Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version: 1.4b

Title: Introducing Security to the Small Business Enterprise

Author: Jeff Herbert

Date: 28 April 2003

Introduction

A recent survey by American Express found that 71% of Small Business Enterprises (fewer than 100 employees) are now using the Internet for a wide variety of tasks [1]. SBE's are now implementing Internet enabling strategies for globalisation and to compete with larger competitors. They connect to the Internet via dedicated broadband services and enable clients to interact with business systems and use it for a variety or purchasing, marketing and administration functions.

However, many SBE Internet strategies overlook both Internet and internal security principles such as Defence in Depth, and SBE management often has very little understanding of the threats, risks and implications for the business. This discussion paper outlines the issues and constraints that a SBE faces, the common misconceptions managers have regarding Internet security, and how to introduce security to the Small Business Enterprise.

SBE Threat Model

Security for the SBE is no different to any larger business. However, the SBE has the same risks, but has to recognise and manage these without the resources available to a larger business.

The SBE has a number of vulnerabilities that can manifest threats to the business. These represent the risks that the business needs to manage.

- Lack of Internet Policy

  Frequently, no definition of business requirements is made and no business Internet policy exists for any Internet facing host, service, or function. This often leads to poorly implemented and configured systems with little change control, and ultimately, a security breach.

- Broadband Internet Connection

  Broadband offers three primary benefits to the SBE. It's inexpensive, it's fast, and it's dedicated. It allows the business to open its doors to the Internet [8].

Attackers far prefer to utilise broadband connections to facilitate attacks and subversion of internal system resources.

- Internet Facing Hosts

  The typical SBE is implementing a range of Internet facing services. Email servers, FTP servers and Web servers are common. Citrix and MS Terminal servers are now widely used for remote access.

  Most of these services and servers are not implemented as bastion hosts and are not maintained to the patch and security levels expected of an Internet facing host. Often they are located inside the live network. These services introduce risks and contribute significantly to a poor security posture for the business.

- Poorly Secured Internal Systems

  SBE's frequently have poor Defence in Depth strategies. Internal systems have very little security implemented and password security is particularly weak.

  Internal systems represent resources and opportunities for the attacker to utilise, and once the perimeter security is penetrated, most internal systems are completely vulnerable to the attacker. The attacker has free reign to further compromise or trash internal systems at whim.

- Internet Content Control and Management

  Many SBE allow their employees considerable scope for email, web browsing and downloading files without managing or controlling the content. Aside from legal ramifications, this allows not only viruses (which can be detected) but also allows Malware, Adware and Spyware to be introduced onto business systems [15].

  Layer 7 port 80 applications such as Kazaa are now the major bane of all businesses as they can bypass many security controls. [2]

- Confidentiality and Reputation

  Many businesses have a responsibility to manage the confidentiality of both their own proprietary information and client information. If confidentiality is breached and the fact published, the business may suffer from a loss of reputation that will affect it considerably from a commercial perspective.

- Poor Education

  Poor education may not be immediately recognised as a threat. Unfortunately this, however, is the case. It results in wrong decisions,

and the consequence is that a risk may not be adequately managed simply because it was not understood in the first place.

The SBE represents an ideal target for the attacker due to the combination of probable poor security at the SBE and the resource rewards for the attacker (bandwidth, hosts, file space, information).

Understanding the SBE Business Drivers

In this section, we examine the SBE drivers and how Internet security is viewed so we are able to re-educate and position a strategy for securing the business. Many of these points will apply to medium and enterprise businesses as well, but the SBE in its own right has distinct operational differences from its larger counterparts.

- Low Risk

  SBE managers often consider the business a low-risk in regards to threats from the Internet. Communicating the need for security to these businesses can be very difficult [3].

- Thinking Small

  One of the key mindsets that small business managers have is that they think of themselves as of “no interest” from a global perspective. “We’re too small – who would want to attack us?”

- In-sourcing

  Many SBE’s have an in-sourcing attitude. They hire technical employees that are often required to install, configure, and maintain systems as they see fit. They are usually not trained appropriately in either technical aspects or professional procedures pertaining to the systems they are responsible.

- Costs

  Although all businesses are concerned with costs, each additional cost to a small business makes a larger percentage difference on the annual profit/loss, and ultimately, its e-bit. Any expenditure is usually analysed carefully as to whether the business really needs it.

- Control

  SBE’s often perceive letting specialists work with their IT as a loss of control. Their administrators can have an unwillingness to let others be involved in an aspect of their infrastructure citing loss of control as a negative for the business (and also introducing “unneeded” costs to the business.

- Tangible vs Intangible

  Often SBE management, especially those with Accountancy based backgrounds, have difficulty with the Tangible vs Intangible concerns with Internet security, and often will only react once the business has suffered an attack (and sometimes only after repeated attacks). They refute the intangible benefits they may get from “best practice”.

- Confidentiality

  Many SBE managers do not view confidentiality of their own data an issue. Some have even quoted “they’ll be lucky to get anything useful out of the system”. SBE managers tend to overlook their responsibility to maintain and protect client information they may be storing such as documents and communiqués.

- Availability

  A typical SBE will be able to function without Internet access for a 24 hour period, although many will be chafing at this restriction. Availability is a nice to have, but the SBE can manage without it for a reasonable length of time.

- Existing Security

  Most SBE have essential Internet security products in place – antivirus solutions are most common and many now recognise the need for firewalls as well. However most SBE’s have no security “best practice” maintenance and management processes to ensure the products are doing what they should.

- Decision Making Structure

  SBE’s have a very flat management structure. As opposed to a larger business where a business case can be built by a solid multi-level sales strategy, you have one or two managers (generally non-technical) to present to and convince.

Overall, the SBE is usually prepared to take greater risks on board operationally. Risk management and security threats are commonly regarded as FUD (Fear, Uncertainty and Doubt) sales tactics.

The SBE will progressively reduce risk as managers can be convinced of the needs, and as the business (and profit) grows. They will decide whether the business can manage (or suffer the consequences of) the risk effectively internally.

Communicate Security Concepts

It is important for the SBE manager to understand some high level concepts of security in order to make solid decisions. The following concepts are presented in a non-technical straightforward manner. Security needs to be understood by management if they are to invest in it. We don't want to scare them!

- Security is not an "open door/closed door" issue

  Security is not about open and shut. It's about how closed the door should be to reduce the business's risk. This will depend on the nature of the business and is for every business to decide.

- Security is a Process

  The concept of "Security is a Process" is not communicated to managers. Product vendors outline a real security issue and convince the SBE managers that "Product XYZ" addresses meet their needs and will provide an excellent solution. The expectation by the SBE manager is that nothing is required but purchasing and installing the product.

  Because most products are pitched in this manner, it makes it considerably more difficult for security professionals to convince managers that "Security is a Process". Many businesses with security products such as firewalls and antivirus have suffered breach and intrusion subsequent to installing a product due to lack of a sound process.

- The Attack Process

  Conceptually, managers tend to view that their security product stops a particular attack i.e. a firewall stops Internet hackers, antivirus packages stop viruses.

  They also tend to be limited in their understanding of the criticality of attacks, and that minor attacks and breaches can be part of a far larger attack strategy. It is important to ensure the SBE manager understands the principles of an attack strategy. To aid the explanation, we use the door open/closed principle.

  Security is not about "closing the door". It is about deciding how far closed you want the door to be. The attackers' attack process is to assess how far to being closed the door is. Then, they open the door bit by bit at a time, possibly using a variety of attack techniques, until they have achieved the compromise they desired.

  An attack strategy may involve a combination of attacks such as network level attacks, web server compromises, taking advantage of poor coding, and password cracks. It is for this reason that managers need to

understand the importance of protecting the business with Layered Security (Defence in Depth).

- An Attackers Tools

  There are now a variety of hacking tools and toolkits freely available (and constantly updated) on the Internet. Examples include Nessus and Nmap as some of the most well know names. The tools are easy to configure and can be automated to attack an entire address space (like a section of the telephone book).

  This is why SBE businesses are attacked. They are an Internet address, not a name or a business, and the tools target Internet addresses.

Risk Implications

Risks to the SBE are the same as for larger businesses. However the SBE is often far less insulated to the subsequent effects of a breach, and generally has fewer resources to cope with the reactive and business implications.

Typically, SBE's have a core set of Internet services being provided to the business. When introducing or reviewing Internet security with the SBE manager, these must be ascertained and used to explain the implications

- Bandwidth theft

  Bandwidth theft occurs when a business system is compromised and your bandwidth is used by the attacker for his own purposes. The bandwidth is not available to the business, and performance degradation can occur affecting users. Typical examples include:

  a) the attacker using an insecure disk to upload illicit files (pornography, pirated software), publishing the business IP address to the Internet for anyone to upload

  b) Compromised systems being used as zombie hosts used to attack other organisations.

- PC and Server Downtime

  Attacks can affect system stability and cause unplanned system business downtime. Attackers may well be able to access, modify or delete key files, including system files, prevent PC's and servers from booting. Rebuild and reinstallation is the most common course of action in these situations

Many issues arise from this such as additional IT support costs, time consuming demands on internal support people and often corruption of data. Systems can be down for days during the recovery process.

Note that unless the cause of the breach is identified and rectified, the attacker could repeat the entire process again until the business is appropriately detected.

- Loss of Employee Productivity

  Employee productivity issues arise in two main areas:

  a) Loss of productivity due to system downtime

     System downtime results in an increased employee cost. Not only are employees not as productive, but also time is required to complete backlogged work. Note this not only applies to issues cause by compromise or DoS from the Internet, but also system failure.

     Run through a typical cost scenario with a SBE management. Let the manager provide his or her own figures, and you can do the math. This is not intended to be a robust analysis, but to demonstrate to the manager a SLE (Single Loss Expectancy) estimate. In depth SLE can be derived during a audit and review process [7].

     Every business can calculate an apportioned cost per employee (total operational cost / number of employees). This can be converted into an hourly rate. Call this figure the ACPE.

     Most SBE managers will claim that employees do something else during downtime. This is true although it is not usually directly productive. Most managers will agree that productivity would average around the 50% mark but it's up to them. Call this figure APR.

     Agree to a typical number of hours downtime. I suggest a 8 hour day as this is a reasonable time for a straightforward server full system rebuild and restore. Call this figure H.

     The last figure you need is number of employees affected. Note that although some employees may not have computers, their job function requires computer output. A good example maybe warehouse order fulfilment. Call this figure E

     Productivity cost = ACPE x APR x H x E

     A "catch up" percentage can be added to this figure, although many SBE managers will express that employees will make up the work in their own time.

  b) Loss of productivity due to inappropriate web browsing or email

Unproductiveness from inappropriate Internet use during working hours is now a significant management issue, and a burgeoning market for Content Management solutions from companies such as TrendMicro, Websense, NetIQ [14] and a host of other security vendors.

Many SBE managers will claim to manage it themselves. However, with personal web browsing, personal email, Internet banking, shopping, most companies are incurring employee costs.

Many SBE managers will state that staff Internet access is part of the company culture and that it's a company cost. This can be challenged in a non-confrontational manner to ascertain whether management realise the cost implications they are committed to in the name of "culture". Calculating an Annual Loss Expectancy estimate for the average employee's loss of productivity can be easily achieved.

SBE managers will have a "gut feeling" of the amount of non-productive Internet activity employees do. Generally this activity happens for 5-10 minutes 3-4 times per day and most managers will agree that is appropriate. Note that most employees will not do this personal browsing during their lunch hour.

Add the minutes per day together. I find that 30 minutes per day is not unreasonable, although can be talked down to 15 minutes (with some scepticism I might add). Call this figure M

Productivity Loss = M x 20 days per month x 10 months of work / 60 (minutes per hour) / 8 (hours per day)

Based on 30 minutes per day, this equates to 12.5 days per year of unproductive activity. Would manager give an employee an extra 12.5 days leave? The answer is resoundingly no – this is a massive cost implication for the business.

Many firms such as NetIQ offer online ROI calculators for management of employee productivity [10].

- Production Delays and Costs

  Many manufacturing businesses are productionised with PLC's and computers driving them. A compromise of internal systems by an attacker can have a devastating impact on manufacturing. Systems halts and restarts can be a huge cost of resources and raw material wastage.

- Confidentiality Breach

An attacker may be able to access confidential files, email or databases that contain commercially sensitive, personal information, or client information [11]. This can arise from poor internal system security or password files being cracked allowing the attacker into the system.

These types of breaches can be hard to identify and losses are harder to calculate commercially. However this situation can lead on to the next point.

- Negative Media Exposure

  The media love Internet attack stories. These can be disclosed anonymously by the attacker, by internal personnel, or even by clients who have been approached by the attacker with proof of breach. Antivirus mass mailers can cause significant embarrassment and effectively publish to the SBE clients and suppliers the breach of security.

  All businesses carefully nurture and grow their reputation and build client trust. Entire years worth of marketing campaigns can be lost by a single attack event that makes it to the public arena. This can cause a direct reduction of sales and profit as client confidence drops. [9]

These are the main direct cost implications that a SBE may face, although it is by no means exhaustive. These contribute directly to the bottom line, although some are tangible and some are intangible and harder to measure.

SBE managers need to recognise that some of these apply to their business. Without a need being recognised by management, it is impossible to further security initiatives.

Introducing the Vision and Strategy

Introducing security to the SBE will vary completely on the type of managers being presented to. Each manager has their own focus and drivers. These need to be identified and need to be catered to. Presentations need to suit the level that the decision makers have [4]

Management needs to be convinced that issues exist in their business, and that risks presented to them are pertinent.

- Remember, the first goal is to educate.

  This may require effort as the expectations of what security solutions should do have been set from a product perspective. Security is a process is the key concept they need to understand, and what can go wrong without it. Try an analogy using their business (example follows).

Most businesses have an accounting software package. By itself, it does NOT ensure you have trouble free accounts and end of month processing. If it's not set up correctly in the first place, it won't report the right information. Once the accounting software is setup, the business builds processes and checks to ensure that key functions and reports (bank reconciliation, trial balance, compliance etc) are operating correctly, and the trained accountant identifies and fixes any problems.

Security products are much the same. Without the processes and people trained in the specialist area, there is no information what is really happening and whether something should be done about it.

There are multitudes of ways that the wrong information gets into the accounting system, inadvertently through lack of training, lack of processes, errors, and occasionally - deliberate accounting errors. Some of these methods are complex and can take weeks of specialist forensic analysis to identify.

Like the accounting systems, there are multitudes of threats from the Internet and although the business may have some form of security, who is looking after it? Unlike the accounting system however, events on the Internet are real time – happening second by second.

- Get top level management involved early on in the process

  Everyone knows that unless the top level management is committed to the security principles that may affect other aspects of the business, it is very, very difficult to succeed.

- Present a Vision and a Strategy

  It is important at the outset to present a vision, a goal, of where the business should be heading. With smart thinking and little additional cost, they can progressively integrate "best practice" security principles to the business to manage Internet risks.

  The vision should be one of Layered Security, with management receiving monthly activity reports that summarise activity, alerts, actions and recommendations for any threats or incidences that occur.

  A typical SBE security strategy will include policy, awareness, risk assessment, technology and process [5].

  Commence with plain English policy definition. All managers should be able to understand and approve what is going in and out of the business Internet connection. Where 3rd parties are involved in accessing business systems, additional policies and inter-connect agreements should be considered.

Reviewing areas of risk and hardening existing Internet facing systems should be undertaken.

Once completed, options should be considered for technologies that address the security risks, and how the on going management of the Internet facing systems will be approached. Outsourcing Internet security is a realistic approach for the SBE [12].

Antivirus solutions should be reviewed to intercept viruses at the Internet perimeter, although desktop solutions should be included as virus scanners are not able to open password or encrypted files for scanning. These are opened at the desktop, and it's the desktop scanner that is the last line of defence again viruses.

Firewall requirements should be identified early on. Many SBE's have minimal requirement for open inbound ports (often only SMTP is required) and firewall can provide immediate protection to the business infrastructure.

Management of employee Internet access should be considered. Commence tactically with a policy, which is required in any case. Should policy be insufficient to manage the problem, solutions to manage usage should be investigated. Specific features should include allowing personal sites to be access at approved times (lunch hours, before and after work) to maintain the company culture.

Supporting processes should be documented and implemented for reporting and Incident Handling. The objective is to ensure issues are identified, reviewed and action taken as required by the appropriate resource.

Other important solutions should be included but at a later date. Modems, intrusion detection, remote access policy are all parts of perimeter security. Internal security must be considered in the vision and strategy to introduce Defence in Depth and protect internal systems should the perimeter be breached. This would include password standards, hardening internal PC's and servers and reviewing access controls.

- Don't use Fear, Uncertainly, Doubt (FUD)

  FUD is now considered a complete oversell or over-scare by many managers [6]. Any FUD approach stands a strong chance of being rejected, and this can affect your credibility in trying to deal with a genuine risk the SBE may face.

  Talk "best practice" and use risk examples based on the business drivers goals.

- Don't try do it all at once

  Make security a long term plan and prioritise the strategy. Like everyone, SBE's have a limited funds that need to be wisely spent where it will do the most good.

  Plan and align with business growth and replacement of systems.

Conclusion

Security for Small Business Enterprises is a growing issue as they embrace the Internet without understanding the risks to the business.

SBE managers have different drivers in dealing with business issues such as Internet security and risk management. It is essential that they understand why securing the business from the Internet is important and what the implications are should they not decide an appropriate security strategy.

Security is a management issue. Communication to SBE management should be high level, incorporating analogies, concepts and direct risk management examples.

Most security statistics and research available pertain specifically to Enterprise and governmental organisations [13]. Consequently, most SBE managers believe that the statistics and issues relevant to the larger businesses are not particularly relevant to the SBE. References to issues and risks should reflect similar SBE sized businesses, rather than an enterprise business.

SBE managers need to see a relevance to their operation. In recognising and addressing the SBE needs, you can re-educate and present the risks specifically for the SBE and set a holistic "best practice" vision. Many SBE's can be moved from a poor security posture to a solid Defence in Depth implementation with the appropriate approach.

References

[1] American Express. "OPEN Small Business Network Semi-Annual Monitor". 22 October 2002 http://home3.americanexpress.com/corp/latestnews/osbnm2002.asp (28 April 2003)

[2] Tolly, Kevin. "'Always on' programs pose an 'always on' threat". 30 September 2002 http://www.nwfusion.com/columnists/2002/0930tolly.html (28 April 2003)

[3] Rowland, Carolyn. “Selling Security to Management in a Low-Risk Environment”. April 12, 2001
http://www.sans.org/rr/start/selling_sec.php (27 April 2003)

[4] Hall, Jeff. “Selling Security To Management”. 25 July 2001
http://www.sans.org/rr/aware/selling_sec.php (27 April 2003)

[5] Shaffer, David A. “Small Business Technology: Learning To Deal With Internet Threats”. February 2002
http://www.bizmonthly.com/2_2002_focus/f_22.html (26 April 2003)

[6] Naraine, Ryan. “Banking on Fear?”. 12 February 2003
http://boston.internet.com/news/article.php/1583201 (27 April 2003)

[7] AllState Technical Services. “White Paper on Information Security Auditing / Implementation Procedures “. November 2002.
http://www.allstatestech.com/pdf/Information_Security_Auditing_White_Paper_v3.pdf (27 April 2003)

[8] Information Services for Profit. “Broadband ADSL - The Guide for Small Businesses” 2003
http://www.is4profit.com/busadvice/broadband/ (28 April 2003)

[9] Larkin, Judy. “Strategic Reputation Risk Management”. ISBN: 0333995546

[10] NetIQ. “Return On Investment Calculator:
http://www.webmarshall.com/ (28 April 2003)

[11] BBC. “Patient confidentiality 'at risk on internet'”. 18 November 1999
http://news.bbc.co.uk/1/hi/health/525091.stm (28 April 2003)

[12] Gartner Group. “SMB’s: Consider outsourcing your firewall protection”. 13 May 2002

[13] Computer Security Institute. “2002 Computer Crime and Security Survey”. 7 April 2002
http://www.gocsi.com/press/20020407.html (29 April 2003)

[14] TrendMicro: www.trendmicro.com
Websense: www.websense.com
NetIQ: www.netiq.com

[15] Spyware Guide
http://www.spywareguide.com/ (29 April 2003)

Last Updated: July 23rd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor