Published in association with

Journal of

Business Continuity & Emergency Planning

Volume Two *Number One*

Henry Stewart Publications
Russell House, 28/30 Little Russell Street,
London, WC1A 2HN, UK
Tel: +44 (0)20 7404 3040; Fax: +44 (0)20 7404 2081
Website: www.henrystewart.com

Henry Stewart Publications
North American Business Office
PO Box 361
Birmingham, AL 35201-0361, USA
Tel: 800 633 4931; Fax: 205 995 1588
e-mail: hsp@ebsco.com

Journal of Business Continuity & Emergency Planning
Volume Two, Number One, October 2007

ISSN 1749-9216

Printed in Europe by the Alden Group, Oxford

Utilising information security to improve resilience

Jennifer Bayuk* and Ken Silverstein

Received (in revised form): 18th July, 2007

*Bear, Stearns & Co. Inc., 115 South Jefferson Road, Whippany, NJ 07981, USA
Tel: +1 212 272 2000; E-mail: jbayuk@bear.com

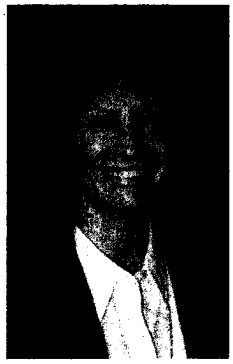
Jennifer Bayuk *is the Chief Information Security Officer for Bear Stearns & Co., Inc. She is responsible for information security policy, process, management and metrics. Jennifer has been a manager of information systems audit, a security consultant and auditor, and security software engineer at AT&T Bell Laboratories. She has written on information security and audit topics ranging from security process management to client/server application controls, including two textbooks for the Information Systems Audit and Control Association. She chairs the SIFMA Information Security Subcommittee and the FSSCC Technology R&D committee. She has lectured for organisations such as ISACA, NIST and CSI. She is a Certified Information Security Auditor, and Certified Security Information Manager. She has masters degrees in computer science and philosophy.*

Kenneth Silverstein *is currently Senior Managing Director in Operations Administration at Bear Stearns & Co. Ken is currently responsible for coordinating the business continuity activities of Bear Stearns. He has been with Bear Stearns for over 24 years and has extensive experience in the financial services industry. Prior to Bear Stearns, Mr Silverstein was an auditor for Coopers & Lybrand. Mr Silverstein is Chairman of the Security Industry and Financial Markets Association (SIFMA) Business Continuity Planning Committee. Mr Silverstein received his BBA from the University of Massachusetts and his MBA from New York University.*

ABSTRACT

When it comes to cyber-related events, the information security professional plays the same role as the business recovery professional. The more the business process recovery professional is closely tied to information security activities within the organisation, the more influence they will have on the development of information security countermeasures. This influence will allow these countermeasures to be better suited to the needs of the business process recovery programme. While the business recovery processes and the information security processes may, in most cases, be separate and distinct, it is vital that they be linked in order to provide the greatest level of resiliency. This paper will provide the framework for how to plan and address the effects of cyber-attacks to technology systems. In addition, the paper will also discuss the role of the information security professional in non-cyber-related events. In all events, it is vital that the role of information security be incorporated in the organisation's business recovery processes.

Keywords: information security resiliency, information security business continuity, information security business continuity planning (BCP)



INTRODUCTION

A comprehensive business process recovery programme anticipates every predictable threat. Of course, the premise upon which business process recovery

Journal of Business Continuity & Emergency Planning
Vol. 2 No. 1, pp. 7–12

efforts are based is that the business process is interrupted. Events that are typically considered business process interruptions include physical disturbances to places of business, interruptions in infrastructure including telecommunications, power and water, and outages in information technology systems. These range from high-impact physical disturbances (eg bombed buildings) to relatively low-impact disturbances (eg a hard drive crash). When applied to a business process that relies heavily on technology, concentration on physical alternatives for operations processing is often focused on alternative data centres, redundant network routing, and backup power, water and hardware. While necessary to ensure business process recovery, these physical approaches are not sufficient to thwart direct attacks on technology itself — often referred to as 'cyber-attacks'.

Information security professionals confront cyber-attack scenarios and plan appropriate responses. While the effects of a cyber-attack may not appear to be as dramatic as a building destroyed by fire, the effects on the business process may be more devastating. The business process recovery from a cyber-attack may be much more involved than moving to another location or replacing a server. This paper will provide the framework for how to plan and address the effects of cyber-attacks to technology systems. In addition, the paper will also discuss the role of the information security professional in non-cyber-related events. In all events, it is vital that the role of information security be incorporated into the organisation's business recovery processes.

INFORMATION SECURITY REVIEW

An information security review is a process whereby the confidentiality, integrity and availability of a technology system or service are reviewed for compliance with a given business objective.[1] The scope of such reviews often directly coincides with the set of systems used by a given business process. Because a security review is done in support of a business objective, it is focused on the business requirements of the systems and the associated business processes. These are the same risk-reduction requirements that frame business process recovery efforts, but looked at from a different angle. The context of risk-reduction requirements in an information security review is in situations where a known threat intersects with a known vulnerability.[2] Threats can come in a variety of categories. Some threats are inadvertent and may arise as a consequence of something very innocent. Some threats are targeted at a component of the firm's infrastructure and are designed to cause damage to the organisation.

THE INFORMATION SECURITY PROGRAMME: CONTROL, IDENTIFICATION AND COUNTERMEASURE

It is the responsibility of the information security coordinators to institute a programme to safeguard information systems assets. A major component of any information security programme is a strategy to identify any potential vulnerabilities and protect against threats that may exploit them. However, not all threats are identifiable. For threats that are identified in advance, the programme should implement protective measures to ensure that the system's infrastructure will not be damaged by corresponding exploitation. For threats that cannot be identified (and thus prevented) in advance, the programme should include processes to

detect when threats have been enacted and mitigate their effects accordingly. This process should include a plan for procedures to return to business as usual. Information security threats are thus addressed via a hierarchy of *controls*: prevention, detection and correction.

Controls are combinations of people, processes and technology designed to prevent the enactment of a threat, detect its occurrence, or mitigate its effect. Preventive controls are measures designed to prevent exploitation. Detective controls are measures designed to detect damage that has not been prevented. Corrective controls include methods to recover from damage. Within the realm of controls is a subcategory of countermeasures. Countermeasures are combinations of people, processes and technology designed to mitigate the impact of a specific type of threat enactment. A robust information security programme will have performed a thorough security review covering the range of vulnerabilities associated with a system, the likelihood of threat enactment, and the risk to the organisation. Preventive, detective and recovery controls will be planned accordingly.

A simple example of a preventive control is a virus protection or anti-spyware program that resides on a PC. The program is designed to identify and eliminate threats from known viruses/spyware that can cause the computer to overload. The corresponding detective control thus monitors CPU utilisation for processes that utilise high levels of processing power, which have not previously been identified as viruses. PC overload is often caused by programs planted by advertisers or other websites which run in the background, and of which the user is unaware. Because virus prevention software only prevents known viruses, it cannot prevent these programs from utilising the CPU. However, the tool designed to detect viruses may be able to detect damage due to advertising software. Thus, the corresponding corrective control for the virus threat could be an automated routine that deletes (or quarantines) those programs found to utilise high levels of CPU power. Note that, if this was the set of preventive, detective and corrective controls chosen for implementation, then the countermeasure would also correct damage caused by advertising software.

In an effort to protect systems from viruses, information security professionals have also implemented an alternative countermeasure. Rather than detecting known viruses, it is designed to allow only authorised software to be installed on a given machine. Administrators create a list of programs that are authorised to run on each PC and automated processes to prevent any unlisted program from running. This control will prevent unknown processes from running on the organisation's PCs, thus reducing the likelihood of PCs crashing due to overload. In this case, the preventive control would be effective against advertising software, thereby reducing reliance on damage detection and corrective controls. The detective control may still be monitoring for increases in CPU-utilisation, but the corrective control may be used so infrequently as not to require automation, for example, it might be to deploy desktop support technicians to investigate and resolve the utilisation problem prior to the PC crashing.

The basic idea is that, once a threat is identified, the information security professional may institute a countermeasure to mitigate its effects; this countermeasure may be reusable for situations other than those originally identified. As information security professionals identify risks and develop countermeasures to mitigate risks

related to information security threats, those measures then become instantly available to the business process recovery team. In some cases, they may be used for situations not even envisioned by the information security team. For example, the PC utilisation monitoring detective control may be used to assess how many PCs are still available on the network after a disaster that caused a network outage.

COUNTERMEASURE: PHYSICAL EVENT VS CYBER EVENT

In comparing the countermeasures employed for a physical break in a telecommunications line against an information security incident to the telecommunications line, the response is dramatically different.

When a physical break in a telecommunications line occurs, the network operations centre is not usually the first to diagnose it. Yet long before those who do know how it happened report in, communications links become over-utilised or dead. Error-logging servers reach disk capacity or monitoring systems report hardware failures. Calls from customer support desks report application outages. Red lights and blinking screens report that something has happened. The network operations centre knows the network is down but does not know why. Once a physical cause is ascertained, the response is clear. The business process recovery plan goes into effect. If certain resilience is built into the network, backup communication lines may have been brought online automatically. Offsite recovery locations are activated, staff engaged, systems are failed over and check-out tests follow standard procedures. Users are redirected to the backup site while damage assessments are made and options weighed.

By contrast, when an information security incident occurs, the network operations centre is usually the first to diagnose it. The same communications lines become over-utilised or dead. Servers reach disk capacity or monitoring systems report hardware failures. Calls from customer support desks report application outages. Red lights and blinking screens report that something has happened. Yet in addition, information security has set up diagnostics that point to the root cause. For example, a spike in a given type of network traffic from a network segment will be reported by the information security monitoring devices.

When an incident is diagnosed as security-related, countermeasures will usually call for a network-isolation strategy. This means that the network origination point of the incident will be restricted from routing traffic to or from the rest of the network. To accomplish this, network security engineers identify all interconnection points between each logically separate 'branch' network and implement safeguards that stop routing at these points. As an incident's impact subsides, these points are then 'brought up' in a controlled manner to ensure that reconnection does not have any negative impact on the rest of the network. Network information security responses must also include the ability to assist local IT management in recovery. In order to accomplish this, they identify in advance alternative communications paths between the network operations centre and local offices for use in the event of a communications failure between them.

Business process recovery can utilise network isolation responses. For example, the set of network segregation control points may be monitored to diagnose which parts of the network are running. Business process recovery efforts may also use strategies devised for communication with local administrators as alternative

communication paths for communicating with local offices.

From an end-user perspective, the effects of a physical event and a cyber event may be very different. If resiliency is built into the physical networks and the physical outage results in an immediate failover to a backup network, the end user may never know that an outage has occurred. If an outage does occur, the initial effects of both a physical event and a cyber event may look the same, but the long-term effects may be very different. In both cases, the end user will most likely be contacting a helpdesk to report a communication problem. Once a physical event is diagnosed, the remediation is straightforward as described above and the time to recover is known as it is outlined in the plan's recovery time objectives. Unfortunately, as the remediation effects to prevent recurrence of a cyber event are much less defined, the time to recover may be unknown and exceed recovery time objectives originally developed in anticipation of physical threats.

INFORMATION SECURITY IN A NON-CYBER-RELATED EVENT

There are many non-cyber-related incidents where information security performs a key role in the business recovery process. Many other non-cyber-related countermeasures have been developed by information security for incident response in the course of business recovery efforts. One such scenario is a potential pandemic.

When an increase in flu cases prevents people from coming into work, the network operations centre is not usually the first to diagnose it. Their observations consist of an increase in helpdesk calls for remote access assistance, above-average usage of remote access communications links, and possible reports of slowness on the networks which connect frequently-used services to remote access equipment. There are no red lights or blinking screens reporting any outages or explaining any physical cause for the pattern of increased usage.

Once a physical cause is ascertained, the response is clear. The business process recovery plan goes into effect. Alternative remote access scenarios such as redirecting business phone lines to home phone numbers go into effect, branches with low levels of staff are supplemented with staff travel. Users who were not previously set up for remote access are provisioned as quickly as possible. Upfront planning for these types of events would be extremely beneficial in expediting the recovery process. If information security were to determine in advance the need for increased levels of remote access, there could be a procedure in place whereby the network operations centre is immediately enlisted to assist. Emergency identification and authorisation procedures could allow for immediate access for authorised individuals, bypassing the need for following standard workflow. Calls from authorised individuals could be met with immediate network access. Procedures whereby computer operators frequently review audit trails could be established to ensure that response procedures are followed in a controlled manner.

This would be possible because, when an incident requiring emergency remote access is diagnosed, response procedures will usually include a pre-established pattern-of-access strategy. Security review will have established that, under certain situations, the risk of allowing remote access is offset by the damage that could occur if a lack of systems access by an authorised individual prevented a business process from being executed. There is a precedent for this situation in the case where a complex piece of equipment may be on the brink of failure

and the equipment vendor is urgently needed to diagnose the problem. To accomplish this access in a secure manner, the security team may have set up a 'maintenance vendor' remote access platform which can be activated only by the network operations centre. When the incident is over, these access platforms are brought back into a dormant state to await the next incident.

In most technology-related business recovery events, it is very rare that an end user community will have direct contact with the information security group. The pandemic scenario highlights a situation where the business users and the security group must work together. In fact, the only way for an organisation to have a successful outcome in this scenario is to have a process where business users work very closely with the security department. This type of planning is often overlooked, but the planning required to address a pandemic scenario requires an organisation to widen its scope. This scenario highlights the interdependencies between the business continuity team, the information security department and the end users.

CONCLUSION

Almost all scenarios used in the business recovery process must include a component of information security. In addition, the information security professional plays the same role within an organisation as the business recovery professional when it comes to events that are cyber-related. The closer the business process recovery professional is closely tied to information security activities within their organisation, the more influence they will have on the development of information security countermeasures. This will allow information security countermeasures to be better suited to the needs of the business process recovery programme. While the business recovery processes and the information security processes may, in most cases, be separate and distinct, it is vital that they be linked in order to provide the greatest level of resiliency. Finally, as is crucial in all business continuity planning, upfront coordination between the business recovery professional and the information security professional will make the organisation's recovery programmes more successful.

REFERENCES

(1) Bayuk, J. (2005) 'Security review alternatives', *The Computer Security Journal*, Vol. 21, No. 4, Fall 2005.
(2) National Institute of Standards and Technology (2006) 'Information Security Handbook: A Guide for Managers', NIST Special Publication, 800–100.