The current economic downturn has caused enterprises to reassess their overall IT expenditures, and cybersecurity spending won’t be exempt from this increasingly intense scrutiny. During the reassessment process, cybersecurity programs will have to justify—and, in many cases, significantly reduce—their expenditures.

However, crime rises when economies fall, and as the global recession worsens, more people will be tempted to do things they would never do during boom times. We’re already seeing this pattern in the physical world, with reports of shoplifting, theft, burglary, and even armed robbery on the rise. It’s also happening in the virtual world, with online and data security threats continuing to increase both in number and sophistication. As more threats continue to originate from petty theft, professional hacking, and organized crime, it’s important that enterprises properly manage their cybersecurity risks during cost-cutting periods.

**Cost-Cutting Tactics**

Financial stress often leads to changed priorities, so cybersecurity risks that might be unacceptable during normal times are increasingly viewed as hypothetical. As a financial crisis progresses or worsens, we’ll see even greater levels of compromise. To combat a potentially devastating series of trade-offs, companies should consider three core cost-cutting tactics.

**Understand Your Risk**

Risk assessment is essential for providing visibility into the increased risks that can stem from a falling economy and crisis-driven budget cuts. Today’s enterprises rely heavily on information systems in cyberspace for their business operations, and with the rapid movement to use new technologies such as Web 2.0 and new platform choices such as mobile systems, cloud computing, and messaging systems, the risk possibilities have increased in recent years. Consequently, cybersecurity has become more critical to business continuity than ever before.

Each cost reduction action therefore requires a full risk assessment. Enterprises should analyze their assets by identifying those at risk, estimating the risk of losing them, and developing mitigation options. In addition, risk managers should be aware that the interactions among various cost-cutting schemes could create unforeseen additional risks, so they should strive to identify as many such interactions as possible.

**Maintain Baseline Protection**

The key challenges facing security managers in a period of constrained resources and increasing security demands is the need to reduce costs while managing security risks to levels that business stakeholders deem acceptable. To this end, security managers must have a clear understanding of the minimum necessary level of security required for the entire enterprise. An enterprise-
A wide cyberdefense framework can help ensure that baseline operations include all basic security mechanisms.

A basic level of security is no luxury—it’s mandatory. Hostile code will compromise an unpatched system within minutes of direct Internet connectivity, and attackers will quickly exploit unprotected network perimeters. Security managers should treat mechanisms such as vulnerability and identity management, firewalls, antivirus operations, intrusion detection, and incident response as essential.

Communicate Changes and Effects to Stakeholders

Cost cutting results in altered services for stakeholders, so security managers should discuss the proposed cybersecurity changes and their potential impacts with stakeholders so that they fully understand them and can adjust their expectations accordingly. If the reduced budget can’t meet the demand for cybersecurity services, then the security group must find alternative approaches.

No matter who’s responsible for cybersecurity, decisions to cut security programs and services must be recorded, as should decisions to reduce or postpone improvements. The signed decision documentation should include the business rationale, any compensating controls that will be put into place, the residual risk’s anticipated form and level, and the trigger conditions that would enable service resumption or improvement plan acceleration.

The current financial crisis could lead to increasing regulations, so this isn’t the time to ignore cybersecurity risk management and compliance. Practical cost-cutting tactics can help security managers properly assess and consciously consider various cutback options.

In this Issue

The articles in this special issue offer tips to implement the three previously described cost-cutting tactics. In the Insecure IT department (“Understanding Insecure IT: Practical Risk Assessment”), Rick Kuhn, Hart Rossman, and I argue the need for a practical risk assessment. We outline some processes and approaches, review methods and tools, and emphasize the importance of risk assessment’s practicality and usefulness.

The first feature article, “Cyberattacks: Why, What, Who, and How,” analyzes the challenges associated with cybersecurity, including attack patterns and trends. It also examines the initial causes of cybersecurity problems, analyzes cybersecurity challenges, discusses potential internal and external malicious attackers, articulates attack patterns, and outlines upcoming security attack trends.

The second article, “From Ancient Fortress to Modern Cyberdefense,” proposes an enterprise security framework that mimics an ancient fortress via five major components: an observation tower, fortified walls, gates, alarms, and guards. The article reviews core security mechanisms in each of these components.

In the third article, “Evaluating the Security of Enterprise VoIP Networks,” Peter Thermos summarizes some findings of VoIP security studies and recommends best practices for VoIP deployment. The article also defines a threat taxonomy and discusses a security evaluation methodology to evaluate VoIP network security.

In the fourth article, “Useful Cybersecurity Metrics,” Shari Lawrence Pfleeger suggests cybersecurity metrics to assist both practitioners and policy makers in understanding the impact of changes in security investments, policies, and procedures. The article proposes a multiple metrics graph to depict attributes that contribute to security and a process query system to test hypotheses about system security.

As organizations suffer through a declining economy, many will be forced to make security cutbacks they wouldn’t ordinarily consider to be acceptable. IT leaders and managers making security cuts must ensure that their cyberdefense continues to meet organizational obligations to protect enterprise cyberspace and corporate assets. As you read the articles in this issue, I invite you to comment on these models, approaches, tactics, practices, tools, and discussions. Please send your comments to our lead editor, Jenny Stout, at jstout@computer.org.

Simon Liu is the director of information systems at the US National Library of Medicine, National Institutes of Health. He’s also an adjunct faculty member at Johns Hopkins University. Contact him at simonliu@mail.nih.gov.