WHITEPAPER

INFORMATION SECURITY

IT SECURITY

A STEP BY STEP GUIDE FOR GROWING BUSINESSES

STAGE 3: FILLING IN SECURITY GAPS

AUTHOR: DR. JOHN LEACH, SECURITY RISK CONSULTANT

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 3 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 2 described the second of the three stages, how organisations can develop a profile of their security needs and then customise those basic security controls to reflect that profile. Parts 1 and 2 can be downloaded from www.messagelabs.co.uk/essentials. This, Part 3 of the paper, describes the third of the three stages. Organisations that have completed Stages 1 and 2 can find out how to identify where there is a mismatch between their security needs and their security provision and can start to take on the additional controls that will do the most to strengthen their security posture.

Stage 3

Switch on the lights

- Activity logging
- Vulnerability checks
- Security Incidents Register

STAGE 3 – START TO FILL IN THE GAPS

Stage 3 is mainly for larger SMBs and those with information "crown jewels" they need to protect. It is where organisations start to broaden out the range of security controls they apply, dealing with a wider range of threats to their more complex operations and systems. As with the transition from Stage 1 to Stage 2, the transition from Stage 2 to Stage 3 should not be undertaken until the Stage 2 controls have been well bedded in and shown to be effective.

As mentioned at the start of this paper, large organisations can take Stage 3 a long way. There is no end to the security measures they can apply to keep the large attack profile they present resilient to all the attacks they face. This paper is not aimed at helping them. It is aimed at those who have got what they can out 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.

SWITCH ON THE LIGHTS

Where Stage 1 was the same for every organisation, and Stage 2 started the differentiation, Stage 3 can mean very different things for every organisation. Stage 3 is fundamentally about how each organisation can work out, of all the many tens of extra security controls they could apply[1], which are the ones they should bring in next. Which are the controls that are right for them, so they can raise their security bar, progressively building on what they are already doing in a way that makes the most sense.

For Stage 3, organisations need to do what I call "Switch on the lights". If someone walks into a totally darkened room and has no idea what might be in there, it is not going to be long before they crash into a heavy piece of furniture or trip over something on the floor. They need to switch on the light before they can move about in the room. That is what Stage 3 is about in a security sense. Before an organisation can make progress on this next stage of its risk management journey, it needs to switch on the light so it can see which are the security issues it needs to negotiate around first.

There are three lights to be switched on:

- Activity logs to illuminate the threats bearing down;
- Vulnerability checks to illuminate the weak spots in the organisation's ability to resist the threats that are coming at it;
- Incident registers to illuminate where there is a real, rather than just potential, mismatch between security need and security practice.

[1]ISO/IEC 27002, the main international standard for information security controls, lists well over 100 security controls that organisations should consider applying.

Activity logging

The purpose here is to illuminate which of the threats being faced are the most prevalent and most likely to cause the organisation security problems. To do that, an organisation needs to monitor its ICT estate. This includes monitoring activity – the uses, authorised and unauthorised, people make of ICT systems and infrastructure – and monitoring data movements – where information is held, where it goes and with whom it is shared. From this, each organisation will build a profile of what Business-as-Usual looks like for its ICT estate, both appropriate and inappropriate activities. Then it can start to deal with the most pressing inappropriate activities.

Stage 1 identified a number of generic threats that all organisations face. These can be characterised as 'things that come in from the outside', 'things that go out from the inside' and 'things going on inside'. Stage 2 might have helped an organisation to refine its view of the threats and identify particular areas that cause it concern.

To monitor the activity of the threats identified in Stage 1, look to the logs from the countermeasures being used. These are the countermeasures used to stop unwanted traffic coming in from outside (anti-spam, anti-virus, firewalls), those that tell if there is unwanted traffic going out from inside (logging), and those used to stop unauthorised use of internal systems (authentication and access control, zombie detection). If there are any additional threat streams of interest arising from Stage 2, then these can be added in. For each additional threat, identify the primary countermeasures used to address those types of attack, and look to the logs those countermeasures generate.

For activity logging, switch logging on for each of the above countermeasures and then put some time aside on a regular basis to look at what the logs are saying. Log analysis systems can be used to automate much of this work if the logs are large enough to justify the additional costs of these.

Don't spend too much time worrying about what the logs say is being blocked, look at what the logs say is not being blocked. The areas to cover are:

- incoming traffic: look for things of interest such as unusual protocols or sequences of traffic that might indicate external scans or attempts to connect to internal systems;
- Outgoing e-mail traffic: look for interesting files or content going out and interesting destinations (e.g. personal mail accounts, competitor or unusual country domains) that mails are being sent to;
- Internal system and data accesses: who is using systems they shouldn't normally have any reason to use, who is accessing data files when there is no straightforward reason for them to be doing so, or who is saving files locally when the files should only ever be server-resident.

Look to the differences between business hours, out-of-hours, and lunch-time patterns of activity. And look for anything else that suggests itself based on the Stage 2 answers or anything else that, owing to specific ICT or business details, seems of particular relevance to Stage 3.

Having identified interesting, odd or unusual activities, the next step is to follow things up. To start with, a lot of what initially looks unusual will probably turn out to be perfectly legitimate. That provides an opportunity for organisations to learn about how their ICT is actually used by the people it is there to serve. Some activity will be less than perfectly legitimate. Simply by asking questions about it and letting staff know that attention is being paid to logs, much of that activity will go away. And the rest will be activity that warrants more concerted action. Dealing with that forms phase 1 of a Stage 3 action plan.

Vulnerability checks

The purpose here is to find out where there are weak spots in the security armour. As before, the organisation needs to be probing around in the right places and to know what is normal and appropriate and what is not.

The organisation should, from Stage 1, already be checking for ICT vulnerabilities on a regular basis and chasing up persistent vulnerabilities that don't seem to be getting fixed. But there are lots of possible vulnerabilities that these types of ICT scan will not be able to detect. These are the 'people-oriented' vulnerabilities, and to discover these there are two additional things an organisation can do.

The first is to conduct periodic walk-arounds through the office. This is not to name-and-shame individuals who do things like leave their machines logged on when they go out for lunch but to enable the organisation to get an idea of how good or bad daily security practices are across the various parts of the organisation. Examples seen of something not being done right should be addressed at an organisation-wide level rather than at an individual level. If the walk around shows that in one office at least one person seems to be having a problem with one particular important security practice, then the chances are that other people elsewhere are having a similar problem with that one too but that that has yet to come to light. People do not need to be named for them to know they have been identified for doing something wrong. They will know as soon as the organisation says it is taking steps to help improve that security practice.

The second thing is for organisations to talk to their people to find out what security weaknesses their staff see around them. Staff are the best eyes and ears an organisation has, and different staff will pick up on different things. Some will talk about common practices within the office they think are a bit insecure. Others will see a potential security weakness in the way a business process has been designed or put into practice that other people have continually overlooked.

This fits in well with the aim of building a strong security culture across the organisation, and most staff respond well to being asked for ideas provided they feel they are being listened to. People should be given the opportunity to explain why they think something is not right. Often, practice vulnerabilities arise because a business process no longer fits well with how people need to do their jobs. Staff create work arounds that get the job done but happen, unfortunately, to be insecure. Staff shouldn't be criticised for doing that, they are being driven by the need to maintain productivity levels. Fixing the problem will reduce staff frustration as well as make a contribution to the organisation's security.

Dealing with 'people vulnerabilities' forms phase 2 of a Stage 3 action plan.

Security Incidents Register

The purpose here is to identify where there is a real mismatch between the organisation's security arrangements and its security needs, as demonstrated by the real security incidents that happen. In some senses, this is the most difficult of the three lights to switch on, but because it is based on real incidents it is also the most important.

Every organisation has its security failures, most of which never get recorded in the rush to deal with them. The benefits of maintaining a Security Incidents Register in which the details of each incident are captured as it comes to light is two-fold. The immediate benefit is that the incident can be dealt with in a more controlled manner. The longer-term benefit, and its value to Stage 3, is that incidents provide crucial insights that are difficult to obtain from anywhere else. With risk being an amorphous and intangible thing, keeping a register of the organisation's security incidents and, importantly, of the near misses too, is possibly the best means available to putting a face on what the organisation's risks really are and where its security arrangements need to brought up to par.

As with keeping a Health & Safety Accidents Register, the main purpose of the register is to build a corporate memory of what things went wrong when, and for the organisation to learn from its mistakes. There is no automated way to capture incident information, so it has to be captured by getting staff to report incidents as and when they happen. Staff will need to be told (and periodically reminded) that a central Security Incidents Register is being maintained. Also, that the only way keeping a register will contribute to success is if staff take the time to report the incidents they come across. People would normally report anything serious without needing to be told. The emphasis here is to get people to report the less serious incidents too, the 'near misses' (e.g. social engineering attempts that didn't work that time but were convincing for a moment) as well as actual incidents that happen, and the less serious (i.e. those where the organisation was lucky that time and got off lightly) as well as those incidents that delivered a nasty bite.

It is unlikely that there will be large volume of incidents taking place in a short period of time, so it will take time to build up a register with more than just a small number of individual entries. Each entry provides a snapshot of something that went wrong at least once. Several entries together can start to tell a story. And they don't have to be closely related incidents. Each incident is a manifestation of an underlying problem, and an underlying problem can manifest itself twice in two very different ways. For example, if the underlying problem is, say, a tendency for staff still to think that security is someone else's responsibility and definitely not theirs, this could manifest itself as a data loss incident one day and a malware infection the next.

This shows that the key to a successful Security Incidents Register is working out what the underlying problems are that are leading to the various things that are seen to have gone wrong. Sometimes these are obvious, sometimes they are not. Some incidents will be one-off incidents that are unlikely ever to be repeated, others will be indicators of some security measure or control that has been overlooked or is being neglected. The skill, which comes only through practice, is to unpack each incident and get to the problems underlying it. Addressing these problems as they surface then forms phase 3 of a Stage 3 action plan.

FILL IN THE GAPS

With these three lights switched on, an organisation can start to see where it has security gaps that need to be filled. Each individual light will illuminate some of the things that need to receive attention. Looking across the data from all three lights together could provide extra pointers too.

There are no hard rules to be given on how to use the information being built up in Stage 3. Each organisation will see different features and will need to interpret what it sees in terms of its own ICT and business environment. But this flow of information is crucial if it is to understand the contours of the security landscape it faces. Dealing with what these three lights show provides the organisation with stage 3 of its security journey.

CLOSING REMARKS

Security is not easy but it is important, and it can be taken one stage at a time. People shouldn't feel they have to rush to put everything in place all in one go, but on the other hand they shouldn't give security such a low priority they don't get on top of it until it's too late. Most SMBs survive their first major security hit. Some take that to mean that they can get by without having to do much this year, always thinking they might get round to dealing with security properly next year. But they would be making a big mistake. Having the business blown off course by a serious security incident isn't pleasant, and business is never the same afterwards.

Of all the things I have learned over the years, the most telling thing of all is this. If I ask any organisation that has suffered and lived through a significant security hit in their recent past what they regret the most, they will, to a man, say that what they regret the most is not having done more to protect themselves beforehand. They thought they could give security a low priority until the day that backfired on them. Then they realised their mistake. Nothing, but nothing, demonstrates the point more compellingly than that. Security cannot be ignored. It won't make the business, but not having it could break the business.

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.