INVITED KEYNOTE ADDRESS

Survivability and Business Continuity Management

Gerald Quirchmayr [1,2]

[1] Institut für Informatik und Wirtschaftsinformatik, Universität Wien
Liebiggasse 4, A-1010 Wien, Austria

Gerald.Quirchmayr@univie.ac.at

[2] University of South Australia, School of Computer and Information Science, Mawson Lakes Campus
Mawson Lakes, SA 5095, Australia

Gerald.Quirchmayr@UniSA.edu.au

Abstract

With the number of attacks on systems increasing, it is highly probable that sooner or later an intrusion will be successful. Not having to execute a complete shutdown in this situation will soon be a standard requirement. The intention of this paper therefore is to give an overview of business continuity management and to address selected issues in system survivability and business continuity management. The core question is how systems should be built in order to cope with a successful intrusion, i.e. being able to balance the necessity to be up and running with the potential damage that can be done by an intruder.

Keywords: Business continuity management; system survivability; stability and intrusion.

1 Background

As we have seen with the first wave of e-commerce systems, once an intrusion is successful, the only alternative to stop the attacker from causing serious damage mostly is the complete shutdown of the attacked system. As several forms of attacks are aimed at achieving exactly this result (DoS, DDoS), the relatively new paradigms of survivability [www.cert.org] and business continuity management [BT 2003] are becoming crucial. With a 24x7 service expectation from the customer, the complete shutdown of an attacked system is not an option anymore. It is therefore essential to develop integrated solutions based on the technology available today. Intrusion detection systems, firewalls and virus scanners are in the majority of implementations considered as completely separate systems. An integrated approach to IT security is rather the exception than the rule, which leaves systems vulnerable to attackers. Several layers of defences are too often considered as too expensive or too difficult to administrate, which leads to denial of service attacks usually being successful.

2 Towards a more comprehensive approach

A more comprehensive approach to IT security is definitely needed if systems are to survive successful intrusions. Like fault tolerance, intrusion tolerance will become a necessity for the reliable operation and management of information systems and IT infrastructures. As stated by David Smith [Smith 2003], "Most organisations face a business continuity event at some point". It is therefore very astonishing that business continuity management was largely ignored until the Y2K problem demonstrated the possible impact of failing IT infrastructures. It did however take the events of September 11, 2001 to make the management of larger corporations realize the size of potential exposure to unmanaged risk. Business continuity planning and the survivability of IT infrastructures have since then become a major issue. Warnings related to cyber terrorism and other forms of attacks are now taking far more seriously. Changing the corporate culture however is still a major effort and management needs to be convinced that it pays off to invest in business continuity, layered defences and survivable systems.

The stages of the business continuity management life cycle described by David Smith [Smith 2003] show the necessity for a wider integration and do clearly demonstrate the link between technological and organisational issues related to business continuity management.

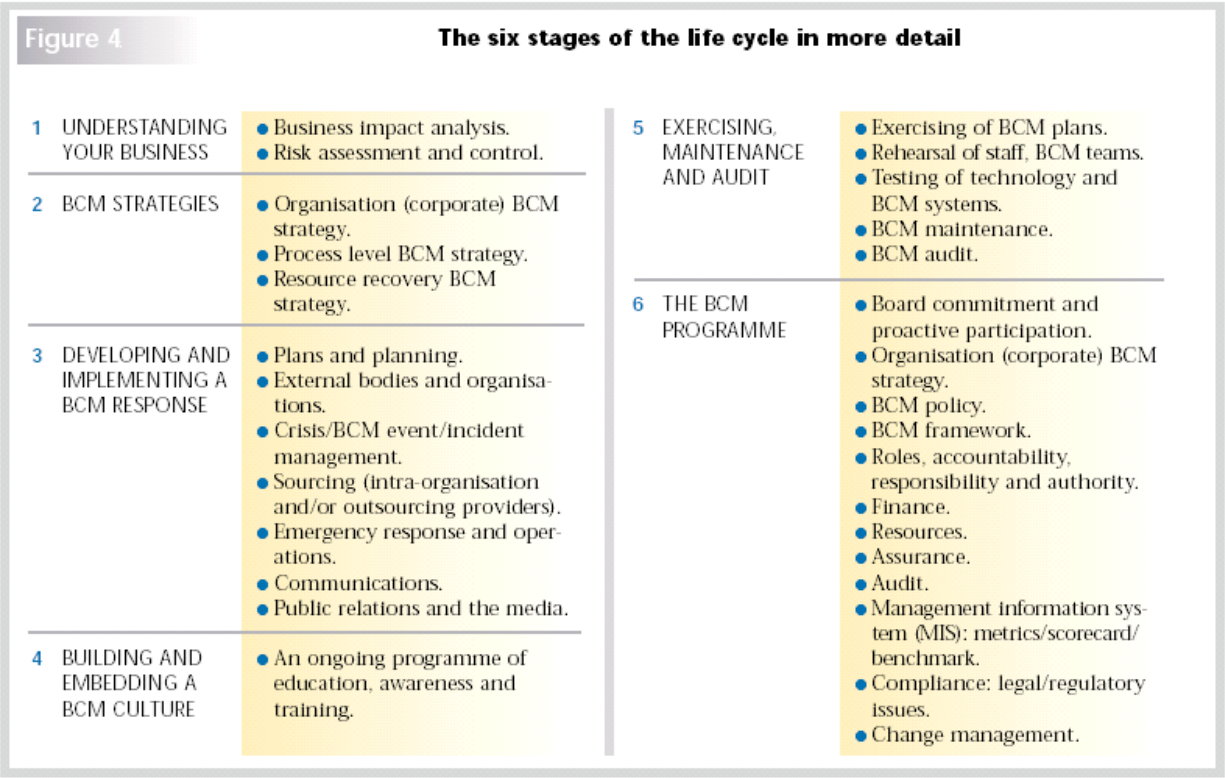

Figure 4 The six stages of the life cycle in more detail

1 UNDERSTANDING YOUR BUSINESS	• Business impact analysis. • Risk assessment and control.
2 BCM STRATEGIES	• Organisation (corporate) BCM strategy. • Process level BCM strategy. • Resource recovery BCM strategy.
3 DEVELOPING AND IMPLEMENTING A BCM RESPONSE	• Plans and planning. • External bodies and organisations. • Crisis/BCM event/incident management. • Sourcing (intra-organisation and/or outsourcing providers). • Emergency response and operations. • Communications. • Public relations and the media.
4 BUILDING AND EMBEDDING A BCM CULTURE	• An ongoing programme of education, awareness and training.
5 EXERCISING, MAINTENANCE AND AUDIT	• Exercising of BCM plans. • Rehearsal of staff, BCM teams. • Testing of technology and BCM systems. • BCM maintenance. • BCM audit.
6 THE BCM PROGRAMME	• Board commitment and proactive participation. • Organisation (corporate) BCM strategy. • BCM policy. • BCM framework. • Roles, accountability, responsibility and authority. • Finance. • Resources. • Assurance. • Audit. • Management information system (MIS): metrics/scorecard/benchmark. • Compliance: legal/regulatory issues. • Change management.

Figure 1: Business Continuity Management Life Cycle Details [Smith 2003]

The next logical step upward after business impact analysis will be to have a closer look at business processes and see how security aspects can be integrated directly into business processes. One way of achieving this goal was shown in [Quirchmayr & Slay 2001].

As presented in a guide to business continuity management by the Bank of Japan [BOJ 2003], the necessary processes and activities leading to successful business continuity management can be grouped as follows:

1) Formulating a framework for robust project management

(1) Basic policy

(2) Firm-wide control section

(3) Project management procedures

2) Identifying assumptions and conditions for business continuity planning

(1) Disaster scenarios

(2) Critical operations

(3) Recovery time objectives

3) Introducing action plans

(1) Business continuity measures

(2) Robust back-up data

(3) Procurement of managerial resources

(4) Decision-making procedures and communication arrangements

(5) Practical manuals

4) Testing and reviewing

5) Other issues

(1) Precluding and mitigating disaster damage

(2) Location of back-up facilities

(3) Use of outside service providers

Other very similar guides are made available by leading consulting groups, such as Gartner, Deloitte Touche Thomatsu and PWC. Guides issued by financial institution do however have the advantage of being backed by a traditionally security aware source. As banks have always had a highly developed security culture that could, with some transformations, also be migrated into the e-business world, it was to be expected that e-commerce sites operated by banks would be the most secure. To this point banks have kept their promises and today are always pointed to as examples of how to best approach IT security, business continuity planning and management. The above referenced guide issued by the Bank of Japan has, due

to its comprehensive approach, been widely referenced.

For another leading approach to the identification of risks and the specification of security requirements the reader is referred to [CERT OCTAVE]. An overview of very recent research developments related to the work presented here can be found in [Trustbus 02] and [Trustbus 03]. Leading industry approaches can be found in [Business Continuity], [Deloitte 2002], [IBM 2003]. Pioneering books that make an interesting reading are [Toigo], [Hiles & Barnes] and [Barnes]. Several papers in [Slay 2003] give excellent examples of the sort of problem organisations are confronted with and show ways towards solving the problem.

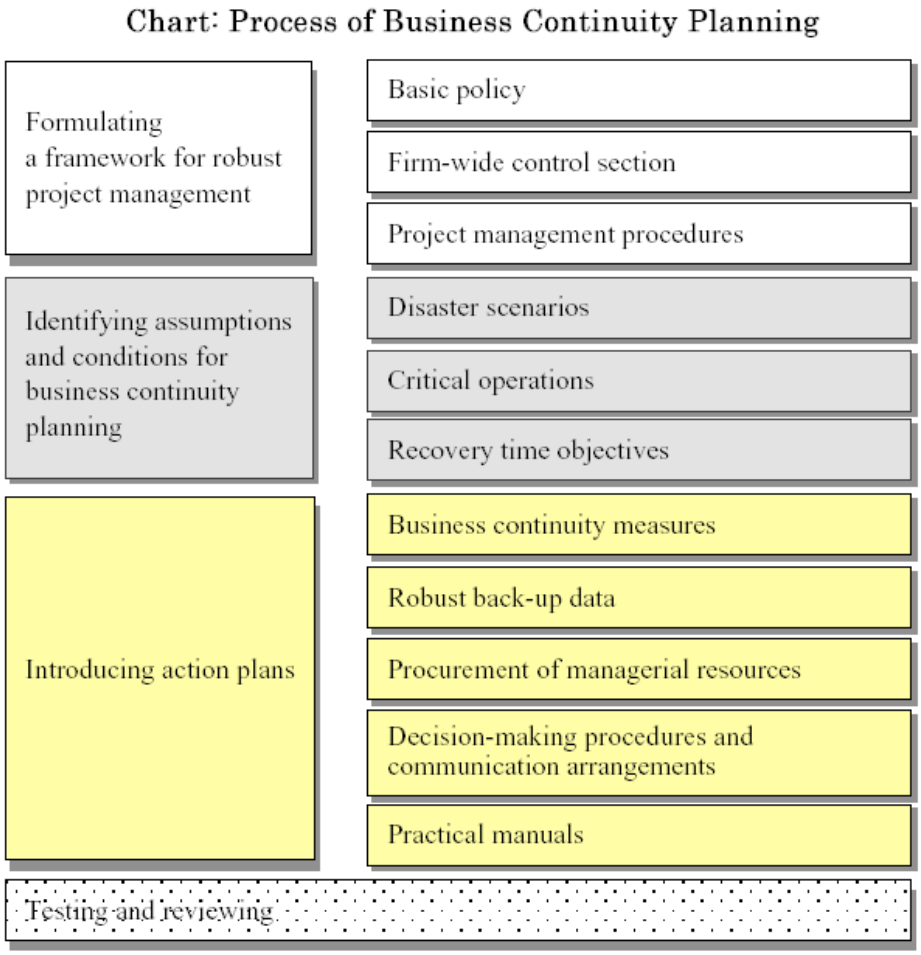

Figure 2: Business Continuity Planning Framework [BOJ 2003]

3 Integrated IT security as technological basis

As already stated in the previous chapter, an integrated and more comprehensive approach is needed to make information systems and IT infrastructures more stable and to give them a much higher chance to survive attacks. It is usually the unprotected interfaces between different layers where the intruder comes in. Based on this assumption and the excellent experience of Boeing with their model for the IS 2010 case study [McNurlin & Sprague 2002], the following system architecture principle might become successful for implementing a strategic approach to IT security.

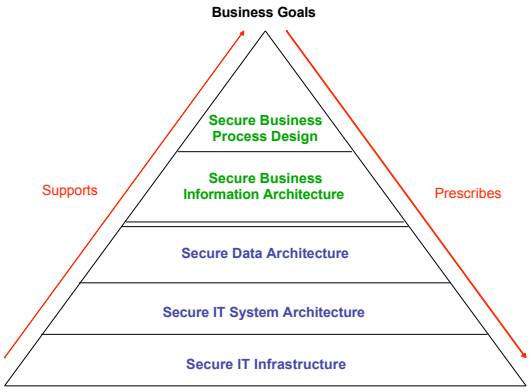

Figure 3: A secure environment derived from business processes, building on the Boeing IS 2010 case study in [McNurlin & Sprague 2002]; source: [Quirchmayr 2003]

The concepts shown in figure 3 then serve as guiding principles for the design and the reorganisation of information system architectures. By adhering to these principles security requirements can be tracked and through the support (feedback) loop pointing back to higher levels in the model, additional safeguards made possible by the introduction of new technologies can be identified and incorporated at these higher levels.

4 Conclusion

Business continuity management and system survivability are two very closely linked concepts. As shown in this paper, awareness has rise in certain industry sectors, but approaches towards a comprehensive and integrated framework are inmost parts of the world still in their infancy. Useful research and practical implementations to build on do exist, but in order to satisfy the coming needs, especially IT security infrastructures need to be better integrated. Business processes and the – hopefully existing - right corporate attitude towards security and business continuity management are major initial building blocks towards improving the situation.

5 References

[Barnes] James C. Barnes, A Guide to Business Continuity Planning.

[BOJ 2003] Business Continuity Planning at Financial Institutions, Bank of Japan 2003.

[BT 2003] Business Continuity Management - Exploiting agility in an uncertain world. BT Guide 2003.

[Business Continuity] Business Continuity Magazine.

[CERT OCTAVE] www.cert.org/archive/pdf/01tr016.pdf

[Deloitte 2002] Deloitte, Touche, Thomatsu, A New Paradigm for Business Continuity Management, 2002.

[Hiles & Barnes] Andrew Hiles and Peter Barnes, The Definitive Handbook of Business Continuity Management.

[IBM 2003] IBM Business Continuity and Recovery Services - Business continuity services managed by IBM.

[McNurlin & Sprague 2002] McNurlin, B. C. (Editor), Sprague, R. H. (Editor): Information Systems Management, 5th edition, Prentice Hall, Pearson Education 2002, ISBN 0-13-034073-1.

[Quirchmayr 2003] Gerald Quirchmayr, Trust as Prerequisite for Successful Electronic Business, in: Jill Slay (ed.) Proceedings of the 4th Australian Information Warfare & IT Security Conference. Adelaide 2003, ISBN 086803995.

[Quirchmayr & Slay 2001] Quirchmayr, G. & Slay, J. 'A BPR-Based Architecture for Changing Corporate Approaches to Security', in Proceedings of the 5th Australian Security Research Symposium, 11 July 2001, Perth.

[Slay 2003] Jill Slay (ed.) Proceedings of the 4th Australian Information Warfare & IT Security Conference. Adelaide 2003, ISBN 086803995.

[Smith 2003] David Smith, Business continuity and crisis management, in: MANAGEMENT QUARTERLY January 2003.

[Trustbus 02] Trust and Privacy in Digital Business 02; held in conjunction with the 13th International Conference on Database and Expert Systems Applications (DEXA 2003), in: Tjoa, A.M. & Wagner, R.R., Proceedings of 13th International Workshop on Database and Expert Systems Applications.

[Trustbus 03] Trust and Privacy in Digital Business 03; held in conjunction with the 14th International Conference on Database and Expert Systems Applications (DEXA 2003), in: Tjoa, A.M. & Wagner, R.R., Proceedings of 14th International Workshop on Database and Expert Systems Applications.

[Toigo] Jon William Toigo, Disaster Recovery Planning: Strategies for Protecting Critical Information Assets.

[www.cert.org] See CERT website for detailed information.