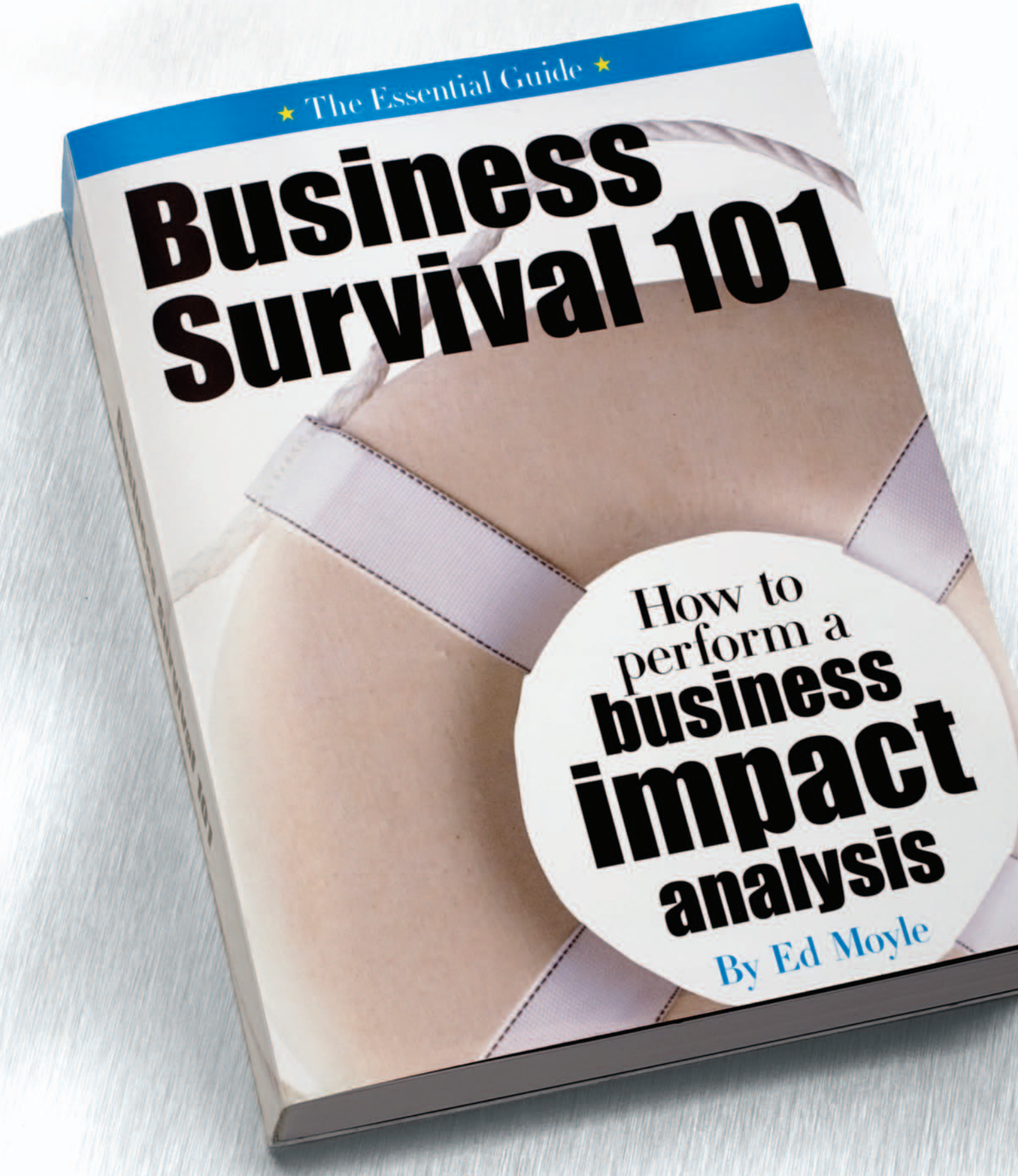
Creating Effective Policies and Procedures

SOUND INFORMATION SECURITY programs have the right technology in place but also appropriate policies and procedures. By using risk management methodologies, creating formalized architecture diagrams and devising plans in the case of a disaster, you'll be prepared for whatever comes your way.

INSIDE

INFORMATION SECURITY®



Photograph by JOHN KUCZALA

A business impact analysis can be a manual that helps your company weather disasters.

In IT, the idea of anything shutting down business—even for a day—is terrifying. Downtime costs money, and there are areas of the business that must stay running despite a disaster, natural or man-made. Nevertheless, trying to ensure near-total uptime for every machine and process would bankrupt most companies long before an outage would.

The challenge for IT managers is prioritization: determining which areas of the business must stay operational and which can afford to be down. We know that the company will lose money if revenue-generating areas can't function, but how much money? We know that without access to tools and resources, marketing and human resources are less productive, but how much less productive?

Knowing which areas of the business need to get up and running first after a system goes down can mean the difference between survival and extinction. That's where a business impact analysis (BIA) comes in. Like a survival guide for your business, it lays out which areas are most critical—either because they directly generate revenue or the company depends on them for successful day-to-day operation.

A BIA can also help drive other security functions, such as vulnerability assessment, risk management and incident response. Strategic planning and handling will make your BIA an effective guide to ensure your company stays alive.

BIA Basics

Business impact analysis is used within business continuity planning (BCP) to refer to a systematic process of measuring, analyzing and documenting how various business functions are affected by outages—both as individual processes and for the company as a whole.

The goal of the BIA is to allow a business to understand how its various revenue-generating and support organizations operate and interact. Firms can then develop a more accurate picture of which areas of the business will be hit hardest by disruptions and how failures in one area of the business could cause other parts to fail.

At the end of a BIA project, organizations should understand which processes are most critical to keeping the firm running. This allows them to prioritize investments in preparedness, orchestrate continuity activities and implement contingency measures for the most critical systems to reduce the impact of a disruption.

The key to getting maximum value from a BIA is to encourage wide distribution, high visibility and flexibility in a way that makes the guide easy to use and maintain. *(See "Your BIA Survival Guide," next page.)*

An effective BIA is a living document.

Content Collection

While there are many methodologies available for performing an impact analysis and numerous conventions for structuring the final document, effective BIAs have more to do with content than format.

At a minimum, the BIA should contain a comprehensive catalog of business and support functions within the organization; some description of those functions, lists of critical systems and other resources involved in maintaining them; and a spider web of dependency/support relationships between the surveyed business functions.

Getting this minimal data can be a serious chore. Typically, most BIA endeavors begin by asking managers directly for specific details about the areas of the business for which they are responsible. Many BIA initiatives will start by sending questionnaires to sales managers, marketing executives and business unit directors that ask for information related to the function, operation and dependencies of the processes they oversee. These questionnaires are less intrusive to the business than gathering the information via an interview, so they're used more often.

Responses from the key managers can be used to map out dependency relationships and locate "hidden" processes, such as low-visibility functions or those performed outside the firm by a vendor or trusted partner. Examples are outsourced support-desk help or vendor-provided maintenance. These functions might be critical to business operation, but given their vendor-supplied nature, they may not be apparent in budgets or have dedicated personnel. These previously untracked activities can be added to a master inventory and their managers invited to participate in the BIA process; their input may yield even more areas to examine.

At the end of the exercise, the business is left with a comprehensive catalog of all functions and a precise road map of how they interact. The remaining task is to document those relationships and ensure updates are made as processes change.

In addition to documenting how business processes interact, it's important to collect financial information about them. Access to finances allows you to predict potential lost revenue, productivity costs and opportunity costs related to downtime in individual business units. Business managers will likely have basic profit and loss information for systems, but since you ultimately want to shed light on total downtime costs, you'll need to gather additional data.

To create this more detailed financial profile, enlist other areas of the firm to help. For example, the compliance department can provide insight into the fines or penalties that may be incurred if a particular process suffers downtime, while the legal department can help you understand what potential contractually defined fees you might owe if you are unable to provide service to clients for an extended period of time.

This financial picture can then be tied to the dependency information collected so that you can see, in dollars, the impact of one or more processes being unavailable.

Integration

An effective BIA is a living document; creating yet another document to gather dust on a shelf obviously isn't useful. Integrating the BIA into other areas outside BCP ensures that the document will continue to be relevant.

In other words, once an organization has invested the time and resources required to gather, correlate and document its business processes, that investment can be maximized by using the BIA in as many other areas of the firm as possible. Additionally, using the BIA for other activities outside BCP will keep it current. After all, the business processes documented in the BIA are continuously evolving—updating the document as they evolve is critical.

A good place to make broad use of the document is in the "non-disaster planning" information security world. Vulnerability assessment, application assess-

ment, risk management and incident response can all benefit from having a BIA.

For security organizations that perform automated vulnerability assessment, the information in the BIA can increase an assessment's effectiveness by taking into account a machine's criticality. During assessment planning, organizations can decide whether to include critical servers in their scans to help harden those machines or to preclude scans of those servers to minimize potential downtime. Alternatively, organizations may want to use a blended approach with less intrusive scan settings against critical servers than they would against non-critical ones.

A BIA can also assist in application assessment by allowing assessors to use them as a means of gathering intelligence. Specifically, the BIA can provide dependency information to help companies understand how these applications interact, how they relate to the business, and how data flows into and out of the application.

Data gathered during application and vulnerability assessments can drive changes to the BIA. Assessments may highlight application changes, and those changes can reflect updates to the underlying business process. Personnel evaluating applications can periodically "freshen" the BIA by aligning it with those changes.

Risk management is another area outside continuity planning where the BIA can help. Often, information security teams that try to quantify overall risk either cannot assign dollar amounts to risk or are forced to use soft dollar values derived from rough estimates. However, by drawing on a BIA that contains hard dollar values, you can replace estimated costs with actual costs to enhance the precision and credibility of risk management activities and provide more effective communication of risks to business partners.

Some risk management activities are also limited by the domino effect caused by compromised systems cascading risk to dependent systems. Having those interactions documented in a BIA can provide insight into this phenomenon and allow risk management activities to include these risks in the overall risk profile for a given application.

BIA content can also help incident response. If the BIA includes operational information about critical applications—such as application owners' contact information and addresses/platforms of critical servers—response personnel can take proactive steps in the event of an incident to ensure that these critical applications stay up. For example, if a worm is spreading through the network, personnel can contact the managers of the highest priority systems early on to relay protection measures—hopefully before those critical machines become infected.

Critical Factors

There are a few simple steps that can mean the difference between the success and failure of a BIA: ensuring open communication and buy-in, establishing a high-level tracking framework and assigning accountability.

Writing Tips

Your BIA Survival Guide

When it comes to the mechanics of writing a BIA—formatting, organization of data and cataloguing business information—there are many methods from which to choose. Keeping the following goals in mind when writing the document will make it easy to use and facilitate ongoing maintenance:

Readability–The sheer amount of data in a BIA can make it difficult for a reader to quickly find specific information—unless the format encourages rapid lookup. Providing a by-subject index and/or detailed table of contents can mean the difference between readers finding content quickly and giving up on the BIA as an information source.

Maintainability–A document is only useful as long as the information within it is current. Take measures to ensure that the document receives periodic updates or input from other activities. The document format itself can encourage updates: Soft-copy artifacts written in Microsoft Word or Excel are much easier to keep updated than paper copies, file formats that require special tools to modify such as PDF or Visio, or documents that are incorporated by reference.

Comprehensiveness–The more data that is included in the BIA—such as IP addresses associated with critical servers and software packages used to support business—the more useful the document will be in the long term. If there's an authoritative source for the data, it's helpful to include this to ease future updates and allow readers the option of going to the most accurate source of information. If the BIA includes contact information for server managers, it's helpful to also include a link to the corporate directory so that readers know where to go for the most updated contact details.

–ED MOYLE

Definition

Risky Business

BY PAUL ROHMEYER

A business impact analysis must be performed in a risk context.

An early step in conducting a BIA is to define what is meant by the phrase "business impact" within the context of an organization's risk environment. Assessing the impact of a system outage or other technical event requires an understanding of the risks associated with underlying business processes and supporting information systems.

Organizations face many different types of risk, including health and safety, customer satisfaction, reputation and financial.

Health and safety risk applies to the physical well-being of customers, company employees and the public. Customer satisfaction risk is typically focused on the organization's ability to continue delivering high quality products and services to customers. Reputation risk is often the most serious to businesses, as events can quickly destroy a good name that had been fostered over many years and at a great expense. Financial risk relates to the impact a disruption may have on a company's ability to generate revenue; another financial consideration is the cost associated with responding to and recovering from an outage or disruption.

The degree or value of impact can be estimated by considering the factors associated with each risk type. For example, customer satisfaction risk can be estimated by considering the effect of potential system unavailability for any period of time. Several factors can decrease or increase the actual impact, such as the day or time of the risk event; your BIA should summarize the individual risk factors and present an aggregate rating for each function or process.

Ultimately, your BIA should include a recovery time objective (RTO) for each business function that identifies the longest tolerable disruptions. Cyclical industries should adjust their RTOs to recover faster during traditionally busy times.

Once the relevant risks are understood, your organization can use its BIA to estimate the impact of events on critical business processes and functions, the supporting information systems and their interdependencies.

Paul Rohmeyer, Ph.D., is an assistant professor at Stevens Institute of Technology and an IT risk management consultant.

From the earliest planning stages until after the document is created, it is important to have open lines of communication with key organizational players. Obtaining appropriate buy-in from upper management and the business community early in the lifecycle is also a must. Managers of critical business functions have a lot on their plate, but fully communicating the purpose and value of the BIA can ensure their cooperation in making the data they supply complete and accurate. After all, the BIA is ultimately a document that helps them—it is their processes you are trying to protect.

Keeping the lines of communication open after the data is gathered is also important to make sure the document reflects changes in business processes and remains relevant. Additionally, maintaining a dialogue with internal auditors, compliance managers and the rest of the information security organization can guarantee the document has a broader scope outside of contingency planning.

A high-level framework for project management over time is an essential part of building a proper foundation for your BIA. Even smaller organizations will have numerous interdependent business processes that will need to be accounted for—probably too many to track without careful organization. Intelligence-gathering for the BIA will uncover many other processes, and new business functions are likely to be put in place during the engagement.

Setting up a mechanism for tracking these processes as they are discovered and created will ensure that nothing slips through the cracks. The project will likely have high visibility, and using a metrics-driven approach streamlines status reporting and allows rapid schedule modifications if dates slip.

Assigning accountability for BIA tasks is also an important step. BIAs can contain quite a bit of data, but harvesting that information is extremely time-consuming. Allocating and tracking individual tasks ensures that the data gets collected and the project stays on schedule.

If created and used strategically, a BIA can be one of the best investments your firm can make—both for contingency planning and for information security as a whole. Once the document is in place, taking steps to keep its contents current ensures that the BIA is useful as a survival guide for years to come.

Ed Moyle is a manager for CTG, an information security services and consulting firm.

DON'T WAIT

FOR DISASTER. SECURITY MANAGERS ARE COVERING THEIR BASES TO CURB THE EFFECTS OF AN AVIAN FLU PANDEMIC. HERE'S WHAT SOME ARE DOING.

BY MARCIA SAVAGE

IN THE INSURANCE BUSINESS, PLANNING FOR THE unexpected is all in a day's work. But for the past several months, Paul Klahn has been planning for the unthinkable: an avian flu pandemic.

As information security officer for Assurant Employee Benefits, a Kansas City-based unit of insurance firm Assurant, Klahn is part of a team preparing the company should a pandemic strike. Team members plot out how to weather scary scenarios like severe workforce shortages, the need to keep employees apart and a possible surge in claims.

"You have to start planning," Klahn says. "Everything I've read from the Centers for Disease Control (CDC) and the World Health Organization (WHO) characterizes it as a real threat."

The warnings from experts about the possibility of an avian flu pandemic are certainly ominous. According to WHO, the H5N1 virus—a strain of avian influenza—has "considerable" pandemic potential. If the virus becomes fully transmissible between humans, it will spread throughout the world in three months, the organization believes.

If a severe pandemic similar to the devastating 1918 Spanish flu hits, U.S. officials estimate that 90 million people could become infected and 1.9 million may die. They advise businesses to expect an employee absenteeism rate of up to 40 percent due to illness, employees caring for ill relatives and fear of infection. The World Bank forecasts the economic impact of a pandemic on the U.S. at $350 billion.

A number of organizations, especially large companies, are heeding these dire predictions. They're figuring out ways to have employees work remotely, initiating employee education campaigns, identifying critical business functions, stockpiling hand sanitizers and masks, and making sure their suppliers are also preparing.

"You have to start planning. Everything I've read from the Centers for Disease Control (CDC) and World Health Organization (WHO) characterizes it as a real threat."

–PAUL KLAHN, information security officer for Assurant Employee Benefits

Photograph by SCOTT MILLER

AVIAN FLU FACTS

OUT SICK

- Avian influenza, also called "bird flu," is an infection caused by influenza viruses that occur naturally in birds.
- One strain of avian influenza, the H5N1 virus, is endemic in much of Asia and has spread into Europe.
- Human H5N1 influenza was first seen in 1997 when the virus infected 18 people in Hong Kong, causing six deaths.
- Close contact with infected poultry has been the primary source of human infection. There have been rare, isolated reports of human-to-human transmission of the virus.
- H5N1 mutates rapidly. Should it adapt to allow easy human-to-human transmission, a pandemic could develop.
- Vaccines to protect humans against H5N1 viruses are under development.

SOURCE: U.S. government (www.pandemicflu.gov)

"If we have a 1918-like pandemic, it's going to be brutal," says Jay Schwarz, vice president of information systems at Alex Lee, a Hickory, N.C.-based wholesale and retail food company. "There are things that companies can do to prepare that could be the difference between survival or not for any organization."

A survey of 222 North American companies conducted by Gartner last year showed only tepid interest in conducting pandemic planning, but analyst Roberta Witty says that's changed this year, with about 20 percent looking to plan. Certain industries are more proactive than others, including financial institutions, food distribution companies and transportation firms, she says.

Aside from planning to have employees work at home by beefing up VPN capabilities and adding videoconferencing technologies, companies need to look at how they'll handle inventories—especially in our just-in-time economy—and adjust human resource policies to handle extended absences, travel and the myriad issues a pandemic presents.

"Some say it's like Y2K, a non-issue…but responsible companies put steps in place so the Y2K issues were addressed," says Ken Wilson, a management consultant who specializes in pandemic planning. "If responsible companies prepare and educate employees, we have a good chance of minimizing the [pandemic's] impact on our country."

CATASTROPHE PLANNING

At Assurant, planning for a possible avian flu pandemic began in earnest earlier this year. The employees involved in the effort serve on a handful of committees representing various departments, including IT, healthcare and human resources.

"It's a significant effort," says Klahn, who is on the IT committee. "We're running down every scenario we can."

For example, a pandemic may cause claims to go up, so the company—which has about 12,000 employees—needs to plan accordingly so it can best serve its customers.

Being able to have employees work remotely, either at home or elsewhere, is a top priority that comes with plenty of challenges. Experts suggest that paper-based processes and privacy regulations such as HIPAA are some of the issues companies face in creating offsite work situations. In some instances—such as customer-service representatives needing sensitive data to handle calls—having employees work at home raises privacy issues if that data is on their personal computers, Gartner's Witty says.

Understanding the company's critical business functions has been crucial in the planning effort, especially for IT, Klahn says. Rather than just throwing up a lot of remote-access technology, understanding essential processes can lead to other solutions.

"We have to prioritize which business functions are most critical to keep running. We might repurpose people and give them the opportunity to work in different parts of the company to keep those critical functions going," he says.

In the end, the planning will help the IT department become stronger because it will be more aligned with the business and more agile with enhanced work-at-home capabilities, Klahn adds.

"The reality for us, as a company, is that this type of broad planning just increases our capabilities to serve our customers and employees in the long run," he says.

Officials in Orange County, Fla., also expect a long-term payoff in preparing for a pandemic, which is part of the county's comprehensive emergency management strategy. The county's pandemic planning group includes emergency medical service agencies, hospitals and other community organizations that would respond in the event of an outbreak. The group considers issues such as how to continue services that can't be provided remotely.

"Even if we don't have a pandemic, the planning and infrastructure will serve us well no matter what the emergency is," says Dave Freeman, Orange County health and medical disaster coordinator and manager of the county office of emergency medical services.

"The most important element is the planning process itself. It brings together community partners working toward a common goal," Freeman adds. "As you do this consistently, your overall capability becomes more robust because people are used to working with each other. You become much more adaptable no matter what the event is."

Photograph by JUPITER IMAGES

HISTORY OF PANDEMICS

Influenza pandemics are rare, but have typically occurred every 10 to 50 years throughout recorded history, with three in the last century.

1918

- **Spanish flu**–The most devastating flu pandemic in recent history, it killed more than 500,000 people in the U.S., and 20 million to 50 million worldwide.

1957-1958

- **Asian flu**–First identified in China, this virus caused roughly 70,000 deaths in the U.S.

1968-1969

- **Hong Kong flu**–First detected in Hong Kong, it caused roughly 34,000 deaths in the U.S. H3N2 viruses still circulate.

SOURCES: National Institute of Allergy and Infectious Diseases and WHO

A DIFFERENT KIND OF BCP

The business continuity team and medical staff at Constellation Energy had been monitoring the avian flu situation since the middle of 2005. At the time, even though the probability of it becoming a pandemic appeared low, its impact would be high, making it a high risk, says Robert Cornelius, director of business continuity at the Baltimore-based Fortune 150 company.

"We look at everything from a risk perspective," he says. "We felt that the prudent thing to do was to start planning for this [possible pandemic outbreak]."

Protecting its 9,700 employees and keeping critical businesses functioning in the event of hurricanes or other disasters have always been priorities for Constellation. While the company could have used its existing business continuity plans (BCPs)—which identify critical business processes—as a starting point, a pandemic required additional work.

"This is an attack on your human resources," Cornelius says. "We felt we needed very specific plans."

Together with Constellation's medical and safety departments, his team spent time with experts to understand the threat, educated upper management on the risk, won senior leaders' endorsement for the planning effort and reached out to the company's business units.

In a worst-case scenario, in which a pandemic results in many infections and deaths, companies need to plan for how they'll take care of employees who must come into the facility to perform critical functions, Cornelius says.

INFLUENZA PANDEMIC RESOURCES

www.pandemicflu.gov • U.S. government avian and pandemic flu information, managed by the Department of Health and Human Services (HHS); includes a business pandemic planning checklist developed by HHS and the Centers for Disease Control and Prevention (CDC)

www.cidrap.umn.edu • University of Minnesota Center for Infectious Disease Research and Policy; includes a pandemic analysis by food company Alex Lee

www.who.int/topics/avian_influenza/en • World Health Organization resource

www.cdc.gov/flu/avian/index.htm • CDC resource

"There are certain crucial functions that people have to come into our facilities to perform, like control room operations, electric substation repairs and gas emergency response," he says. "We need to have plans for those people to work. Other folks, we'd have work at home…. We're going to try to protect our people as best we can. So for the people coming in, we need to make sure we have the proper operational plans and supplies."

To that end, Constellation has stocked up on gloves, masks and bacterial cleaners. It is also educating employees on how to prepare at home for emergencies, including a pandemic. Using "lunch-and-learn" seminars and department safety meetings to educate employees has been effective, Cornelius says.

Every company should focus on educating employees about the pandemic threat, says Harold Bingham, business continuity program manager at Monster.com. He's done presentations throughout the online career firm to prepare employees.

"To the extent that your employees are informed, it's a higher likelihood that the panic and fear will be diminished," he says. "That's going to be key."

LESSONS LEARNED

For Intel, the SARS crisis was a learning experience that's helped the chip giant prepare for a possible avian flu pandemic. In 2003, when Severe Acute Respiratory Syndrome was hitting Asia, Intel was forced to cancel conferences in the area and close an office in Hong Kong after an employee showed symptoms of the disease.

As the crisis unfolded, Intel put in place safeguards and established mechanisms for staying in touch with WHO and other health agencies about outbreaks, says spokesman Chuck Mulloy: "We'll monitor their activities closely and step up the response depending on what's called for in any place in the world where we have facilities."

A company-wide leadership task force has developed plans and supplemented existing policies so that Intel can respond in the event of a pandemic.

For example, the company has had a telecommuting policy for years, but needed to make sure it would apply in the event of an outbreak, says Jim Wick, task force chairman and environmental health and safety manager for the Americas at Intel. Human resources policies, including pay practices and travel support, have also come under scrutiny.

Workforce planning has included telecommuting, but,

Photograph by KATHERINE LAMBERT

"This is an attack on your human resources. We felt we needed some very specific plans."

–ROBERT CORNELIUS, director of business continuity, Constellation Energy

since Intel is a manufacturer, it has had to plan how to maintain business functions while protecting employees who must work onsite. The company has developed facility cleaning procedures, which include personal health and hygiene practices, such as the usage of antibacterial hand cleaners.

"And, we've tested. Every major business unit and site has gone through a pandemic exercise or drill," Wick says.

Intel has shared its preparations with its contractors and suppliers, and has encouraged them to plan, too. "We have some key suppliers; if they are crippled by the disease hitting their employee base, that hurts our business, too."

The task force has also done a lot of education for its nearly 100,000 employees, including an intranet site with tips on how they can safeguard their families from contagious diseases.

All of the planning is what Wick calls prudent preparedness. Unlike other companies, such as airline firm Virgin Atlantic, Intel made a policy decision not to stock antiviral medicine Tamiflu.

"I think we've done the prudent thing for our business—to protect our people, which are our most valuable resource," he says.

If a pandemic hits, it could last for weeks or months, notes Don Ainslie, global security officer at Deloitte & Touche. Once it's over, organizations will be evaluated on "how well they treat their people and how they service their clients," he says.

FOOD INDUSTRY PREPS

After the epidemiologist who advises Alex Lee on food safety issues told executives last year about the pandemic threat, the company didn't waste any time. Information systems VP Schwarz pulled together a task force of 16 people from all parts of the business to brainstorm how the industry would be affected by a pandemic, and how the company would respond. The group came up with more than 120 ideas, which are summarized in a document that Alex Lee has made publicly available.

"We're in the food business, and we serve a lot of communities in the Carolinas. People have to eat—we have to keep this food supply going. We made a decision that this [planning] isn't going to be a competitive thing," Schwarz says. "We wanted to get the industry to wake up to this risk."

The group's report takes into account various scenarios

STRATEGY

STARBUCKS PLAN BREWS WORLDWIDE

The global coffee company has already implemented precautionary measures in regions of the world where avian flu has been reported.

With operations in 37 countries, Starbucks Coffee Company has already put its avian flu pandemic planning into action.

A multinational task force including Starbucks executives and outside medical experts created a plan to handle a potential global pandemic. With the avian flu centered in Asia and Europe as of this fall, parts of the strategy have been implemented at Starbucks operations in those regions:

- **Advising** employees to follow the World Health Organization's advice for travelers, including avoiding animal markets and not handling sick or dead birds.
- **Requiring** suppliers of products that use eggs or chicken to adopt safety standards above the standards Starbucks already requires; suppliers who don't adhere to additional safety requirements cannot supply chicken and egg products to Starbucks.
- **Reinforcing** the importance of personal hygiene, including hand-washing.
- **Providing** each store with equipment, chemicals and protective gear to help employees and customers protect themselves from the avian flu.

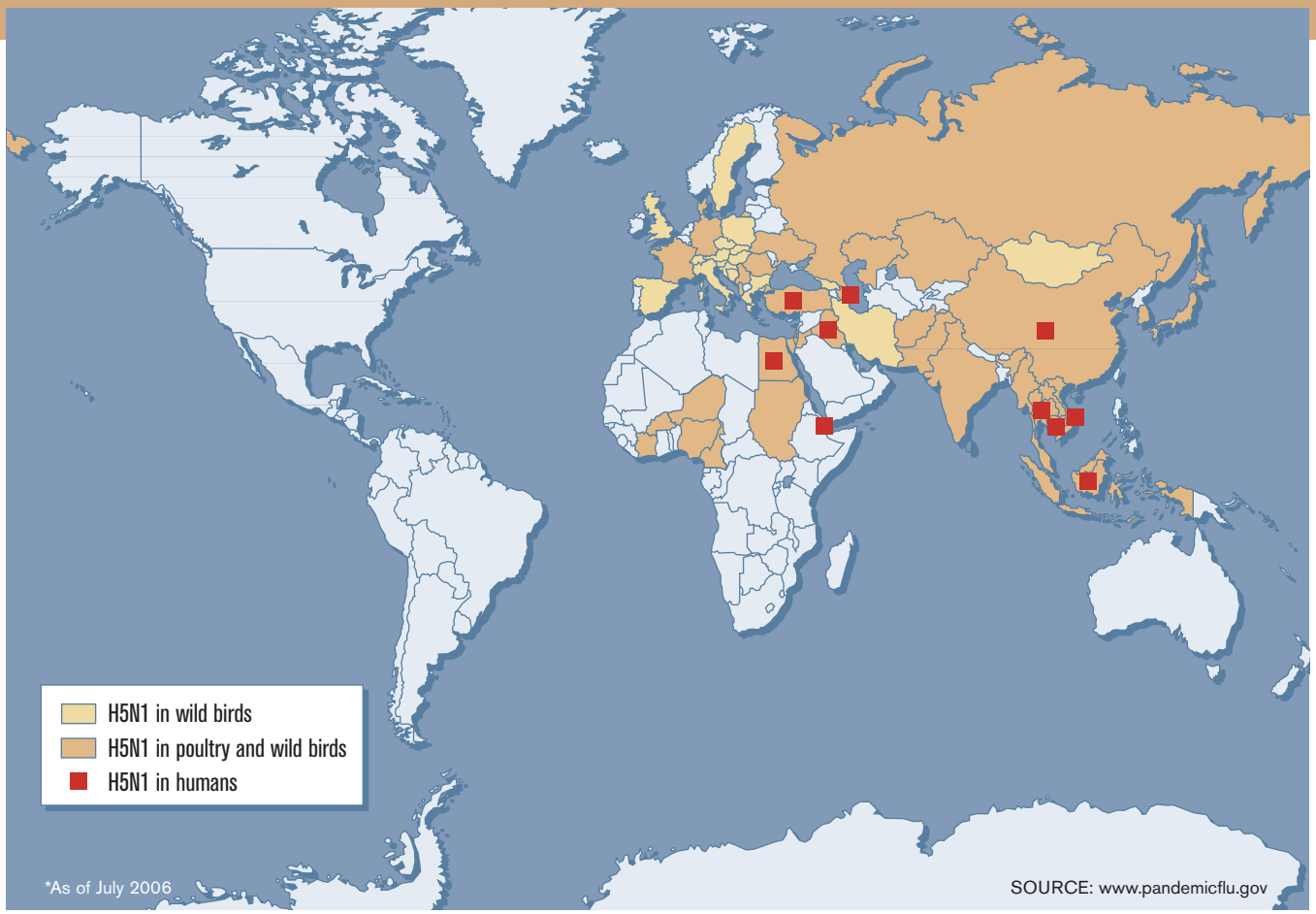
"Starbucks is fully prepared to implement and update additional pieces of the plan as necessary and where appropriate," the coffee company says.

—MARCIA SAVAGE

Photograph by JUPITER IMAGES

PANDEMIC WORLD MAP OUTBREAKS

This map shows the global scope of the current human avian flu diagnoses.* Though the H5N1 strain has yet to hit North America, this most virulent strain of the flu has caused 256 confirmed human cases of avian flu resulting in 151 deaths worldwide, according to the World Health Organization.



Map by ANNIE BISSETT

such as consumers avoiding restaurants, and increased demand for online shopping and home delivery, and lists recommendations for dealing with those situations.

Coming up with the ideas was fairly easy, but putting them into action is difficult, and Alex Lee has a long way to go in its preparations, he says. The company has spent a lot of time analyzing its employee base, thinking through situations such as filling in a shortage of truck drivers with employees who aren't drivers but have the credentials.

Another focus is employee best practices in a pandemic: using phone and email instead of face-to-face meetings whenever possible. But having employees work remotely is fraught with problems, including security, ample VPN bandwidth and a reliance on the Internet running properly, Schwarz says. "If your job requires paperwork, how's all that going to flow?"

A big part of what his company does is distribute food to grocery stores, a job that obviously can't be done remotely. "We get pallets in from manufacturers and get them to grocery stores. You can't do that from home," he says.

Making sure its vendors also are preparing for a pandemic is another big focus for Alex Lee, and company executives have met with vendors to discuss how to maintain the supply chain in the event of an outbreak.

Schwarz advises other organizations embarking on pandemic planning to get upper management on board: "It's impossible to address this issue without top management support. You need resources in terms of people and money if you're going to do it seriously."

Preparing for such a catastrophe raises a lot of tough issues, but companies are better off thinking through them now, he adds.

"Even though it's difficult, it's got to be easier than waiting for the pandemic and having chaos," Schwarz says. "Pandemic planning is not optional."

Marcia Savage is features editor of Information Security.


NIST's 800-30
COSO
ISACA
ISO 27002
SANS 6 04
CobiT
ISO17799

Alphabet Soup

Confused by all the risk management acronyms? We'll sort through the jumble to help you choose a methodology or framework that's right for your organization.

BY SHON HARRIS

REGULATORY REQUIREMENTS ARE DRIVING COMPANIES TO LOOK into risk management more than ever before. SOX, HIPAA and GLBA all require risk analysis and management. But organizations looking for a solution can quickly find themselves swimming in a sea of acronyms that includes NIST 800-30, AS/NZS 4360:2004, OCTAVE, COSO and CobiT.

Sorting through the array can be confusing. While some are truly risk management methodologies, others are frameworks that can help with compliance, but provide only high-level risk management goals.

Adding to the confusion is that risk management has different connotations in different industries and on what level it's applied. At the operational level, risk management deals with technology; at the strategic level, it has more to do with business drivers and decisions.

We'll make sense of the soupy mix by taking a closer look at the various methodologies and frameworks, and examining what each has to offer.

Illustration by JOE TAYLOR

Risk Methodologies: NIST, OCTAVE & AS/NZS

The most commonly used risk methodologies are the National Institute of Standards and Technology's (NIST's) approach, as outlined in its 800-30 document; the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) approach; and the Australian/New Zealand Standard (AS/NZS) 4360:2004.

It's important to understand the difference between risk and a vulnerability: A vulnerability does not represent risk; risk determines the business impact of someone exploiting the vulnerability. Businesses also have different types of risks, including information and computer security, business decisions and finances.

The NIST approach is specific to IT threats and how they relate to information security risks. It lays out the following steps:

- System characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentation

This methodology is commonly used by security consultants, security officers and internal IT departments, and focuses mainly on systems. An individual or small team collects data from network and security practice assessments, and from people within the organization. This data is used as input values to the risk analysis steps outlined in the 800-30 document.

OCTAVE also focuses on IT threats and information security risks, but looks beyond the system level to people and processes. It uses a self-directed workshop method in which a team made up of management, operational personnel, security and business heads walk through several scenarios, questionnaires and checklists. The scenarios cover a range of potential security incidents, from someone gaining unauthorized access to sensitive data to how a lack of redundant controls affects availability.

The goal is to train these employees on risk analysis steps and have them use these steps as a group to identify and control the company's risks. Team members are chosen because they are closest to the processes, technology and issues that result in company risk.

While both the NIST and OCTAVE methodologies focus on IT threats and information security risks, AS/NZS 4360:2004 takes a much broader approach to risk management. This methodology can be used to understand a company's financial, capital, human safety and business decisions risks. Although it can be used to analyze security risks, it was not created specifically for this purpose.

If your company is not sophisticated in risk management and needs to comply with SOX, HIPAA or GLBA,

it's best to start with the NIST risk analysis approach. You will likely have a small internal group—made up of security and IT staff—overseeing the compliancy steps, and this methodology is based on security and IT.

After this group understands the ins and outs of the NIST methodology, your company can look at implementing OCTAVE, which is the more time-consuming approach; it trains others outside of the security group in risk management. A company cannot understand its business and technology risks unless both security and business managers are engaged and involved. Workshops provide a way for managers to understand other risks outside of their areas. OCTAVE also is a great tool to increase the awareness of security initiatives and helps the security team members to get more people on their side.

Once a company evolves in its understanding and practices of risk management at a basic level and can map business objectives to security and technology requirements, it can then start incorporating other business risks and start building an enterprise risk management (ERM) system. At this stage, the company can advance to AS/NZS 4360:2004.

Although it seems as though a company has to learn three different methodologies, they have about a 70 percent overlap. Each lays out a roadmap for identifying and controlling risks. A company can start off with applying a focused risk management process (NIST), expand into the business units with a broader method (OCTAVE), and then grow into a holistic approach to risk (AS/NZS 4360:2004). The real key is to get going and keep the ball rolling.

Frameworks: CobiT, COSO, & ISO 17799

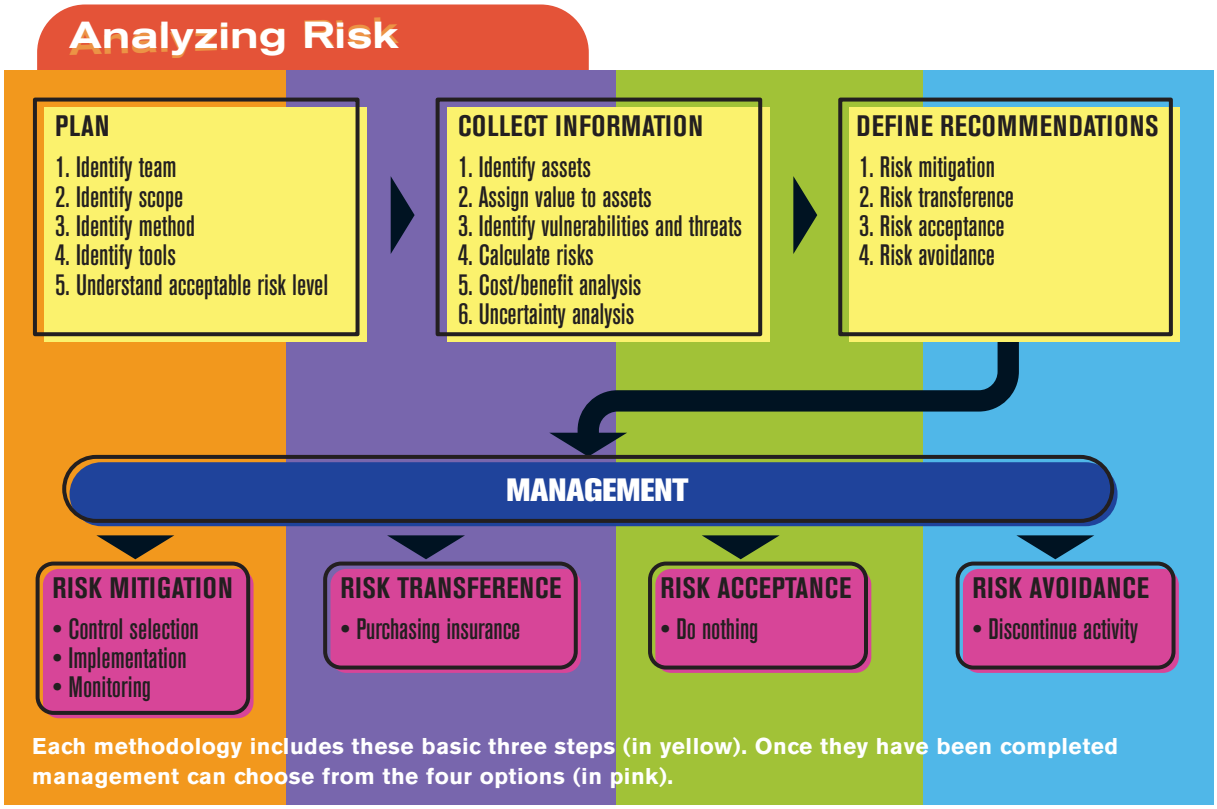
Frameworks such as the Control Objectives for Information and related Technology (CobiT) and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework aid regulatory compliance, but don't provide actual risk management methodologies. Rather, they include some high-level goals for risk management as part of their overall scope. While CobiT helps a company define risk goals at an operational level, COSO helps a company define organizational risks at a business level.

Developed by the Information Systems Audit and Control Association and the IT Governance Institute, CobiT is a framework that defines goals for the controls used to properly manage IT and ensure that IT maps to business needs. It's broken down into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Each category drills down into subcategories. For example, the Acquire and Implement section includes information on acquiring and maintaining application software and managing changes.

Although CobiT is not a risk methodology, it does spell out the goals an organization should aim to accomplish in its risk management processes. These goals are outlined in these subcategories: Business risk assessment; risk assessment approach; risk identification; risk measurement; risk action plan; risk acceptance; safeguard selection; and risk assessment commitment.

While CobiT is a model for IT governance, COSO is a model for corporate governance. CobiT was derived from the COSO framework, which was developed by the Committee of Sponsoring Organizations of the Treadway Commission in 1985 to deal with fraudulent financial activities and reporting. COSO has these components:

- Control Environment—Management's philosophy and operating style; the company culture as it pertains to ethics and fraud
- Risk Assessment—Establishment of risk objectives; the ability to manage internal and external change
- Control Activities—Policies, procedures and practices put in place to mitigate risk
- Information and Communication—A structure



Each methodology includes these basic three steps (in yellow). Once they have been completed management can choose from the four options (in pink).

that ensures that the right people get the right information at the right time

- Monitoring—Detecting and responding to control deficiencies

COSO focuses on the strategic level while CobiT focuses more on the operational level. You can think of CobiT as a way to meet many of the COSO objectives, but only from the IT perspective.

Like CobiT and COSO, ISO 17799 includes some high-level risk management guidance, but doesn't provide an actual risk methodology.

Updated last year, ISO 17799 provides guidelines on how to set up a security program from A to Z. Where COSO and CobiT call out requirements for various security structures and countermeasures, ISO 17799 provides the details on how to develop and implement these components.

The newest version of this framework includes the following categories: security policy; asset management; physical and environmental security; communications and operations management; access control; and information security incident management.

These categories are controls that need to be put into place to reduce risk. For a company to know the right type and level of access control, incident management and physical security, it must first understand its current risk level and its acceptable risk level. Risk management is a foundational piece of each component of ISO 17799 but the framework does not specify what methodology an organization should use to accomplish it.

Tricky Business

No matter how a company goes about it, risk management is ultimately a complicated undertaking. For business people, risk management deals with business decisions, such as launching a product line or purchasing another company. For security professionals, it's more about operations, including fighting hackers and internal fraud. Each group has different vulnerabilities and threats to worry about.

In slowly recognizing the need for each group to understand how the other's set of vulnerabilities directly affects its own risk levels, the industry is having growing pains. Business and technology are complex in their own right; truly understanding their overlapping components and assessing risk at a more holistic level is the difficult hurdle we face.

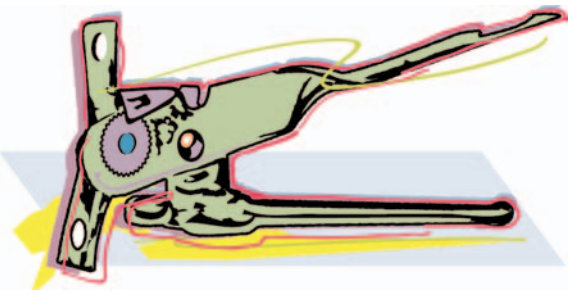
But the array of methodologies and frameworks that deal with risk can help, depending on your organization's needs. Once you've sorted through the alphabet soup of risk assessment methodologies, you can choose the most appropriate one for your business.

It's important to at least start the process of managing risks. In an era of increasing security threats and regulatory requirements, it's something that no company can afford to ignore.

Shon Harris, CISSP, MCSE, is the president of security training firm Logical Security. She is a security consultant, instructor and former engineer in the Air Force's Information Warfare unit.

Risk Management Tools

Since companies are paying more attention to risk management these days, more vendors are jumping into this space. Unfortunately, almost every vendor with a product pontificates on how it carries out "risk management," but in reality most of these products are not true risk management tools.



Rather, many of them are actually vulnerability assessment and vulnerability management tools, which are much different than risk management tools. The easiest things to do in security are identifying a vulnerability and getting rid of it. One of the most difficult things is calculating the risk associated with that vulnerability—that requires estimating the probability of the vulnerability being exploited, the frequency of this occurrence and the associated business impact. Just finding an open port is one thing, but understanding how it will or will not affect the company is a whole other skill set.

RiskWatch has a suite of analysis tools that follow the NIST 800-30 methodology. While most risk assessments are carried out in a qualitative manner, RiskWatch provides quantitative analysis, which is more useful to management when they need to understand how security affects the bottom line.

This suite provides questionnaires and reports, and illustrates a company's level of compliancy to a range of standards and regulations.

One of the most powerful assets of the RiskWatch suite is that it pulls data from trends and incidents in the industry and its customer base to give the quantitative values true meaning. A quantitative risk analysis is dangerous and misleading if the formula variables are populated with guesswork and unsubstantiated values.

Since SOX and other regulations require that organizations be more responsible for understanding the risks that third parties introduce, there are products that help—mostly for financial organizations—with this task.

Accuvant's AccuCERTT provides extensive questionnaires and tracking mechanisms to identify risks outside of your company. This tool is also built on the NIST risk methodology. Risk Management Technologies (RMT) has a very robust ERM tool, First Priority Enterprise, for larger organizations that are more sophisticated in their risk management processes. This tool is based solely on AS/NZS 4360:2004.

These tools incorporate and automate the risk methodologies, but just purchasing and using a tool does not relieve you of the task of actually understanding the necessary steps and liability issues of risk management. A tool can only automate and control manual steps of the risk management process.

—SHON HARRIS

RE-working RISK policy

WHETHER YOU MANAGE POLICIES MANUALLY OR USE AUTOMATED TOOLS, IT IS IMPERATIVE TO GET YOUR POLICIES AND SYSTEMS IN SYNC. ✱ BY HARRIS WEISMAN

In a way, your information security operation is like a crew boat. It operates most efficiently and effectively when everything is in harmony. To make sure the metaphorical oars all hit the water at the exact same time, you need to establish some rules. Forget about a coxswain; sound policies and strong management systems steer your crew.

Part of managing risk requires periodically evaluating your policies and your enforcement program, and updating the guidelines and technology that ensure employee and system adherence to them. Similarly, vendors now offer products that can convert policies into specific configuration criteria and commands.

Illustration by JOE TAYLOR

Policy management isn't just a matter of good practice—today's regulatory requirements make it an imperative. You can create and manage policy manually, or you can turn to automated tools that implement controls enabling them to adhere to various regulations. Either way, by taking steps to ensure policies are established and managed consistently, you can steer swiftly through threats of security breaches, regulatory glitches and failed audits.

Setting the Rules

When it comes to writing policies, there are many resources available, including the SANS Institute's Security Policy Project and the ISO 17799 security standard, which provides a policy framework. A number of organizations, mostly colleges and universities, have posted their infosecurity policies on the Internet, which can provide helpful sample materials. *(For examples, see "Policy Resources," p. 23.)*

If you don't want to write your policies from scratch, there are a number of vendors that provide canned policies; however, they tend to be generic and must be tailored to be effective. No matter what route you take, make sure the policies fit your organization—those that don't meet an organization's needs are often neglected, exposing the enterprise to risk.

Also, it's critical that policies not be too specific—let the details be addressed in subsequent procedures and guidelines. In policy development, policies should not need to be rewritten every time something changes: If you change your antivirus solution, you should not need to change your antivirus policy, although you may need to modify your antivirus procedure.

Keeping policies as nonspecific as possible will also help your organization deal with emerging threats. If a policy is too specific, it will need to be rewritten every time a threat emerges.

A policy should outline how to assess threats; procedures or guidelines can then be created to handle attacks as they develop. If policies are written openly without naming or describing specific attack vectors, such as spyware or phishing, they will help give your IT security the advantage by establishing criteria for recognizing possible problems, such as abnormal network traffic.

Management Essentials

Once policies are established, you need to figure out how to use them to best manage your enterprise's information security posture. (Everyone has a different definition of policy management. For our purposes, policy management is the conversion of policies into practical and enforceable controls that can be implemented across the enterprise.)

To have an effective policy management solution, several key support mechanisms must be in place:

- Employees must be subject to a communication and training program. Staff members cannot be expected to

policies & regulatory COMPLIANCE

Prior to the Enron and MCI/WorldCom debacles, corporate management and boards of directors paid little attention to IT security policies. That's changed with the passage of SOX and the potential of fines and jail time for companies and their executives if there's a violation.

SOX is intended for publicly traded companies and focuses on the accuracy of financial reporting. Section 404 looks at information systems and the controls around them; failure to have an IT security policy and policy management are considered exceptions, causing problems for the company. There really aren't any must-have policies for SOX compliance—auditors are looking for a strong overall information security program and policies, plus in-place monitoring of users and systems for compliance.

In addition to SOX, HIPAA and GLBA are other legislation that impact security policies. Both require keeping data private: HIPAA with regards to healthcare information, and GLBA with regards to financial data. Companies involved with either financial or healthcare information must develop, deploy, monitor and manage policies that govern how data is stored and transmitted. These policies can affect the entire IT infrastructure of an organization from firewall configuration to the data stored on workstations.

HIPAA and GLBA auditors will look for a solid data classification policy, or a policy that describes what types of data are used within the organization and how they are classified for privacy and security. Policies describing cryptography and cryptographic standards for the storage and transmission of sensitive data need to be outlined and deployed. Overall, auditors look for policies and procedures/guidelines that outline your data classification program and describe how that program will protect data within the organization.›

—HARRIS WEISMAN

comply with policies if they don't understand them; training also provides a way for them to provide feedback on what is and isn't working.

- Management must enforce the policies in a consistent manner across the enterprise; otherwise, employees will not take the policies seriously. Work with your human resources department on how to handle enforcement. At the very least, HR should always be informed when enforcement issues arise.
- Metrics must be developed to measure policy effectiveness. Measuring metrics can be tricky, particularly in the security space (after all, if there's no breach, you have done your job properly). Metrics can examine how many users are being blocked from inappropriate Web sites, the number of viruses blocked in a given time period and the overall strength of user passwords.
- Implement a maintenance schedule to ensure that policies are reviewed and updated on a regular basis. Most regulators like to see this happen on a yearly basis.

Most importantly, an organization needs to decide what it's trying to accomplish through a policy management program. Will the program focus on a limited number of areas, such as access control or antivirus, or will it be deployed enterprise-wide? Is the program designed to meet compliance issues from SOX, GLBA or HIPAA, and, if so, will you need a system to measure compliance?

The Manual Way

There are two approaches to developing a policy management program: manual and automated. With the former, there is manual intervention to track adherence to the policies. For the latter, software tools are used to enforce policy compliance.

The first step in developing a manual policy management solution is creating a set of procedures that reflects your policies' goals. Keep the policies as high level as possible; the procedures and guidelines will provide the details necessary for day-to-day operations.

Some typical procedures include antivirus, password aging and log monitoring. Each procedure/guideline is an interpretation of a specific section of the policy and is used as criteria for implementing and configuring specific software solutions.

Using our procedure example, the antivirus policy sets the tone by establishing that an antivirus solution will be used within the enterprise. The antivirus procedure will outline exactly how the policy will be enforced, addressing issues such as updates and outbreak response. Normally, that is managed by a central console and the rules are pushed out to workstations and servers.

An acceptable-use policy is interpreted in several procedures that address e-mail usage, data storage and Internet usage, among other activities. A Web usage procedure outlines which sites employees are allowed to visit, what type of technology—such as Web content filtering—will be in

TOOLS policy management

Altiris ✱ SecurityExpressions ✱ www.altiris.com
Employs agent-based or agentless system for policies across Windows, Linux, and UNIX desktops, servers and notebooks

Archer Technologies ✱ Policy Management
www.archer-tech.com
Provides best-practice templates for policy creation, online distribution, user education and compliance

BigFix ✱ Enterprise Suite ✱ www.bigfix.com
Implements and enforces configuration standards across desktops, laptops and servers; vulnerability management component

BindView (Symantec) ✱ Policy Manager
www.bindview.com
Defines and distributes policies, maps them to multiple regulations and automates compliance issues reports

CA ✱ eTrust Policy Compliance ✱ www.ca.com
Automates configuration assessment and remediation for heterogeneous systems

Configuresoft ✱ Enterprise Configuration Manager
www.configuresoft.com
Monitors hardware and software configurations across Windows, UNIX and Linux systems; offers pre-built compliance toolkits to create and enforce policies

Consul risk management ✱ InSight Security Manager
www.consul.com
Consolidates and analyzes user and system activities for policy violations

Cybertrust ✱ Risk Commander ✱ www.cybertrust.com
Consolidates asset information and vulnerability data; monitors for compliance with enterprise controls and regulatory standards

Elemental ✱ Elemental Security Platform
www.elementalsecurity.com
Uses agent-based integrated policy management, host configuration and access control; policy library has more than 2,000 rules and templates

IBM ✱ Tivoli Security Compliance Manager
www.ibm.com
Audits systems for vulnerabilities and identifies violations against security policies; offers pre-defined recommended policies

Polivec ✱ Compliance Management System
www.polivec.com
Creates policies and maps them to regulatory requirements; uses agent-based and agentless technology to monitor systems for compliance

Solsoft ✱ Policy Server ✱ www.solsoft.com
Centralizes policy and configuration management across a heterogeneous security infrastructure; role-based change management

Tripwire ✱ Tripwire Enterprise ✱ www.tripwire.com
Audits changes across the IT infrastructure; enforces compliance with change and configuration management policies

Virsa Systems (proposed acquisition by SAP)
Continuous Compliance Suite ✱ www.virsa.com
Monitors the enforcement of application access and controls across disparate systems

POLICY resources

FEEL LIKE YOU'RE CONSTANTLY ROWING UPSTREAM? THESE RESOURCES CAN HELP.

- **The SANS Institute's Security Policy Project**
  www.sans.org/resources/policies
- **NIST's ISO 17799**
  http://csrc.nist.gov
- **Murdoch University**
  www.murdoch.edu.au/admin/policies/itsecurity/policy.html
- **University of Georgia**
  www.infosec.uga.edu/policymanagement/index.php
- **Western Connecticut State University**
  www.wcsu.edu/technology/wcsu_security_policy.pdf
- **University of Illinois**
  www.obfs.uillinois.edu/manual/central_p/sec19-5.htm

place to enforce the restrictions and how often the logs on the devices are checked.

Another example is the password-aging setting in Microsoft Windows. If the policy requires complex passwords, the guideline dictates the maximum age of a password, and Active Directory will be set to the maximum password life.

It's easy to see how information security policies can be used to create practical and enforceable controls for managing the enterprise. However, this process is extremely hands-on—someone has to intervene to correlate the data between the various control points, including antivirus programs, IDSes, firewalls and authentication systems such as Active Directory. Manually monitoring for policy compliance can be quite cumbersome. Potential problems include the following:

- The antivirus management console could occasionally lose connectivity with individual servers or workstations, leaving an exposure point on the corporate network. Detecting this policy deviation and correcting it can be extremely time-consuming.
- It's not unheard of for content management providers to misclassify Web sites. For example, chocolate-maker The Hershey Company's site was once misclassified as pornographic. This type of error can lead to false positives and, if the site is not classified at all, can give users a way to bypass the system. Monitoring this control is time-consuming and frustrating. Plus, managing user exceptions—those who can bypass the filtering system to conduct research—complicates matters by creating a need to track exceptions for compliance reporting.
- Although systems like Active Directory can stipulate that users have complex passwords, it is possible to bypass the intent of the control, resulting in the user having a weak password. Because of this, it's important for security administrators to occasionally audit users' passwords with a password-cracking tool.

Automation to the Rescue

The time and effort involved in manual policy management can make automated tools an attractive alternative, especially for large organizations.

In recent years, several vendors have come to market with policy management solutions, including Elemental Security, Solsoft and BindView (acquired by Symantec earlier this year). Most of these vendors' products couple the creation of policies with management software. Essentially, managers create the policies, and the software enforces them and measures compliance.

Elemental Security takes a host-centric view of policy management, implementing polices into servers and workstations on the network. Solsoft uses a network-centric approach by applying policies to network devices. BindView takes a host-based view, but also has an add-on component that helps write policies, push them out to users, and track user acceptance and exceptions.

Automated tools work by taking your security policies and procedures and implementing them into control points. As noted, some tools operate by controlling network devices—they convert policies into configuration criteria for network devices, such as routers. With host-based tools, policy is converted into configuration commands.

What is especially helpful about some policy management products is that they provide the templates for different standards, such as ISO 17799 and CobiT, and cross-correlate them with relevant regulations. With the templates provided, you can choose the policies necessary for your organization.

Another noteworthy feature of many policy management products is that they integrate across the enterprise, pulling data from a variety of sources, including backup, antivirus, content filtering solutions, firewalls, operating systems and routers; these data feeds should reduce the amount of data the user has to sift through. Some automated tools also integrate vulnerability management, keeping systems up to date and addressing emerging threats and zero-day exploits.

The ability of policy management tools to automatically correlate large amounts of disparate data can also facilitate regulatory compliance and reporting since it allows users to pull compliance data for specific regulations. A major complaint among security professionals is the redundant requests for the same audit-related information from external auditors, internal auditors and government regulators. Instead of having to complete several different audits that address similar issues, these tools allow you to generate reports tailored for different groups.

Automated policy management tools can also monitor for violations and track policy exceptions. A key benefit is

that all reports are consolidated into one management console, making them easier to track than with the manual approach. But they are not really active monitoring products—they won't act like a fire alarm. Symantec, however, plans to integrate BindView with technology that manages incidents; other tools are designed to integrate with security event management products.

None of the products are plug-and-play—all take time to implement; some even require companies to convert their policies into a specific format. Implementation times vary depending on the product and the state of the organization's policies.

Along with implementation times, software cost is a key consideration with automated tools. For instance, the Elemental Security Platform 2.0 starts at about $35,000 with server agents costing around $600; workstation and laptop agents cost $60.

Which Is Best?

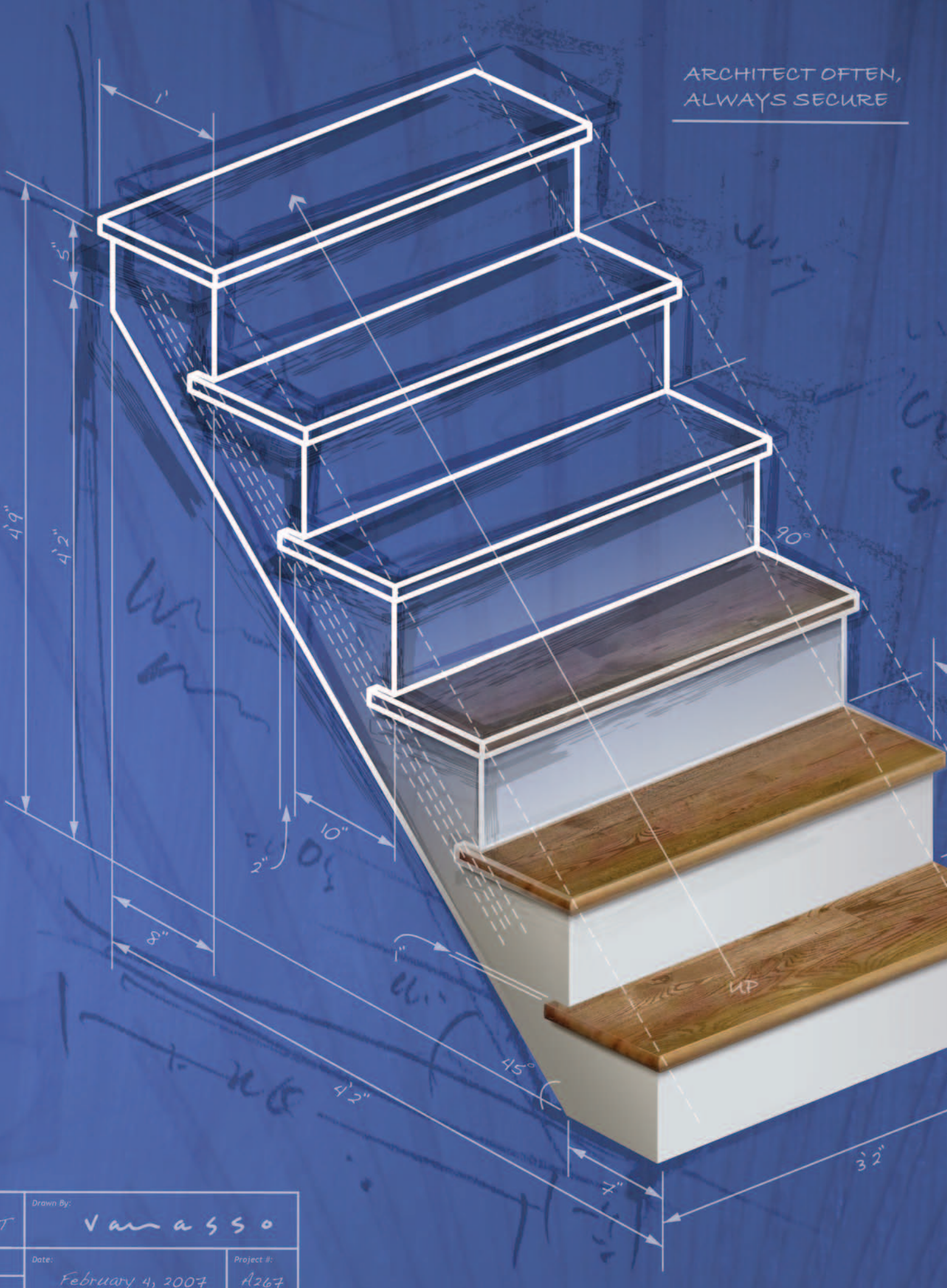
Both the manual and automated approaches can do the job well, but they clearly have limitations. In a large enterprise, automated policy management tools can be a tremendous help. But for smaller organizations, they may not be worth the cost.

Another possible problem with automated tools is that, instead of making customized policies for the enterprise, users can modify the company to fit the policies. Right now, many automated products are limited in scope by only taking a slice of the pie—either the network- or host-based approach. To truly be effective, a policy management solution needs both. Symantec is moving in that direction, with plans to add a network-based component.

Policy development and policy management are a complex series of daily tasks, but companies must face the challenge. As our IT infrastructure becomes more complicated and threats continue to grow, we will increase our reliance on manual and automated tools to enforce policies and report on compliance. As policy management products continue to mature, we will see automated tools that are better equipped to deal with the problem holistically, and hopefully prices will drop to where businesses of any size can afford to implement them.

To be sure, effective policy management will only become even more critical in the future.›

Harris Weisman is information systems security manager at Chemung Canal Trust Company in New York.


ARCHITECT OFTEN,
ALWAYS SECURE
1'
5"
4'9"
4'2"
90°
10"
2"
8"
1"
45°
4'2"
7"
3'2"
UP
Drawn By:
Vamasso
Date:
February 4, 2007
Project #:
A267

SECURITY BLUEPRINT

A FORMALIZED ARCHITECTURE DIAGRAMS HOW TO HANDLE THE CHANGING THREAT AND REGULATORY ENVIRONMENTS.

BY MICHAEL S. MIMOSO

Illustration by ENRICO VARRASSO

EVERY SO OFTEN, SOMETHING BEASTLY CROSSES THE DESK OF an enterprise security manager. Be it a digital disaster or a new regulatory mandate, these nasties have transformed a CISO's professional existence into a series of policy and process adjustments, and reallocations of resources.

Any measure of standardization and repeatability becomes a welcome ally in warding off the effects of a shift in the threat or regulatory environment.

Jim Brockett takes heed, but isn't fazed, by the sophistication of new phishing schemes or insider threats. Shifts in the landscape mean the senior vice president and CIO of Washington Trust Bank, a $3.5 billion regional commercial bank in the Pacific Northwest, reaches for the virtual blueprints of his security architecture. These steps are the foundation of his enterprise's security program, the pillars upon which customer and proprietary data is kept safe and auditors and the board of directors are satisfied.

Brockett, his security teams and application developers, four years ago laid out the underpinnings of the bank's architecture. They established four areas of concentration overarching enough that they remain tried and true to this day. Underneath those four umbrellas is where the tweaks and transitions are made when a new threat or regulatory requirement commands attention.

"It's important to have a talk about it and get it written down," Brockett says. "You're hit with a lot of different best practices, products and processes. Does it fit under one of our [steps]? If not, we don't do it."

Draw It Out

BLUEPRINTING YOUR ARCHITECTURE? HERE'S WHAT IT MIGHT LOOK LIKE.

The tools for creating a virtual blueprint of your security architecture are likely on your desktop already.

"I heard from an enterprise architecture colleague that the most common tool is called EVP—Excel, Visio and PowerPoint," says Gartner analyst Tom Scholtz. "It typically takes on the form factor of a set of models, templates and principles on a combination of things like spreadsheets, Word documents, PowerPoint designs, diagrams and visual workflows [created in Visio]."

Keeping it to these familiar formats facilitates the constant tweaks an architecture will require.

"The structure should be in a consistent format and hierarchy," Scholtz says, "so that you can use it at different levels of planning."

—MICHAEL S. MIMOSO

Gartner analyst Tom Scholtz estimates that a little more than half of the Global 2000 have formalized their security architectures and successfully integrated them with the enterprise architecture.

"The more explicit driver for a security architecture is the need to become more consistent in your terminology, language, strategy, modeling and tools. A large part of what you're trying to achieve is the avoidance of duplication and get to the point where you leverage and reuse as much as possible," Scholtz says. "Formalizing an architecture demonstrates to stakeholders that the organization is serious about security."

Four Pillars, One Architecture

FFIEC compliance is the latest challenge for Washington Trust. A Dec. 31, 2006 deadline mandated that banks conduct risk assessments of their online banking infrastructure and remediate any shortcomings, especially in the areas of strong authentication for consumers. Banks are spending millions on compliance with FFIEC, yet those with formalized architectures are taking on less water than those without a spelled-out strategy. They're able to roll in these requirements and beef up existing procedures without major overhauls. A periodic tweak of an existing architecture heads off compliance and threat anxiety.

"Because of regulatory changes and laws like FFIEC and Gramm-Leach-Bliley, there was a lot of regulatory guidance that set precedent on IT best practices," Brockett says. "The thing I keep saying is that being in compliance isn't good enough. Every year there are projects and accomplishments that improve security and mitigate risks that exist. We want to get better at that every year."

In 2003, the Washington Trust board of directors approved an architecture that addresses risk from a business point of view, rather than strictly from a technical standpoint. Brockett's team, in conjunction with security and a risk management committee, identified four areas of concentration to best combat the changing threat environment, address regulatory demands, and manage vendors and systems:

- Information security
- Vendor management
- Business continuity/disaster recovery
- Information and systems integrity

Under each heading, the bank has identified components such as policies, profiles and inventories, and procedures.

"What we've had in place—this four-pillar framework—does not change. It's static. The changes are made within each pillar to monitor, measure and improve risk management," Brockett says. "We tweak and fine-tune components of the program as the threat environment evolves."

For example, under information security, user and consumer electronic security banking policies are spelled out. Applications and IT infrastructure profiles are detailed here, and IT resources are inventoried. Reporting and monitoring procedures are explained, as are user account administration procedures and profile maintenance.

With the architecture blueprinted, Brockett can prioritize threats and address them in a standardized, repeatable way that not only deals with today's problems, but lays a foundation for heading off tomorrow's problems.

"Where we tend to have most vulnerabilities is with internal threats—people with legitimate authorization and access to systems and potentially defrauding us via legitimate access. That's where we are spending a lot of our time," Brockett says.

Brockett's biggest step toward countering employee fraud was an endpoint security deployment (Cisco Clean-Access) that determined device integrity and forced policy on deficient devices. Washington Bank also monitors insider activity (NextSentry's ActiveSentry) on the desktop.

The bank's architecture also includes its disaster recovery and business continuity plans, focusing on recovery information for each application and infrastructure component, plan testing and maintenance schedules, and notification procedures, among other components.

Information and systems integrity puts in print change-management policies, including system configurations and coding. It also spells out who is authorized to make systems changes, when those changes may be made and with whose approval. Database profiles, change logs, system maintenance and the systems development lifecycles are stored here as well.

"WE TWEAK AND FINE-TUNE COMPONENTS OF THE PROGRAM AS THE THREAT ENVIRONMENT EVOLVES."

–JIM BROCKETT, senior vice president and CIO, Washington Trust Bank

Photograph by BRIAN SMALE

What To Do

Don't Fixate on Format
Focusing on the architecture itself to the detriment of solving problems isn't productive. Security architecture is a means to an end, not an end.

Long-term Initiative
Architecture is not a one-off activity. It's a living document, not just a vision.

Allocate Resources
This is a continuous process; allocate full-time people to do architecture.

Up-sell Architecture
Board review and approval enables upper management to prioritize security.

Take It to the People
Appoint business unit managers as liaisons between security office and users.

SOURCES: Gartner, Washington Trust Bank, SABSA

Brockett's teams went so far as to blueprint policies for dealing with vendors, including the business risks posed by each vendor relationship.

To help execute on the blueprints, Brockett has engaged business leaders to act as liaisons between IT and a business unit. These risk coordinators have no formal security backgrounds, but have responsibility in coordinating, implementing and communicating the security program drawn up in the architecture. The coordinators' performance is measured and bonuses are handed out based on effectiveness.

"The benefit is that it gets everyone talking the same language," Brockett says of the bank's security architecture. "By having a documented framework, it gets everyone understanding where things fit and what we're trying to do."

Opportunistic Architecture

Used to be that security architectures were technical reference guides under which a security program is executed. But much the same way the responsibilities of a CISO are evolving to include risk management and an understanding of the business, architectures are similarly evolving. As with the approach Washington Trust Bank adopted, many security architectures now include policy structures, process information and information models.

"Architectures can be a continuous set of models and templates that evolve and are used on a much more opportunistic basis where the main objective is to avoid reinventing the wheel with every new project," Gartner's Scholtz says. "You're able to formalize decisions and principles, so that the next time you develop a similar application, for example, you're not reinventing the wheel."

Many organizations take a contrary approach where the architecture represents a desired state, and gap analyses are conducted to determine what new initiatives need to be undertaken to reach that desired state. "This is a common approach with enterprise architectures, for example," Scholtz says.

Ultimately, a security architecture must integrate as seamlessly as possible with the overall enterprise architecture, especially with the rapidly evolving threat and regulatory landscapes. This necessary integration makes it almost impossible to design a standalone enterprise security architecture. "It's impractical to do a 35-year plan," Scholtz says. "You have to be more dynamic."

Architectures are blueprints that not only explain an enterprise's technology roadmap, but the controls—processes, policies and technology—to satisfy an auditor.

Scholtz says most architectures are built on three levels:

Conceptual, where abstract goals and models are laid out. This is the high-level vision of the architecture, where processes and designs are modeled, and trust levels mapped out.

Logical, where those goals are applied against the environment and available resources, and alternatives are discussed. This is where organizational, informational and logical design models are blueprinted.

Implementation, where the conceptual and logical levels are carried out. Here the architecture is tweaked as ripples in the environment warrant. Security applications, infrastructure and services are architected at this level; data is classified and the security organization as a whole is architected.

Each level accounts for a business, information and technical viewpoint, Scholtz says.

"This is the time when you get to a position where you have the flexibility to adapt to new risks and changing environmental factors, but do it in a way so as you get as much reuse and repeatability as possible," Scholtz says. "A real benefit of an architectural approach is that you formalize and externalize learning and experience. With environmental changes in IT risk and volatility, the more you get to this point, the more you don't have to address everything as a new solution or initiative."

The secret sauce, however, is in how to best integrate with the enterprise architecture. Overcoming a language barrier is the first step, Scholtz says.

"Enterprise architecture guys talk a language different

than typical security guys," Scholtz says. "When a security guy talks about a service or domain, he's talking about something different than when an EA guy talks about a service or domain."

The onus is on security to learn enterprise architecture principles and develop a security architecture that structurally aligns as close as possible, Scholtz says. Some forward-thinking enterprises have folded security architecture teams into the overall enterprise architecture organization. Most, however, operate in isolation from infrastructure-planning teams, application developers and systems integration specialists.

Washington Trust Bank's Brockett takes it a step further, not only integrating his operations with the overall enterprise architecture, but ensuring his teams are in sync with the bank's risk management function—the operational risk coordinator.

"You can't operate in an environment where you're adversarial with the audit or regulatory function. It can't—and won't—work if you get to the point where the audit group is not risk focused," Brockett says.

Business Application

Security-specific architecture blueprints exist that organizations can use as a template for their environments; several tackle architecture strictly from a business point of view.

SABSA, or the Sherwood Applied Business Security Architecture, is a model that considers business requirements, then assures those requirements are met strategically and conceptually, as well as in design and management of an architecture.

"Unless the security architecture can address this wide range of operational requirements and provide real business support and business enablement, rather than just focusing upon security, then it is likely that it will fail to deliver what the business expects and needs," says John Sherwood, developer of the SABSA model.

Sherwood's model implores security architects to always think in terms of the business, and gird themselves for the scrutiny of those who shun strategic architecture for solely technical.

SABSA is a layered model with six different views of an architecture: contextual, conceptual, logical, physical, component and operational. The contextual view is a description of the business context under which security systems are built, while the conceptual view defines the principles and concepts that guide the logical and physical views. The component view assembles the products and begins the integration within security and the overall enterprise architecture. Finally, the operational view executes and maintains the previous concepts. However, this view needs to be interpreted in detail at each of the other five layers, Sherwood says.

RESOURCES

LOOKING FOR A SECURITY ARCHITECTURE FRAMEWORK? A FEW TEMPLATES ARE A CLICK AWAY.

SABSA (Sherwood Applied Business Security Architecture)
www.sabsa-institute.org/

Information Security Forum (ISF)
www.isfsecuritystandard.com/index_ns.htm

Department of Defense Architecture Framework (DoDAF)
www.dod.mil/cio-nii/docs/DoDAF_v1_Volume_I.pdf

Zachman Institute for Framework Advancement (ZIFA)
www.zifa.com/

SABSA is not your only option as far as risk-oriented architectures go.

The Information Security Forum (ISF) standard also addresses security from a business perspective, and is a reference on how to architect security into systems management, critical business applications, installations, networks and development.

The ISF standard compiles best practices and lays out how to best measure the effectiveness of a program via its Information Security Status Survey.

The Department of Defense Architecture Framework (DoDAF) is another popular blueprint on which an enterprise can model its security architecture.

DoDAF is a military-grade security architecture, and it guides not only military strategy, but business processes and procedures. It too is broken into separate views: operational, systems, technical standards and an overarching view.

These established frameworks, along with homegrown architecture models, should enable enterprises not only to counter today's issues, but lay down a foundation for warding off future threats and inevitable regulatory changes.

"Use your architectural frameworks to do future planning," Scholtz says. "Treat IT risk as an architecture problem."

Michael S. Mimoso is editor of Information Security.