INFORMATION SECURITY

IT SECURITY

A STEP BY STEP GUIDE FOR GROWING BUSINESSES

STAGE 2: CUSTOMISING THE SECURITY ESSENTIALS FOR YOUR BUSINESS

www.jlis.co.uk
john.leach@jlis.co.uk

ABOUT THE AUTHOR

John Leach has been an Information Risk and Security professional for more than 20 years. He has held senior positions in the security teams of several organisations, including NatWest Bank, and has directed the security teams of a number of boutique technical consultancies. In December 2002, he formed his own company to enable him to provide consultancy services independently.

John Leach has an academic scientific training. Many of the services he provides build on his ability to analyse security data, model the dynamics behind security risk, and quantify how the countermeasures people apply measurably reduce the security risks they face. He has been an active member of the Management Committee for the Information Assurance Advisory Council (www.iaac.org.uk) continuously since May 2002, and is a member of the International Board of Referees for *Computers and Security*.

This paper would not have been so well informed as to the profile of today's threats without the assistance of Symantec Hosted Services and the global threat data they provide through MessageLabs Intelligence. Given the nature of its hosted services, Symantec is in an excellent position to capture an enormous amount of homogeneous data about internet-borne security threats. This huge volume of clean data can be used to generate valuable security insights, objective insights based on hard data rather than the more subjective insights, usually based on small-sample surveys or averages across widely diverse data, to which we are normally limited. I am grateful to Symantec Hosted Services for allowing me access to their MessageLabs Intelligence data while I was writing this paper.

Dr John Leach

www.jlis.co.uk
john.leach@jlis.co.uk

MANAGEMENT OVERVIEW

Most SMBs find that their security needs are not well catered for by the marketplace. There is ample detailed technical security advice available for large enterprises with deep pockets and the need for their security to be comprehensive. However, organisations with more limited needs and resources often find it hard to find guidance on what to prioritise and where to draw the line. If they are to stop short of trying to do everything contained in the security pantheon that their larger brethren might take on, then what security controls do they discard? And doesn't that make them hostage to fortune, open to accusations in retrospect that they had fallen short on their security duties if the organisation ever gets hit by a security problem?

This White Paper has been written for those organisations that do not have deep pockets. It sets out a flexible three stage approach that helps organisations sort out what their security priorities should be. It sets out a baseline of security controls that all organisations should apply, and shows how those organisations can build on that baseline, maximising the security protection they can gain from each additional security step they take. Each organisation can set the height of its security bar at the level that is right for it today, and can raise that bar if it needs to as their business grows and their security needs evolve.

This is Part 2 of a 3-part paper. Part 1 introduced the three-stage approach, summarised the threat landscape, and described the first of the three stages. It detailed the essential basic security controls that all organisations need to have in place as a minimum. Part 1 can be downloaded from www.messgaelabs.co.uk/essentials, as can Part 3. This, Part 2 of the paper, describes the second of the three stages. Before organisations that have completed Stage 1 proceed to take on a wider range of security controls, they should customise the Stage 1 controls to maximise the return those controls provide. In this paper we will describe how to do that. Every organisation should make a start on Stage 2 even if it decides not to make it through to the end.

STAGE 2: CUSTOMISE THE BASICS

Stage 1 is much the same for every organisation: putting the basics in place and making sure they are working properly. Stage 2 starts to differentiate between organisations. Before taking on a wider range of security controls, organisations should stick with the same list of basic controls but work them harder to get the maximum out of them, doing that in a way that starts to reflect the differences between individual organisations.

There are two sets of questions that drive Stage 2. The first ask how much damage the organisation believes it could realistically suffer if it had to face each of a number of serious security scenarios? The second asks what level of security exposure does the organisation face? An organisation's answers to the first set of questions will enable it to decide which security measures to prioritise over others. Its answers to the second set will show how high overall it needs to set its security bar.

HOW MUCH DAMAGE IS POSSIBLE?

The next page contains a table that shows each of the damage questions and each of the basic security controls discussed in Stage 1. Each damage question asks the IT Manager to give their organisation a score between 1 and 3 for how disastrous it could be for their business if that scenario took place. Alongside each scenario are ticks to show which of the basic security controls should be strengthened if that scenario warrants a score of 3. We will describe how to use this table in a moment. IT Managers may wish to print out the table so they can record their answers on it as they work through the questions.

With the damage questions, the IT Manager gauges roughly how bad the business consequences of a serious security incident might reasonably be given the type of organisation theirs is. The scenarios have been arranged into three security dimensions: A for Availability; I for Integrity; C for Confidentiality. For each question, the IT Manager rates how disastrous it could be for the business, on a scale of 1 to 3, if that scenario took place. The key is to base the ratings on the possible business impact and not to worry at this stage about what would have to happen to cause that scenario to take place. A 3 rating means that the scenario would be a big disaster for the organisation, the business would be as badly hit by that security incident happening as it would be by a major disaster happening in some other non-security area. A 1 rating means the scenario would be a sizeable bump in the road but the business would be able to carry on adequately whilst the problem was being corrected. The scenario lists below can be customised if wished by adding further scenarios for each dimension, scenarios that reflect the type of organisation being considered and the ways that a serious security problem could materially affect the business.

Record your organisation's score on the table against each of the Damage questions. Some organisations need to be better at some aspects of security than others. Your organisation's scores will tell you which aspects of security your organisation needs to strengthen most.

The table shows, alongside each Damage question, which controls should be prioritised if that Damage question warranted a score of 3. For example, if your organisation scored a 3 on the first question because it has a strong need to avoid having its network down for a long time, then the controls to strengthen the most are those that have ticks in that row, namely the anti-spam, anti-virus, firewalls, patching and scanning controls. If your organisation scored a 3 on the second question, then the controls to prioritise are the authentication and access controls, security culture and AUP controls.

For each question that attracted a score of 3, look along the row to see which measures are ticked and then put a tick in the bottom row of the table (Measures to prioritise) under that measure. That way all the measures that need to be strengthened in response to the main ways your organisation can be damaged by security problems will get ticked in the bottom row. That provides a basis around which to build a Stage 2 security plan.

WHAT IS YOUR LEVEL OF EXPOSURE?

After the first table is a second table that shows the questions relating to exposure. With this second set of questions, the IT Manager gauges how exposed their organisation is to security threats generally and how sensitive the business is to any security breaches that might occur. These questions get scored on a scale of 1 to 3, as before. Again, further questions can be added if that helps reflect the ways the organisation uses its ICT.

Your organisation's exposure rating is the average of its scores for the six exposure questions in the table. The higher the organisation's average score on the Exposure questions, the more the IT Manager should work to raise the overall security bar, i.e. to strengthen the Stage 1 security controls across the board. This paper will describe how to do that shortly. The lower the organisation's average score, then generally the more the organisation can afford to leave the baseline controls as they were at the end of Stage 1, just making sure they are all being done properly. A score of 2.3 or above is a high score.

Security Measures		Back-ups	Anti-Spam	Anti-Virus	Firewalls	Authentication and Access Control	Logging	Patching	Vunerabilty, config. and s/w scans	Security culture	AUP	Clean out zombies
Damage Questions	Score (1-3)											
A1 Your organisation lost its main internal office network for a whole day (for whatever reason)?			✓	✓	✓			✓	✓			
A2 Your organisation lost a large chunk of its client or customer data and it took 24 hours (elapsed) for it to be recovered?		✓				✓	✓			✓		
A3 A central billing system crashed and you couldn't say to start with how long it might take to get it back up and running?		✓		✓		✓		✓	✓			
A4 A routine overnight IT maintenance process went haywire and 20% of your end-users had to wait two hours at the start of the day before they could use their PCs?		✓				✓			✓	✓		
I1 One or more of your organisation's important internal systems were showing traces of having been broken into at some stage recently and you couldn't immediately work out what the hacker might have changed or done?			✓	✓	✓	✓	✓	✓	✓		✓	
I2 A backup went wrong and instead of backing up to a recycled tape it wrote the old contents of that tape onto live systems?		✓				✓						
13 An important customer complains that your organisation has been mischarging them and your initial investigation indicates someone might have been involved in some kind of data fraud?						✓	✓				✓	
I4 One or more of your organisation's machines seem to have decided to send out tons of spam overnight and now your domain has been blacklisted and all your e-mail is getting treated as spam?			✓	✓	✓		✓	✓			✓	✓
C1 Details of your organisation's input costs and product margins became public knowledge to its customer community?					✓	✓	✓	✓	✓		✓	
C2 One of your customers was sent details of the work being done for another customer, including that customer's proprietary financial information?						✓				✓	✓	
C3 A senior staff member reports that a key management system they use seems to have been accessed by somebody else and some sensitive business plans and financial figures could have been exposed?					✓	✓	✓	✓	✓		✓	
C4 Options being debated internally about a reorganisation and cut-backs got leaked to shop-floor or front office staff?						✓	✓				✓	
Measures to Prioritise												

www.jlis.co.uk
john.leach@jlis.co.uk

WHAT IS YOUR LEVEL OF EXPOSURE?	EXPOSURE SCORE			YOUR SCORE
How immediately would the business be affected by a security problem in its ICT infrastructure?	ICT is used primarily for general administrative purposes and is not central to core operational processes.		It would be affected immediately (e.g. the business is built around the provision of real-time or just-in-time services to clients or customers)	
	1	2	3	
What is the average number of incoming non-junk e-mails per day per member of staff?	0 – 5 e-mails	6 – 10 e-mails	11+ e-mails	
	1	2	3	
What is the average amount of time spent on the Internet per day by staff?	< ½ an hour	½ an hour to 2 hours	more than 2 hours	
	1	2	3	
Does your organisation have, or would an outsider expect it to have, highly sensitive and exploitable data (e.g., government, commercial, personal financial or personal health data)?	No		Yes	
	1	2	3	
Does your organisation have a highly mobile workforce?	IT is essentially all static and office-bound		Laptops are continually connecting in from outside	
	1	2	3	
Does your organisation have ...	A stable base of loyal permanent staff and little use for non-permanent staff		A high proportion of temporary, contract or recently taken on staff (e.g. TUPE[1] staff brought in from another employer)	
	1	2	3	
			AVERAGE EXPOSURE SCORE	

[1]TUPE stands for Transfer of Undertakings (Protection of Employment) – the regulations that come into effect when one organisation, such as an outsourced service provider, takes on a chunk of another organisation's staff

www.jlis.co.uk
john.leach@jlis.co.uk

SO WHAT DO THESE SCORES TELL IT MANAGERS?

Broadly, the Exposure scores tell the IT Manager how much to raise the level of all security controls together. The Damage scores point to which particular controls should be prioritised over others.

Some security controls, generally the majority, work to reduce the likelihood of security accidents or breaches from happening. Others work to help reduce the impact of security problems when they do happen. For example, a look at the list of controls in Stage 1 will show that all but two of the controls (backups, logging) work to reduce the likelihood of problems happening. It is when organisations get beyond the basics (Stage 3 and beyond) that they start to bring in more of the controls that reduce impacts.

One small word of caution. Use the table as guidance, not as a precise specification of what to do. Security is not (yet) a science. No one can say that an unticked security measure adds nothing to help protect against the scenario in question, or that precisely defined scenarios tailored more closely to what each organisation does and how it uses its ICT would not lead to a slightly different set of priorities. Use the table as the starting point for building a Stage 2 security plan, not as the end point.

STRENGTHENING THE BASIC CONTROLS

For most of the security controls in Stage 1, strengthening that control means simply paying more attention to how it is being done, monitoring it more closely, updating it more frequently, and so forth. However, for some of the Stage 1 controls, there are further things an organisation can do to strengthen that control, and these are things the IT Manager should consider if that control was ticked.

ANTI-VIRUS, ANTI-SPAM, FIREWALLS

Perhaps the single most effective way an organisation can strengthen these three baseline security controls in one step is to take on 'hosted security' or security as a service. The sophistication of generic technical security threats has now become so great that conventional product-based blocking solutions (anti-virus, anti-spam, firewalls) are getting left behind.

Over the past couple of years, malicious code has become easier to cloak, meaning it gets past commercial blocking products more readily than in previous years[2]. It has become better at exploiting vulnerabilities, making any chink in the organisation's armour a dangerous weakness. And payloads have become stealthier, so once dropped they are harder to find.

Whether looking at anti-spam, anti-virus or the firewall blocking of malicious URLs, the list of today's bad software and bad sites changes so rapidly that even the best commercial products can never do more than chase hard to catch up. Hosted security from a proven provider leverages the dedicated expertise of a specialist provider to offer a level of protection far superior to that any organisation can achieve using commerical products it runs itself. The extent to which this has become the case has been shown recently in some research I undertook that pitched a service provider's hosted e-mail service against a combination of leading commercial AV products. The service provider's malware protection won by a staggering margin[3].

The results make compelling reading. From that research's results:

- For large organisations of 500 or more staff, their total daily e-mail volume is normally sufficiently high that the margin of difference between hosted and commercial products makes hosted security a no-brainer for them. If your organisation is of this size, then look very very seriously at my research's and at using a hosted security solution.

[2]Symantec, for example, produced more malware signatures last year than in the previous 20 years put together!
[3]The Accuracy Project – John Leach, 2009: http://www.jlis.co.uk/Papers/JL_Accuracy_Project_Slides_081203.pdf plus the three papers that follow on the page.

- Micro organisations (fewer than 25 staff) normally have much lower total e-mail volumes. Consequently, their exposure to malware is much lower. The research showed that commercial products could keep micro organisations safe roughly three years out of four. Each micro organisation has to decide whether having a major malware incident on average one year in four is acceptable to them or not. If not, they should consider taking on a hosted security solution.

- For organisations with more than 25 staff, the protection afforded by hosted security can make a significant difference to the real annual infection rates they experience.

In addition to these research results, a tipping point has now been passed. Over the past five years, so many large organisations have overcome their initial nervousness and taken up outsourced security, that hosted security service providers can now offer SMBs economies of scale that were previously unavailable to them. Any large SMB, or any small SMB that scored any 3's in the exposure questions, should take a serious look at hosted security. It could make an enormous difference to the organisation's security resilience.

For an organisation that decides it is not ready to move to hosted security yet, there is an alternative by which it can strengthen its level of AV protection. That is to use two leading brands of commercial AV software, one at the network perimeter and a different one on client machines. It does actually make a lot of difference to have two products in tandem, it isn't just duplication and a waste of good money. Each product needs to be set to update automatically at least once a day, and if the update frequency can be made more than once a day then all the better.

I am not convinced there is any other worthwhile option for strengthening malicious URL blocking besides using hosted security.

OTHER STAGE 1 CONTROLS

We shall look now at how some of the other Stage 1 basic security controls can be strengthened.

PATCHING

For patching, once you have established a regular patching cycle, the most valuable next step to take patching to a higher level is to perform a simple High / Low prioritisation of patches and to develop the ability to apply high priority patches on a faster time scale.

Most patches will be normal priority patches that can be applied under your normal patch management regime. But every now and then, a patch comes out that needs to be given a higher priority. For example, a patch to close a zero-day vulnerability that is already being actively exploited in the browser you use. Develop the ability to recognise a high priority patch when it comes out and to rush those through straight away rather than leaving them to wait for the normal patching window. The SANS @ Risk security alerts are great for exactly this type of High / Low prioritisation.

USER AUTHENTICATION

For user authentication, people are now used to seeing 'password strength meters' when they register and set up an on-line account on a web site somewhere. These are those 'slidey bar' graphics that show how strong a chosen password is based on its length and whether it contains numerals or symbols as well as letters. Users are realising that choosing a decent password is not difficult and just takes a second or two of thought. Bring that graphic into the work place. There are plenty of free scripts or gadgets available over the Internet that show a password's strength, and a quick search should identify one that can be run in-house.

VULNERABILITY SCANS

From Stage 1, your organisation will be checking for ICT vulnerabilities on a regular basis and chasing up persistent vulnerabilities that don't seem to be getting fixed. Create and distribute a league table of which vulnerabilities have been around the longest without being fixed. That way those parts of the business or those parts of the ICT estate that are not dealing with vulnerabilities well can see that they are persistently to be found at the bottom of the table and are letting the side down.

SECURITY CULTURE

For building a stronger security culture, the attitude adopted is all-important. So often, security is treated like a nasty disease: nobody wants to get near it, nobody wants to talk about it. People need to get over that hurdle. That can take a bit of time, but persistence will pay handsome dividends in the end.

Bite the bullet and talk with staff openly about the organisation's security concerns and what can be done to make a difference. Work with staff to address the points they raise and try out the good ideas they come up with. They will soon come to realise that talking about security doesn't mean that staff or other people aren't trusted, and that making security part of everyone's daily regime isn't simply a way for the IT Manager to pass the buck to everyone else.

ENCRYPTION

There is one security control that wasn't on the list of Stage 1 basics that should be brought in at this stage if your organisation's profile suggests it is needed. That is encryption. If your organisation holds any sensitive personal data, encryption really does need to be considered. With so much visibility being given these days to organisations that lose personal data, and with the increased powers that the ICO has had since April of this year, no organisation, however small, can make excuses for not protecting the sensitive personal data it holds. Encryption doesn't solve every aspect of the problem but it is just about essential for those organisations that handle sensitive personal data.

Personal data includes personal data about staff as well as any personal data held about customers or other people. Sensitive personal data needs to be encrypted whenever it leaves the organisation's controlled premises, and ideally it should be encrypted within organisation-controlled premises too.

When used properly, encryption can be a powerful tool helping to secure access to sensitive information. Unfortunately, it is not trivial to apply encryption to every channel through which in-formation can be taken, meaning there will always be some ways that sensitive information can exit your organisation unencrypted. Therefore, it is important for encryption to be backed up with other data loss prevention controls.

- Organisations should develop and promulgate clear internal policies regarding the protection of personal data.
- They should monitor and, where they can, block, the copying or transmission of data in violation of those policies.
- They should use access controls and logging to maintain visibility and close control over personal information that hasn't been approved for external distribution.
- And they should make staff aware just how badly the organisation would be hit by a mistake that led to the loss of personal data. Everyone has a clear responsibility to be careful and stay vigilant.

WRAP UP

A final word. Revisit your Stage 2 thinking periodically. One of the strengths of SMBs is their ability to grow and change rapidly. Look at how your organisation is changing with time. Have its damage or exposure ratings changed since last time you looked, or are they likely to change over the coming six months? Are staff numbers growing? Is the number of servers being operated on the increase? Is the organisation's ICT becoming more complex or difficult to manage? As the organisation changes so too will its security needs and these should be reflected in the security programme.

And one of the things that makes security particularly challenging is that threats can grow and change rapidly. Even if the business does not change much, the threats faced might. Develop a list of your favourite security news and discussion sites (I have mentioned MessageLabs Intelligence and SANS already, but there are plenty of other good sites out there too). Track what they are talking about. Think if it affects you. Act if it does.

NEXT STEPS – MOVING ON TO STAGE 3

Part 2 of our guide to IT Security has described how organisations can develop a security profile for themselves that shows which of the Stage 1 controls they most need to build up and strengthen. Part 3 is aimed at those organisations that have worked through to the end of Stage 2 and find they still have some fuel left in the tank, organisations that are ready to look at what else they might want to be doing over and above the Stage 1 basics, and want to know how to go about shaping the next stage of their security journey. Stage 3 can be downloaded from www.messagelabs.co.uk/essentials.

HOW SYMANTEC HOSTED SERVICES CAN HELP WITH YOUR SECURITY ESSENTIALS:

Symantec Hosted Services, is a leading provider of hosted messaging and web security services, with over 30,000 clients ranging from small businesses to the Fortune 500, located in 99 countries.

Our core offering is MessageLabs Security Safeguard, an integrated service which combines email security with web and IM protection. All-round defences like this have significant benefits:

- Cost effective security across email, web and IM from a single supplier, with full 24/7 support
- Protection against new and emerging threats, 'in the cloud' before they even enter your network
- Policies applied across email, web and IM to prevent IT misuse and enforce acceptable use
- Unrivalled spam & virus capture rates
- Quick and easy set-up

We secure more than 3 billion email connections and one billion web requests every day for businesses all over the world. As the leading provider of hosted security services, we are likely to see emerging threats soonest.

MessageLabs Security Safeguard runs in our data centres, so it doesn't require lots of expensive capital equipment on your premises. We take care of maintenance, availability, updates and patches, and provide full 24/7 support to all our customers, no matter how big or small they are.

Our approach makes it easy for us to support multiple offices and remote users. It also means that internet criminals can't download our software and use it to test their malware. It's an integrated solution from a single supplier which gives you easier management, a single management console, better reporting and economies of scale.

You can trial our service for free – simply visit www.messagelabs.co.uk/trials/web_smb

>EUROPE
>HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733
Support: +44 (0) 1452 627 766

>LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

>NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 1452 627 766

>BELGIUM/LUXEMBOURG
Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

>DACH
Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

>AMERICAS
>UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

>CANADA
170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

>ASIA PACIFIC
>HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

>AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

>SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

>JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130

symantec™

Confidence in a connected world.