# IT Security

**Morris Chang,** *Iowa State University*
**Rick Kuhn,** *US National Institute of Standards and Technology*
**Tim Weil,** *US Department of the Interior*

Change is a factor in every area of life, but it often seems even more so in IT—particularly in IT security. Organizations must manage patches daily, continuously monitor for vulnerabilities and attacks, and install an endless stream of new releases of application software. Even in established IT fields, such as database management, new challenges are emerging—for example, we're witnessing a shift from huge relational databases to even larger, but often less structured, big data repositories, which present new challenges for information security. In addition, completely new problems frequently appear, such as bring your own device (BYOD) security challenges, because every employee's cell phone now has capabilities and risks that used to be concentrated in mainframes or desktop computers. The dynamics of the rapid change affecting the IT industry give rise to the question, how can IT professionals adapt to these ever-changing security challenges quickly and without draining their organizations' resources?

## Adapting Securely to Change

As with many problems, one of the best approaches is to break the security problem down into component parts and separate concerns before considering how the different components interact. Security is more than firewalls and cryptographic protocols, and a focus on these technical aspects can often lead to neglecting other issues, resulting in a breach.

We can view security from at least the following four perspectives, analyzing problems accordingly.

### Technical

This is the most commonly discussed concern, and indeed it can have an extraordinary impact. A recent example is the "Heartbleed" bug (http://heartbleed.com), an apparently simple coding error in the OpenSSL library that allowed a storage boundary to overflow, revealing sometimes sensitive information or, in some cases, compleletly compromise systems.

Heartbleed also illustrated the difficulty of analyzing security impacts. From one angle, Heartbleed appears to be a moderately severe buffer overrun vulnerability that can lead to a compromise of random bits of memory. But with repeated runs, it was possible to obtain critical data, such as authentication information, allowing attackers to log into systems. The key point here is that security can be very difficult to analyze outside of its particular application context.

 Published by the IEEE Computer Society 

### Behavioral

One of the most poorly understood aspects of security is the problem of making mechanisms easy to use while retaining adequate strength for a particular application. Security principles, going back nearly 40 years, included the need for ease of use for security mechanisms, but the problem can be surprisingly difficult to solve, because of the needs of different application domains. A mechanism that is easy to use for employees with only minimal training might be unacceptable in a customer-facing application, because, of course, customers won't have any training in its use.

### Legal

Regulations and laws have always been a part of life in industry and government, and legal complexities have multiplied along with technology. While technical aspects of security might be relatively similar across application domains, laws and regulations vary enormously, not only across industries but among jurisdictions as well. Further complicating the issue is the fact that corporations often conduct business in hundreds of countries. Successful methods for automating the regulatory and legal aspects of IT increase in importance as more and more, daily life happens online.

### Basic Principles

A common theme apparent in the three aspects of security just discussed is the fact that often, everything depends on the context and application domain. But what are the basics that IT professionals can apply in analyzing security problems? Not only computer security principles, which are well known, but broader questions of protection and conflict should be considered, with lessons that can be learned from other fields entirely outside of IT.

## In this Issue

The first theme article in this issue, "Security—A Perpetual War: Lessons from Nature," by Wojciech Mazurczyk and Elżbieta Rzeszutko, provides thought-provoking analogies between the natural world and cybersecurity issues, including botnets, intrusion detection, and distributed denial of service. Considering the basic principles involved can spur creative thinking about how to improve cyberdefenses.

Another article, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," by Jan Kallberg, deals with a controversial topic: the legalities and practicalities of a "self-defense" approach to cybersecurity. When an organization is the target of a cyberattack, is it possible to accurately identify the attack source? If so, is it reasonable for the organization to take an offensive approach to stopping the attack? Industries and governments are currently asking these questions, and IT professionals should be aware of the issues involved.

In "Securing Health Information," A.J. Burns and M. Eric Johnson provide an overview of security issues in healthcare IT. The authors suggest that healthcare has lagged behind other industries in its use of IT but is changing rapidly now. The field is complex, in particular because of the tradeoff between security and a capacity to provide prompt and informed care, but solutions apply to many other industries as well.

"Protecting Web Components: Hiding Sensitive Information in the Shadows," by Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, Frank Piessens, and Wouter Joosen, deals with the ubiquitous problem of protecting Web-based information and commerce using new features of the document object model. The authors also include statistics on the disturbingly high prevalence of security weaknesses in real-world websites, which suggest that many organizations might be more vulnerable than they realize.

Articles in this issue highlight emerging trends and suggest ways to approach the four aspects of cybersecurity we outlined. The breadth and depth of discussion in these articles should help readers recognize both problems and potential solutions. IT


## Acknowledgment

*Certain products may be identified in this document, but such identification doesn't imply recommendation by the US National Institute of Standards and Technology or other agencies of the US Government, nor does it imply that the products identified are necessarily the best available for the purpose.*



***Morris Chang** is an associate professor at Iowa State University. Contact him at morrisjchang@gmail.com.*

***Rick Kuhn** is a computer scientist at the US National Institute of Standards and Technology. Contact him at kuhn@nist.gov.*

***Tim Weil** is a risk manager (contractor) at the US Department of the Interior. Contact him at trweil@ieee.org.*