by Ian Kilpatrick, Chairman, **Wick Hill Group**

Ian Kilpatrick, chairman Wick Hill Group, explains why senior managers now need to be more involved in data security and offers his top tips

The networking environment has changed radically in recent times. In today?s world of increasing wireless use, widespread BYOD, more home working, more remote access, more consumer devices and the huge popularity of social media, the network is becoming ever more distributed. In this situation, security breaches are inevitable, as is evidenced by the regular reporting of breaches at major organisations.

These breaches are of course only the tip of a large cyber-insecurity iceberg. As we have seen from many of the post-mortems, and increasingly senior level sackings, many of the problems relate to poor management and the oversight of relatively junior individuals, rather than a fundamental failure of business security across the organisation.

There is now a growing groundswell of change in the way we approach and look at data security. Clearly, in a world where breaches, and the associated consequences, are inevitable, relying solely on, or blaming, the information security team is no longer viable. With the

business cost of a departmental (or individual within that department) breach now directly impacting business reputations and bottom lines, security needs to come from a bottom-up approach as well as from the CEO down.

Security has often been seen as a business disabler, rather than enabler. It is sometimes seen as a costly nuisance, to be avoided if it impacts projects delivery or performance. The responsibility for all security is often left to the security team. This attitude is now sharply changing in many organisations (particularly those with significant retail or B2B profiles), with a root and branch review of security taking place at many of them.

We?re all (or should be) aware that security is the responsibility of everyone in the organisation, top-to-bottom or vice-versa. But sometimes, in the heat of trying to achieve tactical business objectives, that responsibility gets overlooked.

We are in a time of rapid and brutal change in cyber risks and cyber security failures. Below are reminders of some of the areas we need to revisit and review from time to time, to ensure we?re protecting the company and everyone?s jobs, including our own.

Starting from the premise that, as all the high profile cases have shown (and the significantly greater number of unreported failures), it is now not possible to guarantee defence against data breach. However, it is still possible to defend critical data against breach, if that data is identified and defended.

There's no rocket science here. Just a review and reappraisal, from a business perspective, of what our goals are and what is important, coupled with a desire, through defence and training, to protect it.

Define goals

The first place to look is at what is actually important. ?Everything? is the wrong answer. Priority one is what is business critical or business threatening. This is a much smaller departmental and organisational list. Then decide what risk profile, and associated costs, you

are prepared to accept in order to defend key data, given that the perimeter will be breached. That, almost certainly, will throw up some interesting discussions.

Protect the key data

Decide how to protect key data, rather than just defending all assets and all of the perimeter. Breach defences need to be in place, alongside consolidation and regular reporting, as breaches are now taking longer and longer to detect.

It may also move some defences and focus from broadline perimeter defence to specific areas. All key relevant stakeholders should be aware of the risk analysis and risk acceptance involved. This not only gets buy-in and increased security awareness, it also creates recognition that just having a defence doesn?t guarantee security.

Risk analysis and risk acceptance

Before any mobile device, access, application, new technology or service is added to the company network, it should be signed off as accepted by the Board, and the proposing department or users, with a risk analysis as part of the sign-off. This is a similar process to the previous point and needn?t be too onerous. Interestingly, building-in security, as part of deployment rather than post-event, often provides better security at a lower overall cost.

Planning and deployment

Planning for deployment should include security implementation and acceptance of the risk. Security needs to be deployed with the solution, not post event.

Deployment of security for mobile devices and remote access is a key element in protecting networks today. However this can often be honoured more in the breach than the reality, with individuals and departments seeing security as a disabler, to be circumvented, rather than as an

enabler to be appreciated.

Web applications (and indeed the cloud) present some specific risk points. Understanding and securing data in these areas needs particular focus, based on the risk and consequences of failure. I?ve seen many poorly implemented projects fail through lack of consideration regarding the security implications.

Policies

Given that there is a shift from a belief in security to acceptance that there will/could be a breach, policies need to change to encompass this.

Policies need to be clearly enunciated, not just contained in a policy document.

Given the rapid shift in risks based around wireless, mobility and social media, co-opting some younger staff members onto the team can provide enlightening insights into what the risks really are.

Education and staff involvement

Security processes need to be clear, as do the consequences of not following them. It?s not sufficient to have security policies, if it is clear to staff that you aren?t managing them and that, actually, nothing will happen if they don?t follow the correct security procedures. Education and defence training are essential and should be ?education?, not just a list of things staff can?t do.

This is an easy thing to say, but much harder in practice. It needs leadership from all staff, but especially from all IT professionals. Given the jaded view, sometimes deservedly so, of IT security in some organisations, it is a difficult culture change to now embrace security as everyone?s responsibility. Training needs to reflect that.

Monitoring and feedback

It is crucial to not only monitor, but also to be seen to be monitoring mobile security measures. High visibility and regular feedback to all staff, on both success and failure, are very important. Reinforcement across all levels means that security awareness can infiltrate the DNA of an organisation.

Analysis

All the relevant stakeholders, need to have regular reporting of the security landscape, so they are aware of the level of threat, and the levels of risk that they have accepted. Ideally, the Board should also have a disaster plan to implement, in the case of failure. That would certainly guarantee to focus an individual director?s mind on security issues!

Forensics

After a breach, particularly for mobile devices, organisations want to understand what has happened, what the failure was and what action they can take. Forensic tools are key to success here. A post mortem with findings needs to be produced and delivered so that, assuming the breach wasn?t terminal, lessons can be learned and implemented.

Go **Wick Hill**

About the Author

Ian Kilpatrick is chairman of international value added distributor Wick Hill Group, specialists in market development for secure IP infrastructure solutions. Kilpatrick has been involved with the Group for almost 40 years. Wick Hill supplies organisations from enterprises to SMEs, through an extensive value-added network of accredited VARs.

Kilpatrick has an in-depth experience of IT, with a focus on networks, particularly security. He has a strong vision of the future in IT, focussing on business needs and benefits, rather than just technology. Ian Kilpatrick is a published author and has written numerous articles and features, both domestically and internationally, as well as being a regular speaker at conferences, seminars and exhibitions