IT AUDITING

Third Edition

USING CONTROLS TO PROTECT INFORMATION ASSETS

Mike Kegerreis • Mike Schiller • Chris Davis
With Brian Wrozek

Mc Graw Hill

IT Auditing: Using Controls to Protect Information Assets

Third Edition

Mike Kegerreis
Mike Schiller
Chris Davis

with Brian Wrozek

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

ISBN: 978-1-26-045323-2
MHID: 1-26-045323-5

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-045322-5, MHID: 1-26-045322-7.

eBook conversion by codeMantra
Version 1.0

quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

To my family and friends—thank you for all of your support.

—Mike K.

To Steph, Grant, and Kate—thank you for being the brightest spots in my life.

—Mike S.

ABOUT THE AUTHORS

Mike Kegerreis, CISSP, has over 20 years of experience in IT, including 11 as a security professional. Mike graduated from Texas A&M University and spent 12 years as a software developer before moving into information security. He has participated in SANS course and certification development; has spoken at venues such as InfoSec World, CAMP IT, the University of Texas at Dallas, and the Dallas IIA Super Conference; and in a prior life, developed human interfaces for oilfield systems in West Texas. A lifelong fan of golf, Mike also enjoys playing a round whenever he can, and his favorite course as of now is the TPC Las Vegas. Mike is currently the lead security architect at Texas Instruments.

Mike Schiller, CISA, is the chief information security officer at Texas Instruments and has more than 15 years of experience in the IT audit field, including as the IT audit director at Texas Instruments and Sabre. He has been a speaker at conferences such as CACS, InfoSec World, and ASUG (Americas' SAP Users' Group); an instructor of IT audit curriculum at Southern Methodist University; and part of the writing team for all three editions of *IT Auditing: Using Controls to Protect*

Information Assets. Mike graduated from Texas A&M University. He enjoys watching baseball in his spare time and has attended games in every Major League stadium. His baseball allegiance is to the Texas Rangers and Cincinnati Reds.

Chris Davis drives product and architecture strategy for customers building secure and compliant hybrid cloud infrastructures using Caveonix. He has trained and presented in information security, advanced computer forensic analysis, hardware security design, auditing, risk management, and certification curriculum for enterprise and governments worldwide. He has held positions at Oracle, Amazon, VMware, VCE, Critical Start, Accudata Systems, ForeScout Technologies, and Texas Instruments. Chris holds a bachelor's degree in Nuclear Engineering Technologies from Thomas Edison and a master's in business from the University of Texas at Austin. Chris has written and/or contributed to several books covering information security, forensics, and auditing, a few of which are *Hacking Exposed: Computer Forensics* (first and second editions), *IT Auditing: Using Controls to Protect Information Assets* (first and second editions), *Anti-Hacker Toolkit* (second and third editions), and *The Computer Security Handbook* (fifth and sixth editions).

About the Contributors

Brian Wrozek is a seasoned cybersecurity executive with 20+ years of experience in IT and information

security and management. As vice president of corporate security, risk and compliance management, and physical security at Optiv, Brian oversees all corporate security functions, including cyber operations, incident response, vulnerability management, and security governance activities. As an adjunct professor in the Satish and Yasmin Gupta College of Business at the University of Dallas, Brian teaches graduate-level cybersecurity courses. He is also a board member for the Texas CISO Council, an Information Sharing and Analysis Organization (ISAO).

Bobby E. Rogers is an information security engineer working as a contractor for Department of Defense agencies, helping to secure, certify, and accredit their information systems. His duties include information system security engineering, risk management, and certification and accreditation efforts. He retired after 21 years in the U.S. Air Force, serving as a network security engineer and instructor, and has secured networks all over the world. Bobby has a master's degree in information assurance (IA) and is pursuing a doctoral degree in cybersecurity from Capitol Technology University in Maryland. His many certifications include CISSP-ISSEP, CEH, and MCSE: Security, as well as the CompTIA A+, Network+, Security+, and Mobility+ certifications.

Kevin Wheeler is an industry veteran with over 20 years of information security, IT audit, and compliance

experience. Kevin is the founder and managing director of InfoDefense, an information security solutions provider based in Plano, Texas. He has performed information security audits and assessments as well as network security design, computer incident response, business continuity planning, and IT security training for organizations in the financial services, healthcare, manufacturing, government, and IT services industries. Kevin's project and employment portfolio includes organizations such as the U.S. Department of Defense, Bank of America, EDS (now DXC Technology), Symantec, and the state of Texas. He has also been an adjunct IT governance, risk, and compliance professor at Southern Methodist University and is a frequent speaker at information security and information technology audit conferences.

About the Technical Reviewers

Tim Breeding, CISA, CGEIT, currently has the privilege of serving as the IT audit manager at Centennial Bank, where he is responsible for building and leading the IT audit service to meet the present and future needs of the bank. Previously, Tim was blessed to lead IT audit at Walmart Stores, Inc., and Southwest Airlines. At both Walmart and Southwest Airlines, Tim presided over substantial growth of the IT audit functions. His responsibilities included full and complete oversight for all aspects of IT audit. This included managing project teams that assess information technology risks and

mitigation strategies from both an audit and consulting capacity. While at Walmart, Tim also spent several years as a senior director in the Walmart U.S. Program Management Office to promote effective program and project governance. In addition, Tim served more than 13 years in several IT capacities at Texas Instruments. His responsibilities included computer operations, software development, software quality assurance, and IT audit. Tim serves on the board of his local ISACA chapter and has 25 years in the IT audit, controls, and governance profession.

Michael Cox currently works as an information security analyst for Texas Instruments, where he has also worked as an IT auditor developing numerous audit programs and automated audit tools. Prior to this, he worked as a network engineer for Nortel, and he enjoys doing Linux sysadmin work whenever he can get it. Michael has a bachelor of arts degree in history from Abilene Christian University and also served as a technical reviewer for the first two editions of this book.

Gregory Gordon has worked in the information technology industry for over 20 years with an extensive background and certifications in information systems security and auditing (CISSP and CISA) and has served on the IT security board of a global semiconductor design and manufacturing company. As an IT manager of a global B2B integration development and operations team, he is passionate about bringing creative solutions

to technical problems and developing people by helping them to take their next steps. Outside of the office, Greg enjoys all things soccer, traveling and experiencing different cultures, and relaxing with friends and family.

John Clark, CISSP, CISA, CISM, CIPP/E, CIPT, FIP, is an information security executive advisor to CISOs, CIOs, board rooms, and business executives. With over 20 years of experience in information technology and security, he has developed a passion for working with clients, large and small, to develop business-aligned information security and operational risk management programs. John has provided information security consulting and risk assessment services across a wide variety of industries, including financial services, gaming, healthcare, biotech, and telecommunications services. In his current role as executive director of oCISO Services at Optiv, he is part of a select team that assists clients in developing and executing information security program strategies and enabling effective information security program operation. Prior to joining Optiv, John held a variety of information security and risk management leadership positions at Andrews Kurth, American Express, and First National Bank of Arizona. In addition to multiple industry certifications, John has a bachelor's degree in management information systems and an MBA from the University of Houston.

CONTENTS

ACKNOWLEDGMENTS

We simply could not have done this without the help of many, many people. It was an amazing challenge coordinating the necessary depth of corporate, legal, and technical expertise across so many subjects. Many old and new friends; organizations such as ISACA, NIST, and OWASP; and many others donated knowledge, time, techniques, tools, and much more to make this project a success.

Writing this book required tireless hours of writing, research, and corroboration among the authors, contributing authors, technical editors, industry peers, copy editors, layout team, and publisher leadership team while our loved ones took the brunt of our efforts. It is only appropriate that we thank and acknowledge those who supported and carried us despite ourselves. We are truly grateful to each of you.

The wonderful and overworked team at McGraw-Hill is simply outstanding. We sincerely appreciate your dedication, coaching, and long hours during the course of this project. Wendy Rinaldi, thank you for your excellent leadership, coordination, and guidance to bring this project to fruition. Your willingness to step in and

provide solutions when we hit snags was impressive and appreciated. We would also like to extend a big round of thanks to Claire Yee, our acquisitions coordinator, for her coordination and work with the technical editors. Thank you so much for being a part of this. We also would like to thank the wonderful efforts of the project editor, Rachel Fogelberg; copy editor, Lisa McCoy; proofreader, Paul Tyler; indexer, Ted Laux; editorial supervisor, Patty Mon; production supervisor, Lynn Messina; and compositor and illustrator, Cenveo Publisher Services.

A special thank you goes to Brian Wrozek and Bobby Rogers for coming on board at the eleventh hour and helping to fill in some critical gaps. Your involvement was valuable and truly made a difference. And thank you to Tim Breeding, Michael Cox, Greg Gordon, and John Clark for their deep technical reviews for the third edition. Your reviews were wonderful, detailed, and significant in providing a useful product for the readers. Thank you also to Kevin Wheeler for your contributions.

We also want to acknowledge and extend our thanks to the many people who were involved with editing, reviewing, and publishing the first two editions. Without your work on the first two editions, there would be no third edition. Thank you to the contributing authors for the first two editions: Stacey Hamaker and Aaron Newman. Thank you to our previous technical reviewers: Barbara Anderson, Mike Curry, Subesh Ghose, Keith Loyd (we miss you, Keith), and Vishal Mehra. And thank

you to the fine folks at McGraw-Hill who played critical roles in the first two editions. First edition: Jane Brownlow, Jennifer Housh, Madhu Bhardwaj, Jim Madru, Ragini Pandey, Kevin Broccoli, Janet Walden, George Anderson, and Jeff Weeks. Second edition: Megg Morin, Joya Anthony, LeeAnn Pickrell, Lisa Theobald, Martin Benes, Karin Arrigoni, Jody McKenzie, James Kussow, Jeff Weeks, and Lyssa Wald.

We are truly grateful to three organizations that allowed us to borrow content. We would like to thank the people at ISACA for bringing a cohesive knowledge set to the auditing field and the CISA certification. There is still much work to be done, and we as a team would like to encourage our peers to contribute to this wonderful knowledge base. Likewise, thank you Jeff Williams and Mark Curphey for founding and contributing to OWASP. Your selfless investments are helping thousands of professionals worldwide and many more who would never know where to start securing their websites. Thank you. And thank you to NIST for adding much-needed guidance and standards to the world of cybersecurity.

Finally, thank you to everyone who bought, read, used, and supported the first two editions of this book. We have been extremely honored and humbled by the response we received to the earlier editions and inspired to improve on our work with this third edition.

—Mike, Mike, and Chris

Thank you to Mike Schiller for considering me for this project and taking a risk on me as a new author. Your

confidence in me and support during this effort and for my career in general have been terrific, and I've been honored to work with you.

A big thanks to Greg Gordon for his technical review of my work, and thanks to all of the other technical reviewers who helped make this happen.

Thanks to Brian Wrozek for jumping into this project late in the game and for opening that door for me into the security field almost 12 years ago. I'm thankful for your guidance and influence over the years.

Thank you to all of the auditors, security practitioners, software developers, businesses, and others who share what you've learned in books, papers, magazines, conferences, forums, blogs, and more. A book like this isn't a compilation of things we as authors just "know"—we don't sit down and just start cranking out complete chapters from memory or experience. A lot of this is the result of research and learning from other people, and I couldn't have written any of these chapters without your help. You make the rest of us better by sharing what you know; if you learn something useful from this book, please help the folks around you and pass it on.

To my friend Billy Rodgers—thank you for your priceless expression after seeing the second edition of this book on my counter, saying something about it sounding like a real page-turner, and then hearing that I was working on the third edition. Thanks for keeping me grounded, for helping me remember that this is not really Pulitzer-type stuff, and for being such a terrific

Christian role model for me and my family.

And most of all, thanks to my family for your incredible love and support. Thanks to Kristy, for putting up with a cardboard desk so I could work on this project while we were moving and, of course, for considering this book for a future book club selection. Thanks to Leah, Brian, and Caroline for your understanding as I disappeared, was distracted, or delayed vacations or events so I could meet a deadline. Is it break time?

—Mike Kegerreis

Thanks to Mike Kegerreis for agreeing to come on board for this project and for doing the lion's share of the heavy lifting. This edition wouldn't have happened without your involvement. You're clearly the MVP of this edition, and I'm constantly amazed by your skills as a security professional.

I would like to thank my good friend Tim Breeding for somehow making the time to be the technical reviewer for most of my chapters. You're an amazing audit professional, and your audit expertise and quality review comments made a difference. Thanks to Michael Cox, the Cal Ripken, Jr. of technical reviewers on this book, for agreeing to review the Unix chapter for a record-breaking third straight edition. And thanks to Greg Gordon for agreeing to provide the technical review for my unassigned chapter.

I would also like to thank Chris Davis for his friendship and partnership through the years.

Thanks to Brian Wrozek for the diving catch and, more importantly, for being a great friend and valued peer.

Thanks to Subesh Ghose for letting me pick your brain about recent changes in the audit field.

In previous editions, I listed a large number of people who I've worked with and learned from over the years. In the interest of brevity, I'm not going to duplicate all of those names here, but to all who were mentioned in those books, I remain grateful for you and your impact on my life and career.

Of course, thanks go to God and Jesus Christ for my salvation and for the many blessings in my life.

Most of all, thanks to my family. I have been blessed with the perfect wife, son, daughter, mom, dad, and brother. Thank you all for your love and support. Steph, thank you for being my best friend and for believing in me. Grant and Kate, thank you for making me happy and proud and for giving me an excuse to go to Disney so often.

—Mike Schiller

INTRODUCTION

When we began writing this book, we had a fundamental tenet: Write a clear handbook for creating the organization's IT audit function and for performing their IT audits. We wanted this book to provide more than checklists and textbook theories and instead to provide real-life practical guidance from people who have performed IT audit work day in and day out in real corporations. If we've been successful, reading this book will accomplish three objectives for the reader, above and beyond what can be obtained from most IT auditing books and classes:

Guide the reader in how to perform the IT audit function in such a way that the auditors maximize the value they provide to the company.

Part I of this book is dedicated to providing practical guidance on how to perform the IT audit function in such a way that it will be considered an essential and respected element of the company's IT environment. This guidance is pulled from years of experience and best practices, and even the most experienced of IT auditors will find a plethora of useful tools and techniques in

those chapters.

Enable the reader to perform thorough audits of common IT topics, processes, and technologies.

Part II of this book is dedicated to guiding the reader with practical, detailed advice on not only what to do but also *why* and *how* to do it. Too many IT audit resources provide bullet-oriented checklists without empowering the auditor with enough information to understand why they're performing that task or how exactly to accomplish the step. Our goal is to fill that gap for the reader.

Give the reader exposure to IT audit standards and frameworks, as well as the regulations that are currently driving the IT audit profession.

Part III focuses on standards and frameworks such as COBIT, ITIL, and ISO 27001, as well as regulations such as Sarbanes-Oxley, HIPAA, and PCI. Another goal of this section is to demystify risk assessment and management, which is required by most regulations.

A wealth of knowledge and resources for hardening systems and performing detailed penetration tests are available in other texts. That is not the focus of this book. In our experience as auditors, we have been called on more often to judge the quality of internal controls from an insider's standpoint. Therefore, the majority of audit steps in this book are written with the assumption that the auditor has full access to all configuration files,

documentation, and information. This is not a hackers' guidebook but is instead a guidebook on how an auditor can assess and judge the internal controls and security of the IT systems and processes at his or her company.

HOW THIS BOOK IS ORGANIZED

This book is organized into three parts. Part I, "Audit Overview," helps you understand the IT audit process, how to build and maintain an effective IT audit team, and how to maximize the value of the IT audit function. Part II, "Auditing Techniques," then helps you understand what specific components or audit steps might be necessary for an audit of a specific system or process. Finally, Part III, "Frameworks, Standards, Regulations, and Risk Management" covers the frameworks, standards, regulations, and risks that govern the scope of the audit function.

Audit Technique Chapters

Part II contains a series of suggested audit programs or techniques for commonly audited systems and processes. The chapters in this section are structured to help you quickly digest the information that's most useful to you.

Background

This part of the chapter contains information about the topic's history or background information that helps you acclimate to the subject matter.

Auditing Essentials

For chapters dealing with a specific technology, this part of the chapter describes getting around within the technology and introduces you to basic concepts, commands, and tools.

Test Steps

This is the meat of the chapters in Part II and provides details about what the auditor should look for, why they should do so (that is, what risk is being addressed), and how the step can be performed.

This is the audit step that should be performed

The text immediately following the step states why this step is important. This section states the reason why, such as the risk and business need, the step should be performed.

How

This describes how to perform the step. We commonly use design elements such as tables and code listings to help you navigate the content.

```
This is an example code listing.
```

Tools and Technology

This section lists the tools used in the test steps and other tools not covered but mentioned as popular for more closely examining the technology. The purpose of this is to provide in a shortened format some of the tools readers might want to consider as they look further into

the technology.

Knowledge Base

This section provides a list of websites and books where readers can find more information about the topics covered in the chapter. We can't discuss everything, but we can point to places where others discuss more than you could possibly want to know.

Master Checklist(s)

This check-boxed table summarizes the steps listed in the chapter. Similar to other checklists, you may need to customize this according to what makes sense to you and what you consider to be your own high priorities.

A FINAL WORD TO OUR READERS

Thank you for taking the time to read this book. Technology continues to evolve, and audit techniques need to evolve as well. In the years since the second edition of this book was released in 2011, areas such as cybersecurity and big data have matured and entered the mainstream. In this third edition, you will find all-new chapters providing guidance on auditing cybersecurity programs, big data and data repositories, and new technologies (technologies that aren't specifically covered in this book). In addition, all other chapters have been updated and enhanced to reflect recent trends and advances.

We have put countless hours and enormous effort into

creating something we hope will be useful for you. Read this book all the way through, and then, when you are done using it as a tutorial, you can keep it around as a reference. Auditing is a detail-oriented job, and it is easy to get overwhelmed and overlook something. In addition, it is easy to get in over your head. This book is a great place to start, learn, and expand on what you know. We hope you enjoy reading this book as much as we enjoyed writing it. Good luck in all your audits.

PART I

Audit Overview

CHAPTER 5

Auditing Data Centers and Disaster Recovery

Information technology (IT) processing facilities, usually referred to as data centers, are at the core of most modern organizations' operations, supporting almost all critical business activities. In this chapter we will discuss the steps for auditing data center controls, including the following areas:

- Physical security and environmental controls
- Data center operations
- System and site resiliency
- Disaster preparedness

BACKGROUND

Ever since the first general-purpose electronic computer (the Electronic Numerical Integrator and Computer, or ENIAC) was created in 1946, computer systems have had specific environmental, power, and physical security requirements. Beginning in the late 1950s, as mainframe computers became more widely available, data centers were created for the express purpose of meeting these requirements. Now, many organizations have their own

data centers or co-locate their systems in a shared facility, although more and more companies are using the cloud for services that were previously hosted in dedicated or co-located data centers (see Chapter 16 for further discussion of this concept).

Today's data centers provide physical access control infrastructure, environmental controls, power and network connectivity, fire suppression systems, and alarm systems. This data center infrastructure is designed to maintain a constant optimal computing environment. The auditor's role is to verify and validate that all of the necessary systems and procedures are present and working properly to protect the confidentiality, integrity, and availability of the company's systems and data.

DATA CENTER AUDITING ESSENTIALS

A data center is a facility that is designed to house an organization's critical systems, which comprise computer hardware, operating systems, and applications. Applications are leveraged to support specific business processes such as order fulfillment, customer relationship management (CRM), and accounting. Figure 5-1 shows the relationships among data center facilities, system platforms, databases, applications, and business processes.

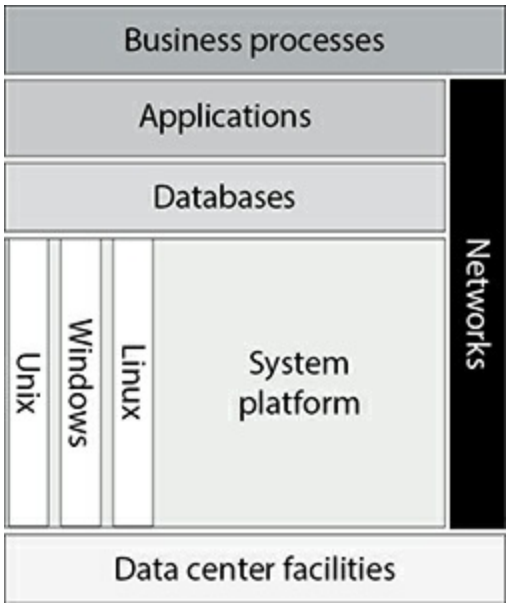

Figure 5-1 Data-processing hierarchy

As you can see, data center facilities are at the foundation of the hierarchy, which is why it is so important that they have the necessary controls to mitigate risk. Major data center threats include the following:

- Natural threats, such as weather events, flooding, earthquakes, and fire
- Manmade threats, such as terrorist incidents, riots, theft, and sabotage
- Environmental hazards, such as extreme temperatures and humidity
- Loss of utilities, such as electrical power and telecommunications

You may notice that most of these threats are physical in nature. In this age of advanced technology, it is easy to

forget the importance of physical controls and focus your energy on logical controls. However, even with excellent logical access controls in place, these physical threats can compromise your systems' security and availability.

For those who have not worked in a data center environment, data centers can be a little overwhelming. Particularly in large environments and co-located facilities, data center access might be experienced through intimidating man-traps (doors specifically designed to allow only one person through at a time), physical guards, biometric readers, and card-key-access authentication systems.

Once you pass into the computing environment, you should notice racks of computer systems sitting on a raised floor. Most of the time, miles of power and network cables are run beneath the raised floor, although many data centers run cables through open conduits that hang from the ceiling. You also will notice generators, large power conditioners, and UPS (uninterruptible power supply) devices or rooms filled with batteries to ensure that clean, uninterrupted power is available at all times. Most data centers have industrial-strength heating, ventilation, and air conditioning systems to maintain optimal temperature and humidity levels within the facility.

The brain of the data center facility is the control center. It usually consists of a series of consoles and computer monitors that are used to monitor temperature, humidity levels, power consumption,

alarms, and critical system status. Many times, if the control center is actually physically located within the data center, the control center and tape operations may be the only areas consistently manned by data center personnel.

For the purpose of the data center audit, we will explore physical security and environmental controls; system and site resiliency controls; policies, plans, and procedures used in governing data center operations; and controls that enable disaster preparedness.

Physical Security and Environmental Controls

Data centers incorporate several types of facility-based controls, commonly referred to as physical security and environmental controls, including facility access control systems, alarm systems, and fire suppression systems. These systems are designed to prevent unauthorized intrusion, detect problems before they cause damage, and prevent the spread of fire.

Facility Access Control Systems

Facility access control systems authenticate workers prior to providing physical entry to facilities, with the goal of protecting the information systems that reside within the data center. Physical access control systems use the same concepts as logical access control systems for authentication based on something you know, something you have, and/or something you are. For example, the “something you know” may be a PIN code

for a door. The “something you have” might include card-key systems or proximity badge systems, or you may have a physical key to unlock a door. In some cases, the access control system can be a standard key lock or simplex lock, although you’ll see later that these are not preferred stand-alone mechanisms for controlling access. The “something you are” may include biometric devices that read fingerprints, hand geometry, and even retina characteristics to authenticate individuals who need to enter the facility.

Access control systems may use a man-trap to enforce the authentication mechanism. Man-traps consist of two doors that are separated by a corridor or a small closet-sized room. People entering the facility must first authenticate to open the door that allows them to enter the corridor. Once the first door closes behind them, they must authenticate again to open the door leading to the data center facility. The two doors cannot be open at the same time. Even if someone is able to circumvent security and gain access to the corridor via the first door, the person will be effectively trapped when the access control system blocks his or her access to the data center itself.

Alarm Systems

Because fire, water, extreme heat and humidity levels, power fluctuations, and physical intrusion threaten data center operations, data centers should implement several different types of alarm systems. Specifically, you will

normally see the following types of alarms:

- Burglar alarms (with magnetic door, window, or cabinet sensors; motion sensors; and sometimes audio sensors)
- Fire alarms (usually heat- and/or smoke-activated sensors broken into zones that cover different parts of the facility)
- Water alarms (usually with sensors beneath the raised floor, near bathrooms, or in water pipe ducts)
- Humidity alarms (normally with sensors dispersed throughout the facility)
- Power fluctuation alarms (with sensors that can detect dips and spikes in the power grid)
- Chemical or gas alarms (sometimes in battery rooms and near air intakes)

These alarm systems usually feed into the data center operations center. During an alarm condition, the operator can drill down to specific sensors and reference a surveillance camera to isolate the cause of a problem.

Fire Suppression Systems

Because of the large amount of electrical equipment, fire is a major threat to data centers. Therefore, data centers normally are equipped with sophisticated fire suppression systems and should have a sufficient number of fire extinguishers. Generally speaking, fire-