winners
WE RECOGNIZE THE INDUSTRY’S BEST SECURITY PROFESSIONALS

TELECOMMUNICATIONS
Phil Agcaoili

RETAIL
Ezzie Schaff

MANUFACTURING
Brian Engle

FINANCIAL SERVICES
Blanca Guerrero

GOVERNMENT
Christopher Ipsen

HEALTH CARE
Nick Mankovich

EDUCATION
Julie Myers
FEATURES

19 Information Security’s 6th Annual Security 7 Award
SPECIAL SECTION Information Security magazine announces the winners of the sixth annual Security 7 Award.

40 Give In!
DATABASE AUDITING Database administrators are overcoming their distaste for database auditing tools; compliance and security are turning the tide. BY ADRIAN LANE

47 It’s Your Fault
SECURITY AWARENESS The “people problem” continues to hammer information security efforts. What can be done? BY LANCE SPITZNER

ALSO

5 EDITOR’S DESK
Insight from the Frontlines
This year’s Security 7 winners offer advice for tackling enterprise security challenges. BY MARCIA SAVAGE

12 SCAN
Security Shopping Spree
Flurry of acquisitions in information security industry expected to continue through 2011. BY ROBERT WESTERVELT

14 SNAPSHOT
Merger Mania

16 INFOSEC LEADERS CAREER ADVICE
Stay Put!
Experts Lee Kushner and Mike Murray explain how sometimes the best job is the one you have. BY LEE KUSHNER AND MIKE MURRAY

53 Advertising Index
Database protection and compliance made simple.

Guardium, an IBM Company, provides the simplest, most robust solution for continuously monitoring access to high-value databases and automating compliance controls for heterogeneous environments – assuring the integrity of trusted information and enabling enterprises to drive smarter business outcomes.

• Gain 100% visibility and control over your entire DBMS infrastructure.
• Reduce complexity with a single set of cross-DBMS auditing and access control policies.
• Enforce separation of duties and eliminate overhead of native DBMS logs.
• Monitor privileged users, detect insider fraud and prevent cyberattacks.
• Automate vulnerability assessment, data discovery, compliance reporting and sign-offs.

For more information, visit www.guardium.com/InformationSecurity
Insight From the Front Lines

This year’s Security 7 winners offer advice for tackling enterprise security challenges.

BY MARCIA SAVAGE

INFORMATION SECURITY PROFESSIONALS are often unsung heroes, quietly going about the business of securing their organizations’ assets without fanfare. Their work is incredibly complex yet recognition can be rare. But every fall, we fill the gap with our Security 7 Awards, which honor outstanding security pros in seven vertical markets.

This is the sixth year we’ve handed out the Security 7 Awards, and the honor roll is certainly illustrious with industry pioneers and thought leaders such as Dorothy Denning and Gene Spafford. But the list of winners includes many hard-working security pros whose names aren’t well known but who are on the front lines of enterprise security, finding innovative ways to ensure data is protected against an ever-changing threat environment.

The security profession has come a long way from the days of focusing on firewalls to keep intruders out. Today, it’s about risk management and balancing data protection initiatives within the context of the business. This year’s winners have proven adept at that tricky balancing act.

Beginning on page 19, you can hear directly from them on how they meet the security challenges of today and their visions for the future. We’re pleased to add to our Security 7 honor roll: Phil Agcaoili of Cox Communications; Brian Engle of Temple-Inland; Addison Avenue Federal Credit Union’s Blanca Guerrero; Christopher Ipsen of the state of Nevada; Philips Healthcare’s Nick Mankovich; University of Rochester’s Julie Myers and Ezzie Schaff of Ice.com.

For the third year in a row, we’ve turned the presentation of the awards in our publication over to the winners, inviting them to write an essay on an information security topic they felt passionate about. The results have been spectacular and this year is no exception. We are fortunate to have them share their thoughts and you would be well served to absorb their insights.

While the winners all have unique perspectives and face specific challenges in their particular industry, some of overriding themes should resonate strongly for anyone in the business of information security. The need to achieve a balance between security risks and business concerns for cost and productivity is paramount across industries.
Ongoing oversight and monitoring is critical for successful risk management. And any business that provides online services to its customers must walk a fine line between security and usability.

These days, what organization isn’t grappling with the influx of consumer devices like iPhones and the security risks they bring? At the same time, companies are eagerly shifting to cloud services, raising all sorts of issues for corporate data security.

This year’s winners have implemented authentication systems and fraud detection technologies, devised risk management methodologies, and educated their users and customers. Some have worked tirelessly with industry groups, federal officials, standards bodies, and elected leaders to ensure security efforts are realized. They are dedicated, industrious and determined.

You’ll get a sense of the passion these security pros feel for their jobs. Their essays are both enlightening and inspiring. But you don’t have to hear it from me. Our winners express it best.

Marcia Savage is editor of Information Security. Send comments on this column to feedback@infosecuritymag.com.
COMING IN

NOVEMBER

PROVISIONING TOOLS

Today’s provisioning tools are seen as an IT administrative tool for enterprise account management. In reality, provisioning tools are an organization’s first line of access control. By implementing the “optional” components that ship with these tools, like reporting, roles-based access management and advanced workflow, and integrating them with other security tools, like audit recertification and SIEM tools, the provisioning system can become a vital component of an organization’s access control infrastructure. This feature will also look at the compliance benefits of provisioning systems and deployment pitfalls.

COMPLIANCE IN THE CLOUD

Cloud computing requires a shift in thinking on many fronts, particularly regulatory compliance. As businesses rush to the cloud, what should information security professionals do to ensure their organizations meet regulatory compliance requirements? This feature will look at the ramifications of cloud computing on compliance with regulations such as HIPAA, GLBA, SOX, state breach notification laws, and European Union. It will discuss the importance of data location and data encryption in the compliance equation, and steps enterprises need to take.

JOBS SURVEY

What are the most important factors for information security professionals in their choice of a job? How much has certification helped them advance their careers or increase their pay? Are many receiving bonuses this year? How much do they want to pursue a career in security in the future? We recently surveyed readers on a variety of career oriented topics and will reveal the results. The answers might surprise you.
Let’s face it - Who really wants to remember dozens of usernames and passwords to log into all the systems you need. With Single Sign-On - you don’t have to. One “key” really can rule them all.

Contact Prolifics, the largest end-to-end Systems Integrator specializing in IBM technology and IBM AAA-level rated for Tivoli Security and Monitoring, to learn more! Download a valuable whitepaper at: http://www.prolifics.com/portal-security-white-paper.htm
Security Risk Tolerance

Has regulatory and other guidance missed the most important aspect of information security?

BY SUSAN L.T. NEUBAUER

IN INDUSTRY BEST practices and regulatory requirements, much is written about information security programs and what these programs must address. As recently as this year, Massachusetts’ law regarding protection of personal information put forth explicit requirements for written information security programs.

Regulations and best practices contain useful advice and generally sound requirements, but rarely—if ever—do they address the issue of ensuring the information security program is aligned with the company’s tolerance for risk. Why is this topic absent, both in regulations and in best practice advice? How many companies actively discuss and manage information security risk tolerance?

Understanding a company’s risk tolerance related to securing information means that the information security department knows the degree to which the company’s senior management requires their information be protected against a confidentiality leak or data integrity compromise. And using that knowledge, the information security department has put policies and practices into place to support that risk tolerance. Without this understanding, the company may be overspending (protecting data too much) or not protecting its assets to the level expected and required by the business leaders.

The absence of this requirement from regulations and best practices may be due to the extraordinary challenge of discussing risk tolerances. To achieve a well-understood security risk tolerance, a frank and clear conversation with the company’s senior management on the degree to which information should be protected has to occur. The conversation must include the discussion that not all data should be protected and even that not all important data should be protected at the same level.

The conversation must lead to such conclusions as, for example, customer and employee information should have a very low level or six sigma level of known exposure points (six sigma level represents a very low tolerance for information compromise—fewer than 3.4 defects in one million occurrences), while non-confidential information can tolerate higher potential exposure levels such as one sigma—close to 700,000 defects per one million occurrences.

It is only with that degree of understanding that security professionals and technical engineers can build systems and measurements to satisfy the company’s requirements and risk tolerances.
It is important to note that this is not simple and one conversation will not suffice. This will take many conversations and ongoing discussions. It requires discipline, common terms and language, and an ability to recognize that calibrating risk tolerances understood by business leaders and actualized by technology leaders is an ongoing process. Risk tolerances are not easy to articulate nor are they static. Many companies find that their risk tolerance changes when an event occurs—their stated tolerance may be too high when faced with an actual security event that compromises data.

The core of any effective information security program is protecting and reporting on the ability to protect information commensurate within three main categories: 1) regulatory guidance, 2) commercially reasonable and/or best practices, and 3), the company’s risk tolerance for data compromise.

Programs have become mature over time related to regulatory guidance and best practices. However, a new maturity level needs to be achieved: securing information in alignment with the company’s stated risk tolerance. It is only with this level of maturity that an information security program can fulfill its mission: to protect information to the level defined by the organization, its regulators, and commensurate with its industry.

Many companies find that their risk tolerance changes when an event occurs—their stated tolerance may be too high when faced with an actual security event that compromises data.

Susan L. T. Neubauer is the CISO at TIAA-CREF, a Fortune 100 financial services company. Send comments on this column to feedback@infosecuritymag.com.
How do I do more with less?

Slash your compliance and insider threat management costs with PacketMotion’s User Activity Management Platform

>> Learn more at www.packetmotion.com
A SLEW OF ACQUISITIONS and several whopping billion-dollar deals shook the security industry in the first nine months of 2010 and experts say the pace of deals are likely to continue through 2011—a sign that some security technologies are maturing.

The current economic conditions pose more potential buying opportunities for the largest, cash-heavy vendors. Additionally, many security technologies have reached their prime in maturity and are seeing adoption among even the most conservative leaning enterprises.

Many eyebrows were raised in September, when security information and event management vendor ArcSight was acquired by Hewlett-Packard for $1.5 billion. Meanwhile, chip maker Intel announced plans to dive head first into the security market by shelling out $7.7 billion for McAfee. Symantec has also made major acquisitions this year around encryption; the company bought PGP and GuardianEdge Technologies for a combined $370 million and VeriSign’s security business for $1.28 billion.

“I think we’re seeing that the timing was right and many of these vendors have the cash on hand,” says Rich Mogull, analyst and CEO of Phoenix, Ariz.-based research firm Securosis, who calls the acquisitions a part of the normal ebb and flow of the security industry. While many of the deals just made good business sense for the vendors involved, Mogull says he has seen security technologies mature to the point where larger vendors begin to take notice.

“Many security technologies are no longer in the early incubator stage,” Mogull says. “I can now recommend technologies that I couldn’t recommend a few years ago.”

Mogull is still poring over the results of a survey of more than 1,000 IT practitioners on the kinds of technologies they use to secure data, avoid a data breach and ensure compliance. The Securosis survey found that many enterprises are relying on traditional security controls in the form of network segregation and system hardening, rather than technologies that focus solely on data security, such as data loss prevention,
Mogull says. But today, DLP is gaining more traction, he adds.

“I couldn’t recommend DLP a few years ago because it was too complicated to deploy and too difficult to manage, but the technology has come a long way in a short time,” Mogull says.

Respondents to the Securosis survey identified network data loss prevention, full drive encryption and Web application firewalls as technologies they use to reduce the number of security incidents in their organization. Meanwhile, email filtering, encryption of USB/portable media drives and device control rated highly for reducing the severity of incidents.

“We’re hitting around 30 percent adoption rates for traditional security technologies at a lot of these organizations,” Mogull says. “It’s gone beyond just early adopters.”

Meanwhile, larger security vendors want to tap into new markets and keep the pace of revenue growth, says Alan Paller, director of the SANS Institute. Inevitably, it leads to a one-stop shop for a variety of security technologies, but many enterprises like the idea of standardizing with one major player, Paller says.

“Technology buyers no longer like to purchase security one piece at a time,” Paller says. “They don’t think they get as complete a picture or as rich a view of what is going on so they want to buy more security baked-in.”

Many of the network and systems management segments matured to the point where consolidation of smaller vendors just made sense, says Mark Nicolett, vice president at Stamford, Conn.-based research firm Gartner. In a smaller market segment like SIEM, with more than 20 vendors vying for a $1 billion market, acquisitions take place as the market reaches maturity, he says.

“We were seeing a natural evolution of some of these point solution markets,” Nicolett says. “Every market segment eventually consolidates as it matures.”

What do IT professionals make of all the acquisitions? A Boston-based network security administrator says he keeps pace with the major acquisitions, but ultimately they don’t affect the day-to-day business of securing the network.

“As long as the technologies we use continue to be supported and [improved], acquisitions aren’t a big deal,” he says. “We just want to keep our systems running and the bad guys out.”

Robert Westervelt is the news editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.
SNAPSHOT

Merger Mania  By Information Security staff

The information security industry has seen two mega deals so far this year with Intel's move to acquire McAfee for $7.7 billion and Symantec’s $1.28 billion acquisition of VeriSign's authentication business. Consolidation is certainly no new trend for the security market, but M&A activity picked up steam in recent months with security companies snapped up, often by large infrastructure providers:

SEPTEMBER
- Hewlett-Packard acquires SIEM company ArcSight for $1.5 billion.
- IBM acquires GRC software supplier OpenPages.

AUGUST
- Private equity firm Thoma Bravo acquires system management vendor LANDesk Software.
- HP acquires application security vendor Fortify Software.
- Tektronix Communications, a supplier of network performance monitoring and network diagnostics products and services, acquires network security and traffic management provider Arbor Networks.
- Web security provider St. Bernard Software acquires email security supplier Red Condor.

JULY
- IBM acquires configuration and vulnerability management vendor BigFix.
- McAfee acquires mobile security services provider tenCube.
- Juniper Networks buys mobile security software supplier SMobile Systems for $70 million.
- Commtouch, a messaging and Web security supplier, acquires Command antivirus division of Authentium.

MAY
- McAfee acquires mobile security management software vendor Trust Digital.

APRIL
- Symantec buys encryption companies PGP and GuardianEdge in a $370 million deal.

Threats continue to grow, compliance requirements proliferate and organizations continue to spend accordingly, resulting in some security leaders thriving. This has attracted increased investment through acquisition, with decent premiums being paid for performing assets such as ArcSight. Considering that the cash positions of many corporations remain large, this trend may continue for some months.

—SCOTT CRAWFORD, managing research director, Enterprise Management Associates
Cloud computing and virtualization present new challenges to the security of a business enterprise.

Essextc provides expertise to address the unique challenges of cloud computing, virtualization and security.

Our offering includes IBM Virtual Server Protection (VSP) for VMware. VSP offers integrated threat protection that provides protection for every layer of the virtual infrastructure, including host, network, hypervisor, virtual machine (VM) and traffic between VMs.
Stay Put!  

BY LEE KUSHNER AND MIKE MURRAY

Sometimes the best job is the one you have; it’s the best place to build skills and develop new ones.

Information security professionals change positions with great frequency, because in our experience, they are constantly in search of new challenges and opportunities to apply their skills to solve problems. While a new position may provide this type of opportunity, in most cases information security professionals change positions prematurely. Changing positions before you are able to extract maximum value in your role can be detrimental to your career development and execution of your long-term information security career plan.

By leaving a position too soon, you risk forfeiting opportunities for promotions, developing new skills, or creating a brand as a risky employee (a job hopper). You could also create doubt in your abilities to execute and see a task to completion. Being viewed as an information security professional that runs from problems before they have been solved is a red flag for future employers.

In many cases, your best job is the one you have; it’s the place where you can best apply your skills and develop new ones. This is especially true in information security where challenges constantly evolve. Considering the constant churn of new technology, new compliance requirements, and the talent shortage in many information security organizations, opportunities for professional growth are plentiful. The key for you is to recognize these opportunities and figure out how to insert yourself.

One of the better ways to do so is to be recognized with your company’s internal system for honoring top performers. By doing so, you build a reputation of trust and confidence with people who can accelerate your career and afford you more responsibility. For example, if you can demonstrate to your manager that you can excel in computer forensics, they may provide you with the opportunity to help them develop the company’s incident response plan. In many cases, information security professionals who build their brand as technically proficient are afforded the opportunity to evolve their skills towards areas of information risk management.

Awareness training is another opportunity for recognition and success. Because information security touches all aspects and functions of a corporation, you often have to evangelize the need for security. You must share your knowledge with employees who are not as aware of information security and risk-related issues. This internal need should provide
information security professionals with a combination of personal opportunities.

The first is the development of non-technical skills, such as communication, public speaking and teaching. By placing yourself in a position to educate others, you will have an opportunity to build these skills and become a more effective communicator, which is key, especially as you move into information security leadership roles.

In order to be successful, you will need to have the ability to lead and motivate others by influence and persuasion.

The second are sales skills and persuasion; like it or not, these are important tools for any security leader. In order to be successful, you will need to have the ability to lead and motivate others by influence and persuasion. Volunteering for activities that enable you to educate others who may be reluctant to receive the message will provide you with a unique challenge. If you are able to convince unwilling parties about the importance of security and effect measurable organizational change, you may find yourself being offered the opportunity to respond to other information security challenges.

Although information security and information technology may be second nature to you, it is challenging to others. Many business leaders do not understand technology, and their experiences with information security may not always have been positive. It is important for information security professionals to make themselves available to others who may require their assistance. Whether it’s the executive assistant or CEO, people are people. Providing assistance to others to ease their frustration, or expertise to help solve a problem, is appreciated.

By providing value to these diverse teams, you have the ability to learn about different components of the business that you can apply to your main role. Injecting yourself this way also helps provide key reference points when employers are considering internal promotions and succession plans. Many times being helpful and having a positive attitude can serve as key differentiators when these career-enhancing decisions are made.

Your current position often holds many hidden opportunities for career development if you seek them out. By leveraging your current position to build other skills, you provide yourself with opportunities to showcase your abilities to your current employer and demonstrate your value on a daily basis. If you are successful in doing this, you may find yourself in a situation where you do not have to look elsewhere to find a role to develop the skills you require to achieve your long-term goals.

This may sound funny coming from an information security recruiter, but this would be an optimal situation.

Send comments on this column to feedback@infosecuritymag.com.
Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today’s IT-security professional. Free.

IT security pro’s turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We’re the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — all at no cost.

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.

Breaking news, technical tips, security schools and more for enterprise IT professionals.

www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.

www.SearchFinancialSecurity.com

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.

www.SearchMidmarketSecurity.com

www.SearchSecurityChannel.com
Information Security

WE RECOGNIZE THE INDUSTRY’S BEST SECURITY PROFESSIONALS

TELECOMMUNICATIONS
Phil Agcaoili

RETAIL
Ezzie Schaff

MANUFACTURING
Brian Engle

FINANCIAL SERVICES
Blanca Guerrero

GOVERNMENT
Christopher Ipsen

HEALTH CARE
Nick Mankovich

EDUCATION
Julie Myers
Disruptive Technologies

Consumer devices in the workplace and the shift to cloud services require new security standards and heightened security awareness.  

**BY PHIL AGCAOILI**

**WE HAVE A** problem with new disruptive technology and we need to treat all endpoint systems as hostile. New consumer technology that’s brought into the workplace (a trend known as consumerization of IT), the consumer use of free or low-cost cloud services for the connected online life, and the enterprise shift towards the cloud for vertical business applications are rapidly affecting the way workers access decentralized information for personal and business use and the way important information needs to be protected.

Despite corporate firewalls and other existing controls, some employees are using their mobile devices to access services with unauthorized and insecure devices. In other cases, companies are enabling employees’ mobile lifestyles with fewer restraints, perhaps in recognition that consumer technology innovation will continue to outpace business adoption of certain devices.

Altogether, we are seeing a significant increase in the blending of personal and corporate computing, access to personal and corporate clouds, and the blending of data through personal and enterprise cloud services and consumer technology.

Rightfully, the debate over the security protocols used by the burgeoning personal and enterprise cloud industries continues. Data protection and privacy control issues stem from external parties outside of a company having physical control of corporate data. It is imperative for vendors to provide basic assurances of data protection and privacy for their customers’ data and it is also important for employees to understand the need for security when they use their personal devices to access and store corporate data (if they are allowed to do so).

New security standards are needed to address the wave of disruptive technology and practices that are converging to decentralize and consumerize IT, and mix corporate and personal data. Employees must also be engaged to support awareness and practices that include an understanding of security expectations and how to implement basic security and data protection controls on the devices they manage (and on cloud-based services they access). The best advice historically—and the consistent message in regulations such as **PCI**, **SOX**, **HIPAA**, and **Safe Harbor**—continues to be not to store or transmit sensitive information at all. My advice also is to treat everything accessing the data centers as hostile. Control and security of the

---

**Phil Agcaoili**

**TITLE** Chief Information Security Officer  
**COMPANY** Cox Communications  
**CREDENTIALS** CISM, CISSP  
**KUDOS**

Oversees the Security Program Office at Cox Communications, a privately owned cable operator that is classified as a critical infrastructure provider for the U.S.

Established an information risk management program and established a year one security awareness campaign (Security is Everyone’s Job).

Founding member of the Cloud Security Alliance and co-authored the CSA Controls Matrix in 2009 to help cloud providers design in security and provide a set of basic security controls for customers to gauge the security posture of their cloud providers.

Established one of the largest and most successful global Security Development Lifecycle (SDL) programs at Dell, where he previously led the company’s global information security assurance and consulting organization.

Member of ISSA, InfraGard, OWASP, Merchant Risk Council, Domestic Security Alliance Council (DSAC), co-founder and board member of the Southern CISO Security Council, and advisory council member for the CISO Breakfast Club.

Appointed to the FCC Communications Security, Reliability and Interoperability Council (CSRIC) and has represented GE, Dell, VeriSign, Alcatel, Scientific-Atlanta, and Cox in their respective corporate security, risk, and/or privacy councils.
endpoint is under siege, so start there because the countermeasures change when all endpoints are considered hostile.

New standards in remote access will include client virtualization technology that has adapted to gesture-based technology (e.g. iPhone, iPad, and Android). We should expect to see this technology coupled with protection measures that provide virtualized data center and application access. Data leak prevention and monitoring should continue to serve as a bastion defense in detecting inappropriate data comingling. Security teams also need to implement controls that enforce security standards on enterprise-activated devices and industry standards also need to be developed to ensure corporate data remains safe despite these trends.

Additionally, companies should identify which information is most valuable and assess the balance between protecting custodial data and secret data. According to a 2010 Forrester Research study, security teams need to focus more on protecting secret data that provides long-term competitive advantage such as mergers and acquisitions, product plans, earnings forecasts, and trade secrets and then protect custodial data that they are “compelled to protect” such as customer, medical, and payment card information that becomes “toxic” when stolen or exposed.

Furthermore, companies and cloud providers need common standards to attest for online security practices and to evaluate third-party relationships. There is an urgent need for customers of cloud computing and third-party technology services to be able to make an objective comparison between providers on the basis of their security measures. Existing mechanisms to measure and provide security assurances are often subjective and in many cases unique. This makes quantifiable measurement of security practices difficult, which impacts time and cost.

We are at the crossroads. Security needs to continue to evolve with disruptive technologies and to support employee mobile lifestyles. However, we must look for standards and common technology, and we must provide continual, evolving awareness to our user communities. We should set expectations and controls—where we can—to help transparently integrate new security measures to minimize these new risks. We must prepare for this now and educate ourselves and our users.

Send comments on this article to feedback@infosecuritymag.com.
Removing Uncertainty

A successful information security program uses ongoing oversight and monitoring to manage risks.  

**INFORMATION SECURITY** can often present us with many variables and complexities. We are typically concerned with the variables presented by unknown attackers, evolving threats, and the difficulty in determining the probability of all the things that can go wrong. Often we must also face the additional complexity of unknowns presented by the organization itself. Expansion and growth can result in distributed operations at varying levels of maturity with a lack of standardization. The variables produce complexity, and complexity can be the breeding ground for uncertainty.

To limit risks to an acceptable level, an information security program must remove uncertainty. The objective is to deliver the proper level of effective controls to protect information resources without excessive cost and without inhibiting required business operations. The italicized words form the gray area that regularly defeat information security metrics and risk equations. Achieving a balance between secured and useful, within budgetary constraints and organizational complexity, is the challenge we all face. These are the principles of business risk that essentially define our role. The gray area is where we either sink or swim.

In the physical world, we can calculate, measure, and quantify the characteristics of the things around us on a molecular level. Why then is the ability to convey a non-subjective, factual, understandable and consistent account of the status of security within an organization an elusive gray area of uncertainty? Physics and quantum mechanics are used to form a fundamental view of the physical world. Explore Heisenberg’s Uncertainty Principle or Schrodinger’s cat in the box theory to see that the thought leaders in the realm of physics have deeply evaluated aspects of uncertainty. These theories consider how the act of observation can affect the subject. The act of observation could change the factors while determining the relative position, direction and velocity of any particle using a single measurement at a point-in-time cannot accurately describe all of the characteristics.

Applying the logic provided by these physics theories, I would submit an Information Security Certainty Principle: “That which is not observed will cease to move, and single observations will only determine an inadequate description of the current state.” This should not be earth-shattering for any security practitioner. The adage that you cannot manage what you do not measure applies to the management of information security as it does generally within other disciplines. Oversight...
of information security is an ongoing and constant process.

The activities that provide information security are numerous, and include functions performed by people, processes, and technology. Activities may be integrated into a centralized IS&T operation or distributed across many technology groups and business functions spread throughout the organization. These factors produce a degree of complexity and uncertainty that can only be overcome with the frequent measurement and reporting of oversight.

To obtain the level of assurance necessary to achieve a state of security rather than compliance, you must move beyond this infrequent evaluation and move towards a constant level monitoring with reporting.

In the past, trust but verify typically equated to an audit performed at a regular if not infrequent interval. To obtain the level of assurance necessary to achieve a state of security rather than compliance, you must move beyond this infrequent evaluation and move towards a constant level monitoring with reporting. A fundamental component of a successful information security program is oversight and monitoring of the numerous individual functions. Define reporting to ensure that the function is completed regularly, trend the output over time to detect changes, and constantly evaluate the environment to define monitoring for functions that effectively secure information.

At Temple-Inland, we have improved our level of security while reducing costs by distributing information security operations into IS&T operations. Our Information Security Program includes oversight of the functions with reporting performed by the IS&T operational groups themselves, where failures can be quickly identified and corrected. Oversight of a self-monitored process permits the Information Security Team to focus on identifying control deficiencies and protection gaps as well as areas where technology risks can be further reduced.

The success of an information security program depends on lowering risk efficiently and effectively. Too often, information security professionals begin with a focus on metrics and dashboards that measure the value of the overall program. Instead, we must start with implementing processes that help secure our environments along with the oversight that provides the monitoring and management of those processes. Uncertainty is present in many aspects, but it should never be found within the security processes you assume are performed within your organization. The metrics that demonstrate the value of the overall program will be determined by the percentage of implemented security processes with defined oversight. Effective oversight of distributed information security operations can reduce uncertainty and improve security.

Send comments on this article to feedback@infosecuritymag.com.
Balancing Act

Provide users with choices in order to minimize online risk without becoming intrusive. BY BLANCA GUERRERO

ADDISON AVENUE FEDERAL CREDIT UNION serves more than 140,000 members, a good percentage of whom don’t live or work near a branch. As people move away from the area or change jobs, they would rather continue to do business with Addison Avenue online than change to a local bank. So it’s important that we offer secure online and mobile access.

Sounds simple, right? But finding the right mix of security and convenience can be a bit tricky.

The convenience of our online banking is a big draw for our “remote” members. They appreciate having access to their money from any computer, 24 hours a day, every day. Our goal is for all of our members to feel that banking with us online is not only convenient but absolutely safe, just as safe as doing their banking at a branch.

Behind the scenes, of course, is an infrastructure designed to keep our members’ money and confidential information as safe as it can be. Specialized hardware, software, and a dedicated staff of information security specialists are hard at work to keep information in and intruders out.

But the truth is that there are some things that are out of our control. Identity theft is continually on the rise, and fraudsters are becoming cleverer at pilfering electronic information. Our firewalls may be virtually impenetrable, but members themselves can do things inadvertently to put their money or personal information at risk, like doing their banking on a public computer, or jotting down their login information and accidentally leaving it where someone else might find it, or not noticing the person behind them at the checkout watching as they enter their PIN.

Adding complexity is the fact that some people have a greater tolerance for risk than others. Our default security settings aim for the “sweet spot,” where the majority of members feel their information is absolutely secure, and yet they are not annoyed by seemingly endless rounds of passwords and security questions.

But everyone’s threshold is different—some may prefer security that is less strict, while some feel the need for added protection. So how can we minimize risk without becoming intrusive?

Our answer to this problem can be summed up in one word: choices. The fact is that if you let someone choose what they’re going to do, even if the choices are limited, they will feel more in control of their situation and less inconvenienced or forced.

So, at every step of the way, we strive to provide choices for our members, within a multi-pronged approach to information security.

Blanca Guerrero
TITLE Senior Vice President, Chief Information Officer
COMPANY Addison Avenue Federal Credit Union
KUDOS CIO of a full-service financial institution that serves more than 150,000 members and offers a secure online banking portal, a 24/7 call center, and 23 branch locations.
Led team that developed and implemented the first online account opening system using electronic signatures and automatic fraud detection in the credit union industry.
Implemented a cloud-based, strong authentication system for members who regularly perform a greater proportion of higher risk online transactions.
For the past 12 years, has been in leadership positions that oversee IT security directors, IT security architects and engineers.
Member of the Credit Union National Association (CUNA) Technology Council.
Education. We are committed to educating our members on Internet safety. Our website has plenty of information on best practices when conducting online transactions, and we host presentations at our sponsor company sites on identity theft and other security related issues. When you log into Online Banking, you are automatically given suggestions to strengthen your security settings. The goal is to raise our members’ awareness, and then give them choices to implement whatever level of security setting they decide is appropriate for their situation and comfort level.

Fraud detection software. We have specialized fraud detection software to protect our members from unauthorized login to their account. The program analyzes a member’s behavior—the location where they normally log in, the computer they use, the time of day, the kinds of transactions they do—to construct a behavioral pattern for that person. If their transactions fit the pattern, we don’t intrude. But if we detect some change in that behavior—for example, an unusually large withdrawal request or logging in from a different city or country—we ask them to provide extra proof of their identity.

Multiple levels of security. Email is the default security notification—all members are emailed automatically if there’s been a request to reset a password, change security settings or perform a wire transfer. In addition, we offer authentication by phone, text message or Security Key; some people will gladly perform this extra step at every login for added reassurance.

Our Security Key is the option that offers the most security for the least inconvenience. With phone or text authentication, members who travel may not be in an area where they can receive a one-time password over their mobile device. The security token is a self-contained system that is not subject to a carrier’s coverage area, and generates your one-time password wherever, whenever you need it. And because the key is separate from your computer, it’s not susceptible to viruses or fraud.

We calculate the success of our security programs by tracking the rate of adoption and surveying members for their reactions. We hope that members will perceive additional security choices like going through airport security, knowing that the scanning and checks are intended to protect them, not inconvenience them.

Another key measure of success is a reduction in fraud. We are already seeing a tangible drop in inappropriate online activities, and to date we have not incurred any loss of funds through fraud. Still, we are constantly researching new ways to continue to provide the most convenient and secure online banking services for our members.

Send comments on this article to feedback@infosecuritymag.com.
Opportunities in Adversity

The economic crisis gives government entities the opportunity to change for the better.  

BY CHRISTOPHER IPSEN

Christopher Ipsen
TITLE Chief Information Security Officer
COMPANY State of Nevada
CREDENTIALS CISSP, CISM, Information Systems Security Architecture Professional (ISSAP)
KUDOS
Responsible for information security oversight of the statewide network infrastructure known as the Silvernet.

One of several drafters and the primary technical contributor of the revised Nevada Data in Transit Encryption Law, SB227. Testified in support of the legislation’s technical merits as well as to why government agencies should be subject to the same encryption requirements as business. The legislation passed unanimously last year amid political contention and unprecedented gubernatorial vetoes.

Developed and fostered relationships with key IT, law enforcement, legislative, and business leaders within the state, which led to his selection as state representative on several key intergovernmental workgroups, including the Nevada Technological Crime Advisory Board (TCAB), and the Nevada Shared Information Technology Systems.

Instrumental in developing a statewide unified business portal that will provide a consolidated security capability that can be leveraged by all state entities. The multi-million dollar project received legislative approval despite a state budget reduction of 30 percent.

Under his leadership, Nevada has been at the national forefront of developing security standards for emerging technologies. Nevada was the first state to produce a statewide security standard on server virtualization.

GOVERNMENT, BY NECESSITY, is undergoing significant transformation. This is particularly noteworthy because resilient governments, by design, change slowly. Radical changes in democratic states can create scenarios where citizens lose rights and control over their freedoms. We need to be mindful of both the opportunities and potential outcomes as we make decisions about how transformation will occur.

The first condition in transformation is a sense of urgency, as cited by Harvard Business School professor and change expert John Kotter in his eight-step framework for change (other conditions can be found in the National Association of State Chief Information Officers’ “Transforming Government Through Change Management” research brief). When the national economy plummeted in 2008, Nevada state government responded immediately by reducing projected budgets by 20 percent. Now, two years later, Nevada is facing an additional 45 percent budget shortfall. Our state government is being challenged by a significant increase in demand for services compounded by a decrease in funds to respond. Nevada typifies the sense of urgency condition facing most government entities today.

Technological innovation is a core response many government entities consider as they face fiscal challenges and undergo transformation. Technology, if developed correctly, can bring the efficiencies needed to address the growing mismatch between increased service demand and diminishing financial resources. It can provide citizens with a central, easy to find, place to do business. This efficiency can also be extended to encompass multiple scenarios whereby many governmental bodies share the same technology to provide multiple services to the same citizen. A good example is a one-stop online shop for creating a business—a single place to incorporate, buy a business license, and pay business taxes.

Even democracy itself can be transformed by modern technology. One of the arguments for the creation of the Electoral College was the geographic inability for all candidates and electors to travel and vote. If individual votes can be validated by technological means through online voting, why maintain the Electoral College with its face-to-face validation of the decisions of electors?
Technology can allow governmental leaders to rethink how government works without the constraints of geographic requirements. DMV functions (like reissuance of driver licenses) that reside with state governments can be leveraged across the intergovernmental boundaries of counties and municipalities without a local physical presence. Similar capabilities can be leveraged from a county or city statewide. This capability, if captured and expanded, could make legacy governmental boundaries porous, allowing evolution of government functions toward more capable, more widely distributed, technologically-enabled entities.

Confidentiality, integrity, and availability needs are amplified concurrently with the aggregation of data stored and processed.

Of course, in any aggregated service model that is geographically distributed, information security becomes critical. Confidentiality, integrity, and availability needs are amplified concurrently with the aggregation of data stored and processed. Moreover, if the integrity of technology—such as electronic voting—is compromised, the results would be catastrophic.

So how do we intelligently embrace emerging technologies in the transformational model described above? To capture the most favorable outcomes, I believe we need to focus on four major areas:

- **Vision and Empowerment to Act.** Without strong leadership and executive sponsorship for the technologically enhanced vision, effective transformation does not occur. Once formed, the vision must be implemented and individuals empowered to act.

- **Strong Architecture and Rigorous Security Controls.** Good architecture reflects business needs that have been distilled into an appropriate IT response. It also provides a means to measure outcomes and quantify costs in a manner meaningful to those who control government budgets. Rigorous controls, including continuous monitoring, build confidence and trust in the reliability of information stored and utilized by government and in the shared understanding that information security represents money well spent. Reliable data and the security of confidential information is a fundamental requirement of many governmental functions. Governments fail if they cannot provide trust with the systems they use.

- **Effective Intergovernmental Collaboration.** In an efficient, citizen-centric world, governmental entities collaborate. Without the geographic constraints, successful technical solutions developed at any level of government can be leveraged for all citizens. Contract costs can be reduced and IT capabilities can also be improved by capturing larger enterprise economies of scale.

- **Effective Public/Private Collaborative.** The transformational model is incomplete if we limit the scope of solutions. There are civic-minded individuals in the private sector who provide necessary feedback on security solutions and dedicated and effective IT professionals in the public sector who bring context and capability to solutions. When we value and capture the capabilities of all entities, we form communities of collaboration and defense. We also provide better service to the citizens.

While Nevada faces tremendous challenges, we are not searching blindly for a path. Four years ago, Nevada embraced intergovernmental collaboration through regular meet-
ings of the State of Nevada Entities Technical Alliance (SNETA) and formal adoption of the Nevada Shared Information Technology Systems (NSITS) governance. The “Nevada Experience” has been underpinned by the continuing evolution of the state Technological Crime Advisory Board, which is comprised of key federal, state, local and private sector decision makers spanning the legal, law enforcement, commercial, technological, education, and legislative communities. The advisory board’s actions and recommendations support Nevada IT security professionals at all governmental levels, who, themselves, communicate regularly on current challenges and shared responses.

The fiscal crisis has been sufficiently long so that political posturing is decreasing along with a genuine realization that cooperation is the only remaining option. At the same time, security is a fundamental component of change that ensures rights and democracy.

By necessity, I’m optimistic. When the economy improves, Nevada will emerge from the crisis with streamlined capabilities that embrace information security as both a business and government enabler. ·

Send comments on this article to feedback@infosecuritymag.com.
Driving Force

In the world of health care, the more we value privacy, the harder we work to protect it.  

BY NICK MANKOVICH

I CONFESS I used to run away from all professional discussions about privacy. I found them murky and contentious: a bit like religion or politics but peopled with lawyers, legislators, and lobbyists! Still, from my comfort zone of managing security controls I wrestled with the notion of privacy, which seemed to be something inside of confidentiality that kept squeezing out through the cracks to be much, much more. Worlds collide when a researcher says, “Well, it’s my data about these patients, so I can give you access.”

My turning point was purchasing an out-of-print copy of Alan Westin’s 1967 book Privacy and Freedom. This prescient, insightful work provided a context for these difficult conversations and prompted me to adopt the following definition: “Privacy is the right of the individual to control information about him or herself.” When feeling devilish, I’ll throw in “perceived right” just to dangle the red cape and begin a lively discussion among colleagues from different countries.

Beyond giving me a chance to reflect on one of the big questions behind security, that definition essentially provided the driving force for my security work. In my world of health care, the need for security and privacy arose more than 2,500 years ago in the Hippocratic dictum, “All that may come to my knowledge in the exercise of my profession…ought not to be spread abroad, I will keep secret and will never reveal.” The more we value privacy, the more we search for the best ways to protect it. Many of us who have worked in health care recognize this relationship as we support people in their efforts to stay and get well, providing the best care with the safest equipment. The high principles of safe, effective, and secure health and wellness allow us to carry on our daily work with a genuine passion. We recognize on a personal level our deep dependence on our industry’s products and services during the most vulnerable times in our lives and the lives of our loved ones.

Five years after jumping off the security cliff into the problematic world of privacy, I feel more comfortable tackling the difficult discussions around both of them. They are meaningful discussions but seldom are they easy. That’s because they test the limits of what people will tolerate as they meet head-on the life-changing aspects of technology in the 21st century. Many of us are not ready to give up our location every minute or share our...
innermost thoughts with strangers, but some of us are. How can we help companies and health care organizations navigate this diverse new world? Our seemingly miraculous IT-based devices and services have made the delivery of care much more effective but, unfortunately, very complex. We must reduce the complexity to give people choices and, when we don’t know their choices, act conservatively and both secure and keep confidential their personal information.

I have learned that there are many security risk management practices that are transferrable into the world of privacy. As has been noted in these pages over and over again, it’s not just a matter of marking off a checklist a set of features, settings or practices. It’s about balancing the risks of security or privacy breach consequences with the cost of maintaining security and privacy. The underlying theme is risk management—really thinking about how risk accrues if we fail to comply with law, regulation, policy, contract, ethical behavior or the choices of the individual. Working under the risk management umbrella led Philips Healthcare to create two global interrelated programs—one for product and services security and the other for privacy compliance—both led by me.

Less than five years ago, Brian Fitzgerald of the U.S. Food and Drug Administration called together a diverse mix of health care folks to talk about the harm that was being done from poor networking of medical devices in hospitals. His agency had reports of injury and death as a result of improperly connected networked devices. In that first brainstorming meeting of December 2005, there were biomedical engineers, IT professionals, regulatory specialists, medical device risk management specialists, security professionals, and medical device engineering staff. Brian urged us to organize and do something to help the world avoid this harm. To avoid international mismatches and “not invented here” issues in government regulatory authorities, he suggested this be pursued as a global standard. In September, the first international standard to address Application of Risk Management to IT-networks Incorporating Medical Devices (IEC-80001-1) received final approval.

This standard lifts security and privacy risk out of the afterthought category into the mainstream of health care delivery. It does this by building around the principle that decisions in any new device integration project in health care need to be built around some simple concepts. In the parlance of IEC-80001-1, medical IT-network risk management proceeds with a careful examination and understanding of three key properties: (1) safety, (2) effectiveness and (3) data and systems security. By considering all three, we can first “do no harm” while effectively delivering on the organization’s health care mission. This is done with careful and explicit treatment of the appropriate level of confidentiality, integrity, and availability.

Of course, today’s IT staff and biomedical engineers are skillful at keeping the highest levels of safety and effectiveness. However, with IEC-80001’s explicit inclusion of data and systems security breach into its definition of harm, we have paved the way for an open and honest discussion of the C-I-A impacts of an interconnection project or a network change. It allows a consideration of the harm brought to individuals when confidentiality is threatened and, for the first time, consideration of the harm of privacy compromise is an essential part of the IT, biomedical engineer, caregiver, and compliance discussions.
This is an exciting time. I believe that this new risk-based framework for bringing together caregivers, biomedical/clinical engineers, security professionals, and privacy professionals will improve the quality of care. Although not without effort or difficult choices (and some free falling), we now have a framework to discuss and decide on the best way to provide the highest levels of safety, effectiveness, and security.

Send comments on this article to feedback@infosecuritymag.com.
Fighting Fraud

Battling online fraud requires a delicate balance between security and customer service. By Ezzie Schaff

I’VE BEEN BATTLING online fraud for a decade and the job doesn’t get any easier. The fraudsters are continually looking for new ways to deceive and steal, requiring constant vigilance. In the past, fraudsters were easier to spot, such as someone in another country ordering an international shipment. Today, sophisticated fraudsters are using tactics like spoofing their IP addresses and using U.S.-based shippers.

Every day, we’re up against new schemes. What may have worked to fight fraud even just a year or two ago can quickly become ineffective.

At Ice.com, where we sell high-ticket jewelry items that cost anywhere from $50 to $50,000, we have to be especially on guard. In retail, jewelry usually commands a higher street value, making it particularly attractive to criminals.

While you can’t completely eliminate fraud, you can minimize it. One countermeasure we’ve found to be highly successful in beating back fraud is knowledge-based authentication (KBA). We use the technology to verify the identities of customers calling into our call center with high-risk transactions – cases that have been flagged for potential fraud.

The KBA system provides our call center agents with a series of questions about the individual customer—ones that technically could only be answered by the person conducting the transaction. The system accesses a mix of public records, such as those maintained by credit bureaus, and commercially available databases. It also measures the level of risk associated with a particular identity and can address high-risk identities by adjusting the difficulty of the questions.

However, using the KBA tool requires a delicate balancing act so as not make customers feel uneasy. Many of our customers are shopping for special occasions like engagements and weddings and the last thing we want to do is spoil the event. We’ve learned to mold fraud prevention into a customer service experience. We conduct the conversation in a way so that the customer understands the series of authentication questions is to his or her benefit, not just the company’s. Once we explain the risks people face in using their credit cards for online purchases, our customers appreciate the fact we go the extra mile for them.

With the KBA tool, we’ve seen a substantial reduction in fraud-related chargebacks, saving Ice.com money in reimbursing customers whose cards have been used fraudulently. At the same time, the security system hasn’t affected our customer satisfaction rating.

Sometimes battling fraud also involves physical security measures. We’ve seen an increase in “soft fraud”—specifically,
cases in which a customer claims non-receipt of merchandise and return fraud. We believe these recent fraud trends may be a result of bad economic conditions. To combat the problem, we videotape on high-resolution tape every shipment from the time it’s packed to the time it’s sealed. We do the same for returned packages. Anytime a package is returned—from the time it’s received in the shipping facility and sent to the packing station—we videotape it so it’s very clear what was in the package.

We have to do this—especially in our business of selling high-end merchandise—because someone can claim to have returned an item but actually return an empty box. Our diligent gathering of physical evidence has led us to win every time we take a fraud case to court.

To deal with the rapidly evolving nature of fraud, we’re constantly evaluating our data and investigating new technologies. But more importantly, we speak often with others in our industry. Industry collaboration is critical in the fight against fraud. If a fraudster is targeting one jewelry site, they’re likely going to do the same to another the next day. When it comes to battling fraud, competitors quickly become collaborators.

Send comments on this article to feedback@infosecuritymag.com.
Critical Collaboration

Implementing an information security strategy in a decentralized environment requires a collaborative approach.  BY JULIE MYERS

IN MANY INSTITUTIONS of higher education, computing environments are generally characterized by some degree of decentralization, with greater decentralization in large research universities, according to a report by M. Santosus. There are certainly advantages to fulfilling the needs of individual users and groups, to the greatest degree possible, with decentralized computing environments. However, information security is inherently a central function. The information security paradigm—you are only as strong as your weakest link—recognizes that we must be able to measure the effectiveness of information security policies, technologies, and programs at the lowest levels of the organization. In addition, since the university as a whole is the registered legal entity, the institution implicitly assumes all liabilities, including those that might be due to the lack of security in any one departmental unit.

At the University of Rochester, we have learned that successful information security programs depend on mediation by someone who knows the members of the department, is seen by those members as having department-wide responsibility and credible with the communication of best practices. To this end, we are formalizing the role of Information Security Liaisons in the divisions and departments. These individuals will help to evaluate and mitigate security and compliance concerns and risks, while giving Chief Information Security Officers the visibility needed to develop metrics and monitor progress. This distributed approach to information security ensures that each department is aware of and accountable for its role with regard to the communication of information security education and training materials, compliance with policies and standards, and implementation of information security technology solutions.

The University of Rochester’s information security program also employs several layers of defense through a combination of policy, technology, and community awareness in collaboration with the units. The university has made significant investments in information security technologies. These technologies span all levels of a defense-in-depth strategy from our perimeter to the individual endpoints. The distributed computing teams are engaged in defining requirements and designing technology solutions that support their departmental needs. In addition, where possible, the tools selected allow the departments to administer and manage the technology with overall monitoring maintained within the central organization.

Finally, we have institutionalized a University Data Security Committee, which is co-chaired by the Provost and General
Counsel. The committee membership consists of the Chief Information Officers, Chief Information Security Officers, Divisional Information Security Liaisons, and representations from audit and other areas with high-risk data. The University Data Security Committee helps to prioritize information security activities based on the results of annual risk assessments, sponsors university-wide information security policies, and monitors overall performance metrics.

With ever-evolving threats to information security, it is essential to properly secure data and minimize risk while still enabling users to educate, collaborate, and innovate in this digital environment. Centrally managed information technology solutions help to make information environments more secure almost by default. However, the rapid transformation of information technology towards highly flexible, consumer-oriented tools increases the opportunity for users to make choices that may put an organization’s information at risk of a breach. Much of the success of an information security program depends on the everyday choices that members of the community make when using information technology and accessing information.

Much of the success of an information security program depends on the everyday choices that members of the community make when using information technology and accessing information.

In such a decentralized computing environment, strategies to protect the institution’s information assets can only truly succeed with a collaborative strategy between the central information technology teams and decentralized units.

From the development and deployment of an Information Technology Strategic Plan for security and compliance, to measurement of our overall progress in meeting our information security goals, we have strived to include members from across the university community. In a decentralized environment, it is critical that we recognize that one size may not fit all. Understanding the unique needs of the different groups within the university community and leveraging the expertise of the decentralized teams has helped position us to reduce our information security risk and increase our overall compliance posture in a more comprehensive and sustainable way.

Send comments on this article to feedback@infosecuritymag.com.
Mark Weatherford won the 2008 Security 7 Award in government, when he was CISO for the state of California. In July, he became vice president and CSO at the North American Electric Reliability Corporation (NERC), an international regulatory authority.  

**ON HIS RESPONSIBILITIES AT NERC:**
The NERC mission is to ensure the reliability of the bulk power system in North America and my CIP (Critical Infrastructure Protection) group is relatively new. I’m only the second CSO and I want to evolve this program with a more enterprise vision. That means focusing on providing advice and services as necessary to help industry meet and understand existing critical infrastructure protection standards while working with industry to revise those standards where there is ambiguity and develop new standards where there are gaps. There are about 2,000 companies, both public and private, and local governments in the U.S. and Canada that provide electricity generation, transmission and distribution functions. It’s a big group—everything from companies that service millions of customers to companies that only serve a few hundred customers in rural areas. Resources and expertise obviously aren’t spread evenly; some companies need more assistance than others. We want to help those companies that may not have the resources, but are just as important to the bulk electric system from a grid perspective, to understand and achieve compliance with the security standards.

**ON HIS PRIORITIES:**
The first is to establish a strategic plan for the CIP organization. NERC was already working on strategic priorities and planning issues when I joined the company in July; I want to set goals for my organization that are a subset of the company’s goals…The other big and time-critical priority is development of a threat and vulnerability management program. Right now we don’t have a streamlined process for gathering information on threats in the wild, like Stuxnet, and then coordinating with industry, vendors and the government. We want to make sure we’re collecting the right information and disseminating it to the people who need it in a timely fashion.

**ON STUXNET:**
As far as we know, no U.S. companies have been affected by it yet. Right after Stuxnet became public in July, we put together a CIP Malware Tiger team with a number of
catching up with Mark Weatherford

cybersecurity experts from industry, government, antivirus companies, educational institutions, and control system companies. We’ve already issued two advisories and are preparing to release some very specific guidance to industry very soon.

ON WORKING FOR THE STATE OF CALIFORNIA WITH NO FUNDING:
Like most CISO’s, I’ve never been in a position where I had all the people, money and time to do everything that needed to be done, so that helped me learn to be creative. There are some smart, dedicated people working in the various agencies and departments in California state government and most of them didn’t work directly for me. When I needed help on a project or issue, I would bring a group of the “go to” people together; I was very creative with other people’s resources—that’s how we got a lot of things done. I also succeeded in winning grants. Of about $21 million in homeland security funding the state received last year, my department received almost $4 million.

ON HIS ACCOMPLISHMENTS IN CALIFORNIA:
I put together a strategic plan that laid out a five-year vision for the state’s cybersecurity program. This had never been done before and provided a roadmap for both the state and our vendor partners. We also developed comprehensive security policies for state government, which was one of the hardest things I’ve done in my life. Working with so many different agencies and collective bargaining units and agreeing on so many policies was a Herculean effort. Probably what I’m most proud of is how we created a culture of security and we created that cadre of security professionals—people were proud to be security people.

ON HIS ADVICE FOR WORKING WITH A TIGHT BUDGET:
Get creative. Money isn’t everything. There are a lot of open source tools out there. Some people in the security business seem to shy away from open source and while I’d never say embrace them without doing your due diligence, there are good open source tools that cost no money and perform better than things you can spend a lot of money on. Also, be able to look at the big picture. At the CISO level in the security business, if you focus on small problems, the minutia, you’ll get buried. It’s important to keep a strategic vision and provide the leadership that people expect of the CISO.
Information Security’s list of past Security 7 Award winners:

2009
Jerry Freese
Melissa Hathaway
Bruce Jones
Jon Moore
Adrian Perrig
Bernie Rominski
Tony Spinelli

2008
Bill Boni
Mark Burnette
Michael Mucha
Marc S. Sokol
Gene Spafford
Martin Valloud
Mark Weatherford

2006
Stephen Bonner
Larry Brock
Dorothy Denning
Robert Garigue
Andre Gold
Philip Heneghan
Craig Shumard

2005
Edward Amoroso
Hans-Ottmar Beckmann
Dave Dittrich
Patrick Heim
Christofer Hoff
Richard Jackson
Charles McGann

2007
Michael Assante
Kirk Bailey
Michael Daly
Sasan Hamidi
Tim McKnight
Mark Olson
Simon Riggs

For a 2011 Security 7 nomination form, go to: www.searchsecurity.com/securityseven
Teaching you security...one video at a time.

Traditional learning methods have always been about flooding students with as much information as possible within a given time frame -- often referred to as 'drinking from a firehose'.

The Academy Pro allows information security professionals to learn about today's most important technologies on demand and at their own pace.

Check out The Academy Pro at www.theacademypro.com

Sponsored by:

www.theacademypro.com

The Academy Pro © Owned by Black Omega Media Group Incorporated
Database auditing is a core component to compliance and security programs, and a generally accepted practice by IT operations. Relational databases were the first enterprise application to embed auditing as a native platform feature. Yet part of this heritage is the stigma associated with auditing. Vendors provided the basic function but they failed to provide the performance and ease of management demanded by database administrators (DBAs), who remain loathe to enable the feature, and remain one of the last holdouts for accepting the use of database audit trails.

The reasons for their distaste of native audit are fully justified: from performance and data management nightmares, to the fact that these audit trails were not originally designed for the tasks they are being applied to. Regardless, regulatory compliance demands accurate and complete records of transactions, and relational database audit trails produce just that.

Security and compliance drive the use of database auditing, and these log files provide a unique perspective that needs to be captured. Database vendors are building better auditing features into their products, minimizing historic impediments, but careful deployment is required to avoid these known issues.
WHAT IS DATABASE AUDITING

Database auditing is the examination of audit or transaction logs for the purpose of tracking changes with data or database structure. Databases can be set to capture alterations to data and metadata, along with modifications to the database system storing the data. A typical audit record will include the database operation performed, the data values that were changed, and who performed the operation, along with a number of other attributes. Auditing capabilities are built into all relational database platforms, and ensure these logs have the same degree of accuracy and integrity as the data being stored. Further, the audit trail is able to group a series of statements together into logical transactions, providing a business context that makes it a preferred choice for forensic analysis of business processes.

There are some limitations with auditing because data access statements, commonly referred to as SELECT statements, are not collected. Additionally, native database audits seldom capture the original query or variables passed by the user; rather they record a synthesized view of the event. The logs capture data values, both the before and after, changes were made. That makes audit trails much more useful for detecting what was changed, rather than what was accessed.

For forensic examination of database activity and state, audit provides an accurate view of events. For review of SELECT statements—people trying to view data—the native platform either lacks the ability to collect these statements, or does so by enabling advanced options that incur a significant performance penalty. It's for this reason that, when used for security, audit trails are most useful for when looking for insider misuse—rather than external attacks.

There are easier and more efficient ways of cataloging SELECT statements (e.g., failed logins, attempts to view credit card information) and why organizations choose to supplement native database auditing with other data collection sources. Regardless, built-in database auditing features produce the core information for transaction verification and regulatory controls.

IDENTIFYING DRIVERS FOR DATABASE AUDITING

Before we delve into some of the specific tools to create and collect database audits, let's take a closer look at why these features are being put to use. Your organization may have one, or perhaps all, of the following requirements:

Compliance: Regulatory controls, such as change management, business process verification, system failures or security events material to accuracy and consistency. That’s why database auditing is critical for fraud detection, as well as regulatory compliance requirements related to Sarbanes-Oxley. Change management, transaction history, reporting of ad-hoc events are all the types of things normally required for regulatory controls. Supplementary controls for PCI-DSS are relevant as well, with system privilege changes, or any administrative activity and alterations of system functions needing careful scrutiny.

Keep in mind that database auditing is not specifically listed as a requirement in any compliance mandate, including SOX, PCI-DSS, HIPAA, FERPA or any of the state privacy
regulations. In practice, audit fills an essential role by providing an accurate and concise history of business processes, data usage and administrative tasks—all necessary elements for policy enforcement. As databases back all enterprise applications, and are the sole authority on data state—the net results of business processing—they are the most logical and effective place to implement controls. As such, most audit requirements that center on tracking a specific set of users, objects, or data elements require database auditing.

Security: Data security and privacy, over and above what is required for the regulations listed above, is the other major driver for database auditing. Capturing failed logins, failed queries and misuses of administrative functions is a way of detecting system probing. Monitoring the add-on of views that can expose data, public permissions to use system functions, and privilege changes that provide administrative capabilities to regular users, are all common use cases. Forensic analysis of who, what, when and where attributes provide fair indication if database usage was legitimate or a probable attack. In the event of database tampering, the audit trail provides enough information to determine what changes and help understand required corrective action. The audit trail is commonly used to feed security tools such as SIEM and log management for correlation and security event notification.

Operations: Database auditing was originally designed to help database administrators examine database activity so they had a better understanding of how to allocate resources and what queries needed tuning. While there are better tools to accomplish these tasks today, auditing still provides failure analysis and business process analysis to ensure reliability of database activity. Because let’s be perfectly honest, when a catastrophic failure occurs and you are asking “What just happened?” having an audit trail is a pretty handy tool for recovery.

DATABASE AUDITING TOOLS AND APPLICATIONS
There are four basic platforms used for creating, collecting and analyzing database audits: the native database platform; system information and event management and its cousin log management; database activity monitoring; and database audit platforms.

1. **Native Audit**: Refers to the use of native database auditing for data capture, but use of the database system itself to store, sort, filter and reporting of events. IBM, Microsoft, Oracle and Sybase all offer slightly different variations, but capture essentially the same information. Data is typically stored within the database, but can be exported into flat text files or sent as an XML data feed to other applications. Using the native features saves on the costs associated with acquiring, deploying and managing a dedicated auditing tool, but suffers from additional performance overhead on the database, limited management features over and above basic collection and storage, and requires manual administration. Native auditing occurs within the database, and is used just for the analysis of the databases housed within a single installation.
2. **SIEM AND LOG MANAGEMENT**: Security information and event management and similar log management tools are capable of collecting audit files, but offer many more features that the native database tools. Keep in mind that these tools pull the native audit trails from the database, but a dedicated server is used for storage and processing, relieving much of the burden from the database. They also collect information from network devices, operating systems, firewalls and applications in addition to database audit logs. SIEM and log management offer integrated reporting, data collection, heterogeneous database support, aggregation and compression — all advantages over native database capabilities. Log management systems, as represented by companies such as LogLogic and Splunk, are specifically designed to accommodate vast amounts of data, and focus more on management and reporting. SIEM, represented by companies such as ArcSight and RSA the Security Division of EMC, are designed more for analysis, with near real-time policy scrutiny, greater depth in event correlation and alerting. Still, differentiation between SIEM and log management will soon be a thing of the past as most vendors offer both platforms, albeit not fully integrated.

3. **DAM**: Database Activity Monitoring platforms are designed to monitor database activity for threats and enforce compliance controls. Vendors such as Application Security, Fortinet, IBM, Netezza and Oracle offer heterogeneous capture of database events. Most offer more than one way to capture information, collecting queries from the network, from the operating system under the database as well as the database audit logs. DAM tools are specifically designed for very fast retrieval of data and real-time policy enforcement. Like SIEM tools, they can collect data from heterogeneous databases, multiple data sources, and are designed for analysis and alerting. Unlike SIEM, and as they are specifically tailored to databases, DAM systems are much more focused on database analysis at the application level rather than the network or system level. DAM products also offer advanced features such as activity blocking, virtual patching, filtering and assessment capabilities in addition to forensic activity analysis.

4. **DATABASE AUDIT PLATFORMS**: Some of the database vendors offer specialized databases that resemble log management servers. These are comprised of a dedicated platform that stores log files captured from the native database auditing, collecting multiple database logs into a central location. Some of these platforms offer heterogeneous database log file collectors. Reporting, forensic analysis, aggregation of log files into a common format, and secure storage are common benefits. They do not offer the multidata sources or fine-grained analysis of DAM, the correlation and analysis capabilities of SIEM, nor log management’s ease of use. But for IT operations focused on database auditing, this is a cost effective way to produce security reports and store forensic security data.

**DATABASE AUDITING SELECTION PROCESS**

To assist with your selection process for database auditing, you will want to consider the following attributes of each platform type, and each vendor’s solution. In the order of importance:

- **Data Sources**: The primary source of information described in this article is database audit logs, which are created by the database engine. However audit logs vary from database to database, and in some cases there are multiple sources of information that are
lumped under the same term: audit log. Further, some platforms can create an activity log of user actions against the database. While this later variation is not as accurate as what is created by the native platform, it does provide all SELECT statements and better performance to boot. You need to carefully inspect what data is available to you from the different data sources, and see if this is enough information to fulfill your security, operations and compliance requirements.

- **Compliance:** As compliance with industry and government regulations is the key driver for adopting database auditing solutions, review the policies and reports the vendor provides with the product. These reports help you meet compliance mandates quickly, and reduce your costs in customization.

- **Deployment:** The single biggest complaint by customers for all of the solutions described is the pain of deployment. Installation, configuration, policy management, reducing false positives, customizing reports or management of the data are also issues. It is for this reason you will need to dedicate resources to evaluate tools in a head-to-head comparison. Further, deployment against one or two databases is insufficient: plan on performing some scalability tests across many databases to simulate real-world conditions. While this creates a burden for the proof-of-concept process, it pays for itself in the long term as UI issues, policy management and poor architectural choices by the vendors only become apparent in real world test cases.

- **Performance:** This has less to do with the vendor platforms, and more to do with tuning the data auditing options of the database itself. There are many variations and options, and the performance of native audit varies radically, so run some tests. You also need to balance what data you would like to collect with what you need, and look for ways to meet your requirements with the least number of policies possible as more policies means more overhead on all systems.

- **Integration:** You will need to verify that the vendors you review offer integration with workflow, trouble-ticketing, system and policy management products you have in house.

Audit logs contain a lot of useful information helpful to auditors, security professionals and DBAs alike, but they impact performance. Any conversation about the wonderful things that database auditing can provide needs to be tempered by understanding the added burden. Auditing incurs a performance penalty, and depending upon how you implement it, that penalty can be severe. But these issues can be mitigated, and for some business problems, database audit logs are essential to compliance and security analysis.

With the exception of native database auditing—which piggy-backs on top of the database resources—all the tools we have described deploy as a standalone appliance or software. All offer central policy and data administration, reporting, and provide data aggregation capabilities. SIEM, log management and database activity monitoring vendors...
provide a hierarchal deployment model for scalability, where multiple servers or installations are distributed across large IT organizations to help with processing and storage requirements.

Aggregating data helps ease management and reporting on the enormous volumes of data being collected. Further, information collection into a central server guards transaction logs from tampering.

Which approach is right for you comes down to your requirements, the business problems you need to solve, and (unfortunately) the time and money you can dedicate to the problem. The good news is there is a wealth of options available, from having your DBA turning on the native audit of your database to capture the basics, to products aggregating data across thousands of devices.

Adrian Lane is CTO of consultancy Securosis. Send your comments on this article to feedback@infosecuritymag.com.
what drives your approach to IT security?

Balancing business priorities and risks is key to a solid approach.

SystemExperts helps you build a comprehensive and cost-effective information security plan that makes sense for your company. Right now, our ISO 17799/27002 Compliance Program helps you to focus resources on your most important business risks and comply with regulations such as Sarbanes-Oxley, FFIEC, HIPAA, PCI, and Gramm-Leach-Bliley. Best of all, our approach works equally well for “Main Street” businesses and the Fortune 500 clients we’ve proudly served for years.

If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at www.systemexperts.com/public.

• ISO 17799/27002 Compliance
• HIPAA and PCI DSS Compliance
• Application Vulnerability Testing
• Security Audits and Assessments
• Security Architecture and Design
• Identity Management
• Penetration Testing
• Security Best Practices and Policy
• Emergency Incident Response
• System Hardening
• Technology Strategy
• ASP Assessments
AT THE BEGINNING of the 21st century, information security was in a deplorable state. Research published in 2001 by the Honeynet Project demonstrated that the life expectancy of default computer builds was measured in hours, if not minutes. Computers had little if any security. By default, most had multiple services turned on, no firewall installed, and patching was haphazard at best. All of these forces combined to create a golden age of hacking. This was a time when you could remotely scan and hack into literally millions of computers without the need for interaction by the end user.

Since then, vendors (led by Microsoft) have worked to build security into computers by deploying firewalls enabled by default, minimizing services, using advanced memory protection, standardized patching processes and other features. As a result, computers are far more secure.
The question is, if we have made such dramatic improvements with security technology, why do we still have a security problem? The answer is simple: the human. Consider a default installation of the latest Windows operating system, Windows 7. Place that default installation on the Internet. Due to all the latest advances in security, that computer on its own may never be hacked because, by default, the firewall is on, it is running few if any services, and it is using a variety of new and enhanced memory protection mechanisms. In addition, Microsoft has invested tremendously in a robust Security Development Life Cycle (SDLC).

Now add the human element. Once people start interacting with a computer, its risk exposure is exponentially increased. Humans read email, click on links, download files and open file attachments. People, not technology, are the weakest link—and attackers know it. In one statistic, Symantec reports that more than 90 percent of today’s malware now requires some type of human interaction for infection to occur. In Mandiant’s 2010 Advanced Persistent Threat report, the primary vulnerability exploited in all successful APT attacks was the human.

What is so surprising is how few resources organizations invest in securing them. Organizations forget that employees, just like computers, store, process and transfer information. You can install all the firewalls, antivirus and intrusion detection systems you want; at some point there will be little return on investment. Attackers simply bypass these defenses by attacking poorly trained employees. The good news is that because so little has been done in securing employees that even the most basic investments can have a large return.

**WHY HUMANS ARE BAD AT JUDGING RISK**

Before we discuss possible solutions, we need to better understand the problem. Why are humans such an easy target? What makes us want to click every link we see in email or make us believe we won the lottery (even though we never entered it)?

It turns out people are bad at judging risk. People grossly overestimate risks that are either highly visual or catastrophic (for example being eaten by a lion), and underestimate risks that happen slowly or not easily seen (for example, heart disease). We also tend to overestimate risks when we are not in control (flying in an airplane) and underestimate risks when we are in control (driving a car).

For example, let’s consider risks when swimming at the beach. A common fear is being attacked by a shark. Statistically speaking, the *Book of Odds* says the odds of being killed by a shark in the United States are 1 in 255,000,000, which means this risk is grossly overestimated. However, something that is twice as likely to kill you at the beach is vending machines. Yes, you read that correctly, vending machines.

Your odds of being killed by a vending machine are 1 in 112,000,000, according to the *Books of Odds*. When people purchase an item at a vending machine, sometimes there is a failure and the food is not dispensed. Some people will proceed to rock the machine hoping it will dispense the food, only to kill themselves when the machine falls on them. People
In most cases, people never know their system is hacked; cybercriminals can easily control a system without people noticing. In most cases, people never know their system is hacked; cybercriminals can easily control a system without people noticing. Nothing visual or catastrophic happens, so once again people often downplay or underestimate the risks. Finally, unlike the physical world, in cyber space you cannot see with whom you are communicating. As a result it has become very simple for attackers to pretend to be individuals or organizations people trust.

One common method is to send emails pretending to have links to online videos, such as YouTube or video sharing sites. After following the links, users are first asked to install a codec, a plugin or driver sometimes needed to view specific video formats. Both the email and the link are actually a lie; victims are not taken to legitimate video sites. Instead, these websites are most likely compromised and under the control of attackers. The codec is not legitimate; instead it is malware designed to infect and take over the victim’s system. The victim believes both the email and website because they look legitimate (attackers simply copy legitimate video-sharing websites). The victims believe there is no great risk because they are in control, and if attacked, it is usually invisible to them. Attacks such as these happen millions of times today. Why attempt sophisticated, time-consuming attacks when you can just send out emails and employees infect the computers for you?

HOW TO CREATE A SUCCESSFUL SECURITY AWARENESS PROGRAM

Now that we have a better understanding of why the human is such a risk, we need to better understand how to address those risks.

Our goal is to change people’s understanding of these risks, and ultimately change their behaviors. Unfortunately this is not simple. Unlike technology, you do not simply install a new application or add a patch. Changing behavior is a long-term effort.

An excellent non-security example was the U.S. Federal government’s effort known as “Click-It or Ticket” where over a period of six years, states were able to increase seat belt usage more than 20 percent. This change in behavior was accomplished through a combination of awareness training and enforcement.

One of the primary ways organizations attempt to change employee behavior is through security awareness programs. This is a long-term effort to train and educate employees about cyber risks and what they can do about them. Most organizations have no such program, and the few that do fail for a variety of reasons. Let’s cover how to
create a successful awareness program and some of the most common mistakes to avoid.

The first step is determining why you want the awareness program—what is your goal? The two most common are compliance and security. Compliance requirements from standards or regulations such as PCI DSS or ISO 27001 state that an awareness program is required. The problem with making compliance your motivation is that often the minimum standard becomes your only goal; you invest the absolute minimum to comply.

Awareness programs such as these are often nothing more then a series of PowerPoint-generated videos loaded into an online learning management system. Employees endure an hour of online boredom as they are repeatedly told what they can and cannot do for the good of the company. If you want to reduce insecure behaviors and improve the security of your organization, go beyond just compliance.

The key to having an awareness program that creates a more secure environment is answering three questions: Who? What? And How?

• Answering “Who” determines the target of your awareness program.
• “What” determines the content of what you want to teach people.
• And “How” is the means by which you communicate content. This is often the most challenging aspect.

Always start with “Who” because that answer determines the “What” and “How.” An organizational awareness program is often designed for full-time employees, but you cannot forget part-timers such as contractors and third-party vendors. It is often these non-employee resources that have employee-like access that can be the greatest risk. Also, there are other roles you may want to target, such as management, IT staff or even your customers. Each of these targets has unique needs; make a conscious decision of whom you are targeting, and if you are targeting multiple roles you may end having multiple versions of your awareness program.

By focusing on fewer topics, not only is there less for your employees to remember (and thus less likely to forget), but it is simpler for you to reinforce those key topics.

Once you have determined “Who,” the next step is determining “What” the content will be. Most organizations have very limited time and resources to communicate key awareness issues. At best you have 30 to 60 minutes for an employee at any one time. In addition, the human mind can only remember so many topics. This means you want to limit how much you focus on. By focusing on fewer topics, not only is there less for your employees to remember (and thus less likely to forget), but it is simpler for you to reinforce those key topics. This is where compliance can become an issue. Often awareness programs that focus on just compliance simply take their entire information security and acceptable use policies and post them in nauseating details. Don’t make this mistake! Have your security team go through the risks in your environment and identify what you feel are the greatest, and prioritize those. By focusing on no more then 10 to 12 topics, you will have a far more effective awareness program.

Next, determine how you will communicate. This is where most awareness programs fail. You have to stop thinking as a security team and start thinking as a marketing team.
One method I have found works best is focus on how the employee benefits. Nothing is more boring to employees than having to sit through hours of training, and being told what they can and cannot do for the benefit of the company. The key to success is not to focus on the organization, but to focus on how employees benefit. About 70 percent to 80 percent of any security awareness program not only applies to the organization, but applies to an employee’s personal life. Most of the same technologies, such as email, instant messaging, mobile phones and laptops, are used in both environments. When teaching these lessons, explain to employees how this information will help protect them at home, in their personal lives and their families. By understanding how they benefit, they are more motivated to learn and the program can more effectively change behaviors.

In addition, many awareness programs are outdated using traditional learning methods. What may have worked for employees 30 years ago no longer works for the YouTube generation. People now communicate in short sound bites. One of the most effective methods we have found is short videos, online communication that grabs people’s attention, videos they want to watch and learn. Then combine these methods with more traditional methods, such as onsite workshops, monthly newsletters, posters and perhaps even screensavers, to reinforce your message.

People are the weakest link in the security chain, yet security professionals continue to pour time and resources into technology that most attackers bypass with a single email, instant message or post on a social networking site. By investing some time and resources into an active awareness program, your organization can make a big difference in securing the human.

Lance Spitzner, director of SANS Securing The Human Program, is internationally recognized as a leader in the field of cyber threat research, training and awareness. He invented the concept of honeynets, is the author of the book Honeypots: Tracking Hackers and co-author of Know Your Enemy: 2nd Edition. Send comments on this article to feedback@infosecuritymag.com.
WE’LL GET YOUR IT systems TO TALK...

Are your network devices holding your logs HOSTAGE? What you don’t know CAN hurt you.

Optics for Security Information Management is an affordable automated log management service that centralizes, analyzes and retains log data and helps you use it to support business functions. Scalable to 100% of your log data, so you can rest easy, GlassHouse has got you covered.

FOR MORE INFORMATION CONTACT: SECURITY@GLASSHOUSE.COM

WWW.GLASSHOUSE.COM