Strategy

The Dirty Secrets of Green IT

The recent push to save the planet from environmental catastrophe in some quarters has dovetailed nicely with organizations' need to pare down budgets – making for some nice PR. But, as Wendy M. Grossman demonstrates, hiding behind some 'green' initiatives are increased security risks

Even if you don't care about the future of the planet, reducing energy usage and carbon emissions has another clear benefit: cost savings. In some cases, there's little choice about becoming more energy-efficient, as companies with massive data centers experience increasing trouble finding sites where there's enough power to meet their needs.

On the face of it, green computing would seem to have little to do with security issues. However, there may just be more to it.

"I'm not sure if there's a direct impact", says Robert Halbheer, chief security advisor for Microsoft, "but these are two trends that actually drive the same decisions when it comes to a CIO." It is, he adds, a chance to rethink system architectures and security, presenting both an opportunity and a challenge.

"One of the big things about it", says Paul Ducklin, a senior technology consultant at Sophos, "is that everything has to be seen to be green, whether it is or not. So one of the issues with the whole green IT business is that some of the people who will sell green IT services will bring almost a sea change in how you do stuff." His – and everyone else's – leading example is replacing the big room full of your own servers with virtualization and outsourcing. A second, much smaller set of issues center on recycling: it is easy to forget that recycled paper and equipment – not just hard drives but also routers – can be vectors for disseminating information that should have been kept confidential.

Typically when people talk about being 'green', what they really want is just to save money, according to Proband's Gary Price

"You can be green by completely changing the way you do things, and of course change can easily be the enemy of security. Often when you make a change, things break." But, Ducklin adds, "change can be good for security if you choose it to be."

> **"I went to two events run by IBM and HP on servers, and both claimed to be the greenest**
>
> Gary Price

Simplifying Your Operation

The pitch that virtualization suppliers make is that your security will be improved because they are experts at keeping servers going, and securing and configuring them properly. Besides all that, they'll argue that they can cut your costs because of their economics of scale.

"If the goal is to rationalize things in the server room, get rid of unneeded servers, and reduce power consumption by not thrashing your machines", Ducklin says. "That probably means you're going

to streamline and simplify your operations – and in my opinion, in general when you strip things down on a computer, you actually reduce its attack surface."

A server intended to do only DHCP and DNS, for example, can run on a stripped-down version of its operation system. This will save power by using less memory, CPU, and hard disk; it will also tend to be more secure simply because the installation omits software that could provide additional vulnerabilities.

"I'm amazed", Ducklin says, "to go into server rooms and see services providing authentication, DNS, or DHCP running on full-blown installations of Windows Server, for example. I'm a great fan of the simplification of IT."

Virtualization, however, has its own risks. For one thing, few providers offer much detail about their systems and data centers; imagine trying to get Google or Amazon to give you details of its operations.

"You can see why this is the enemy of security", Ducklin says, "because it means if you ask they can't answer – so I don't know how you satisfy yourself that they're not watching YouTube on your server while you're asleep. They probably don't, but how do you know? When it's your own server you can look at the logs, or have a trusted, smaller team."

"The only assurance we've seen from any cloud providers is around their physical security

Peter Wood

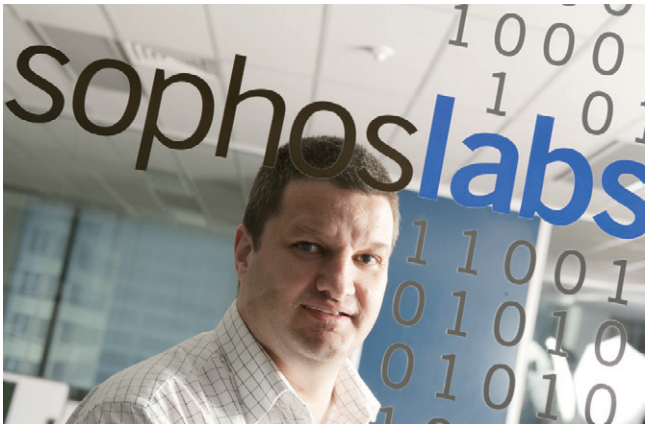
Ramses Gallego, general manager of the Spanish IT consultancy Entel, sees a slightly different set of problems: "As with any new approach, there are risks and concerns", he says. "You are adding a layer of abstraction to the physical world, so there are risks – attacks on that virtualized layer, for example." A key question, he adds, is what kind of isolation you can expect from others whose virtual environments are deployed within the same physical box.

Collateral Damage

Awareness of this issue may have been one of the unintended side effects of the WikiLeaks-related Operation Payback. For one thing, Operation Payback's DDoS attacks that took down the PayPal and MasterCard websites showed how vulnerable even a large organization can be if a key provider is disrupted. For another, even though it either failed or was withdrawn, the announced attack on Amazon.com made it plain that any organization can become collateral damage if someone else sharing the same platform has become a target. Neither scenario is appealing.

"The flip side", says Ducklin, "is that the cloud-oriented approach to computing brings [its] own security challenges. Who has control of the data? In what jurisdiction? Who has access

"You can be green by completely changing the way you do things, and of course change can easily be the enemy of security



Paul Ducklin, Sophos

legally or illegally?" Because cloud computing for the enterprise is still relatively new, these are questions that don't have well-thought-out answers yet.

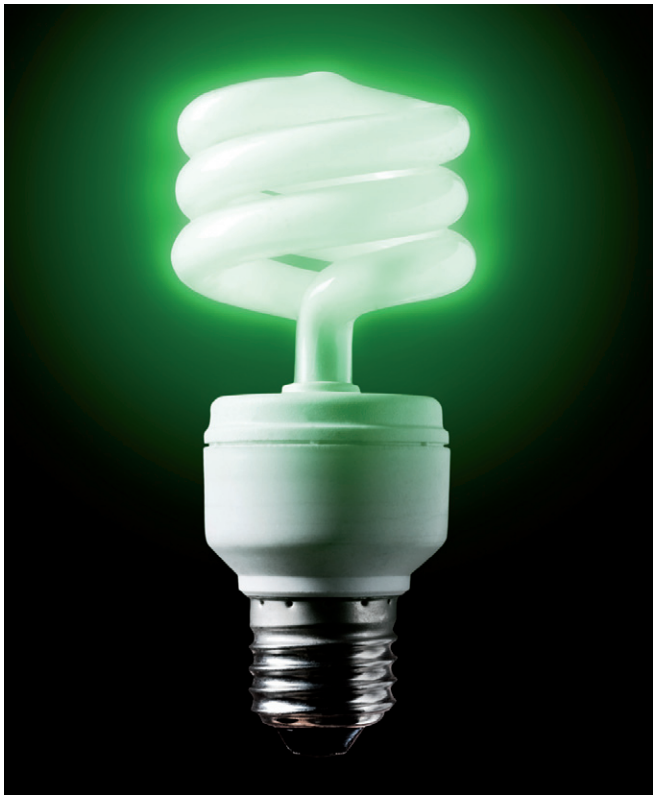
"Auditing is a super-size problem", says Peter Wood, CEO of First Base Technologies, who did a piece of research not long ago studying cloud providers and their auditing policies. "There was no consistent response from anybody – they just shrug it off and say, 'Take or leave the contract'." As an example, he cites Microsoft's head of legal, Dervish Tayyip, who told ZDNet: "What is important is that customers understand the [cloud] offerings are standardized – they are what they are. If the offering does not meet customer needs, maybe the cloud is not a realistic offering."

The upshot, Wood says, is that "feedback from corporate clients indicates that there doesn't seem to be any meaningful way to negotiate with them over the compliance needs they think they have. They can't run tests because it's a shared infrastructure." Often, cloud providers won't even disclose what tests they do run beyond offering compliance with the SAS70 standard. "The only assurance we've seen from any cloud providers is around their physical security", he says.

This issue is of particular concern with respect to the SME market. Smaller businesses do not have sufficient clout to negotiate or demand details, and they often lack awareness of the risk they're taking.

Can I Have a Definition?

As everyone tries to make intelligent – and green – decisions about their IT, however, the biggest issue may be trying to define what it means to say something is 'green'.



Even if you don't care about the future of the planet, reducing energy usage and carbon emissions has another clear benefit: cost savings

"We identified a massive issue and a problem for IT buyers to buy green IT", says Gary Price, a business analyst with UK-based value-added reseller Probrand. His company, which focuses on the public sector, has been trying to use the data supplied with computer equipment to help customers, and he has found it hard going.

"I went to two events run by IBM and HP on servers, and both claimed to be the greenest", he recalls. "It's all about the way the cards are stacked." Price wants to see some continuity and consistency in labeling, much as washing machines are rated because they conform to a known set of specifications.

"You couldn't even do a search", Price says. "There are all these rules and regulations out there around the world, but none are mandatory and none are exactly the same." In any case, he says, most of the time when people talk about being 'green' what they really want is just to save money.

> **If I'm running a company, my job isn't to save the planet but to make money for my shareholders**
>
> Ross Anderson

THE SMART GRID

The traditional 'dumb' electrical meter that's hidden in a cupboard and counts units of electricity use is gradually being replaced with 'smart' meters that give better detail about usage, and they can be read remotely. The upshot is that instead of relying on quarterly summaries, companies can use half-hourly meter readings to understand where and how they are wasting energy and generating unnecessary carbon emissions. The UK, for example, intends to roll out smart meters to every home by 2020.

At the 2009 Black Hat conference, Mike Davis, a researcher with IOActive, demonstrated that smart meters were vulnerable to hacking and argued that they must be built to recover from a full compromise. A virus that shuts down individual computers is bad enough; imagine one that shuts down the electrical grid. In July 2010, Ross Anderson and Shailendra Fuloria argued in their paper *Who controls the off-switch*? that it could happen. In an earlier paper, *On the security economics of electricity metering* they noted the privacy risk of the mass of data collected by these meters and the risk that a government might use targeted power cuts as a "coercive measure."

Green Means Lean

This reality, adds Ross Anderson, a professor of security engineering at Cambridge, makes sense. "If I'm running a company, my job isn't to save the planet but to make money for my shareholders. No company wants to pay two or three times the electricity costs, not when there is an opportunity for savings", Anderson continues. "So I'll avoid the issue becoming salient if I can, and have a story to tell in case this doesn't work."

> **You can be green by completely changing the way you do things and of course, change can easily become the enemy of security**
>
> Paul Ducklin

Most environmental analyses are relatively shallow: we compare computers by looking at how much power they consume, but we do not follow them all the way back to their component manufacturers to compare lifetime carbon emissions.

"The carbon emissions problem is not easily fixable", says Anderson. "It could be the biggest prisoner's dilemma the world has ever faced. Even John Beddington now accepts that. So the incentive on every politician and CEO is to greenwash." A proper security analysis, he says, "would more likely focus on the dodgy claims being made by its proponents."