



Concentrix
a common centre

Security for your Finance and CRM Software

A non-technical introduction on how to ensure your systems are protected from the ever prominent security threats.

Concentrix Limited

20 Granite Way
Mountsorrel
Loughborough
LE12 7TZ

E: info@concentrix.co.uk
T: +44 (0)1509 410500
F: +44 (0)1509 410501

www.concentrix.co.uk

Registered in England No. 3891450
VAT Registration No. 738 0929 09



Copyright © Concentrix Ltd 2009

All rights reserved. No part of this document may be reproduced, distributed, stored in a retrieval system or transmitted in any form or by any means electronic, mechanical, photocopying, in writing, recording or otherwise without the prior express permission of Concentrix Ltd.

Concentrix Ltd cannot be held liable for any errors or omissions in this document. However, if you discover any inaccuracies or have suggestions for improving the document, please contact Concentrix directly.



Introduction

Developments in technology have meant that the use of the internet and email are part of the daily routine for most organisations. And although businesses have existed for hundreds of years without either of these, the vast majority of companies would now struggle to operate if they were not there because they have now become so dependant on them.

The use of the internet and email has increased the speed of communications, transactions and ultimately decisions. It has also opened up a whole new world of threats which companies now need to protect against. Many of these threats can compromise the security of your CRM, Finance or Business Management System and have the ability to cause significant problems and disruptions.

Data is a company's most important asset as it provides a base of knowledge. For example, data within CRM enables you to deliver excellent customer service which in turn helps develop good relationships with customers, creating loyalty. This is essential to ensure profitability and business growth (it costs more to gain new clients than it does to retain existing customers.) However, one of the biggest challenges organisations now face is ensuring the data held in their CRM, Accounts and Business management systems is secure. Securing data means protecting the hardware, software and networks which they run on, not just one of these elements in isolation.

The majority of organisations are now aware of the risks which are posed by external sources and have processes in place to protect against them. Conversely, organisations often do not have processes in place to protect against the increasing internal threats. This may be because they are either not aware of them, or do not know how to secure their systems against them.

This whitepaper discusses the importance of protecting your organisation from both internal and external security threats. It also provides suggestions as to how you can ensure that your organisation's hardware, software and network are protected as well as providing information about the different types of security products available.

Why do organisations need to have hardware, software and network security?

Irrespective of size or sector, information is the critical component for business and is the key to ensuring the future growth and continuing success of a company. Very often all information relating to customers and competitors will be held in a CRM or Accounts system. But, without having processes in place to protect the data, it is vulnerable to misuse or theft. Subsequently, ensuring these systems are secure is a must.

Protecting against one threat in isolation will not ensure your organisation is safe. After all, a company's software is saved on hardware and it is the collection of hardware which forms the network. Therefore, in order to ensure complete security, the company must have security solutions which protect their hardware, software and network. When it comes to security, it is not safe to assume anything.



What are the different types of threats facing CRM, Finance & Business Management Systems?

There are many different types of security risk facing organisations. Traditionally viruses and spam were the two main threats, and these are still prevalent today. The risk posed from these has also moved on; the technicality has increased and viruses can now spread world-wide in a matter of hours. What's more, they have the ability to bring an entire organisation to a halt by affecting the key operating system. In addition, spam has also changed from purely being unsolicited mail, to being offensive, fraudulent and dangerous and therefore it needs protecting against.

As a result of the number of targeted malicious attacks on organisations, many are now aware of the external risks and have processes in place to protect against them. However this is no longer the only type of risk facing organisations. The threat posed from internal sources has increased significantly over the past few years as a direct result of the developments in portable storage and personal devices such as iPods, USB drives and mobile phones. These devices have made it easier than ever for an employee to copy large amounts data from your CRM or Accounting system and take it with them when they leave a company. They could then, for example sell it to competitors, or use it against you. Recent research by Ponemon suggests that 59% of people who have left a company recently have admitted to taking data with them when they left.

Data Leakage

In the current economic environment businesses are looking for ways to reduce their costs and security may be seen as an expense which the organisation doesn't need. However, a reduced level of security, coupled with the ever increasing number of people losing their jobs provides the ideal catalyst for more data to go missing, be copied or removed. This phenomenon is often called Data Leakage and organisations need to be aware of it and have processes in place to protect against it.

According to the Information Security Breaches Survey, 2008, 67% of UK businesses do nothing to prevent confidential data leaving their organisation on portable USB sticks. However, 57% of enterprises have lost confidential data through removable media such as USB drives in the past 2 years (Forrester 2007).

Data Leakage is not always a deliberate attempt to impact on a company's profitability. There are a number of ways data can be lost from an organisation, and often the main cause of the unintended type of loss, is human error. There have been a number of high profile cases in the press recently where important files or documents have been left in public places and have subsequently got into the wrong hands. And although the data was not lost with intent, the implications for the organisation concerned have still been significant.

Data Protection

Today there is a large focus on data protection and keeping data secure is critical as customers want to be assured that their personal information will not get sold, lent or given to any other third party. In the UK, organisations also have legal obligations under the Data Protection Act and must put processes in place to ensure that all data is safe. If there is a breach of security this could be at the expense of the company's reputation. It is likely that



not only would the company lose the custom of the individual who's data got lost but also many others who subsequently become concerned and take their custom elsewhere. It is therefore in the company's own interest to have the correct procedures in place to protect their data. The benefit of investing in security software far outweighs the initial cost of implementation.

What are the common forms of attack?

The most common forms of attack which face organisations include:

Data Leakage -This is an internal threat which can have significant implications on organisations profitability as data can get into the hands of competitors

Spam – A traditional form of attack which is now more than unsolicited mail. For example, phishing emails can result in a company's corporate information being stolen. In addition, Spam can take up valuable space on a company's server and this can prevent business critical information getting through

Viruses – These have developed over the years in terms of technicality – they can quickly bring an entire organisation down –impacting significantly on operations and therefore profitability

Unfortunately it is not just a case of managing one of these threats, as spam can infect your organisation with a virus and viruses can inundate you with spam. It's a vicious circle which means all organisations must protect against all types of risk. On the positive side, all of these threats can be protected against, and once in place, a security solution can often safeguard a company's data and reputation and ultimately the organisations future.



Which type of threat should organisations protect against?

In order to ensure maximum security, organisations should have processes in place to protect against all types of threat both internal and external. But because there are so many different types of risk and so many different products on the market, knowing what protection you have and which protection you need can become confusing. Often organisations invest in one type of security product and think they have all the protection that they need. They could be leaving their organisation wide open to risks of a different type.

As an organisation grows, its security needs also change. Therefore it is important to constantly review the requirements of the organisation to ensure that the security processes are capable of protecting the growing size of the network.

How can I protect my organisation from Data Leakage?

Conventional methods of protecting against data leakage include:

- Banning all device usage in an organisation
- Blocking drives on every computer
- Blocking connection points on every computer.

However, some would argue these methods of prevention are a little extreme and outdated.

Data Leakage is a common problem and the deliberate type can be solved by installing a piece of software which prevents data being stored on portable storage devices. This type of solution is usually called Endpoint Security. GFI and Sophos are among a number of companies who provide this type of software.

So how does EndPoint Security work?

Typically EndPoint Security products allow administrators to actively manage user access and log the activity of all portable storage devices. The software usually works by installing a small "footprint" agent onto all machines such as PC's and laptops. The small size of the footprint means that it will have no implication on the day-to-day operation of the machine and the user will never know it is there.

The key to managing portable devices in your business environment is to give your administrators direct control over what devices are in use on your network. Many EndPoint Security solutions enable administrators to not only gain control over what is in use but also let them know what has been used and by who. Most importantly, they provide in-depth knowledge of what data has been copied.

Concentrix recommends organisations do the following to avoid data leakage:

- Invest in an Endpoint Security solution
- Regularly change passwords on CRM, Accounts and Business Management Solutions
- Ensure all data stored on storage devices such as CDs and USBs is encrypted



How can I protect my organisation from Spam?

The typical answer is to invest in anti-spam software. However, often the process of protecting an organisation from spam needs a combination of effective software and also it requires employees to be mindful of the websites they visit and the emails they respond to.

Anti-spam software usually works by examining incoming emails to try and separate spam from legitimate messages. Filtering software can automatically identify and detect spam, or offensive emails, and prevents those messages from reaching your inbox. However, there are instances where anti-spam software identifies legitimate mail as spam (called 'false positives') and this can result in a significant amount of business being lost. It is therefore essential to ensure that the solution which you invest in has a low number of false positives. What's more it is beneficial if end users can choose to review their spam.

There are many anti-spam solutions available. The most effective solutions feature a number of anti-spam engines to give administrators an extremely high spam capture rate, while keeping the number of false positives as low as possible.

Some of the latest anti-spam solutions also have an extra anti-spam engine which provides an additional layer of protection. The latest versions of software have been designed for ease of use and make the task of managing the software much easier for the administrator.

There are a number of key points which organisations should follow to protect themselves from spam:

- Invest in anti-spam and anti-virus solutions
- Do not respond to emails which have come from an unknown or untrustworthy source
- Encourage employees to set up another email account which they can use when filling in forms on the internet
- Do not put your email address as a link on websites

How can I protect my organisation from viruses?

The first action organisations can take is to invest in anti-virus software. However, having one anti-virus engine is not enough, 97% of organisations surveyed by the FBI in 2006 had anti-virus software installed, yet 65% claim to have been affected by a virus at least once during the year.

Typically anti-virus software scans files to eliminate viruses and other malware. Usually it will do this by using two techniques including:

- Looking for viruses using a virus dictionary
- Identifying any programmes which are running suspiciously as this may indicate that it has a virus.

Because viruses have been around for so many years there are a variety of anti-virus software solutions on the market. However when selecting the right solution for your organisation, Concentrix recommends that you should look for the software which is easy to set up and use and also protects automatically and quickly.



There are a number of key tips which an organisation should follow to protect themselves from viruses:

- Invest in anti-virus and anti-spam software
- Regularly update anti-virus software
- Do not open attachments which are from unknown or untrustworthy sources
- Avoid file sharing
- Ensure all of your data is backed-up

Is there a solution which will protect my organisation from every type of threat?

There are solutions available which will protect your organisation from most types of threat. However, this type of solution is not right for every type of business. Before investing in any type of security solution, Concentrix advises companies to carry out an independent assessment of the company's needs, to ensure that you are investing in a solution which matched your company's requirements.

Implementing security software

To ensure that security solutions bring real benefits to a business, the requirements of the company need to be carefully thought about and planned. It is very easy, especially in the current economic climate to choose the security solution which appears to be the cheapest, however if it doesn't match your requirements it will be a false economy as you will spend more money in the long term, especially if there is a security breach. Security threats are a risk to every facet of a business, therefore it is essential that the security solutions are capable of protecting your whole organisation.

Many organisations appoint an internal member of staff to assess their security requirements. This individual will then be responsible for scanning the market for the best solutions and also for the implementation. However, a professionally implemented security system which matches business needs will usually be more effective.

Whatever the size of your security project, Concentrix recommends working with a supplier who can come in assess your business needs and IT infrastructure and make recommendations based on your requirements. Choosing the security software that you think you need, may not provide you with the security you actually need. What's more security threats are constantly changing and developing. Therefore although you may be protected at the time of implementation, you may not be protected six months afterwards. It is therefore essential to continually review your businesses requirements, to ensure that as your organisation grows, your security solution continues to work for you. It is essential you choose a supplier who will be able to provide you with ongoing support once the solution has been implemented.

Remember the pitfalls

As with all projects, there are a number of problems which can arise when implementing a security solution. However, the majority of these problems can be avoided. Concentrix has deployed many security solutions for companies covering a range of sectors. To avoid the problems, we recommend the following:

- Don't choose a solution or a supplier because they are the cheapest. Like all purchases with security solutions, you pay for what you get.
- Don't just expect the solution to do all the work – there also needs to a cultural



change within the company. Employees need to be mindful of the files they open on their computers. In addition if they are out of the office and carrying confidential data they need to know the potential consequences if the data is lost

- Review the system on a regular basis. As your business changes, so will your security needs

Communication is essential. If anyone in your organisation becomes aware of a threat facing the organisation, they need to speak out.

Further information

- For more information about any of the security products provided by Concentrix visit the Concentrix website or contact us direct.
- Concentrix provides security solutions from GFI ,Sophos and WatchGuard and this enables them to take a product agnostic approach to supplying software.
- Concentrix has a dedicated infrastructure team who will advise you on the security product which is right for your organisation and provide on-going support once the solution has been implemented.

Recommended Products

For Anti-Spam:

- GFI MailEssentials
- GFI MailSecurity
- Sophos Email Security and Control

For Anti-Virus:

- Sophos Anti-Virus
- Sophos Computer Security
- Security Suite

For Data Leakage:

- GFI EndPointSecurity
- Sophos Endpoint Security and Data Protection

For Complete Security Solutions:

- WatchGuard



About Concentrix

Concentrix is a Leading UK business management, independent customer relationship management (CRM) specialist, and IT solutions provider. Founded in 1999, Concentrix helps companies increase competitiveness, profitability and customer satisfaction by improving business process, systems and IT.

Concentrix implements systems and business solutions that are right for their customers' requirements: matching needs, goals and budget. Concentrix works across a wide variety of industry sectors with clients ranging from small companies with a handful of users, right up to household-name PLCs with hundreds of users on multiple sites.

Concentrix supplies Security solutions from GFI, Sophos and WatchGuard and takes a product agnostic approach to supplying software, ensuring you get the solution which is right for your organisation. Concentrix will implement the solution, ensure that it fully protects your CRM, Accounts or Business Management Solution and support it as required.

Today, Concentrix is a one-stop-shop for CRM, accounting, business management and supporting IT. So as well as CRM and business management software, Concentrix also supplies leading brand hardware, a comprehensive range of support, training, course, upgrades, advice and consultancy. In other words, Concentrix provides complete solutions: software, hardware and supporting services.

Concentrix is based in the heart of the midlands in Mountsorrel, Leicestershire, has regional office in Bristol and a satellite office in central London.