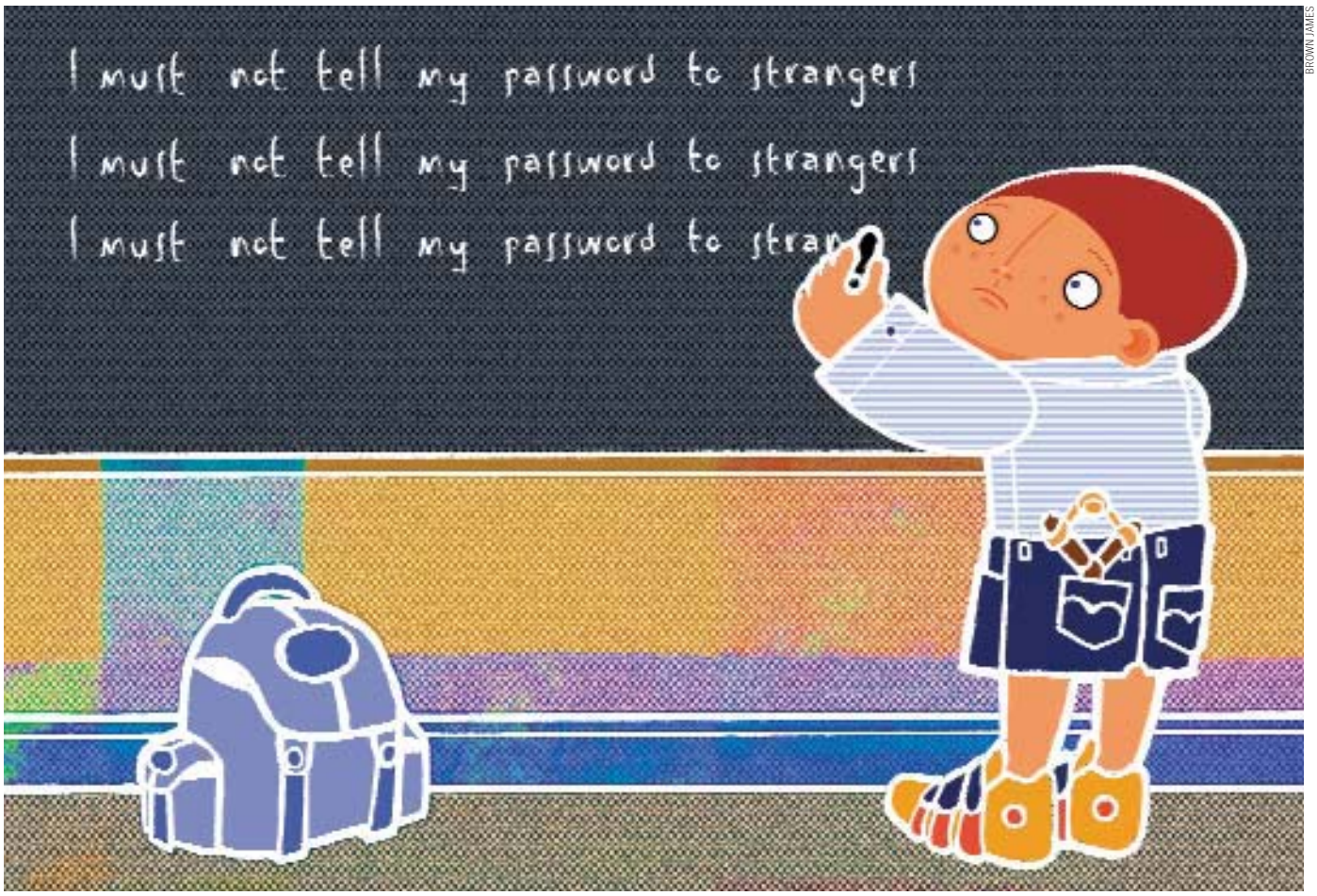

BROWN JAMES

Policy that lives

Enforcing security in spite of the users

Creating a security policy may be hard, says Illena Armstrong, but making sure that users comply is always the biggest problem.

Dog-eared pages, coffee stains here or there, and maybe even some misspellings or highlighted passages are preferable finds in a company's security policy. Such evidence of human interaction with the enterprise infosecurity tome shows that it is a work in progress, a living document that is modified as company changes dictate – not some clean and stilted corporate manifesto that no one really cares to read, much less enforce.

In fact, writing and editing the company security policy is not the main problem for most organisations' IT departments and C-level troops these days. The real dilemma comes into play when they actually want to get other company employees to comply with the mandates they put forth in policies. Just how this task may actually be accomplished still remains a matter of some debate among IT security players, with one group saying persistent education is the way to go and the other countering that education and training is superfluous if the right policy compliance tools are deployed.

"A security policy is really just a piece of paper unless you can enforce its provisions," says Jerry Harold, CISM, CISSP, co-founder of NetSec, a managed security services company. "Compliance audits, training and awareness can help to change behaviour periodically, but effective uses of technology to detect, report and respond to abuse and violations on a real-time basis really get people's attention."

Plus, maintaining the proper educa-

tional momentum is "so hard, subtle and continuous" that companies frequently fail to persistently follow through on security policy training and awareness, adds John de Santis, CEO of Sygate Technologies. While it is generally accepted that education is a component of an overall enforcement plan, it is often "not one you can count on", he says. Therefore, most companies who have actually written an adequate security policy in the first place would be better off automating its enforcement with tools, rather than depending solely on employees to pay attention in training classes.

Enforcing compliance

While NetSec's Harold contends that employees will pay attention to their security responsibilities if they know managers can detect violations (and ignore policies if they know managers lack ways of detecting them), actually deploying compliance tools is demanding.

"In theory, technology is critical to policy enforcement. In practice, however, it is extremely challenging," he explains. "Products are becoming more and more complex and feature-rich. Organisations face a huge challenge when they try to understand those features and then try to customise them to enforce unique policies and security requirements across an enterprise. Then the security product produces huge volumes of data that someone in the organisation must take action on."

Challenges of deployment, customisation and overwork of already busy IT staff are amplified even more when companies attempt to couple the tools with management processes to more effectively enforce the policy, Harold says. Integration of compliance tools with these management processes and the already existing systems they are trying to police can become overwhelming for any organisation with a large number of users.

Finding the right products then requires planning, research and time. And, in the end, a company may conclude that buying new solutions may be ineffective in solving their compliance problems, says Harold. Or they may find a combination of existing security solutions combined with compliance tools is the optimum way to go.

Security policies do not always result in improved security, beause they are too vague, too long or too complex

Robert Coles, head of Information Security Services, KPMG, UK

Enforcement is really problematic because you don't want to put the IT organisation in [a deeper] war with end users

Bill Malik
CTO, Waveset

In this case, the best security solution "uses a 'holistic' approach creating effective policies and management processes that are enforced with technology and validated through compliance audits." Because these have typically been standalone products, he adds, "the challenge is integrating [them] into an effective enterprise solution. In order to do this, commercial and government organisations need support from the top of the management chain and security becomes an essential component of day-to-day management processes."

Looking outside the (tool)box

Prompting employees to comply with security policies for a particular environment will depend on how the policy stacks up to business initiatives, what risks actually exist to the organisation and what security tools are already in place that can be leveraged to help keep end users aware of their responsibilities.

And such a feat will take more than just tools to be achieved, says Bill Malik, CTO of Waveset and a former Gartner analyst who reviewed many a security policy and consequently became partial to the coffee-stained documents that lived and breathed. "I find enforcement is really problematic because you don't want to put the IT organisation in [a deeper] war with end users than they already are," he says.

To get employees to agree with polices and support them through their actions, Malik says an example must be set by top managers, which will help to foster an overall security culture. Education is important here, as "electric shock" tactics on their own can be circumvented, fail, or create an environment where workers feel they are toiling away for managers who cannot bear to trust them.

Once companies have a policy in place that is "rational, acceptable, teachable, learnable" and capable of being explained easily, then they can get the compliance-specific solutions they need to fill in the enforcement gaps that existing tools are overlooking, plus back up such automated enforcement with education.

Simply put, the problem of security policy governance can be remedied with a combination of compliance tools and continuous training. Without the blending of both, the policies will never be as effective as their underlying concepts says SilentRunner's vice president of marketing, David Capuano. So, a programme of education that explains what and why end users should be doing what is set out in the security policy, united with both "block and tackling tools," such as firewalls, intrusion detection or authentication mechanisms, and policy compliance offerings, should help to keep company security policies alive rather than collecting dust on a shelf somewhere.

"It's the same concept of layered security," he says, where policy is tying people and technologies together to encourage everyone to support stronger corporate security through the use of education, auditing and enforcement.

Best of both worlds

To actually get to the point of worrying about policy enforcement, however, companies must ensure that their security policies are not too large, out of date, difficult to understand or inapplicable to the groups reading them, says Adam Lipson, president and CEO of Network and Security Technologies, a network and security consulting company in New York. Plus, he says, the end goal of corporate security governance must be kept in mind, which means involving all those affected by the mandates from the start.

According to KPMG's Robert Coles, head of Information Security Services in the UK, while most large organisations have written formal information security policies, they turn out to be only intermittently implemented and therefore inconsequential to most users.

"Security policies do not always result in improved security, because they are too vague, too long or too complex," says Coles. "They are developed without due consideration as to how they are going to be implemented and without wide enough consultation throughout the organisation. … A comprehensive policy adopted by an organisation is unlikely to be effective in influencing behaviour and day-to-day work if nobody is aware of it."

Todd Lawson, CEO and president of NetVision, suggests that initially, to develop a strong security policy, companies should base their mandates on security risk management.

They should use established industry standards like BS7799, and expect to implement and enforce policies as an ongoing process, which will involve necessary modifications to rules, the use of compliance tools and regular employee training.

Keep it short and simple

Also, when putting pen to paper, Patrick McBride, CTO of META Security Group, adds that splitting policies into hierarchical sections will make them easier to modify, friendlier to readers and simpler to implement with supporting tools and training. For instance, a good policy might have a one-page '-capstone' or statement from the CEO of the company explaining why the security policy and security of the company is important, then follow up with simple, straight-forward policy statements. These statements will then link to specific standards and controls that discuss the actual ways technology will support implementation of the policies and would likely only be shown to certain groups, like the IT department.

Too many companies are using management by vulnerability as opposed to management by policy

Adam Lipson
president and CEO, Network and Security Technologies

"Put claws in at the detailed level and let those who really need to see it, see it," he says. So, you make users aware of the basic policies they should follow, plug the technologies in, ensure that these are maintained, and determine what kind of education programme will be needed.

After all, says NetVision's Lawson, while policy will need to be supported with regular security audits, frequent scans of core systems for vulnerabilities, real-time monitoring, identity management techniques and more, the key factor comes down to employee support of security that ultimately benefits them and their company.

"A security system is only as good as the users' understanding and their willingness to abide by it," he warns.

While more organisations than in the past have overcome many problems in drafting and continuously editing their policies, many more still trip up at some of the early steps in implementation and in following up with the necessary security tools and training, says Network and Security Technologies' Lipson.

Unfortunately, there are still too many companies using "management by vulnerability as opposed to management by policy", seemingly waiting for the arrival of "moments of truth" – events that often call people to action. And, those are the organisations that will learn about such moments too late when a major systems breach, shareholder lawsuit or devastating virus calls their bluff. ■

Illena Armstrong is US and features editor at SC Magazine.

Achieving policy management best practice

The vast majority of organisations have yet to achieve anything like full compliance with effective corporate management, says **Nathan Millard**. Simply drafting a policy statement and pasting it on the intranet does not constitute 'effective management'. Organisations are not helped by the lack of a recognised 'best practice' in policy management – often leaving companies to learn only from their own mistakes.

Below is a five-stage checklist to help organisations avoid learning by trial and error, and take control of corporate compliance to realise a higher value from policies.

1 Establishing policy requirements

Any policy issued by an organisation should be compatible with – and a reflection of – all applicable laws, codes of practice, regulatory requirements and best practice. But the final decision on what goes into the policy must be a matter of personal and commercial judgment. Despite a complex legal backdrop, a policy that sets out to be unnecessarily comprehensive will fail as a usable document.

2 Drafting policies

It is vital that policy is drafted in a way that reflects the culture (or desired cultural change) within an organisation. Above all, the writer should strive to use plain English at all times and shy away from 'legalese' or unnecessary jargon. A policy needs to be capable of being understood and should be unambiguous.

3 Policy deployment

In a minority of policies, a passive approach such as posting a policy on the intranet is acceptable. But for many policies, it is imperative that organisations ensure that policy has been deployed to all relevant parties, and that they can prove employees have understood what is required of them. This can only really be done if the policy is actively 'pushed' to employees, requiring no effort on their part, but also offering no way of ignoring the policy.

4 Testing understanding and affirming acceptance

For polices that are critical to corporate compliance, the organisation needs to be in a position to track the penetration of the policy. This means moving both to collate evidence that individual employees have received the policy, and ensure that they actually understood what they have signed up to. Testing employee understanding is traditionally extremely labour-intensive and so it is often conveniently ignored.

5 Auditing and reporting

Those charged with deploying policy need to be in a position to readily generate reports on the deployment process – both on a macro and micro level. An ability to share reports with interested parties to help authoritatively demonstrate compliance can be a useful tool, for example to win tenders or deal with unwelcome scrutiny.

Corporate policies are no longer just a 'nice to have', culture-shaping tool for large businesses. With the introduction of increasingly strict legislation and the attentions of industry watchdogs focusing in on compliance, policies are now essential for all organisations. Although by no means a failsafe route to achieving 100 per cent compliance, the five stages outlined here should help any organisation increase the value of corporate policies and help reduce the risk of security and compliance breaches.

Nathan Millard is a solicitor with PolicyMatter, a joint venture between leading law firm Morgan Cole and independent software vendor Extend Technologies. This text has been taken from a white paper The Five Critical Stages of Policy Management, *available from www.policymatter.com.*