Every worthwhile experiment relies on an unaltered “control” subject or process for a reality check. So it is with security software. To know how effectively a combination of technologies and policies are guarding against threats, companies need a subgroup of unprotected systems for comparison.

ITV plc, Britain’s popular commercial television broadcaster, runs such a control group, albeit not by choice. The vendor of the custom software ITV uses to edit and manage news presentations grew up in the broadcasting industry and remains insensitive to the security fears that haunt most IT organizations. The company advises its customers to tune the application for performance rather than harden it against security threats.

Nick Leake, ITV director of operations and infrastructure, thinks this approach is shortsighted. “We have undertaken a test of installing antivirus software on some of the machines, and we’ve recognized that the machines function perfectly adequately,” he says. “The vendor would be better off to support security measures.”

This situation offers one unintended benefit: It demonstrates the virus threats ITV faces and unveils the consequences the company would face if its current strategies weren’t in place.

It has been demonstrated that when problems arise, they almost always occur on the unprotected PCs. “It’s not a control I’m happy with,” Leake adds.

Leake isn’t alone with his concerns. Security executives crave universally accepted ways to measure and document the effectiveness of their strategies. The right data, after all, can serve to generate answers to such recurring fundamental questions as: “What additional measures should my company be taking to harden its operations?” and “Where should future spending be targeted for hardware, software, consulting labor, and external services?”

Despite their value, valid security metrics remain elusive for many companies like ITV, which often rely on ad-hoc measures.

“The issue for any commercial organization,” says Leake, “is how much effort you want to put in to gathering any of these metrics, and what’s the value you get back if you do.”
Stumbling blocks
Companies that take the time to develop ongoing security statistics can use the results to justify ongoing funding.

“As the chief security officer, you want a tool that is able to gather data quickly and generate decent-looking reports that a manager can then take to the boss and say, ‘Look at how effective our security operations are, or alternatively, look at all the problems we’ve got,’” says Andrew Jaquith, program manager for security research at the Yankee Group, a technology research company based in Boston, Massachusetts. “The classic technique for gathering this information is to work with the security software vendor, or to roll up your sleeves and use your own tools to gather the data information about the problem you are trying to solve.”

The incentives for doing this work continue to grow. In the United States alone, 2.8 million organizations suffered at least one security assault resulting in average individual losses of US$24,000, according to the 2005 FBI Computer Crime Survey. The agency calls the statistics “very conservative.” Even so, these losses represent US$67.2 billion a year (or US$7.6 million per hour), which equals one-half percent of all the goods and services produced annually by the U.S. economy. The FBI estimates account for only a fraction of the staff, technology, time, and software that organizations commit to preventing security incidents, the agency says.

On the surface, implementing and gathering security metrics seems simple—just track the numbers of incoming and outgoing emails, document the percentage of virus attachments, and record trends in the number of network intrusions attempted by outsiders in recent years. Solid metrics aren’t so easy to quantify, however, for individual companies or for industries. This is what makes developing reliable benchmarks so challenging, Jaquith says.
Companies would be best served by collecting accurate data not only on security incidents but also on the existing investment in security technology. Focal points should include how long it takes companies to respond to individual assaults and how much labor they had to devote to the threat.

“That is your real cost,” says Jaquith, who goes on to say that time and cost are measures of agility and organizational effectiveness. “And those,” he says, “are arguably the best metrics.”

Jaquith warns, however, that three challenges traditionally conspire against the rise of universally accepted security metrics: disagreement among security professionals about how to properly model and quantify risks, a lack of consensus on which security attributes to measure, and insufficient data sharing among companies in vertical markets in regard to documenting the numbers of incidents and ongoing trends in terms of the volume and character of attacks.

Short of industry-wide standards, companies can begin to measure security strategy effectiveness by comparing departments across large organizations that don’t enforce consistent policies. Variations could build a case for both security spending and policy consistency. “Companies might see, for instance, that a North American business unit has, on average, 11 missing operating system patches on its workstations, whereas the European business unit might have five,” Jaquith says. “If you can also show that, lo and behold, one of these units had a lot more security incidents than the other, you could start to draw some connections.”

Coping with the unknown
Leake explains the difficulties in devising security metrics by saying, “there are known knowns, known unknowns, and unknown unknowns.” The third group is the hardest to cope with, he says. “Once you put a measurement in place, that’s only telling you the status of the things that you’re measuring. If there are problems that you don’t know exist, you can’t really put a measurement in place around them,” he points out.

Because IT security focuses on prevention, companies consider themselves successful in the absence of incidents. “But when you’ve got no activity, you’re never quite sure whether it’s because you’ve been extremely successful in what you’ve done or whether you’re not being subjected to any attacks,” Leake says. “It’s very difficult to measure exactly how successful you’ve been. Having said that, you need to take reasonable precautions to protect yourself from being attacked in any particular area.”

For ITV, measuring success comes down to logging downtime or other performance problems resulting from attacks. ITV combines Symantec AntiVirus with an overall security approach that configures most of ITV’s PCs with similar processors, software, memory, and related system components for maintenance ease and fewer complications. ITV also uses software that automatically downloads patches from the source sites, which it then tests and rolls out to its PCs. “Within this ‘lock down’ environment, security is very effective,” Leake says. “We get a very low level of incidents.”

Demonstrate success
Terry Stern, information risk and security manager for the U.K.-based Xansa Ltd., also grapples with the challenge of accurately measuring security strategies intended to protect the technology outsourcing company he works for headquartered in Reading. “The biggest challenge of all is being able to demonstrate compliance with our policies through metrics,” says Stern, who uses Symantec AntiVirus and Norton Ghost. “The whole business of compliance and governance is an essential part of our work.”

When Stern evaluates new security software he bases his buying decisions on the package’s ability to gather security metrics and compile them into reports. “We want easy, high-quality reporting from our security tools so we know what’s going on from a security standpoint. Reporting becomes a critical consideration whenever we’re assessing any security tool. The manageability of the management reporting and how easy it is to paint and present those reports is crucial.”

In addition to measuring effectiveness, the reports help security managers demonstrate success to management. “If we can feed the data into a dashboard, that helps us. Management wants to see all the statistics on one slide.”

A third-party security service tracks inbound and outbound emails for Xansa, and provides monthly reports on how many and what kinds of viruses it thwarted.

When Xansa first established the outsourcing arrangement almost four years ago, it found itself awash in security statistics—data points that
would have previously been available only by “mucking about with the mail gateways,” Stern says. Those investigations didn’t typically occur because “it would have taken people away from their day-to-day jobs.”

Today, Stern can scan online report details for key security metrics such as an unusual spike in incoming and outgoing emails, which might signal a potential virus or spamming attempt.

Stern says that stealth viruses are potentially more destructive than early incarnations that did their damage blatantly when they wiped data from a hard drive. “Now they have moved into the criminal arena as they endeavor to fool people into going to unsafe places and revealing information or installing Trojans and key loggers. That’s a lot nastier,” he says.

Other data points include the number of blocked attachments that carried viruses or the latest list of Web sites Xansa cordons off from its employees because of security breaches. Statistics like these keep Stern abreast of new outbreaks, and provide summaries for senior managers to substantiate Xansa’s security software and services investments.

Stern can also use the data for historical analyses. He compares the number of viruses encountered year to year, and the annual rise in the amount of spam Xansa receives. “We are able to monitor trends and produce reports that show what happened over the last month or over the last year,” he says. “We are able to see whether things have gotten better or worse.”

In addition to statistics like these, Stern would like to see better reporting tools that calculate the possible consequences if antivirus or intrusion-detection technologies weren’t in place to foil specific attacks. “I want reporting to be able to anticipate the type of reports that we want,” he says. “For example, if I want to know the top 100 sites that some of our people tried to go to but were blocked, and the users who tried to access those sites. I don't want to have to be writing too many scripts in order to produce those reports.”

Stern also counts on two additional security metrics that don't appear in the regular monthly reports. While perhaps unscientific, these indicators are nevertheless informative. “One of the most underrated security metrics is your own people,” he says. “If you're doing your job well, then people will be talking about security; they're talking about what's going on in the news—if there is a high-profile phishing or key-logging incident, for example. Hearing people discuss things like that, I would argue, is a metric. It's a good indicator that your awareness training is working.”

And the other informal security indicator? “I always judge how we're doing by how well I sleep at night,” he says, adding that he usually rests easy because Xansa's strategies have proven successful. But he remains vigilant. “I always consider this caveat: Somebody, somewhere will be trying to find a way of doing something, whether maliciously or not, to circumvent the security controls Xansa has in place.”

“The biggest challenge of all is being able to demonstrate compliance with our policies through metrics.”

Terry Stern, Information Risk and Security Manager for U.K.-based Xansa Ltd.