Compliance: keeping security interest alive


Martin Borrett

Martin Borrett, Institute of Advanced Security, IBM

In order to really change behaviours, security outreach has got to be evergreen – it must reinvent and reassert itself regularly into the consciousness of users and organisations.

The changing nature of the security environment is very much related to the disintegration and disappearance of the corporate or organisational security perimeter. Whether through the migration of computing and access beyond the corporate walls on mobile devices, or the dispatch of storage and services to cloud-based systems, or the increased collection and sharing of data, we are seeing the erosion of the long-held and comforting illusion of a protective corporate boundary. This imaginary wall has had the effect of providing a false sense of security for users where there has been little commitment or effort on their part.

As you move forward, developing a plan to keep your users engaged and apply new security practices in this much more open and accessible environment, the most potent new ingredient that you must add to your discussion is responsibility.

"As executives decide to change the models through which client and partner information is stored and accessed, they need to take seriously the trust that has been put into their firms"

Responsibility in this context is a moral and professional driver, one that communicates the changing nature of expectations on multiple organisational levels – from executives through to individual contributors; from business people to technologists to sellers. Customers, partners, shareholders and even other employees will all be impacted by bad security decisions made across the gamut of roles. As a result, your community of users must now accept and embrace a new and very personal responsibility for protecting the data and infrastructure that supports them all.

Taking it from the top: senior management

When most organisations are asked about the reasons they are undertaking new initiatives like Bring Your Own Device (BYOD), or cloud-based services, or instrumentation and data analysis, the goals are related to cost or return. A database administrator doesn't wake up in the morning and decide that she is going to move the corporate crown jewels to the cloud. Senior managers make those decisions, with expectations around increased flexibility, or cost-savings, or maybe reliability. Since these business objectives and rationales originate with the executive level of the organisation, it is a fact that the responsibility for any impacts on security rests there as well. As executives decide to change the models through which client and partner information is stored and accessed, they need to take seriously the trust that has been put into their firms. They must ask themselves hard questions and make appropriate demands in order that such trust is justified and maintained.

As an example, if we take seriously the importance of infrastructure reliability, executives in critical industries must become educated and prepared to do their part. Security has moved beyond the domain of the technologists, and it is now a characteristic to be balanced among other business concerns before decisions are made to change the underlying infrastructure or assumptions. Existing industry and legislative compliance and regulatory standards make this very clear, as they demand assertions of security on multiple angles where private or critical data is concerned. In order to meet these responsibilities, these executives need to ask probing questions to arrive at an appropriate level and language for reporting, and to lead their organisations by example when it comes to applying new initiatives in security.

Keeping it positive: the security team

New technologies and new business models will engender new risks. We all know this, but few security teams find themselves participating in the strategic discussions about whether or not the organisation should move in a particular technical direction.

Currently, the most successful security influencers are offering strategic advice on how to more securely implement or constrain a programme or deployment, but have not yet been brought to the table as an equal partner on what type of direction the company should take. Examples of this disconnect are many – from corporate decisions to cut costs through outsourcing, through improving employee experience through mobile or social computing, to simply rolling out a new customer service or application.

"Security has moved beyond the domain of the technologists, and it is now a characteristic to be balanced among other business concerns before decisions are made"

This lack of involvement is ordinarily caused by an organisational and semantic disconnect. Security teams are seen as filters and architects, providing means through which already formed ideas or solutions need to be made safe. We still see too few examples of security teams who have the early notice and capability to suggest new types of prevention and protection in the inception of new projects. Ideas that have been mentioned here at the Institute of Advanced Security – such as thoughtful data storage practices, elimination or consolidation of applications, integrated logging or monitoring functionality – are only truly useful if considered in the earliest context of the actual generation of requirements for the new solution.

To offer value at this early stage, security teams need to become providers of positive input on security controls that are enablers, and must be able to provide non-apocalyptic predictions of security risks. This balanced strategic input, offered in terms that are familiar and appropriate to a business discussion, will serve ultimately to eliminate many of the ingrained insecure choices that produce most of today's security concerns. A piece written recently by Hord Tipton in Healthcare Info Security provides some advice on how to approach executives and the company board.[1] The advice is not unique to healthcare firms, and has some simple rules for presentation.

"We still see too few examples of security teams who have the early notice and capability to suggest new types of prevention and protection in the inception of new projects"

Every employee has a role

Once outreach and awareness have begun, employees naturally begin to see that they are much more exposed than they previously believed when they thought there was a real perimeter. It is the right time to also help them understand that their own exposure comes with an increased responsibility to manage and minimise that exposure to protect each other, their organisation, and their clients.

"It is the right time to also help employees understand that their own exposure comes with an increased responsibility to manage and minimise that exposure to protect each other"

The typical employee believes that security is the domain of security experts and systems administrators; but this is no longer the case. Their mobile devices can be compromised and used as entry points. Their participation in social networking can bring unexpected programs and people deep within the organisation. The data that they handle is not just 1s and 0s, it is important, and sometimes private, either on its own or if it is combined with something else. Because the nature of their environment has been opened up to help make them more successful and more powerful, the nature of their responsibility has also expanded. They are all custodians and keepers of the overall security of the organisation, and the organisation cannot be secure without them.

Responsibility and reiteration

This messaging, its reformulation, its reiteration as things change and the role of champion and challenger of the security status quo, falls to us – the security leaders. It is our job to maintain our own level of enthusiasm and connectedness to changes in our companies and the security landscape. We must keep those thoughts fresh, and nurture awareness with new information, insights, and advancements. By doing this, we will change the equation through which good security is applied and the ways in which our own success is measured.

About the author

Martin Borrett is the director of the IBM Institute of Advanced Security in Europe. He leads the Institute and advises at the most senior level in clients on policy, business, technical and architectural issues associated with security. Borrett leads IBM's Security Blueprint work and is co-author of 'Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security' and 'Understanding SOA Security'.

Reference

1. Tipton, Hord. 'Demystifying the board presentation'. Healthcare Info Security, 5 Oct 2012. Accessed Jan 2013. www.healthcareinfosecurity.com/blogs/demystifying-board-presentation-p-1366.