for the entire work day or longer. Typically, Internet connections are engineered to support a concurrent maximum of 5% of workers, which means bandwidth will quickly become exhausted. Similarly, there will be increased usage during working hours when partners, clients and suppliers, among other outside users, are simultaneously trying to exchange information to support the pandemic response effort. As a result the organization will end up inflicting a distributed denial of service (DDOS) attack upon itself, which will ultimately lead to network slowdowns and outages.

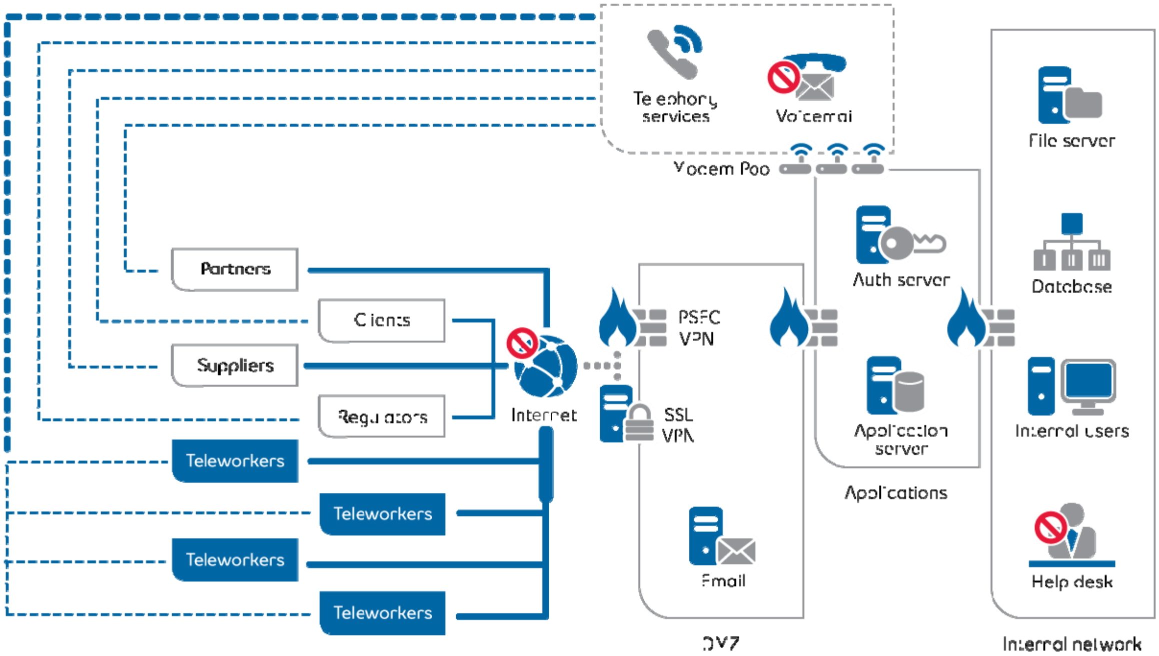

Figure 3: Stage 2 -Internet outage

Stage 3: Telephony degradation

At this point, an organization is operating under pandemic response conditions with a seriously degraded or disabled help desk and voice mail system, degraded Internet connectivity, and absentee rates between 20% and 60%.

At stage 3, we will presume that help desk, voice mail and Internet services are functional, but operating at capacity and unable to meet the levels of service required by the stakeholders.

Figure 4 illustrates the third cascading ICT impact to be felt once a typical pandemic response strategy is implemented. All stakeholders are now experiencing significantly degraded inbound telephony and fax services. Outbound calls to the PSTN (public switched telephone network) would similarly be impacted as inbound calls will likely have used all available resources.

By stage 3, essentially all information and communications channels are degraded. Some will be useless, while others will remain usable but performing at marginal levels. As a direct result, workers will start using public domain communications tools and portals for the management of internal information and communication. If they are working from home or other remote location, they will revert to personal webmail accounts, public chat (instant messaging) services, blogs, personal Web sites, public ftp and file-sharing servers and whatever else they can effectively (but not securely) use to maintain communications and support their organization. The direct result is elevated risk to an organization's sensitive information, or to data belonging to partners, clients and suppliers.

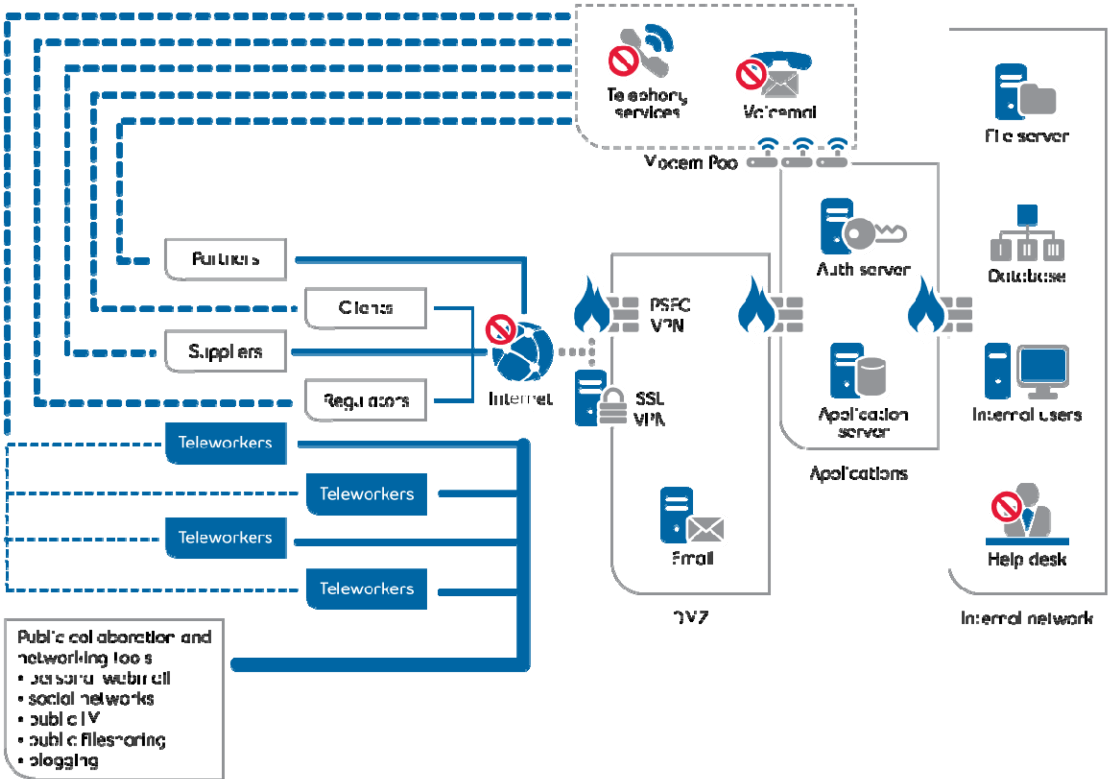

Figure 4: Stage 3 -Telephony degradation

Stage 4: Information assets compromised

In the fourth and final stage of ICT impact an organization is operating with seriously degraded or disabled help desk, voice mail, telephony and Internet services. Internal users are communicating with each other and outside stakeholders through publicly available, personal messaging and file sharing services.

Figure 5 illustrates the last cascading ICT impact to be felt once a typical pandemic response strategy is enacted. That is the compromise of information assets belonging to the organization, as well as partners, clients, suppliers and possibly regulators.

In stage 4, teleworkers have been driven to adopt ad hoc and arbitrary means of communicating using public services available on the Internet, such as personal email accounts which may not have basic anti-virus and malware protection, or file-sharing services that harbour eavesdropping and interception technologies. As a result, at least a small proportion of remote systems used by teleworkers are compromised. These can lead to disclosure, corruption or loss of valuable information assets belonging to any or all stakeholders. It can also lead to an escalation in malware and other threats that could threaten an organization’s entire information management system.

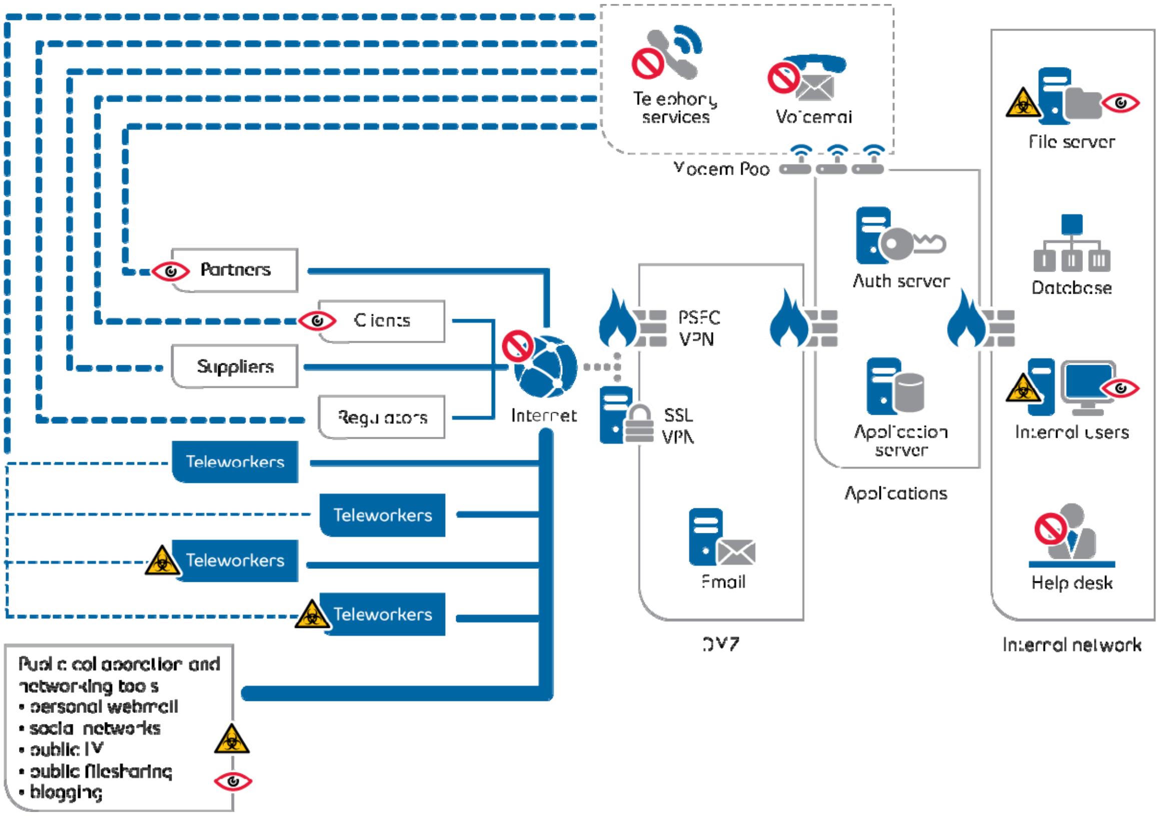

Figure 5: Stage 4 – Information asset compromise

The speed of the cascading impacts will vary from organization to organization, but it is likely that stage 4 – information asset compromise – could be reached within a single day.

Pandemic ICT remediation strategies

There are a number of possible remediation strategies for the various threats discussed in stages 1 to 4 of ICT impact under pandemic response conditions. While not all of the tactics listed will be required, they do provide a framework for risk managers to choose the most appropriate options.

The controls and safeguards will be discussed using the taxonomy of the National Institute of Standards and Technology (NIST): management controls, operational controls and technical controls (NIST 800-53).[iv]

- **Management controls** encompass basic decisions associated with risk response that fall under three possible actions: treatment, transference or acceptance. Treatment decisions directly relate to operational and technical controls that should be deployed. Transference decisions generally relate to contract terms and conditions and/or insurance. Acceptance does not require any mitigation actions, and may be dictated by factors relating to cost or low likelihood of damage.

- **Operational controls** consist of formal and well-documented procedures, as well as the testing and auditing of these procedures to ensure that they are being applied and that they conform to the appropriate policies and guidelines.

- **Technical controls** include the hardware and software elements that enforce the policies at granular levels. Technical controls are managed and configured in accordance with the standards and practices defined by the operational controls.

The following section illustrates how the different controls can be tactically deployed in advance of a pandemic response to manage the four stages of ICT threats.

Stage 1 controls: Help desk and voice mail degradation

Management controls

1. **Update financial authority and delegation** – As ICT threats escalate, managers at all levels of the organization need to know what, if any, resources are available to procure remediation solutions. A general practice is to establish accounting centres and cost-codes for the charging of ad hoc and emergency spending related to any emergency response. These policies will support all future stages of ICT impacts associated with pandemic response.

2. **Update remote access enrolment policies** – Part of the help desk burden may be related to enrolment processes and the need to provision technology such as two-factor authentication tokens. Temporarily reducing these requirements during pandemic response to speed enrolment and simplify deployment may be warranted. Management should consider if they are ready to accept the risks associated with this decision, and formulate a position in advance of pandemic response. Similarly, a policy to temporarily reduce enrolment requirements should be accompanied by a plan for cancelling or upgrading “emergency” accounts as soon as possible.

3. **Establish terms of usage for personal communications devices** – Inevitably, workers will use unofficial telephone numbers for official business once the voice mail system is degraded. Management can establish a temporary policy for the use of personal phone numbers, including guidance related to the retention of business-related voice messages and who in the home should be able to listen to these messages. Where possible, the access code for home voice mail should be temporarily changed or a new voice mail box added by a service provider (costs will be reimbursed by the organization at a later date).

4. **Establish temporary staffing policies** – Organizations frequently recruit temporary or retired staff members to fill in for absent or sick workers. These may be in a position to telework. However, it is important to confirm their home infrastructure in advance and compile their telephone numbers into a single list to enable seamless call forwarding and management. (See operational and technical controls below.)

5. **Introduce flex-hour policies** – Flex hours can be introduced to reduce the strain on ICT resources by spreading usage over different parts of the day. Staff members that usually work standard hours may be broken into teams, for example, with different teams operating throughout the day with only a few hours of overlap to aid communication.

6. **Implement mandatory cross-training of staff** – Cross-training will significantly aid resilience and recovery. Help desk and remote access systems and service support teams especially, should undertake cross-training to enlarge the number of individuals who can support remote access and reduce absenteeism risks.

Operational controls

7. **Develop fast-track procurement processes** – Companies should develop a fast-track procurement policy in order to better manage emergency procurement of pandemic mitigation solutions (including ICT solutions). These procedures will support all future stages of ICT impacts associated with pandemic response and other forms of emergency response.

8. **Enable fast-track remote access enrolment** – Implement policies that allow help desk staff to fast track enrolment and streamline processes during a pandemic.

9. **Establish social distancing procedures for ICT and help desk staff** – This could entail re-locating key personnel to remote locations with all the necessary tools and knowledge bases they require to support users. This will require changes to ICT network resources that include some of the technical controls to be discussed. Alternately, companies can reconfigure working environments to disperse on-site staff as widely as possible. For example, they could convert outbuildings into office space for workers that need to come to work for short durations but fear exposure.

10. **Establish batch processing procedures** – This should be applied to authentication and other services such as directories and databases, so that remote help desk staff can consolidate many changes for a single person to execute on-site. This is particularly important in situations where certain enrolment tools are not enabled for remote access, or remote access becomes degraded.

11. **Establish voice mail conversation policies** – Companies should reduce the length of allowable messages in order to conserve storage space. This will require training and communicating instructions that explain the changes and the new limits. For instance, one could apply a 30-second message limit per caller.

12. **Strategically deploy temporary, retired and part-time staffing resources** – Companies can hire temporary staff or reactivate retirees to support basic ICT support tasks. This allows more experienced or knowledgeable full-time staff to assume critical help desk or other more complex functions.

13. **Enable non-standard system support** – Corporations typically standardize their computing platforms and restrict support for non-standard platforms and tools. Since teleworkers users may be forced to employ whatever systems are available, organizations should have policies in place to sanction support for non-standard system on a best-effort basis during a crisis.

Technology controls

14. **Subscribe to virtual call centre technology services** – This allows for internal calls to be seamlessly rerouted to mobile or domestic numbers. Such services will allow help desk staff to login/logout of a presence-aware application through the Internet or a touch tone phone using the PSTN.

15. **Deploy a wireless mesh network** – This will allow organizations to support a reconfigured work environment. Mesh networks use Wifi (802.11) network equipment which can be easily integrated to any computer with a USB interface; and can be deployed and configured extremely rapidly. A single device will automatically and transparently provide network access to all the other mesh devices and allow workers to work at or near their normal work location.

Stage 2 controls: Internet degradation

Management controls

16. **Establish user prioritization for bandwidth policy** – This strategy can be applied to conserve scarce bandwidth by implementing a variety of different policies that outline who can have access, and when. For instance, teleworkers might be divided into “shifts” according to their division or last name, and their accounts only enabled during their allocated period. Alternately, certain critical or executive roles might have around the clock access and a higher bandwidth allowance applied to their account.

17. **Establish application prioritization policy** – Organizations can also conserve bandwidth by establishing policy-level controls for applications. For example, some applications and services use far more bandwidth than others. When using teleworkers, it is often possible to use alternative, lower-bandwidth substitutions for applications. For instance, management may implement a policy that SSL VPNs should only be used over IPSec VPNs to support heavier applications. Management also needs to establish policies about which heavy applications may be disabled during pandemic response, as well as access controls for remote workers.

Operational controls

18. **Establish user prioritization and network access control procedures** – Organizational networking groups in charge of remote services may be able to prioritize users and applications as part of the VPN feature set.

19. **Establish application prioritization and access control procedures** – It may be that remote access systems cannot effectively prioritize users or applications. In this case the application owners may have to adjust account settings so that only certain users can access applications at certain times and/or from certain locations.

Technical controls

20. **Develop SSL VPNs (secure Web portals)** – Secure Web portals require 50% to 90% less bandwidth than IPSec-based VPNs and the applications that run on them.[v] By creating SSL VPN alternatives for critical applications such as email, many more users can potentially be supported using available bandwidth.

21. **Increase available bandwidth** – Despite rationing and moving to lighter applications and interfaces, there may not be enough bandwidth to satisfy a 15X increase in teleworker demands. In addition, it is possible that current-generation VPNs or applications cannot be reconfigured to ration resources in a reasonable timeframe. In these cases, it may be necessary to increase bandwidth. Bear in mind however that telecommunications service providers will be equally challenged to maintain services, especially when facing a surge in demand. It is therefore advisable to contract and procure the required bandwidth in advance. Wireless connectivity is a rapidly deployable alternative. Some wireless services my be pre-provisioned for rapid commissioning and offered as a stand-by service without incurring monthly charges. Wireless broadband solutions are available off-the-shelf with a few days notice, and can be deployed rapidly in non line-of-sight configurations. 3G mobile communications are available on demand and can provide moderate amounts of bandwidth to allow for the retrieval and delivery of critical data or to support incoming VPN or other services.

22. **De-optimize Web services** – Many organizations develop internal information portals and intranets that are optimized for a particular browser or operating system in order to reduce support calls and development costs. De-optimizing these services enables users with non-standard systems to perform telework tasks or access important information.

Stage 3 controls: Telephony degradation

Management controls

23. **Prioritize suppliers and partners** – Management can direct departments or line-of-business owners to prioritize partners and suppliers for emergency communications. For instance, certain partners and suppliers might be told in advance of a blackout period for communications or to use only certain communications modes (such as couriers). Directives should also account for differing durations for the emergency conditions, rather than assume a single type of response period.

24. **Establish a flex-hour policy** – Flex-hour policies may be authorized where remote and local workers are required to keep non-standard hours to allow for business communications across a larger part of the day. For instance, some workers may be required to work noon to 8:00 p.m. on certain days to allow for communications loads to be spread out.

Operational controls

25. **Prioritize supplier and partner notification procedures, contact lists and service-level changes** – These should be communicated to suppliers and partners as per the management policy. Regulators should also be made aware of impending changes in the communication and information they receive from the organization if such information must be made available under conditions prescribed by statutes and regulations. Notification should include information about what steps are being taken to return to normal service levels and the expected duration of the announced changes.

26. **Establish flex-hour notification procedures for staff assigned to alternative work hours** – These notification procedures should be developed in consultation with employee representatives and in accordance with local labour standards. Notification should include information about what steps are being taken to return to normal work hours and the expected duration of the announced changes.

Technology controls

27. **Enable call re-direct** – Organizations with DID (direct internal dialing) can automatically reroute desk numbers to a worker’s home or cellular phone. Depending on the provider, this service can be activated and de-activated on-demand by the teleworker through a Web-based or touch-tone interface. Similarly, emergency routing plans can be developed to send toll free and other numbers to different geographic locations, or to a pre-recorded message with information about organizational status or other information updates.

28. **Enable virtual transfer** – Organizations with multiple physical locations can reroute calls to other office locations, based on which of those locations has the available line capacity.

29. **Enable virtual queuing** – Depending on the service provider, overflow calls can be sent to a managed call queuing service that can advise the callers of the amount of time they must wait for a line, and then automatically patch them through once a line opens. The service may also offer the capability to perform automatic call-back operations to advise callers when a line is available.

30. **Enable call overflow** – If the organization is already employing a virtual call centre to manage its help desk challenges, central call overflow may be rerouted to off-site/telework help desk operators.

31. **Enable voice conferencing services** – In order to relieve stress on corporate telecommunications lines, managers can set up calls into a bridge owned and operated by a third party. Remote and local workers can use these bridges to take part in meetings rather than using the organization's PBX system.

Stage 4 controls: Information asset compromise

Management controls

32. **Establish public collaboration tools policies** – To reduce risk, companies should develop and distribute a security policy that outlines the dos and don'ts of using public collaboration tools in advance of a pandemic. While it is tempting to forbid the use of these tools in combination with organizational information assets, under the circumstances, a better approach may be to prescribe what these tools may be used for and under what conditions.

33. **Establish counter-party information management practices** – There is a risk that partners, suppliers, client and even regulators counter-parties will use public collaboration tools to maintain operations, elevating the risk to an organization's information assets. These counter-parties should be notified in advance of an organization's position related to this risk. This notification might be presented as a clarification of service levels agreements or other contracted terms and conditions, or provide more specific guidance on the sensitivity levels of the information under their management.

34. **Sanction internal user classification** – Some users within an organization may employ public collaboration tools with lower risk because the information they handle is considered less sensitive; while others might have to be forbidden from using public collaboration under all circumstances. Diverting some users to approved public sites can also help to free bandwidth for users of sensitive information, and ultimately help to avoid the risk of compromise to sensitive data.

Operational controls

35. **Establish online collaboration white lists, education and awareness** – Certain public or semi-public collaboration tools on the Internet may offer better privacy and security features and lower risks than others. It is advisable to develop a list of which sites and tools are considered appropriate for redundant or fail-over communications in the event of organizational ICT degradation. These white lists and any other relevant information about the presence of threats through collaboration tools should be prepared and distributed to teleworkers.

Technical controls

36. **Create private on-line collaboration portals** – It is possible to procure short-term subscriptions to online collaboration resources for subscription-only memberships. These collaboration services will operate on a different network, thereby allowing loads to be diverted from degraded organizational ICT assets. These private services can often be established on short notice based on a pay-as-you-go, per user fee. Private collaboration portals can include Webmail/email, file sharing, instant messaging, voice and video communications, white boarding and a variety of other online applications. They can also enforce stronger login authentication and place controls on information managed within the portal by users. For example, they can apply data loss prevention (DLP) scans on information leaving the portal through email or instant messages.

37. **Leverage upstream security and carrier-grade intelligence** – With increased remote users, the risk of zero-day malware attacks on internal systems will increase. Organizations can deploy on-site, organizational counter-measures against these malware threats by engaging upstream, carrier-grade security services – including scanning, filtering, detection, alerting and response – through their service provider. Upstream security can provide a new layer of organizational security that is applied within the service provider network, and is specifically designed to detect the most serious threats that existing anti-virus and intrusion detection systems frequently miss.[vi]

Conclusion

This paper has presented a range of possible ICT threats and cascading impacts which may affect any organization trying to manage a pandemic response while maintaining operational capabilities. As noted, a pandemic can trigger a series of impacts which will occur in a specific order and will be triggered by directing workers to telework solutions.

There is a variety of security controls which can be applied at the management, operational or technical levels to mitigate these impacts and the resulting risk. All the controls outlined in this paper are intended to be rapidly deployable either proactively or – less ideally – reactively, within five days for any given control.

However, not all the controls in this paper will be applicable to all organizations. While some are inter-related, many are designed to function on a stand-alone basis. Organizations should select the controls accordingly and modify them to meet their specific needs. It should be noted that most management controls require that supporting operational controls be deployed in a complementary manner. The key for any manager is taking the time to consider the longer-term impact of pandemic planning, assessing the risks associated with staff shortages and teleworking, and making an informed decision about what can be done to mitigate potential communications and infrastructure problems.

About the author

Tyson Macaulay is a Security Liaison Officer for Bell. In this role, he is responsible for technical and operational risk management solutions for Bell's largest enterprise clients. Tyson also supports the development of engineering and security standards through the Professional Engineers of Ontario and the International Standards Organization (ISO) SC 27 committee.

Appendix A

Methodology

This work has been developed through a process of interviews and consultations with front-line pandemic-response professionals (medical/police/EMS), their support organizations and critical infrastructure operators generally. The interviews and consultations occurred between June and August of 2009.

Many of the controls in this paper are drawn from security and risk standards such as ISO 27002 (Information Security Techniques) or ISO 27036 (Security of outsourcing). However, since this paper is built to address the specific threat of pandemic flu, we have not adopted a direct mapping approach because ISO standards are threat-neutral (what does this mean).

Appendix B

This chart provides a summary of the four stages of impact and the control measures that need to be taken into account for each.

	Management controls	Operational controls	Technical Controls
Stage 1 impact (Help desk and voice mail degradation)	1. Update financial authority and delegation policy 2. Update remote access enrolment policies 3. Establish terms of usage for personal communications devices 4. Establish temporary staffing policies 5. Introduce flex-hour policies 6. Implement mandatory cross-training of staff	7. Develop fast-track procurement processes 8. Enable fast-track remote access enrolment 9. Establish social distancing procedures for ICT and help desk staff 10. Establish batch processing procedures 11. Establish voice mail conversation policies 12. Strategically deploy temporary, retired and part-time employee resources 13. Enable non-standard system support	14. Subscribe to virtual call centre technology services 15. Deploy a wireless mesh network
Stage 2 impact (Internet Degradation)	16. Establish user prioritization for bandwidth policy 17. Establish application prioritization policy	18. Establish user prioritization and network access control procedures 19. Establish application prioritization and access control procedures	20. Develop SSL VPNs (secure Web portals) 21. Increase available bandwidth 22. De-optimize Web services
Stage 3 impact (Telephony Degradation)	23. Prioritize suppliers and partners 24. Establish a flex-hour policy	25. Prioritize supplier and partner notification procedures, contact lists and service-level changes 26. Establish flex-hour notification procedures for staff assigned to alternative work	27. Enable call re-direct 28. Enable virtual call transfer 29. Virtual queuing 30. Enable call overflow 31. Enable voice conferencing services
Stage 4 impact (Information Asset Compromise)	32. Establish public collaboration tools policies 33. Establish counter-party information management practices 34. Sanction internal user classification	35. Establish online collaboration white lists, education and awareness	36. Create private on-line collaboration portals 37. Leverage upstream security and carrier-grade intelligence

Endnotes

[i] It is projected that many people will suffer only mild effects from flu infection and will not report to authorities or hospitals. Current estimated from public health authorities in the Unites States for H1N1 flu are for 20% to 40% of the population to be infected.(Source: Kansas Department of Health, Activity Update, Aug 10 2009)

[ii] Tremblay, Diane-Gabrielle Tremblay, Telework : A New Mode Of Gendered Segmentation? Results From A Study In Canada, Bell Canada University Labs research 2003

[iii] Cisco System, Unity Voice mail system Administrators Manual, http://www.cisco.com/en/US/products/sw/voicesw/ps5520/products_tech_note09186a008036fd99.shtml

[iv] NIST 800-53 : Recommended Security Controls -http://csrc.nist.gov/publications/drafts/800-53/800-53-rev3-FPD-clean.pdf

[v] Alshami, Abdelnasir, A technical comparison of IPSec and SSL, Tokyo University and Microsoft Corporation, Client Network Traffic with Microsoft Exchange Server 2003 -http://go.microsoft.com/fwlink/?LinkId=106738

[vi] Upstream Security, Bell Canada white paper 2009