

INFORMATION **SECURITY**

JUNE 2010

Laptop Lockdown

Secure the riskiest
endpoints for data
loss with affordable,
useful encryption
options

SOPHOS

- ☒ Malware Protection
- ☒ Data Protection
- ☒ Business Productivity
- ☒ IT Efficiency
- ☒ Compliance
- ☐ Hospital food



SECURITY SO SIMPLE YOU FEEL
INVINCIBLE

WORRY LESS. ACCOMPLISH MORE. WWW.SOPHOS.COM

SOPHOS
simply secure

FEATURES

22 Laptop Lockdown

ENDPOINT ENCRYPTION Laptops are the riskiest endpoints for data loss, but there are plenty of affordable, useful encryption options for your organization. **BY DAVE SHACKLEFORD**

29 Let There Be Light

CLOUD SECURITY Cloud computing alters enterprise risk. Here's what you need to know in order to safely navigate the cloud. **BY MARCIA SAVAGE**

38 In Harmony

COMPLIANCE GRC aims to bring together disparate compliance efforts, but the concept has been stymied by a lack of clarity. Developing a GRC program requires three key steps.

BY DAVID SCHNEIER

18 FACE-OFF**Should Your Company Hire a Hacker?**

Marcus Ranum and Bruce Schneier go head-to-head on the risks of hiring someone convicted of committing a computer crime.

BY MARCUS RANUM & BRUCE SCHNEIER



ALSO

5 EDITOR'S DESK**Let's End the Days of Compliance-Driven Security**

If you're spending more to protect custodial data because of compliance than you are to protect company secrets, you're missing the big picture. **BY MICHAEL S. MIMOSO**

10 PERSPECTIVES**Why You Need to Work with Law Enforcement Post-Breach**

Organizations that stay silent after a data security breach end up paying a higher price and helping cybercriminals.

BY KIM GETGEN AND KIMBERLY KIEFER PERETTI

14 SCAN**PGP, Guardian Edge Acquisitions Cement Encryption-as-a-Feature**

Symantec's late-April spending spree on encryption vendors PGP and Guardian Edge further ensures that encryption is less and less of a standalone security tool.

BY ROBERT WESTERVELT

16 SNAPSHOT**Six-Year Spending Spree****45 Advertising Index**

Find the cybercriminal.

(Never mind. ArcSight Logger already did.)



Just downloaded the customer
database onto a thumb drive.

Stop cybercriminals, enforce compliance and protect
your company's data with ArcSight Logger.

ArcSight 

Learn more at www.arcsight.com/logger.



Let's End the Days of Compliance-Driven Security

If you're spending more to protect custodial data because of compliance than you are to protect company secrets, you're missing the big picture. BY MICHAEL S. MIMOSO

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

DO YOU KNOW what your company's data is worth? I'd like to think you do, otherwise, how can you appropriately allocate security resources to keep that data safe?

Chances are, however, you don't know. Otherwise, you wouldn't be spending as much on compliance as you are.

Compliance-driven security is being forced upon most of you, and it's an approach that's totally contrary to what you should be doing. If data is indeed king, why aren't you following a data-centric approach to security?

A recent RSA/Microsoft/Forrester Research report called "[The Value of Corporate Secrets](#)" tried its best to put a value on the data your company either produces—in the form of intellectual property or trade secrets—or collects from customers and partners. Their conclusion: Regulatory pressures force companies to spend close to half of their security budgets on compliance-driven security projects. The problem is that the report estimates that proprietary secrets are twice as valuable as custodial data.

From the report: "Secrets comprise 62% of the overall information portfolio's total value while compliance related custodial data comprises just 38%, a much smaller proportion. This strongly suggests that investments are outweighed toward compliance."

Now chances are, Forrester's valuations of data aren't totally accurate, but I think their point is well made and for the most part on course. Most custodial data losses are accidental; a backup tape falls off a truck, a spreadsheet is emailed somewhere it shouldn't have been, someone loses a USB stick, or leaves their smartphone in a cab. Even theft of credit card numbers and other personally identifiable information that could lead to identity theft, which are costly to companies in terms of breach notification mandates, aren't as damaging as the theft of pharmaceutical formulas or engineering blueprints would be. These represent a competitive advantage. Imagine the competition getting hold of financial forecasts, competitive analysis, proprietary research, source code, or other strategic documents; the long-term damage is unimaginable to the financial viability of your enterprise.

If data is indeed king, why aren't you following a data-centric approach to security?

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

Yet, because of compliance, you're spending tens of thousands on security technologies that will satisfy a PCI QSA, or a Sarbanes auditor.

Hopefully that tide will change soon. The [Chinese attacks against Google](#) and other large technology companies, manufacturers and government contractors were different for one important reason: they were made public. The vast majority of such targeted attacks against companies or government agencies heavy in trade secrets and intellectual property are never reported. Google, however, changed that. Granted its agenda is more political than humanitarian, nonetheless, the effect is the same. Security's perception and awareness of targeted attacks against company secrets has changed and is out in the open.

Again, from the report: "Targeted zero-day attacks are routine, particularly against government agencies and in the aerospace and defense sectors. What is new is that we are now seeing headlines about it. [Google's] admission that it lost some of its secrets in the recent attack shows that securing trade secrets deserves just as much attention as [attacks on custodial data]."

Security management is quick to repeat the pablum that compliance does not equal security. Yet in the end this is nothing but lip service. Getting a certificate from the PCI Security Standards Council that you are in compliance with PCI DSS does not mean you're invulnerable to attack and data loss. Yet companies continue to invest in security only because of compliance, and in most cases, it's the best driver security management has with executives for budget requests. This paradigm has to change.

Trade secrets, intellectual property and military intelligence are much more valuable to a company's financials or to national security than credit card numbers and customer information. Organized criminals and enemy nation states are conducting espionage in order to steal that information.

You as a profession talk about prioritizing risks and spending accordingly. It's time to walk the walk, and not just talk the talk. Invest in protecting the data you value most. •

Michael S. Mimoso is Editorial Director of the Security Media Group at TechTarget. Send comments on this column to feedback@infosecuritymag.com.

Everything
you want
in an AV
solution.



Internet Security

NEW
Remote Administrator 4
features:

- Intelligent group manager
- Firewall rules merge wizard
- Improved policy manager
- Simplified remote administration
- Cross-platform management



Protection, speed and flexibility.

ESET NOD32 Antivirus 4 + Remote Administrator

ESET NOD32® Antivirus 4 Business Edition is more than simply powerful Internet security. It's a comprehensive network-wide solution. And, when paired with ESET Remote Administrator, it takes the headaches out of IT management. Light on client resource consumption and easy to manage, ESET NOD32 + Remote Administrator (RA) saves money that might otherwise be wasted upgrading computers running sluggish AV. And because it's so easy to manage, your IT department gets back what it values most — hours in the day.

Proactive protection

We scan all incoming and outbound network traffic, email attachments and removable media — but that's not enough. We compare unknown code to millions of database signatures — but that's not enough either. We even have frequent ultra-small updates that incorporate signatures from threats encountered across ESET's 100-million user network — but you still need more.

Superior protection doesn't depend on updates at all. In comparative testing using outdated signatures, ESET consistently outperforms other AV solutions. "ESET offers the highest proactive threat detection," independent AV-Comparatives May 2009.

The difference? Advanced heuristics. Proactive protection that doesn't just passively look for existing features of malware — it actively predicts strains that haven't been written yet and sandboxes them in a controlled disk environment where they can do no harm. And when a block of code seems suspicious — it is immediately repaired or quarantined. Smoothly. Efficiently. Seamlessly.

Unmatched speed

On the user end, ESET runs just two processes — the scanning kernel and the user interface — and together sip just about 44 MB of RAM. Typically, that's less than an instance of Word, Communicator, Excel, Explorer or Firefox. And with minimal interruptions or pop-ups and no scanning slowdown at file open or startup, your users won't even notice its running. But they will notice they no longer need to phone IT for lagging startups or malware infections.

On the server side, mirrored downloads and small signature updates mean your network traffic will never lag because of your antivirus solution. Mail scanning happens in the blink of an eye and compatibility with a variety of protocols and systems, from Cisco NAC to Microsoft Exchange means that you'll never have to deal with multiple antivirus solutions for your mixed network.

Flexible management

For mixed networks, ESET NOD32 delivers comprehensive protection — working natively in Windows XP, Vista and 7; Linux / BSD / Solaris; Mail Server; Exchange; and soon Linux Desktop and Apple Mac OS X.

Vast multiplatform protection doesn't have to be a management nightmare. ESET Remote Administrator allows for simple push-installation of preconfigured NOD32 packages to client computers and now with RA4 — allows Active Directory management of dynamic networks.

The combination of ESET NOD32 + Remote Administrator means simple, powerful management of a network of 10 computers or 10,000 with protection for every system and every platform. Each computer is an attack surface — and you need the best available protection on all of them.

Solutions to fit all
your business needs

- File server security
- Mail server security
- Gateway server security
- Mobile phone security

www.eset.com/business/products

Request your free trial at www.eset.com/business-trial

VIEWPOINT

Readers respond to our commentary and articles. We welcome your comments at feedback@infosecuritymag.com.

The Cost of Doing the Right Thing

I know exactly what [former Pennsylvania CISO Bob Maley, April 2010 issue “[Information Security Profession Takes Two Steps Backward](#)”]

went through—except for the firing. I currently work as a contractor for the US Army as an information assurance security officer. The only thing that got me through and successfully seven years later is that, eventually, everyone leaves the organization for another assignment, and I’m able to train their replacements on computer security from the beginning. But by doing the right thing to protect the government’s network, or anyone’s network for that matter, I got a lot of people angry. People do not like change.

Before Bob Maley, I’m sure life for the state

computer users was easy: everyone was an administrator on their system; no one used passwords or any worth mentioning; all sites were accessible; and any hardware or software was acceptable and used on the network.

When he arrived, he brought rules, structure, policies, and most of all, change—I’m sure, a lot of it. He made them think about computer security. He probably made them sign documents, closed systems, blocked sites, disconnected things and made them users rather than admins on government-owned systems. To me, the company just needed a reason to get rid of

him. He brought policies and changes as the new security officer, and the organization brought him down for not following their policy.

—BRIAN, Fort Hood, Texas

“When [Bob Maley] arrived, he brought rules, structure, policies, and most of all, change—I’m sure, a lot of it. He made them think about computer security.”

—BRIAN, Fort Hood, Texas

COMING IN JULY/AUGUST

SECURITY SAAS

Organizations are finding security threats harder and more expensive to manage. SMBs in particular have a hard time maintaining adequate security. This article will look at the different security software as a service (SaaS) options, and how SaaS can help companies address security threats more efficiently by reducing in-house management burdens, while weighing costs,

support needs and data governance.

UNDERSTANDING APT

Since the attacks on Google, Adobe and other enterprises in a variety of industries, the notion of the advanced persistent threat has been tossed about and abused by vendors and marketers, leaving security pros scratching their heads as to how to address APT. This article will present a clear

and historically accurate explanation of APT, dispel some myths around it and explain what you can do from technical and managerial points of view.

CAREER RESET

Information security is becoming more ingrained in corporate culture. As the profession matures, information security leaders are going to have to develop a more comprehensive skill

matrix that will enable them to effectively lead their organizations as they engrain information security into the fabric of their company’s corporate culture. This article will explain the skills you’ll need in order to command the necessary organizational respect to implement and integrate these programs.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

SECURITY IS ALL WE DO

30,000 Malware Specimens Daily

10 Billion Events Every Day

2,800 Clients in 50 Countries

10% of The Fortune 500®

NOT SURPRISINGLY, THE MOST POWERFUL WEAPON IN INFORMATION SECURITY IS INFORMATION.

At SecureWorks, we turn raw security data into actionable security information. With the massive volume of relevant incidents we collect and analyse every day, we are able to better understand the threat landscape across the globe. We use that information to identify threats sooner and better protect our clients. Of our largest competitors offering security services, we're the only ones focused exclusively on security. Discover what makes us different, and learn how our information can help keep yours safer.

See what the leading analysts say at secureworks.com/focus



Contact SecureWorks at UKenquiry@secureworks.com or call +44 (0)131 718 0600.



Why You Need to Work with Law Enforcement Post-Breach

BY KIM GETGEN AND KIMBERLY KIEFER PERETTI

Organizations that stay silent after a data security breach end up paying a higher price and helping cybercriminals.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

CYBERCRIMINALS HAVE UPPED the ante against organizations by relentlessly targeting them in more ruthless ways. The amount of data corporations are losing is increasing. The costs to repair the damages are skyrocketing and the confidence we once had in the ecommerce infrastructure is fading. Cybercriminals have developed better “firepower” such as new malware designed to evade detection. They have taken the time to understand the vulnerabilities in your network. And, they have learned how to maximize their profit margins by breaking into multiple corporations at the same time, using the same malware and SQL injections they’ve proven can work again and again. They’ve built a very lucrative and repeatable business.

They can do this, in part, because of our unwillingness to work together and share information once we’ve been breached. When organizations are the victims of data breach crimes, they are more likely to stay silent than work with law enforcement. Instead of fighting the enemy, we end up fighting ourselves. In the long run, this ends up costing more and benefits cybercriminals who have valuable time to target more organizations.

As an information security professional, you’ve probably had a hard time convincing your CEO and legal team to understand why it’s in your company’s best interest to work with law enforcement post-breach. This sentiment often falls on deaf ears because corporate leaders foolishly think they can cover up breaches or somehow miraculously fix them before the public finds out. To help you persuade them of the importance of working with law enforcement immediately after a breach, consider the three points listed below. For the purposes of this discussion, we’re not talking about breaches where a couple of unencrypted backup tapes fall off the back of a truck (although the impact from this kind of incident can be equally bad). Here, we are specifically talking about breaches where you are the victim of the crime and we, as an industry, need to get better at reporting it.

Cybercriminals have developed better “firepower” such as new malware designed to evade detection. They have taken the time to understand the vulnerabilities in your network.

1. Reduced legal fees

It's becoming increasingly clear that you can't hide a significant data breach from law enforcement or the public; eventually they will find out. And the more roadblocks you put up trying to cover up the breach, the more subpoenas you will have to fight, which will only increase the amount of resources, time and legal fees spent—resources that could be put toward catching those responsible for the attack. In the credit card heists involving [TJX and Heartland Payment Systems hacker Albert Gonzalez](#), organizations that spent resources to conceal their identity were eventually forced to reveal who they were when the case reached the criminal courts. Trying to conceal the compromise likely ended up costing more in the end.

Instead of fighting to conceal your identity as long as you can, consider how to get in front of a data breach by viewing law enforcement as a partner instead of an enemy. It is a far better strategy to have your legal team prepped on how they can work with law enforcement while putting measures in place that are sensitive to the needs of your business as you cooperate. For example, you could identify any particularly sensitive information, such as network diagrams, and inquire whether this information could be redacted prior to disclosure or disclosed under a protective order. This way you are able to share critical information desperately needed by law enforcement authorities while still protecting your business. In data breach cases, law enforcement often understands that being sensitive to a victim's needs works better for both sides in the long run.

It's becoming increasingly clear that you can't hide a significant data breach from law enforcement or the public; eventually they will find out.

2. Lower forensic investigation costs

Because cybercrime gangs use the same tactics to target multiple companies, law enforcement may know more about how they got into your system than the forensic team you bring in. You can save time and resources right away by cooperating and obtain valuable intelligence for your forensic team so they will know where to begin looking or how to better adjust their technology solution. This information can help you strengthen your network or mitigate the problem faster.

3. It's the right thing to do

We all need to work together to fight organized cybercrime. The longer an organization stays silent, the more time and opportunities the cybercriminal has to use the same tactics to target another organization. Not cooperating only increases their profit margin, which they then re-invest to become better at attacking us.

Data breach victims not coming forward is akin to a neighborhood riddled with gang crime and no witnesses. We end up watching helplessly as the community continues to be terrorized. As we watch these hacking rings get into multiple systems, many feel the

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

effect when one victim decides not to cooperate. By not cooperating, you hurt the greater community.

Criminals like Gonzalez may have never been convicted without the leadership from many of the victims who were willing to step forward and work with law enforcement in an unprecedented way. Reporting cybercrime and cooperating is the responsible thing to do and a giant step in the direction of fighting online financial crime. »

Kim Getgen is principal at consulting firm Trust Catalyst. Kimberly Kiefer Peretti is former senior counsel with the U.S. Department of Justice Computer Crime and Intellectual Property Section, where she prosecuted the Albert Gonzalez-related cases. Send comments on this column to feedback@infosecuritymag.com.



75% of all cyber attacks occur through Web applications

Is your Website safe?

SECURE YOUR WEBSITE

Stay ahead of the Hacker curve: Use CenZic

Cenzic provides software and SaaS products to protect Websites against hacker attacks. Unlike network security and SSL solutions, Cenzic solutions help automate your web security process and test for security defects at the Web application level where over 75% of attacks occur.

Going beyond signature-based tools, we're like your 'hacker in a box' working to find more 'real' vulnerabilities that help keep you secure.

See how easy it can be –
Get a Free test drive today, visit:

www.cenzic.com/gethealthcheck
1-866-4-CENZIC



Analysis | ENCRYPTION

PGP, GuardianEdge Acquisitions Cement Encryption-as-a-Feature

Symantec's late-April spending spree on encryption vendors PGP and GuardianEdge further ensures that encryption is less and less of a standalone security tool.

BY ROBERT WESTERVELT

WHEN BAYLOR UNIVERSITY set out to evaluate whole disk encryption software in 2004, the technology was somewhat separate and isolated from other security tools. The school was deploying encryption on its staff laptops to protect sensitive student data in the wake of new data breach notification rules that were to take effect in Texas in 2005.

“[The acquisition] is an acknowledgement of where security is headed and the value of encryption as something that if you don’t have it in your portfolio, you’re going to be behind.”

—JON ALLEN, information security officer, Baylor University

integrating the technology as a feature in larger security suites. So when Symantec announced its intention to acquire PGP and GuardianEdge, arguably the most widely recognized encryption vendors in the market, Allen says he didn’t bat an eye.

“The biggest advantage with any commoditization of security products is going to be cost and then hopefully more unified management,” Allen says. “[The acquisition] is an acknowledgement of where security is headed and the value of encryption as something that if you don’t have it in your portfolio, you’re going to be behind.”

Symantec paid \$370 million for the two companies. Three weeks later, it laid out

Baylor chose PGP Universal Server, which edged out several other vendors for its centralized management console and ease of use, says Jon Allen, information security officer at the Waco, Texas-based university. With more than 1,300 devices now encrypted, PGP’s recovery system has been crucial in letting IT easily access and reset locked computers if a staff member forgets their passphrase.

Today however, Allen sees the technology in a different light. No matter if its whole disk encryption, email encryption or transaction encryption, security vendors are

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT
ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR
RESOURCES

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

\$1.28 billion for VeriSign's authentication business. The deal would integrate both platforms with Symantec's endpoint protection suite. GuardianEdge has already long been used in the Symantec suite under an OEM relationship and the PGP encryption technology is already part of Symantec's Data Loss Prevention products.

Baylor is a Symantec customer, putting the university even more strategically aligned with the security giant, Allen says. Security components that can be centrally managed could be a key benefit by the new relationship, he says.

"Any time you have a company that falls outside of the big five or so security companies out there, you know there's potential for this," Allen says. "I would hope that we would be able to see them leverage the best part of PGP in conjunction with the Symantec platform."

Michael Osterman, principal of Osterman Research, says encryption has been a growth market, fostered by increasingly stringent regulations from data breach notification laws, now in more than 40 states, and tougher Health Insurance Portability and Accountability Act (HIPAA) rules, to the Payment Card Industry Data Security Standard (PCI DSS).

"When people think of endpoint security of any kind they're going to be looking at encryption as a key component," Osterman says.

Integrated encryption features in DLP products could enable content inspection at the endpoint to include some form of manual or automated encryption if sensitive data is discovered leaving the company network, Osterman says. The technology is being similarly used in email gateways. But even more compelling are cloud-based encryption platforms, he says. Zix Corp. and Approver offer email encryption services and there's no reason why the technology couldn't be extended to other areas, he says.

"Further down the road, we'll see encryption out of the hands of end users and part of a policy management system that allows the IT administrators or senior business managers to say what should and shouldn't be encrypted," Osterman says.

Encryption has been making its way into larger endpoint security suites for several years, says Mike Rothman, analyst and president of Phoenix-based Securosis.

Symantec rival McAfee has been on a similar track with encryption. It acquired SafeBoot in 2007 and uses the encryption technology in its endpoint protection suite. Rothman says he expects Symantec to move in a similar direction as McAfee by creating a centralized management console in which all policies can be created and maintained across the product line. With the acquisition, Symantec also has an opportunity to inject encryption into its Veritas line of storage products.

"I don't treat encryption as a standalone thing," Rothman says. "There's database encryption, disk encryption, email encryption and encryption infrastructure and application-level encryption all generally built into other specific systems."

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

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

Six-Year Spending Spree

Symantec picked up right where it left off pre-recession with its same-day acquisitions in late April of encryption companies PGP and GuardianEdge. That marks 28 acquisitions since June 2004 for Big Yellow; the peak of that spending spree coming between 2006 and 2008 when more than half of those transactions were made.

—Information Security staff

INSIDE THE NUMBERS

\$13.5 billion Symantec's mega-acquisition of Veritas Software in July 2005 in theory turned Symantec into security and storage giant, but integration woes and a general lack of execution has always shadowed this deal.

\$1.28 billion VeriSign's authentication business is the second most-expensive score for Symantec of the decade, bringing important online authentication and trust capabilities to its product lineup.

NOT YOUR FATHER'S SYMANTEC

Remember when Symantec was primarily an antivirus vendor? Not so anymore. Since 2004, Symantec has diversified beyond security (see chart, right).

2005	Veritas	Storage
2006	BindView	Network management
2006	Relicore	Systems management
2007	Altiris Systems	Management
2008	Transparent Logic	Workflow optimization software
2008	AppStream	Application streaming
2008	nSuite	Desktop Virtualization

ONE DAY, \$370 MILLION

On April 29, Symantec dove head-first into the encryption market with its acquisitions of PGP and GuardianEdge, paying \$300M for PGP and \$70M for GuardianEdge. Symantec, however, trails its security rivals McAfee and Sophos in the encryption game. McAfee acquired SafeBoot in 2007 and Sophos picked up Utimaco in 2008.

OVER-
HEARD

Up until a year ago, Symantec was a place where good software went to die. Symantec has aggressively turned that around but they're still fighting years and years of badly managed, badly integrated acquisitions.

—NICK SELBY, managing director, Trident Risk Management

GOOD FORTUNE

Can Be Yours



BREAK INTO IT.

Register for an ISACA certification exam.

Exam Date: 11 December 2010

Registration Deadline: 6 October 2010



www.isaca.org/infosecmag

Introducing ISACA's newest certification:



Grandfathering is now open.





Should your company hire a hacker?

POINT *by* **BRUCE SCHNEIER**

ANY ESSAY ON hiring hackers quickly gets bogged down in definitions. What is a hacker, and how is he different from a cracker? I have my own definitions, but I'd rather define the issue more specifically: Would you hire someone convicted of a computer crime to fill a position of trust in your computer network? Or, more generally, would you hire someone convicted of a crime for a job related to that crime?

The answer, of course, is "it depends." It depends on the specifics of the crime. It depends on the ethics involved. It depends on the recidivism rate of the type of criminal. It depends a whole lot on the individual.

Would you hire a convicted pedophile to work at a day care center? Would you hire Bernie Madoff to manage your investment fund? The answer is almost certainly no to those two—but you might hire a convicted bank robber to consult on bank security. You might hire someone

who was convicted of false advertising to write ad copy for your next marketing campaign. And you might hire someone who ran a chop shop to fix your car. It depends on the person and the crime.

It can get even murkier. Would you hire a CIA-trained assassin to be a bodyguard? Would you put a general who led a successful attack in charge of defense? What if they were both convicted of crimes in whatever country they were operating in? There are different legal and ethical issues, to be sure, but in both cases the people learned a certain set of skills regarding offense that could be transferable to defense.

Which brings us back to computers. Hacking is primarily a mindset: a way of thinking about security. Its primary focus is in attacking systems, but it's invaluable to the defense of those systems as well. Because computer systems are so complex, defending them often requires people who can think like attackers.

Admittedly, there's a difference between thinking like an attacker and acting like a criminal, and between researching vulnerabilities in fielded systems and exploiting those vulnerabilities for personal gain. But there is a huge variability in computer crime convictions, and—at least in the early days—many hacking convictions were unjust and unfair. And there's also a difference between someone's behavior as a teenager and his behavior later in life. Additionally, there might very well be a difference between someone's behavior before and after a hacking conviction. It all depends on the person.

An employer's goal should be to hire moral and ethical people with the skill set required to

"Because computer systems are so complex, defending them often requires people who can think like attackers."

—BRUCE SCHNEIER

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

do the job. And while a hacking conviction is certainly a mark against a person, it isn't always grounds for complete non-consideration.

"We don't hire hackers" and "we don't hire felons" are coarse generalizations, in the same way that "we only hire people with this or that security certification" is. They work—you're less likely to hire the wrong person if you follow them—but they're both coarse and flawed. Just as all potential employees with certifications aren't automatically good hires, all potential employees with hacking convictions aren't automatically bad hires. Sure, it's easier to hire people based on things you can learn from checkboxes, but you won't get the best employees that way. It's far better to look at the individual, and put those check boxes into context. But we don't always have time to do that.

Last winter, a Minneapolis attorney who works to get felons a fair shake after they served their time told of a sign he saw: "Snow shovelers wanted. Felons need not apply." It's not good for society if felons who have served their time can't even get jobs shoveling snow. •

*Bruce Schneier is chief security technology officer of BT Global Services and the author of *Schneier on Security*. For more information, visit his website at www.schneier.com.*

COUNTERPOINT *by* MARCUS RANUM

LIKE BRUCE, I'VE got to say "it depends"—but I definitely lean more toward "no" for a simple reason: it's harder to explain what happened if something goes wrong.

If the time comes to start second-guessing a decision, you're always going to be vulnerable to accusations of "You hired them, even though you knew they had a criminal record." Remember Arthur Andersen, the document shredding scandal, and how quickly they lost their customer-base? The reason a lot of companies dropped it like a hot potato was simply because their executive teams knew it was easier and faster to answer "We changed auditors" on a shareholder conference call than explain how and why they still maintained a comfort level with the firm.

A response that takes two seconds is better (in terms of time and effort) than one that might result in a general discussion consuming several minutes. It seems to me that a lot of decisions get made based on such simple, conservative, thinking, and it's hard for me to argue with; save your time and move on. I've argued in favor of this principle many times in security: It's easier to do nothing than it is to safely do something you know is dangerous.

The real trick comes when you're sure inaction carries its own dangers. In the case of hiring a hacker, it comes down to whether you believe the person in question has extraordinary skills and offers something crucial—an argument that is fairly difficult to make because the talent pool in information security and computer programming has become so large. I guess I must be one of those heartless capitalists who believe that, deep down, we're all pretty much interchangeable, albeit with a greater or lesser gain or loss in efficiency.

It's the question of "crucial skills" that really fascinates me. We hear a lot about "thinking like a hacker," but I think that's largely nonsense—it's really just a matter of "thinking like an engineer" and performing an in-line failure analysis along with your design analysis. Other than



TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

that, there's a lot of detailed knowledge that's application- and technology-specific; consequently, it has a fairly short lifespan as a value proposition.

Perhaps, somewhere out there, is the greatest VAX/VMS hacker ever, but I doubt he's very busy anymore—what we are interested in is not the encyclopedic knowledge of every flaw in a dead operating system, but rather the thought process by which he got there. And, to be completely honest with you, that process is nothing special. It's simply a matter of learning how people make mistakes over and over, and applying that understanding to new things as they come along.

Making mistakes over and over is also something I'd look closely for, if I were considering hiring an ex-hacker. I'd look for signs that he or she had learned something from the experience of getting caught (if he had been caught) and what, exactly, that was. With some criminals, "don't get caught" seems to be the primary lesson; if that was what I heard on a job interview I'd try to get that person out the door as quickly and gently as possible.

"After the first couple of times you get hunted down and arrested, it's not independence—it's refusal to get a clue."

—MARCUS RANUM

Ultimately, I suppose the question boils down to whether we're looking at a pattern of errors of judgment, or a single important life-lesson. Society wants to understand and forgive the lessons, while looking askance at the people who appear to be incapable of learning from experience. That's why I have always been a little surprised at the popularity of some ex-hackers who are still riding on the coattails of their own sociopathy. Are they trying to convince us that stubbornness is a virtue? After the first couple of times you get hunted down and arrested, it's not independence—it's refusal to get a clue.

Would I trust a convicted felon to shovel snow? That's a more complicated question than it seems, because nobody's going to shovel snow with a shovel, anymore. So really, the question is whether I'd trust a convicted felon with an expensive snow-blower or an expensive pickup truck rigged for plowing. And the answer is "probably not"—especially if I were being expected to make a responsible decision for my business rather than risking my own personal gear.

The answer would be "certainly not" if the conviction was for vehicle theft, but I suppose I might risk it if all the prospective shoveler had done was forge a few Renaissance paintings. I'll note that the closest I've come to hiring hackers was contracting out some vulnerability analysis work to experts in that arena because we didn't have time to build the knowledge base in-house. Did I trust them? Of course, or I wouldn't have done it. But I did get grilled on the topic by my board of directors; and, fortunately, was able to explain a good idea rather than having to defend a mistake. •

Marcus Ranum is the CSO of Tenable Network Security and is a well-known security technology innovator, teacher and speaker. For more information, visit his website at www.ranum.com.

Teaching you security...one video at a time.

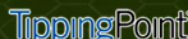
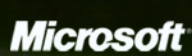
Traditional learning methods have always been about flooding students with as much information as possible within a given time frame -- often referred to as 'drinking from a firehose'.

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

the academy pro

Sponsored by:



www.theacademypro.com

The Academy Pro © Owned by Black Omega Media Group Incorporated

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT
ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR
RESOURCES

LAPTOP LOCKDOWN

Laptops are the riskiest endpoints for data loss, but there are plenty of affordable, useful encryption options for your organization. BY DAVE SHACKLEFORD

ACCORDING TO the nonprofit Identity Theft Resource Center, staggering numbers of sensitive data records were breached in 2009, continuing a trend occurring since 2005. Approximately [498 distinct breaches](#) took place with at least 222 million sensitive records lost or stolen. Roughly two-thirds of the breaches were explained, and of these, 27.5 percent were due to lost laptops and other incidents where data was “on the move,” or accidental exposure. Regardless of how the breach occurred, only six of the 498 had encryption or other security controls in place.

With vast numbers of records being lost or stolen, particularly from mobile systems, more organizations should be using endpoint security controls such as laptop encryption. In addition to the potential loss of customer confidence, litigation concerns, and general “bad press” that come with a public data breach, many organizations need to adhere to

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

multiple compliance and privacy mandates at state, federal and industry levels. Although few compliance requirements actually mandate the use of laptop encryption, it is definitely needed if laptops routinely carry sensitive payment card, healthcare, or financial data that fall under [PCI DSS](#), [HIPAA](#), [GLBA](#) and [Federal Financial Institutions Examination Council security guidelines](#). In addition, new state privacy laws such as Massachusetts' new data law, [201 CMR 17.00](#), specifically require the use of laptop encryption.

There are a number of specific types of laptop encryption available, both as free and commercial products. In addition to product capabilities and implementation types, there are numerous deployment considerations that organizations need to evaluate before rolling out laptop encryption. We'll address the major types of laptop encryption available today, ranging from pre-encrypted drives to full disk encryption software, as well as everything in-between. We'll also examine the critical issues of key management and policy management.

BEST LAPTOP ENCRYPTION SOFTWARE OPTIONS

Most laptop encryption software products today support strong encryption using trusted algorithms such as [Advanced Encryption Standard \(AES\)](#), with acceptable 256-bit key lengths. The major types of laptop encryption in use today include full disk encryption, file/folder encryption, volume encryption, and pre-encrypted drives. Several variations of these types are also growing in popularity, including partial drive encryption and centrally managed file/folder encryption (sometimes called distributed encryption). All encryption products will impose varying degrees of performance impact on endpoint systems—a factor that organizations must take into consideration before jumping into a laptop encryption project.

Full Disk Encryption (FDE): FDE software generally encrypts the entire hard drive on a laptop, preventing unauthorized access to the system overall. Although many FDE systems can encrypt bootable disk partitions, quite a few leave the Master Boot Record (MBR) unencrypted to ensure stability and performance. Some technologies, such as hardware-based options that leverage [Trusted Platform Module \(TPM\)](#) chips in the hardware, are capable of encrypting the MBR with significantly less impact to the overall system performance. FDE solutions offer the best protection for mobile systems such as laptops, because the system cannot be decrypted at all without knowledge or possession of a specific cryptographic key. Downsides include potential performance impacts (including significantly longer boot times) and a lack of granular policy definition for protection from specific users and groups accessing the system. In fact, a major criticism of FDE is the availability of all resources when an authorized user is logged in.

FDE can be problematic in other ways as well. Some products have been known to take quite a while to encrypt the entire hard drive, and if the process encounters any errors during the encryption, the hard drive may suffer irreversible damage. In addition, FDE can sometimes interfere with the normal operation of any existing software on the system that requires read/write operations to the hard drive, such as patching agents and antivirus products. Partial disk encryption deliberately avoids encrypting specific areas of drives that require frequent access from these products, seeking to alleviate the issues FDE may cause.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

File/Folder Encryption: File and folder encryption is most often used when organizations need to encrypt specific resources on systems, leveraging user, group, and role information to create policies for data protection. In many cases, this is most applicable to internal systems or servers with shared drives, but may be used on laptops when they are accessed by multiple parties, or simply for more granular policies that are more content-driven, including policies based on file types such as Microsoft Excel spreadsheets and specific keywords that are recognized by encryption agents or data loss prevention (DLP) products.

File and folder encryption is particularly useful for protecting sensitive data from systems administrators and other privileged users. For example, a CFO may want to encrypt financial spreadsheets to prevent all other users from accessing them, and only she would possess the requisite keys(s) needed to access the data without implementing data or key recovery procedures. However, depending on the product, file and folder encryption software agents may cause some noticeable impact on laptop performance.

File/folder encryption can also inadvertently lead to data exposure. If encryption policies are not defined or applied properly, lost or stolen laptops may have sensitive data that can be extracted by an attacker after cracking user credentials or simply duplicating the hard drive and extracting data. In most cases, policies are defined on a central management server by security and IT administrators. These are then pushed down to each system's encryption agent and applied. For systems that don't connect to the network often, these policies may be out of date or missing.

Volume Encryption: Volume encryption, also commonly referred to as "home directory encryption," is essentially a hybrid of FDE and file/folder encryption, where large data stores in specific directories or volumes on a specific system are encrypted for one or more users and/or groups. In general, this equates to a much more simplistic policy-based approach, where less focus is placed on file types, content, or other policy rule matching capabilities; the entire focus, instead, relates to which user or group is accessing a protected resource or volume/directory. This type of solution can be a good tradeoff in terms of system performance impact and management overhead when compared with file/folder encryption, while still offering more granularity than full disk solutions.

Pre-Encrypted Drives: Many laptop manufacturers are shipping systems with pre-encrypted drives. A number of hard drive manufacturers also are creating standalone encrypted laptop drives that can be purchased and added to preexisting systems. The major drawback to this approach is cost, because pre-encrypted drives can cost two times as much as traditional mobile system drives, although prices are quickly coming down. One other potential issue is enterprise-wide management, as these drives typically need some additional management and monitoring software employed in order to configure

File and folder encryption is most often used when organizations need to encrypt specific resources on systems, leveraging user, group, and role information to create policies for data protection.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

them and ensure encryption is in place remotely.

However, in addition to the benefits of full-disk encryption, this disk encryption technique provides several additional benefits. First, the drive architecture is built specifically to support encryption, and many vendors are following a standards-based approach espoused by the Trusted Computing Group (TCG) in its [Storage Architecture Core Specification](#). This results in enhanced performance in most cases, with reduced likelihood of hardware compatibility issues or drive errors related to encryption. A recent study by consulting and market intelligence firm Trusted Strategies suggests that read/write operations

COST

Affordable Laptop Encryption Options Abound

Free and open source products do the job, but there are limits around management and support.

OBTAINING COST IS a major consideration for any laptop encryption project. Pricing for commercial solutions vary widely, ranging from \$20 to \$60 per laptop, depending on the overall feature set selected.

There are also free, or open source options available. The most popular free solution is [TrueCrypt](#), which provides FDE and pre-boot authentication for Windows, Mac, and Linux platforms, but does not provide true policy-based file/folder encryption. It also lacks enterprise-wide management capabilities. Other popular free solutions include: FreeOTFE (Free On-The-Fly Encryption) for Windows and PocketPC systems; DiskCryptor for Windows; FileVault for Mac OS X; and a variety of Linux distribution packages. In general, free solutions are only applicable for smaller organizations that can manage each laptop's encryption individually, since management consoles with key recovery and other features aren't available.

Organizations running recent versions of Microsoft Windows (Vista and later) can take advantage of built-in [BitLocker Drive Encryption](#). With Windows 7, BitLocker is much simpler to manage via Active Directory, includes more robust and automated key backup and recovery capabilities, and can also be easily extended from laptops to USB drives and other portable media via policies. BitLocker encryption policies can be created and managed entirely through Group Policy settings, which may simplify management significantly for Windows administration teams. BitLocker is available in the Enterprise and Ultimate editions of Windows 7.

For some organizations, the best option might be a combination of encryption methods. For most laptops, FDE or pre-encrypted drives are likely the best and simplest approaches, because laptops will usually be protected from the majority of loss or theft scenarios. However, there may be laptops shared by multiple team members or situations that call for more direct and specific policies around files or content to be encrypted instead of the entire drive. In these cases, file/folder encryption could be installed instead of FDE.

Numerous commercial products today offer both types, and they're generally managed from the same central console. Free and built-in solutions usually don't offer this flexibility. •

—DAVE SHACKLEFORD

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

may actually be twice as fast on [pre-encrypted drives versus encryption software](#). Another advantage concerns the protection of encryption keys. Most software-based encryption products store encryption keys in system memory (dynamic RAM), and this potentially exposes the key to attackers using techniques like the [Cold Boot attack](#) discovered by Princeton University researchers in 2008. Pre-encrypted hard drives typically store the key on a Trusted Platform Module (TPM) chip, so it's never stored in memory.

LAPTOP ENCRYPTION DEPLOYMENT CONSIDERATIONS

There are numerous deployment considerations for a laptop encryption project. Organizations should take the following into account:

Platform support: Regardless of the type of encryption chosen, platform support is a factor in installation and provisioning if software is involved. More organizations are managing diverse laptop platforms and operating systems, and many products provide multiplatform support and are now capable of encrypting Windows, Linux and Mac laptops.

Installer size and deployment options: As many organizations will need to install the encryption software across remote links when laptops connect over VPN, or push out software to remote office locations, the size of the package is important to consider. Size of packages can range from several megabytes to more than 100 MB. The size of the package will vary depending on type of encryption (for example, FDE tends to be somewhat larger), additional security tools included with the agent, etc. Most FDE and file/folder encryption products have built-in deployment capabilities, but organizations using Microsoft's Systems Management Server (SMS) and other provisioning tools can often use those instead, as they tend to be more flexible and integrated into the environment. For large environments, scalability is key as well, where multiple packages can be deployed in groups, on a schedule, etc.

Overall transparency to users: The more transparent encryption solutions are to laptop users, the more successful the deployment will likely be. If encryption leads to significant system slowdown, numerous authentication prompts, or popups and other policy notifications from file/folder encryption agents, users will look for ways to disable or circumvent the encryption solution.

ENCRYPTION KEY MANAGEMENT PRIMARY SECURITY ISSUE

Once the software has been deployed, management becomes the primary issue for security and IT teams. The following are important management considerations:

Key management and recovery: Encryption keys are generated upon deployment of software (or stored in hardware for pre-encrypted drives), and will need to be stored and managed for safekeeping as well as recovery of data in the event a user forgets or loses his/her password or other authentication mechanism used to gain access (smart cards or USB tokens with certificates, two-factor methods, etc.). In most cases, laptop encryption products will automatically store a local copy of the key for encrypting and decrypting, and this key will be accessed once a password or other credentials are entered. For recovery, a copy of this key may be stored in a central management repository, or a "master key" may be generated to allow administrators to access the system and data, and allow creation

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

of a new user or system key. Key storage is important too, because the key repository needs stringent protection. Products should encrypt the centralized keys or the database storing the keys.

Policy creation and management: Most FDE products are straightforward in terms of policy—encrypt the drive on a specific laptop, allowing access based on some authentication scheme (usually a password). For file/folder encryption products, however, policy tends to be much more granular. For example, policies can be created that permit or deny access to encrypted resources based on a user's identity or role, and this often ties back to identity repositories such as Active Directory and others. Most file/folder encryption can also generate policies based solely on file types, such as Microsoft Excel spreadsheets, or particular content in file names or inside the file itself. For example, all Excel spreadsheets may be encrypted by default with a policy that only allows access to the owner of the file and the user's accounting team. Some encryption products are going a step farther in this regard, working in conjunction with DLP systems and enabling encryption policies to integrate with the granular content analysis capabilities DLP policies provide.

Audit and reporting: Depending on compliance requirements or internal policies, the ability to easily report on the state of encryption for laptops that store sensitive data may be a critical management feature. Audit trails and logs are important for key changes and revocation as well as any significant changes to the encryption infrastructure.

With data breaches from lost or stolen laptops increasing every year, organizations need to ensure that endpoint security is in place, and laptop encryption is one of the most capable and simple ways to accomplish this. With most laptop encryption products providing widespread platform support and a variety of features, enterprises are focusing more on performance, ease of deployment, and management capabilities as priorities in selecting a solution, especially larger organizations with numerous laptops to protect. In addition, compliance and privacy regulations may require laptop encryption, so reporting and audit trails are becoming more important as well. As laptop encryption becomes more cost-effective and simple to manage, especially with solutions such as pre-encrypted drives, it's highly likely that adoption rates will increase. •

Dave Shackelford is director of risk, compliance and security assessments at Sword and Shield Enterprise Security and is a certified SANS instructor. 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

 **GLASSHOUSE**

LET THERE BE LIGHT

Cloud computing alters enterprise risk. Here's what you need to know in order to safely navigate the cloud.

BY TIM MATHER

AS CLOUD COMPUTING moves from marketing hype to reality—real customers with real utilization—it's increasingly important that information security practitioners understand the significant change in computing the cloud heralds and how that impacts enterprise risk. Cloud computing is evolving rapidly, and there is no shortage of vendors suddenly claiming to be “cloudy,” which can make it all the harder to discern the critical security ramifications of the cloud for the enterprise.

We'll shine a light on cloud computing and examine how the public cloud model alters the enterprise risk posture. We'll also look at how information security practitioners should prepare for moving into the cloud as well as emerging governance frameworks and other changes that must happen to make cloud computing more trustworthy.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

HOW THE CLOUD IMPACTS SECURITY

To begin, cloud computing is an evolution in computing, and does not introduce new technology. Instead, the cloud is about a different business and operating model—one based on shared resources. Those shared resources are the only way to gain the economies of scale that result in lower costs—one of the primary business drivers for cloud computing, along with agility. However, this change in business model also portends changes in information security that demand to be evaluated. Here are some of the security challenges that come with public cloud computing:

1. Trust boundaries are unclear. In traditional organizational IT, information security practitioners know where their trust boundaries are. Typically that means everything inside the “perimeter” (at least the concept of a perimeter) plus external facing systems and some third-party connections, depending upon an organization’s unique circumstances. With cloud computing, where those trust boundaries are vis-à-vis cloud service providers’ responsibilities is far less clear. What your direct security responsibility is versus a provider’s is probably not clearly defined in the provider’s service level agreement (SLA). Additionally, those changes in responsibility vary from provider to provider. And, on top of that, responsibilities depend on where you are in cloud computing’s service delivery model, SPI (software-as-a-service, platform-as-a-service, and infrastructure-as-a-service). That is, your responsibility versus a provider’s responsibility is different for SaaS than for IaaS. This confusion about trust boundaries is the primary reason that information security practitioners are concerned about the security of cloud computing, along with current cloud service providers’ general lack of transparency about their security.

2. All data separation is now logical. Formerly, organizations used to ensure that their data was physically separated from other organizations’ data. Of course, when data is stored internally in an organization’s own data centers that’s exactly what’s done—physical separation of data. Even when an organization uses a hosting service, it still separates its data physically. For example, while a hosting service provides a shared facility for multiple customers and there is usually some sharing of network resources, customers usually have dedicated (though rented or leased) servers on which to run their applications and store their data. The same is true with application service providers (ASPs). However, with public cloud computing *all* computing resources are shared.

3. Network exposure increases. While this network exposure itself is not new, the magnitude is greater in the cloud than has existed previously. Because users must now traverse the Internet to reach their applications and/or data, as opposed to possibly just an intranet, there is an increased risk that such access is subject to network threats that are usually prevented at the perimeter. For example, a [distributed denial of service \(DDoS\)](#) attack could be directed either against your organization’s Internet gateways or your cloud service provider, impeding access to cloud-based applications and/or data. Imagine if such an attack were launched during your organization’s end of month or end of quarter processing. Traffic interruption through redirection by means of a [Border Gateway Protocol \(BGP\)](#) attack is also possible with public cloud computing.

4. Application exposure increases. Applications that might have previously been safer because of their internal location are external and quite exposed when they are public cloud-based and Internet-facing. Many SaaS providers contend that their appli-

The Basics

Here's a quick overview of the essential elements of cloud computing.

BY NOW, security practitioners should at least have a good, basic understanding of cloud computing. If you've been too busy fighting tactical fires to have that level of understanding, you need to take time to get up to speed. A good place to start is the National Institute of Standards and Technology (NIST).

NIST defines cloud computing as composed of five essential characteristics, three service models, and four deployment models.

Among the five essential characteristics described by NIST, resource pooling is the most important and what sets cloud computing apart from earlier IT business models. Think "shared resources" or "multi-tenancy," as several providers refer to it. The most significant promise of cloud computing is lower costs, and those lower costs come only through economies of scale, and those economies of scale come only through use of shared resources. Unlike earlier IT business models, such as hosted services or ASPs (application service providers), all resources are shared in cloud computing.

Notice that virtualization is not a defining characteristic of cloud computing. Oftentimes, media sources equate virtualization with cloud computing. That is wrong. Virtualization is an enabling technology often used in cloud computing but virtualization does not equate to cloud computing. In fact, the largest cloud computing provider, Google, does not use system or machine virtualization (though it does use application and storage virtualization). It chooses instead to scale horizontally by adding more standardized servers.

In the technology sector, we love our acronyms as almost as much as the military does. But some acronyms are essential to understanding cloud computing. "SPI" refers to the three service delivery models in cloud computing: software-as-a-service, platform-as-a-service, and infrastructure-as-a-service. These three models effectively form a "cloud stack," with SaaS at the top and IaaS at the bottom (see graphic, below). These three different types of cloud services are deployed in four different models, as defined by NIST: private cloud, community cloud, public cloud and hybrid cloud.

From a security perspective, it's important to note that as an organization moves up the cloud stack, it loses operational flexibility and direct control over security. An IaaS customer has far greater control over its configurations, actions, and security than a SaaS customer does. For some users, that is a negative. However, for many organizations, the lack of comparative operational flexibility in SaaS is in fact a benefit. Many companies move to the cloud precisely because of that lack of operational flexibility; the cloud service provider is responsible for providing nearly everything, making it extremely easy for organizations to switch to this new business model. •

—TIM MATHER

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

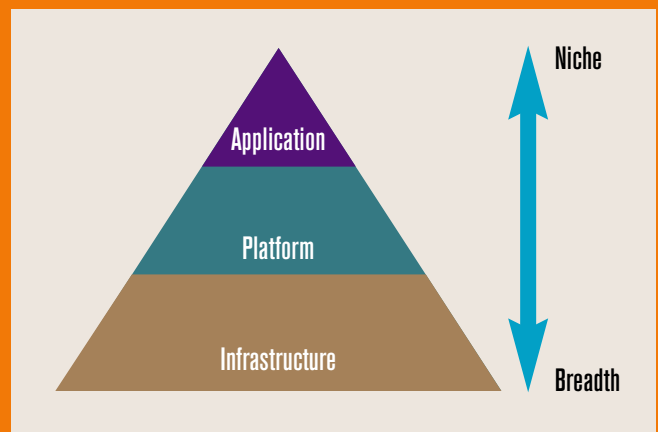
SPONSOR RESOURCES

DELIVERY MODELS

Cloud Stack

The pyramid illustrates the three cloud computing delivery models: software-as-a-service, platform-as-a-service, and infrastructure-as-a-service.

—TIM MATHER





Focused on finance?

Introducing SearchFinancialSecurity.com!

Now there's an online resource tailored specifically to the distinct challenges faced by security pros in the financial sector. *Information Security* magazine's sister site is the Web's most targeted information resource to feature FREE access to unbiased product reviews, webcasts, white papers, breaking industry news updated daily, targeted search engine powered by Google, and so much more.

Activate your FREE membership today and benefit from security-specific financial expertise focused on:

- Regulations and compliance
- Management strategies
- Business process security
- Security-financial technologies
- And more

www.SearchFinancialSecurity.com



SearchFinancialSecurity.com

The Web's best information resource for security pros in the financial sector.

TechTarget
Security Media

 SearchSecurity.com

INFORMATION
SECURITY

INFORMATION SECURITY DECISIONS

 SearchFinancialSecurity.com

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

cations are safe because of the reduced attack surface that these server-based applications have—a browser is used for access; no application-specific code or functionality is on the client—as well as the fact that some SaaS applications are exposed only through their application programming interfaces (APIs). Of course, that assumes that SaaS providers have actually taken steps to secure their applications and APIs, and have tested such. That also assumes that SaaS applications are used as stand-alone services, with no integration with other applications, which is a questionable assumption. The fact that many SaaS applications are actually built by third parties on other cloud services (either PaaS or IaaS) further calls into question the security of SaaS applications. Additionally, many SaaS APIs (including Amazon Web Services, Google, and Salesforce.com) use [REST \(REpresentational State Transfer\)](#), which has no predefined security methods.

5. The governance model changes. More specifically, the issue is that there is no established governance model currently for cloud computing. How exactly are information security professionals supposed to protect their organizational data in what should be considered an untrusted environment? Fortunately, there is now work underway to develop a governance model for cloud computing.

HOW TO PREPARE FOR THE CLOUD

Given the risks, the public cloud—at least for now—is not good for sensitive, regulated, and/or classified information. What it is good for is non-sensitive, non-regulated, and unclassified data—data that is probably already public and most of which is intended to be public. For the vast majority of organizations (except defense contractors, the military, and the intelligence community), such publicly releasable information probably makes up 90 percent of their data. Besides, for sensitive, regulated, and/or classified information, private clouds or cloud infrastructure shared by several organizations (community clouds) are still attractive options. For example, the Defense Information Systems Agency (DISA) operates a community cloud for the Department of Defense, [Rapid Access Computing Environment \(RACE\)](#), which is supposed to begin accepting classified information soon.

With that in mind, here are steps security practitioners should take when investigating the use of public cloud services:

1. Self assessment. The number one priority should not be to investigate the security afforded by cloud service providers. The top priority should be to examine your own data classification policies and how well those policies currently

are enforced. Before figuratively beating up a cloud service provider over their relative lack of security (compared to that implemented by most large enterprises), make sure that your own data house is in order. Do you have an up-to-date data classification policy? How well enforced is that policy? Do you have data stewards and custodians assigned for all data? What is the awareness level of your own organization's privacy policy, and how well is it enforced (assuming that your organization has one)?

The top priority should be to examine your own data classification policies and how well those policies currently are enforced.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

2. Data anonymizing. What tools and capabilities does your organization have for anonymizing data so that any elements that identify individuals are removed? If you do move to the cloud, expect that other business units will likely overwhelm information security with requests for help on anonymizing data so that it can be put into the cloud in compliance with your data classification policy.

3. Due diligence. When these data classification activities have been accomplished by your organization, then your due diligence of cloud service providers' security should begin. For example, what is the connectivity model to the public cloud for administration? What support is there for leveraging existing security monitoring and management tools, including vulnerability scanners, change management and firewall policy enforcement at network- and host-levels (e.g., through use of a virtual private cloud)? Some applications require database connectivity back into the organization and may violate existing policy. Also, your organization might have a requirement for strong authentication support; can the provider meet that requirement?

4. Endpoint security. While you are conducting such due diligence, essentially of your organization's new IT back-end capabilities, don't forget about your organization's IT front-end capabilities. How is the security of all those end-user devices that will be used to access the cloud and your data in it?

If you do move to the cloud, expect that other business units will likely overwhelm information security with requests for help on anonymizing data so that it can be put into the cloud in compliance with your data classification policy.

GOVERNANCE EFFORTS

While public clouds are good for public data (non-sensitive, non-regulated, and non-classified data), there are many organizations that would like to utilize public clouds for other data—provided their security is adequate. And today, public cloud security is not adequate for this sensitive information.

The biggest security problem with public cloud computing is a lack of transparency by cloud service providers about their security capabilities: Generally, they are reluctant to be audited and their service level agreements are worthless. Cloud service providers themselves have begun, privately at least, to admit to such shortcomings. They agree that it is in their best interests, as well as their customers, to have more transparency and to have some sort of standardized security framework to be measured against.

In fact, in the last couple of months, almost the opposite problem has arisen: There are now multiple organizations developing different security frameworks for cloud computing. Frameworks in development include:

- **A6 (Automated Audit, Assertion, Assessment, and Assurance API) Working Group:**

This effort, also known as CloudAudit, is led by well-known security expert Chris Hoff, director of cloud and virtualization solutions at Cisco Systems.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

- **Trusted Cloud Initiative:** Under development by the Cloud Security Alliance. According to Liam Lynch, chief security strategist for eBay and co-chairman of the initiative, the effort will build on the “pillars” of the alliance’s work and will include all vendors with products that enable an end-to-end security platform. The initiative also plans to provide reference implementations and will incorporate the A6 initiative.

- **Common Assurance Maturity Model (CAMP):** A 24-member consortium of mostly vendors, but also includes the European Network and Information Security Agency (ENISA). CAMP originally launched in February as Common Assurance Metric. According to Gerry O’Neill, CEO of the U.K.-based Institute of Information Security Professionals and a CAMP steering committee member, a formal release is planned for November.

- **Federal Risk and Authorization Management Program (FedRAMP):** Related to the other three projects, this is an effort intended to be a U.S. government-wide initiative that would provide joint authorizations and continuous security monitoring of shared IT services for federal departments and agencies that enter contracts with outside providers, including those offering cloud computing solutions. The [National Institute of Standards and Technology \(NIST\)](#) co-chairs this effort.

MORE SECURITY NEEDED

Besides greater transparency, there are other improvements that cloud computing needs in order for enterprises to rely on it for more than non-sensitive and unregulated data. From a technical perspective, the primary security improvement needed is better attribute management, for both identity and (cryptographic) key management. Better identity management is necessary in terms of expanded use of federated identity—both enterprise-centric, typically supported by standards such as [Security Assertion Mark-Up Language \(SAML\)](#), and consumer-centric, supported by standards like [OpenID](#). However, federated identity management still suffers from trust issues (i.e., acceptance of an assurance issued by another organization), as well as the management of credentials themselves.

Cryptographic key management also suffers from a lack of federation. [OASIS’ Key Management Interoperability Protocol \(KMIP\)](#) is an improvement that standardizes use of clients-to-servers protocols. While this effort is significant for private clouds within enterprises, it remains insufficient for public cloud computing. What is really needed for cryptographic key management, in addition to KMIP, is standardized use of servers-to-servers protocols and support by third parties (independent from cloud service providers) for key lifecycle management, including back-up and revocation. But the larger issue is why do we manage identities and cryptographic keys separately, especially when both have evolved similar management frameworks? Both identities and cryptographic keys are attributes, which should be managed in a common framework that also accommodates other attributes. Only such a framework will scale to a public cloud and inter-clouds, or cloud-to-cloud interaction.

We’ve only touched on the surface of the security concerns with cloud computing, especially with use of public clouds. However, before casting too much dispersion on cloud service providers about their security capabilities and offerings, take a step back and look at your own organizational readiness to use the cloud. And, let’s remember

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

that cloud computing is indeed immature at this time. The cloud is maturing, and there is no shortage of standards-type organizations and industry groups now trying to ensure that happens. But before impulsive calls for regulations, we need to give the market some time to find its own level.

There has been a huge amount of progress in this new business and service delivery model in the last two years, and we can expect that the associated security and privacy issues will make progress in the next two years. Will that development be sufficient to enable public clouds to host sensitive or regulated information in the next two years? Highly doubtful. Will that evolution be sufficient to allay concerns by organizations and consumers about how cloud service providers handle their data? Probably. The cloud is evolving rapidly and getting better—be patient and diligent. •

Tim Mather, a long-time information security practitioner, is co-author of Cloud Security and Privacy and a security consultant. Send comments on this article 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.



www.SearchSecurity.com

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.



www.SearchFinancialSecurity.com

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



www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.



www.SearchMidmarketSecurity.com

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



www.SearchSecurityChannel.com

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT
ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR
RESOURCES

IN HARMONY

GRC aims to bring together disparate compliance efforts in the enterprise, but the concept has been stymied by a lack of clarity. Developing a GRC program requires three key steps. **BY DAVID SCHNEIER**

DUE TO THE STUNNING increase in the amount of regulatory and industry requirements over the past decade, a methodology commonly referred to as governance, risk and compliance (GRC) emerged. The most basic definition of the GRC methodology is that it harmonizes efforts across previously detached disciplines that existed in their own silos within an organization.

Historically, compliance was a function of audit, risk management—if it was performed at all—was a function of management, and governance generally didn't exist as a discipline outside of Wall Street and the banking industry until [Sarbanes-Oxley \(SOX\)](#) made it a requirement for publicly traded companies. However, with the emergence of the [Payment Card Industry Data Security Standard](#), the maturation of SOX and the increased scrutiny being brought to bear by industry-specific regulations such as [Gramm-Leach Bliley \(GLBA\)](#) and the [Health Insurance Portability and Accountability Act \(HIPAA\)](#), it's become impossible for organizations to avoid addressing each of these disciplines. And the amount of effort required by an organization in order to fulfill its compliance obligations can be substantial.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

GRC aims to help streamline compliance efforts but the concept has become clouded as vendors tout automated GRC solutions and even compliance practitioners don't all agree on what it's supposed to be. Let's take a closer look at the GRC concept, the key steps for developing a [GRC program](#), and where the discipline is headed.

IDENTITY CRISIS

GRC began making its way into the business community in the early part of this decade. In 2003, the [Open Compliance and Ethics Group \(OCEG\)](#) began designing frameworks to rein in the myriad corporate activities required to achieve compliance. The nonprofit group is comprised largely of volunteers from a wide range of business domains who over the years have published several standards to provide a consistent approach for defining and managing a GRC program (see "*Nonprofit Provides GRC Guidance*," below). Not long after the group started their work, a suite of software products began to emerge that were hyped as complete, automated GRC solutions.

Today, type "GRC" or "governance risk compliance" in any popular search engine and the page fills with a wide range of software products from a variety of vendors. So is GRC a methodology or a software product? David Bachman, a partner with Quasar Associates, who advises clients in audit and risk, says, "I don't think of GRC as either a methodology or software driven solution. It is an overall way to look at governance, risk and compliance and can include methodologies developed in various areas (SOX compliance, [ITIL](#), HIPPA) and the associated software solutions

TOOLS

Nonprofit Provides GRC Guidance

Industry thought leaders produce documentation and other tools to help organizations implement GRC.

Organizations looking for guidance on building a GRC program can look to the [Open Compliance and Ethics Group \(OCEG\)](#). A nonprofit organization, the OCEG has taken a leadership position within the GRC domain by producing a series of standards and guidelines that provide clear direction on how to assess and develop the necessary controls to support GRC. The documentation is designed and vetted by a mostly volunteer group that reads like a "who's who" of GRC thought leaders from across the audit and compliance industry. The de facto standard for developing a GRC framework is the [Red Book 2.0 \(GRC Capability Model\)](#). Included within the document is an overview of GRC and its related disciplines and directions on building out either a complete or partial framework.

A second key document authored by the OCEG is the [Burgundy Book \(GRC Assessment Tools\)](#), which helps institutions evaluate the design and effectiveness of its GRC framework. The Burgundy Book includes an overview of the assessment process, criteria for success and a series of tools to assist in the process. Both of these documents can be obtained free-of-charge after establishing a user account with OCEG. In addition to documentation, the OCEG website offers related information and links to support the GRC community and help advance the adoption of GRC principles. •

—DAVID SCHNEIER

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

for those areas.” Even so, it’s difficult to determine at the onset of a GRC implementation where to begin. Do you need to have [GRC software](#) in place to guide the process? “The methodology drives the strategic end of GRC implementation; the software supports the strategy,” explains Scott E. Cohen, senior manager of IT advisory services at KPMG. “One should not select software until the strategy is developed and requirements obtained.”

To further complicate matters, even seasoned audit and compliance professionals don’t agree on exactly what it’s supposed to be. Carol Ward, a risk management consultant who works in the banking industry, describes GRC as “simply being the natural framework that leaders should use to organize their oversight of risk management in their organization.” However, she’s found that much of the content available to educate practitioners has blurred the lines, adding that recent blogs on the topic have “gone off into confusing intellectual discourse.”

Some practitioners struggle to define the disciplines and how they relate to one another. For example, many view GRC as synonymous with enterprise risk management (ERM). “They are one in the same. If you are implementing an ERM solution you must have all of the elements of GRC included,” Bachman says. But at a fundamental level, GRC is intended to include all of the related disciplines represented in its name, Cohen says: “I view GRC as the convergence between all the disciplines.”

DEVELOPING A GRC PROGRAM

A fundamental truth about developing a GRC program, or framework, is that much of what needs to be built into it is very likely already present in an organization.

After a decade of GLBA, seven years of SOX, five years of PCI and a lifetime of audit, a wide range of related activities need to be integrated into your GRC program. Unfortunately, they are likely isolated by discipline (e.g. audit, project management, legal, etc.) and unique to the business silo they are used to support. This often results in multiple teams with related frameworks in the same functional areas. Ask any key IT stakeholder about compliance and they’ll likely regale you with stories of how they’re being asked to provide evidence for testing non-stop and by different compliance groups. But the silver lining to this sometimes suffocating effort is that it makes it easier to identify and inventory what controls are already in place and which requirements they’re aligned against. Consider these key activities when scoping out the prospects of developing a GRC framework:

- **Inventory what you have.** Manage this much like you would a risk assessment. Develop a standard questionnaire and circulate through your infrastructure, making sure to interview all stakeholders. Identify the compliance requirements, inventory what controls have been aligned against those requirements and who typically coordinates the testing to ensure they’re functioning as documented. But be prepared to meet some resistance during the process as GRC will likely appear as one

After a decade of GLBA, seven years of SOX, five years of PCI and a lifetime of audit, a wide range of related activities need to be integrated into your GRC program.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

more compliance initiative to support. "Most organizations feel like they have all this stuff already: 'We have compliance officers for HIPAA, we have ITIL in place, we are SOX compliant. Why do we need something more?'" Quasar's Bachman says. He adds that the greatest challenge is "selling the idea that you need something that can pull all this information together from these various silos, without having to recreate everything."

Keep in mind that beyond what you find in developing the inventory, you'll also need to conduct a gap analysis in order to identify required controls that may be missing.

- **Align inventoried controls against in-scope regulations.** There are two clear efficiency gains from a properly developed GRC framework: a coordination of efforts between the three domains (governance, risk and compliance) and a consolidation of efforts to implement and maintain the necessary controls. Dorian Cougias, founder of Lafayette, Calif.-based Network Frontiers and lead analyst of the Unified Compliance Framework (UCF), which maps IT controls across international regulations, standards and best practices, says that five years ago, people argued about whether compliance mandates should or even could be harmonized. "Now everyone takes it for granted, because of the ridiculous rate at which compliance mandates are growing, that harmonization is a must for survival," he adds. For example, if you need to test logical access controls in support of both PCI and SOX, you would want to identify that commonality and coordinate your efforts so that both regulations are supported by a single approach. Not all tests can be applied to seemingly related requirements but by working with the internal controls experts, those that are candidates will be identified and managed accordingly.

"Now everyone takes it for granted, because of the ridiculous rate at which compliance mandates are growing, that harmonization is a must for survival."

—DORIAN COUGIAS, founder, Network Frontiers and lead analyst, Unified Compliance Framework (UCF)

- **Sell the benefits of GRC to management.** Perhaps the most significant component of GRC is the point where it engages management. A major element of GLBA addresses management's responsibility to ensure that non-public personal information is handled properly. Consider a similar approach when building out a GRC program. A common practice for banking institutions is to arrange for information security training for their board of directors to educate them on their responsibilities in support of GLBA; think about using a similar approach when designing your GRC framework. Tone at the top is an integral part of a successful program because at the next level down from the executive suite, there's a constant power struggle regarding ownership and direction for each of the related GRC domains. Cougias explains how governance is rooted in methodology, or a body of methods and rules used in a given discipline, that is defined by senior management. Compliance, on the other hand, is conveyed as a process: a series of actions or operations, he says. Fundamentally what that means is that while the rules are set by executive management, the related control activities are developed and supported by stakeholders

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

throughout the organization. Oftentimes, the stakeholders design and support controls to achieve compliance and don't expand them to consider efficiencies and are often resistant to cooperative efforts. Setting the tone at the top is critical because it's from senior management that the rank and file takes their marching orders. Without the C-level team supporting the GRC initiative and providing direction, it's unlikely that the methodology will develop deep roots.

One of the key benefits from a GRC program is the coordination of activities across the silos. If audit isn't directed to work with the risk management team and if both groups don't work with key stakeholders throughout the institution to coordinate and align their efforts, the program is unlikely to succeed. The [OCEG Red Book 2.0](#) (GRC Capability Model) talks about embedding controls within the innumerable business and related operational processes—an effort that requires a bit of organizational muscle. Eventually an institution needs to move past using GRC as a better way to maintain compliance and leverage its capabilities to manage the business; leave it to middle management to drive the GRC framework and that's not likely to happen.

WHAT'S NEXT?

Despite the fact that GRC has been around in some form for several years now, it's still very much in its infancy in terms of widespread adoption. Much like [COBIT](#), another popular governance-based framework that languished for years in relative obscurity until it helped provide clarity in the age of SOX, GRC is poised to become a key business strategy in the near future. While no one is certain what the next round of banking legislation is going to entail, one thing is almost certain: better risk management activities are going to be expected if not required. "Hopefully companies will see the need to expand GRC to not only control compliance risk, but as a means to help manage the overall success of their organization," Quasar's Bachman says.

Also expect significant advances in the availability of automated GRC tools. While they've been around for a while, they've been slow to make significant headway as a straightforward GRC solution; that's going to change. Wider adoption of GRC as a framework combined with better integration of regulations into GRC software will make it easier to see the benefits of implementing a software tool. There are already solutions that highlight interdependencies between various regulations when entering controls, thus ensuring economies of scale are identified automatically; this capability will continue to improve. "If today we are just beginning to make the links between mandated compliance processes and GRC tool methodologies, then in the next couple of years we'll see this bond strengthening," Cougias says. And in the very near future those capabilities will improve as GRC tools begin to pass information to other applications to update them for compliance, he adds.

Perhaps the biggest changes to GRC will be in how it's understood and relied upon. The last thing an enterprise is willing to consider while operating under the constraints of current economic conditions is spending money on or committing

resources to something that's not critical to their bottom line. However, as the various elements of GRC become better understood and practitioners become more adept at articulating their value proposition to their management, you can expect that to change. According to the OCEG GRC Capability Model Redbook 2.0, "a high-performing GRC system will always deliver value." Once that becomes an accepted fact and not just a line embedded within documentation, GRC will have finally arrived. •

David Schneier is managing director at consulting firm R.I.S.C. Associates with extensive experience in developing, implementing and managing compliance programs. Send comments on this article to feedback@infosecuritymag.com.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES

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

ADVERTISING INDEX

Sophos 2
<http://www.sophos.com>

- Security Threat Report: 2010
- How to protect your critical information easily

ArcSight, Inc. 4
<http://www.arcsight.com>

- Whitepaper: Combating Fraud & Data Theft in the Financial Services Industry
- Solution Brief: The ArcSight Protection Suite for PCI Providing Ultimate Protection for Cardholder Data

ESET 7
<http://www.eset.com/>

- ESET NOD32 Antivirus 4 Trial
- 10 Ways to Dodge Cyberbullets

SecureWorks 9
<http://www.secureworks.com/>

- Choosing an Effective Managed Security Services Partner
- Maximising the Value of Intrusion Prevention Systems

Trend Micro, Inc.
<http://us.trendmicro.com/us/home/>

- ZeuS: A Persistent Criminal Enterprise

Cenzic 13
<http://www.cenzic.com/>

- Cenzic's Software Products to Evaluate & Download

ISACA 17
<http://www.isaca.org/>

- Downloads
- Certification

The Academy Pro 21
www.theacademypro.com

- Free infosec videos for the information security community.

Glasshouse Technologies 28
<http://www.glasshouse.com/>

SystemExperts 44
www.systemexperts.com

TECHTARGET SECURITY MEDIA GROUP



EDITORIAL DIRECTOR Michael S. Mimoso

EDITOR Marcia Savage

ART & DESIGN

CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS

Marcus Ranum, Bruce Schneier,
 Lee Kushner, Mike Murray

CONTRIBUTING EDITORS

Michael Cobb, Eric Cole, James C. Foster,
 Shon Harris, Richard Mackey Jr., Lisa Phifer,
 Ed Skoudis, Joel Snyder

TECHNICAL EDITORS

Greg Balaze, Brad Causey, Mike Chapple, Peter
 Giannacopoulos, Brent Huston, Phoram Mehta,
 Sandra Kay Miller, Gary Moser, David Strom,
 Steve Weil, Harris Weisman

USER ADVISORY BOARD

Edward Amoroso, AT&T
 Anish Bhimani, JPMorgan Chase
 Larry L. Brock, DuPont
 Dave Dittrich
 Ernie Hayden
 Patrick Heim, Kaiser Permanente
 Dan Houser, Cardinal Health
 Patricia Myers, Williams-Sonoma
 Ron Woerner, TD Ameritrade

SEARCHSECURITY.COM

SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

SITE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS

GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

VICE PRESIDENT/GROUP PUBLISHER
 Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
 Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES DIRECTOR Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
 Suzanne Jackson

PRODUCT MANAGEMENT & MARKETING
 Corey Strader, Jennifer Labelle, Andrew McHugh

SALES REPRESENTATIVES

Eric Belcher ebelcher@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.

CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

EUROPEAN DISTRIBUTION

Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES

Julie Brown
 Phone 781-657-1336 Fax 781-657-1100

REPRINTS

FosteReprints Rhonda Brown
 Phone 866-879-9144 x194
rbrown@fostereprints.com



INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

All rights reserved. Entire contents, Copyright © 2010 TechTarget. No part of this publication may be transmitted or reproduced in any form, or by any means without permission in writing from the publisher, TechTarget or INFORMATION SECURITY.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT ENCRYPTION

CLOUD SECURITY

COMPLIANCE

SPONSOR RESOURCES