

COMMITTEE:	SCRUTINY COMMITTEE	
DATE:	10 NOVEMBER 2003	
SUBJECT:	IT SECURITY ISSUES	
REPORT OF:	DIRECTOR OF FINANCE AND CORPORATE SERVICES	
Contact:		Sue McHugh, Director of Finance and Corporate Services, Telephone 01323 415104 or internally on extension 5104. E-mail address sue.mchugh@eastbourne.gov.uk

1.0	<u>Introduction</u>	
1.1	Scrutiny Committee at its meeting on 8th September agreed to investigate issues arising from the virus infection which disrupted Council business during August. The Committee resolved as follows:	
	1) "That the Scrutiny Committee should immediately investigate the recent collapse of the Eastbourne Borough Council IT network and email service and that explanations should be sought and provided to Committee members to see how the situation arose and to seek firm assurances that the	

	2) “That a report be immediately drawn up to identify what measures can be taken by Eastbourne Borough Council to halt the rash of un-requested inappropriate spam emails”.	
	3) “That a calculation of the cost of the collapse of our IT systems should be identified and apportioned to the culprits”.	
2.0	Summary of Events	
2.1	On Thursday 21 st August, Eastbourne Borough Council was hit with the MSBLASTER virus, along with many other organisations worldwide. The Director of Finance & Corporate Services was away on annual leave at the time and Ron Cussons, Director of Tourism & Leisure, who was Acting Head of Paid Service, assumed overall responsibility for overseeing the action to manage the situation. A detailed chronology of events over the following week is attached at Appendix A. Following the virus attack the Head of Audit was commissioned to investigate the cause. In addition, Vivista commissioned a review of the Council’s IT security structure with a view to identifying weaknesses and areas for improvement.	
3.0	<u>Conclusions</u>	
3.1	Relevant conclusions from the investigations by the Head of Audit and Vivista and subsequent work by the in-house IT team are as follows:	
	· The virus infection was caused by unprotected access to the internet (not by e-mail).	
	· It is unlikely to be possible to ascertain exactly how the virus gained access to the Council’s systems.	

	<ul style="list-style-type: none"> · One possible explanation could be a user who dialled into the Internet remotely using a laptop and then connected to the Council network. 	
	<ul style="list-style-type: none"> · Another possible source could be through one of the filters that were in place through the Council's firewall. Five Council laptops were configured to allow direct access to the Internet, via filters on the firewall. One of the five laptops had been set up to connect to a home network. It has not proved possible to establish how the decision to create these filters was taken. The users of these filters required limited (FTP) access to the internet in order to carry out their duties including maintenance of websites. None of them required the full access which had been set up and which represented a much greater security risk. 	
	Anti virus protection	
	<ul style="list-style-type: none"> · The virus was designed to exploit vulnerability in the Microsoft Windows 2000 and XP operating systems. Microsoft had issued a patch to help to protect against the virus some two weeks before it hit, but this had not been applied to the EBC desktop units. 	
	<ul style="list-style-type: none"> · Aladdin supplies EBC's desktop anti virus software (e-safe). Aladdin had not issued an update to protect against this virus. Aladdin are withdrawing support for their desktop product from the end of the current calendar year. 	
	<ul style="list-style-type: none"> · If the Microsoft patch had been applied to each EBC PC and Aladdin had supplied an update to protect against the virus, this would probably have prevented the infection from spreading. 	
	<ul style="list-style-type: none"> · The Council's anti virus software did not satisfactorily detect or remove the virus. 	
	<ul style="list-style-type: none"> · Anti virus protection is currently deployed to desktops and the firewall. There is no separate protection for servers. This could provide an additional level of protection. 	
	<ul style="list-style-type: none"> · There are no policy documents for laptop users or remote access users to minimise the risks associated with these activities. 	
	Roles and responsibilities	
	<ul style="list-style-type: none"> · Responsibility for EBC's security arrangements is shared between Vivista and the in-house IT team. The precise split of responsibilities had not been formalised. 	

	<ul style="list-style-type: none"> · The Council did not have an agreed procedure in place for dealing with a major virus attack. Staff from across the Council and Vv Vista co-operated to manage the process of dealing with the virus, in many cases working long hours to do so. As the virus hit during the peak holiday period this also involved a number of staff operating in an acting capacity for colleagues on annual leave. The staff who were involved in this process deserve thanks for the efforts they made. Nonetheless a formalised procedure setting out roles and responsibilities, decision-making and communication arrangements and business continuity priorities would have improved the management of the incident and may well have reduced disruption. 	
4.0	<u>Action Plan</u>	
4.1	<p>In the light of the above an I.T. Security Forum has been established to ensure that the lessons from this incident are learnt and that security issues retain a high profile within the Council. Details are as follows:</p>	
	<p>IT Security Forum : terms of reference</p> <p>The Forum will oversee a programme of work to address a range of IT security issues. The work to address these issues will need to be phased. The following initial phasing has been agreed:</p> <p>Phase I – to 31 December 2003</p> <ul style="list-style-type: none"> · Procure and implement replacement for E safe desktop virus protection product · Procure and implement replacement for E safe gateway virus protection product · Laptop and handheld policy · Consider further security measures to be implemented · Consider actions required in response to concerns raised by staff about the operational viability of security arrangements <p>Subsequent phases</p> <ul style="list-style-type: none"> · Implement procedures to eliminate illegal and unauthorised software from council PCs · Achieve separation of business and personal email accounts for all EBC employees · Develop computer programme to facilitate handling of leavers, joiners, change control, inventory · Non-networked remote users who can dial into network · Management of email SPAM · Implementation of Information Security Policy 	

	<p style="text-align: center;">Membership</p> <p>Sue McHugh (chair)</p> <p>IT Contract and Infrastructure Manager</p> <p>Vivista Contract Manager</p> <p>Head of Audit</p> <p style="text-align: center;">Computer Auditor</p>	
	<p style="text-align: center;">The Forum is on target to deliver the projects prioritised for completion by the end of December.</p>	
5.0	<p style="text-align: center;">Other Issues</p>	
5.1	<p>Alongside the establishment of the IT Security Forum a project has been established with the aim of Improving IT Service Delivery across the Council. A key part of this project is the renegotiation of the current contract and Service Level Agreement with Vivista. As part of this, responsibilities for all aspects of security coverage will be clarified and documented.</p>	
6.0	<p style="text-align: center;">SPAM emails</p>	

6.1

SPAM is a term used to describe unsolicited emails broadcast to large numbers of email accounts. There are a number of types of SPAM emails that Council officers and members receive. Many officers receive marketing emails from providers of products and services that are related to their areas of work. A smaller number may receive inappropriate emails, including those containing offensive material.

6.2

E Safe Gateway scans all incoming email for inappropriate content and blocks any items which contain forbidden text. EBC can specify any words that it wants to trigger a block. In practice banning words is likely to result in some legitimate traffic being blocked which can be frustrating for users. So a balance needs to be struck between the words which are banned and the disruption to legitimate business this causes. Organisations, which send SPAM, have developed techniques for bypassing blocks. These mechanisms include hidden code which prevents words being detected, whilst still being visible

It is known that organisations obtain email addresses for their SPAM distribution lists in a number of ways. One of these ways is searching websites. So EBC email addresses which are displayed on our websites are likely to attract SPAM. In general this is likely to be marketing SPAM targeted at local government services. Another way that SPAM distribution lists are generated is from users who visit web sites. The Council uses a product called Websense to block officers from accessing certain websites. Nonetheless, officers and members who need to visit controversial websites as part of their work may find they attract more SPAM, including inappropriate SPAM.

There are a number of things that can be done to limit SPAM:

- It is possible to block the email source of any item via Websense (although distributors will take steps to avoid this).**
- As explained in section 4 above, officers are in the process of replacing the current desktop anti virus product. As part of the evaluation of products, features that limit SPAM will be considered.**
- The IT Security Forum are due to consider SPAM issues as part of the 2004/05 work programme. In the shorter term, the IT team will be providing advice on measures than can be taken to limit SPAM (e.g. never click 'unsubscribe' to a SPAM email as this will in fact sign you up for future**

distribution).

Where SPAM is a particular problem, one option is to set up a new email address for the user and discontinue use of the old address.

7.0	Costs of infection		
7.1	Following the virus attack an audit of the costs to the Council was commissioned. The costs incurred are set out below:		
		£'000	
	Loss of staff productivity through downtime	55	
	Vivista - additional to contracted service	5	
	Staff overtime directly linked to downtime	2	
		62	
	Overwhelmingly the majority cost comes from lost productivity of Council staff. This is based on returns from managers that together total 552 days. At an average cost to the Council of £100 per day this very quickly becomes a sizeable sum.		
	This is not to say that staff were doing nothing throughout the period of downtime, but it does reflect the very heavy reliance placed on IT systems for the delivery by staff of services to the public.		

	<p>The issue of cost recovery through insurance has been pursued.</p> <p>The Council has in place a policy that allows for the reclaim of direct costs associated with the recovery of IT systems. However, for our particular situation only the cost associated with the additional work performed by Vivista beyond the contracted service may be claimed. Given that our policy carries an excess of £5,000, no claim will be made.</p>	
7.2	<p>The Scrutiny Committee resolution suggests that the costs should be recovered from those responsible for the attack. That is not possible for the following reasons:</p> <ul style="list-style-type: none"> · Responsibility for the attack ultimately rests with the authors of the virus. EBC has no means of obtaining recompense from them. · It has not been possible to establish conclusively how the virus entered the Council's systems. · A number of shortcomings in current security arrangements have come to light as a consequence of the virus attack and the subsequent investigations. However, it cannot be shown that any one of these caused the infection. · The virus succeeded in entering the systems of a high proportion of organisations world wide, including most of our neighbouring authorities and the Audit Commission. It cannot be said that any particular change in the current security arrangements would definitely have avoided the infection. · It is therefore not possible to conclude that any individual or organisation should bear responsibility for the costs incurred. 	
8.0	Consultations	
	Vivista have been consulted on the contents of this report.	
9.0	Implications	
	Action to improve the Council's security arrangements may have resource and financial implications, which will be included in the 2004/05 Service and Financial Plan for the IT service.	
10.0	Conclusions	
	The lessons of the virus infection are being learnt and a programme of work to secure improvements in security is underway.	

Sue McHugh		
Director of Finance and Corporate Services		
Cabinet CMT 20.09.03 MS Blaster Virus Infections August 2003		

Appendix A

REPORT ON COMPUTER VIRUS – AUGUST 2003

Thurs 21 Aug 10.30 am	It became apparent that the IT network was experiencing difficulties resulting in continual dialogue between the Director of T & L and EBC IT Manager. Being aware that the County Council and Wealden District Council were experiencing similar problems.
12.30 pm	<p>A meeting was convened between RGC, Norman Kinnish, Peter Finnis, Peter Byard to discuss the situation. The virus still had to be identified and a solution was being worked up and identified by PB and the Site Manager for Vivista, Brian Hall. RC asked PB to keep Cllr Jon Harris informed as Cabinet Spokesperson for IT. The meeting terminated to allow PB and BH to take action. An arrangement was made to meet again at 4 pm.</p> <p>As Councillor Harris was unavailable, RC contacted Cllr David Tutt to inform and agree a press release. This was not released at this time as services were still operational, in a reduced capacity.</p>
4.00 pm	A patch to eradicate the virus had been identified and was being actioned centrally with a priority list being established – Benefits, Box Office and other front line services. It was thought that this would solve the problems and arrangements were made for night working by Vivista and Council buildings to be manned to provide access. A communication was sent to all staff informing them of the problem and our actions.

Fri 22 August 10 am	The team met again and identified that the overnight working had remedied the pc's in our priority areas but traffic on the network prevented working. All efforts were diverted to keep services operational on our priority list. We identified that weekly paid workers and cabinet reports needed priority action to deliver the service. Solutions were identified with relevant Managers. A second communication was issued to all staff advising of actions and RC visited the main Council buildings.
5pm	The team met to review the situation and was advised that the whole system needed to be taken down after closure of Box Office at 8 pm to try and solve the network traffic. Vivista would work over the weekend and bank holiday to establish where the network traffic was coming from and which pc's were causing the problem and also check the hardware.
7pm	RC had meeting with PB for update.
8.30pm	RC met PB in Box Office for further update.
23,24,25 Aug	Following the weekend working, and all systems put back on line, the only operation live, the Box Office, performed as normal, which indicated that the problem had been solved.
Tues 26 Aug	As the Council became operational following the Bank Holiday, it quickly became apparent that the virus was still present.
10.30am	<p>The team reconvened and was advised:</p> <ul style="list-style-type: none"> · A specialist network company (Pavilion) brought in · 600 computers cleaned over weekend · Communication to advise staff of situation. Instruction that no laptops taken home must be used until cleaned by IT Department · PF to inform Members not to log on · PF to speak to Cllr Harris · The whole system needs to be taken down · Telephone cascade to get message to staff · Instructions given to staff not to copy data onto removable media, floppy disks and cd's · Cllr David Tutt informed and agreed press release that was issued as services were stopped for a period

2 pm

Team reconvened:

- A manual communication system set up with a member of staff in each Council Building responsible for putting on each desk the communication as issued to them from RC's office. As necessary, these communications sent handwritten, faxed or personally delivered.
- The network needed to close down again
- PF spoken to Richard Horne for insurance
- Identified the need in future of emergency procedures to be in place should there be a recurrence at a future date
- A network specialist brought in to detect where network traffic was coming from
- Instruction given to put 1 Grove Road back on
- A number of pc's in Town Hall had now been identified as infected and taken out of service as in other areas and the Town Hall would be back on at 3.30 pm
- RC requested Box Office be given 30 minutes notice of going down to enable plans and tickets to be pulled off to operate manual system (Box Office taking 30K per day)
- BH confident all systems would be up by tomorrow
- RC sent communication to all staff advising of the situation and actions
- Vivista think the problems have been identified
- PF to communicate with Members for their laptops to be brought into his office for onward transition to IT for cleaning.
- 3 communications sent to all staff
- TIC identified to be causing much of the network traffic and cleaned and put back into operation

<p>27 Aug</p> <p>9.30 am</p>	<p>Team reconvened and discussed:</p> <ul style="list-style-type: none"> · Paul Jobbins (Vivista) rang RC to inform that they were sending an IT specialist to check the viability of esafe as a Council protection system and try and identify where the source of virus and actions of Vivista in general · BH confirmed 90% of pc's in main building now operational and now concentrating on satellite sites · Members sent a hard copy to ask not to log on · RC emphasised Sovereign Centre and Coastline should now be a priority · NK concerned about our current protection system. This was being investigated · It was identified that the virus came into the Council twice and had penetrated our firewall · Staff were asked to shut down their pc if there was any evidence of the virus especially if on screen notice · Staff were advised not to share passwords or allow anyone to use their pc · Communication was sent to all staff reminding them of operational instructions issued over last few days
------------------------------	--

Ongoing	<ul style="list-style-type: none"> · RC in dialogue with BH as to progress throughout the day.IT and network now returned to normal operations · All Heads of Service asked to identify any down time and costs incurred in keeping service operation during the virus period · Head of Financial Management asked to collate costs and expenditure caused by the virus
---------	--

VIVISTA

_A report was issued by our contractor, extracts as follows:

Original Outbreak of Lovsan (MS Blaster) Virus

_When the Lovsan (MS Blaster) worm virus was first discovered the update from the “E Safe” authors was slow. This could be due to the fact that the “E Safe” product is being discontinued this year and this manufacturer is releasing no new product. This has seemed to have produced a lack of real interest in releasing updates from the support company as they will not continue this business after this year.

The Vivista On-Site team were advised by Vivista IT of the existence of the virus. Pro-active measures were taken to ensure the Ports exploited by the virus were secure (They were)

When EBC was originally infected with the Lovsan (MS Blaster) virus, the process of cleaning this virus was as follows:

1. Contact the “E Safe” support company.
2. Patch all of the servers with the Microsoft security patch that removes the security weakness this virus exploits.
3. Run the E Safe provided MS Blaster removal tool on all the servers.
4. Waited for virus updates to become available. (After a day we were advised that no Esafe product could protect against the virus as it was exploiting a weakness in the Microsoft Operating System).
5. A Batch script was written to detect ‘msblast.exe’ in the WINDOWS SYSTEM32 directory.
6. This was run to scan all pc’s on the network.
7. The output of the batch file was to a text file that listed the Network Names of the infected machines.
8. These infected machines were then located, the Microsoft Patch installed and the registry cleared of incorrect entries and the antivirus software run to remove the infection.

Subsequent Outbreak of Lovsan (MS Blaster) Virus

_The Second round of infections was purely on the desktops that hadn’t been patched the first time round.

The effects they noticed were:

1. Network grinds to a halt. This is due to a broadcast storm being generated by the infected machines trying to locate further machines to infect.

2. Users connected to the Box Office application that is provided via a Citrix program neighbourhood were being disconnected regularly as these broadcast storms were filling the network.

The following is the processes followed to remove the virus:

1. Users were advised by Internal IT to continue working.
2. The Vivista Contract Manager rejected this advice and instructed the On-Site team to turn off external E-mail.
3. Disconnect the internet connection.
4. Confirm the TCP/IP ports 4444, 135, 69(udp) on the firewall were disabled.
5. Reconnect the internet.
6. Contact E Safe support to try to get an update that would remove the virus as the one being used wasn't successfully removing it.
7. Located where the virus came from.
8. When users reported the antivirus product had detected the virus on their machine (but not cleaned it) they were told to turn off their machines.
9. They again used the batch file to search for infected machines.
10. An attempt was made to patch all infected machines remotely. This failed due to the Network continually locking up and that some were turned off.
11. All machines in the main Council Offices were then visited, the patch installed manually and the infection removed.
12. Over the Bank Holiday weekend additional staff were brought in by Vivista to systematically patch all desktops in all sites.
13. To facilitate the Box Office all system except the Box Office were turned off.
14. On Monday night all desktops and servers were powered up. All links including the fibre were reconnected and another broadcast storm was noticed.
15. Network lockup was still occurring and the On-Site team suspected that a number of machines had been missed. To assist in identifying the network lockups a Network Specialist was brought to site on Tuesday to monitor the Network traffic. This identified some infected machines and an action of identifying these, patching and cleaning took place. They are now reaching the end of this as virtually all machines had been patched and so further infection is prevented.
16. Once located the user is contacted and where practical the administrators proxy onto the machine, install the patch, clean the virus both manually and using the antivirus software.

RON CUSSONS

DIRECTOR OF TOURISM & LEISURE

