

SC

MAGAZINE

FOR IT SECURITY PROFESSIONALS

REVIEWED IN THIS ISSUE

Bit9 P43
Uses whitelisting of files to secure the endpoint



Ceelox P53
Eliminates the need for passwords across the enterprise



Bioscrypt P52
A physical security control device uses more than prints



FEATURES:

FRIENDLY FIRE

Protecting users from threats falls on trusted websites, says Overstock's Sam Peterson **P24**

Slurping the USB port

Portable media devices are being used to abscond with corporate data **P30**

Convergence factor

Enterprises must protect data while at the same time ensure privacy **P33**

GROUP TESTS

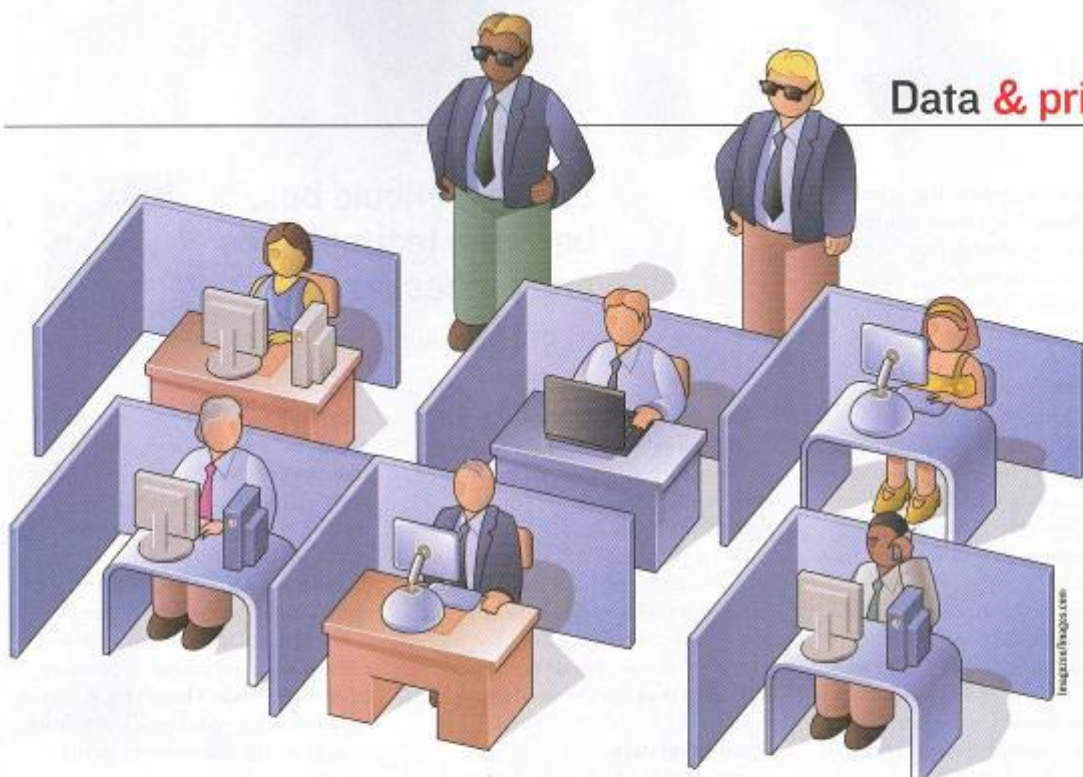
»Endpoint security

Protect corporate assets from moving beyond internal perimeters **P40**

»Biometrics

Safeguard sensitive information, while lowering costs **P50**





The IT department faces conflicting mandates: there are requirements to provide high quality data throughout the organization, but at the same time they must protect the privacy of customers and business partners. Such mandates can operate at odds with one another and any productive IT effort requires this tension be balanced successfully.

According to Steven Adler, director of IBM's data governance solutions, "Security and privacy are key components of data governance, but what is needed is an expansive view of data, such as business

function of the data, provenance, age. All of those factors are intrinsic to protecting information. This approach yields a more holistic view of data governance."

In other words, there must be a strong commitment to the integrity of data governance initiatives, along with a strict adherence to compliance requirements for privacy. This means creating and maintaining a sustainable equilibrium.

Ideally, if focused strategies, policies and controls are fully integrated, organizations have a better chance of meeting their mandates. In practice, however, this goal is dif-

icult to reach, much less maintain. Why? Developing and maintaining a viable data and privacy structure requires a significant commitment and investment of resources. To effectively bring about this evolution, organizations must analyze the convergent mechanisms of governance and privacy.

Any such examination should include consideration of several elements, such as: the existing state of compliance with regulatory requirements; how sensitive information is being protected; and how the value of information assets can be improved and protected simultaneously.

CONVERGENCE FACTOR

Enterprises must protect corporate data while ensuring privacy, reports **Chuck Miller**.

Data & privacy

Though seemingly daunting, at least initially, in the end, improved data governance and commitment to confidentiality can actually foster business objectives by enhancing trust and cooperation among users, IT and top management.

Facing reality

In practical terms, the fundamental operational IT problem is that corporate data resides in myriad locations and under vastly different business initiatives. That is, the same data can exist variously, with limited oversight as to how it is used, transmitted or stored.

In the face of such diversity, how can an organization build policies for its functional and operational integrity while addressing concerns of data privacy, access management, security controls and compliance? Answers to such questions depend on circumstances.

“Ultimately, governance is built on corporate policy. The company develops policies, either driven at the CEO level or by regulatory requirements,” according to Harry Piccariello, chief marketing officer at GigaTrust, a provider of email security and content protection.

But determining who is responsible for developing policy is another challenge. “Ideally this should be done by teams made up of representatives from HR, legal, IT and compliance departments,” says Nancy Flynn, executive director at the ePolicy Institute, Columbus, Ohio.

Decentralized planning and execution may not be effective, however, because few internal lines of business have the enterprise-wide understanding or ability – or objectivity.

“Data governance is a political and cultural endeavor,” says IBM’s Adler. “There are some best practices that you can undertake to avoid pitfalls in the process, such as making sure you have a recognized leader with authority in the organization and making sure that users have cross-organizational representation. It is also important to ensure that you have a charter that delineates functional powers.”

“Security should be... between technologies and processes.”

– Christophe Briguet, CTO, Exaprotect



Moreover, he adds, a budget is critical, too, as well as being sure that your policy decisions have weight – that you can veto proposals if necessary to prevent bad things from happening.

“Many of the people in IT did not go to college to study political science,” he says. “They may not know the fundamentals of governance and policy making. You need people on the team that do understand such nuances so you can avoid pitfalls.”

Discovering data

At a practical level, a key step in the process is figuring out the basics of your data – what it is, where it is and how it is used.

Glen Kosaka, director of DLP marketing at Trend Micro, says, “Many companies, before they can put into place a solution for protecting private data, first have to go through a process of understanding their data workflows and data classifications.”

During that process, they need to map out everything – from who uses the data, where it’s stored and who should have access, he adds. “They must determine where data is authorized to be moved and where it should be stored at rest. Then they can create classifications of data related to sensitivity and privacy.”

Formulation of data governance and information security policies also calls for an examination of assigned roles and responsibilities. This includes documented responsibilities of employees, contractors and third-party users.

In all, once policies are initiated and a proper understanding of data processes is evolving, organizations must be ready to face any problems. For example, privacy mandates can lead to verification problems. Access may depend not only on the role of individuals, but also on processes

with which that person interacts. That may mean limiting access so that fewer employees will touch sensitive records. For those with access, all their interactions with the data must be individually tracked and monitored by an automated audit system. The goal should be to embed security into every business process, say experts.

Additionally, it is also necessary to address issues intertwined in privacy regulations worldwide. Though the American legal system has relied on self-regulation to address data privacy and security concerns, many countries have passed legislation to protect data privacy.

Internationally, data governance and privacy legislation encompasses how business should be conducted, often being spelled out in detail, targeting all communications made with every stakeholder, as well as interactions with all business process technology. It typically involves all facets of an organization: operations, databases, as well as communications with customers, service providers and legacy systems.

Privacy and trust are essential to maintain good relationships with customers, employees and business partners. Though it is important to ensure that parties understand their responsibilities to reduce the risk of theft, fraud or misuse of facilities, companies must take into account the effects data governance and privacy policies have across an organization.

“Security should be like a layer – a layer at the organizational level between technologies and processes,” says Christophe Briguet, CTO of Exaprotect, a Mountain View, Calif.-based provider of security management. “A layer that translates organizational rules and policies to specific technology configurations, driven by compliance.” ■