PLUS: WEB 2.0 SECURITY | WEB APPLICATION FIREWALLS | SECURING A MIDSIZE COMPANY

INFORMATION SECURITY®
MARCH 2009

SKY-HIGH RISK?

CLOUD COMPUTING CAN SAVE MONEY, BUT SECURITY & COMPLIANCE BECOME DIFFICULT

PLUS: Jericho Forum's New Cloud Collaboration Model

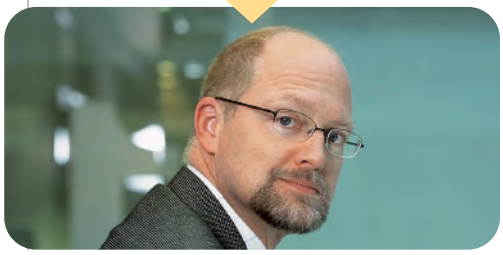
TechTarget
INFOSECURITYMAG.COM

contents

MARCH 2009

VOLUME 11 NUMBER 3

FEATURES



ALSO

The Audacity of Hope

BY MICHAEL S. MIMOSO

The Obama administration is conducting a review of the government's cybersecurity policies and process. We should be encouraged that security could move beyond the useless paper exercise it is today.

THE LEXICON IN Washington around cybersecurity is changing. In the coming weeks, you're going to hear a lot about offense and defense for instance, and it will have nothing to do with the Redskins. It will have to do with militarizing cybersecurity, and making critical infrastructure, and federal and public networks strategic assets.

While previous administrations have treated cybersecurity with policies and toothless national strategies, indications are the Obama administration is going to elevate it beyond a paper exercise.

Beyond the nonsensical distractions of the Obama BlackBerry, the president and those around him seem to appreciate importance of connectivity and the need for security and assurance to national security and commerce. Just about halfway through his first 100 days, Obama has already ordered Melissa Hathaway, senior advisor for the Director of National Intelligence, to conduct a review of the government's cybersecurity policies and processes, including the top secret Comprehensive National Cybersecurity Initiative (CNCI), which she helped build under the Bush administration. There are also rumblings that cybersecurity oversight may move out of the Department of Homeland Security and into the White House, reporting to Obama.

Hathaway's name is on a short list for the top cybersecurity job, and many hope her review actually evolves into an agenda for the position. Others such as Paul Kurtz who led Obama's transition team on cybersecurity have already crafted ambitious agenda items that include the establishment of a national cyberadvisor, declaration of cyber-infrastructure as a strategic asset, calls for cooperation with the private sector on standards that will improve the resilience of infrastructure in case of attack, standards to protect proprietary information from cyberespionage, and a mandate for standards to secure personal data.

One thing that's painfully clear—and has been for some time—the status quo is broken. Influential people are being vocal about the need to bring the NSA and the intelligence community deeper into the conversation. Kurtz's exceptional keynote last month at Black Hat DC urged cooperation between intelligence collection authorities, law enforcement and the private sector to gain what he called a "synoptic" view of what was happening on critical networks.

"For more sophisticated and persistent attacks, we must be willing to fuse data so we can trace back the origin of attacks and warn critical sectors of economy," Kurtz said. "This does not mean the intelligence community is engaging in espionage on behalf of private sector, or will carry out these activities without oversight, whether from privacy organizations or Congress."

This is a big reason for the gap in the past: attack origins have never been understood. As it turns out the wrong people were writing the right policies, and agencies that understood attackers and attack methods were never consulted. For example, policies such as the National Strategy to Secure Cyberspace, written in 2003, was not only birthed when many attacks were hypothetical, but was so sanitized that it was impotent. FISMA, written by NIST, has been

great at producing report cards and compliance reports, but has done very little to change behaviors and the insecure state of critical networks.

Little was being done to dissuade attacks on critical infrastructure, in particular from China. The Titan Rain attacks of 2003 may have shone a light on the situation, but little more. The turning point came in 2007 when attacks hit a dangerous peak—what some have called an intelligence Pearl Harbor.

A series of government agency networks were toppled in '07. Those in the know say the networks were unclassified, yet a lot of data was downloaded and surely a few treasures were left behind. It got so bad that the Secretary of Defense's unclassified email was breached and a Commerce Department website had to be taken offline for nearly a month. The attacks haven't abated here—the United States Central Command (USCENTCOM) has been targeted—or abroad, where German chancellor Angela Merkel's email was read as well. Heck, even the campaign websites of both presidential candidates were attacked last year.

"It's a wake-up call when the departments of defense, commerce and state are hacked or forced offline," says Jim Lewis, director and senior fellow at the Center for Strategic and International Studies.

"You've gotta go to people who understand attacks, such as the Red Teams at NSA, and those who clean up, such as US CERT—forensics people," says Alan Paller, director of research for the SANS Institute. "There has to be a shift from those who write policy, to those who understand attacks. Offense must inform defense. From my perspective, the most critical thing to do is to make sure we stop the bleeding and get serious about international standards and change federal policies so agencies can't get away with just writing reports."

The 2007 attacks got President George Bush's attention. He earmarked $30 billion for cybersecurity and ordered what eventually became the top secret CNCI 12-point plan.

"I think they're finally moving away from that paper-based approach of a few years ago, which was so disconnected from real security," Lewis says. "Now the change has been to attack-based metrics and attention given to attack vectors. It's not enough, but it's progress."

How much progress? Well, that's Hathaway's job to determine. Her 60-day review is under criticism on some fronts, because part of her job is to look at CNCI, which she helped develop. But almost universally, she's praised as a person with considerable program management skills and someone who can coordinate efforts between government agencies.

"When you think about who in government could have done this, only two or three come to mind. She's a logical choice," Lewis says. "She's not a career (government) person. She has an outsider's perspective."

CNCI is a key element moving forward; problem is that most of it is classified, and Lewis, for one, thinks most of it could be declassified.

"It's incredibly dumb that CNCI is not transparent," Lewis says. "Overclassifying CNCI is one of its biggest problems. You could declassify 80 percent of it and not do any damage. The other side of the coin is that if our foreign enemies have penetrated unclassified networks, they probably have a fair idea of what is in CNCI."

Hathaway, or the next cybersecurity advisor, will also have to consider advising President Obama on the development of cyberweapons that can be used either as deterrents or as offensive weapons to disable strategic military capabilities, as Kurtz suggests, or to take out botnets on behalf of either critical infrastructure or private networks—all with Congressional oversight.

The security industry should be encouraged because the Obama administration is willing to listen, and apparently, act on these fronts. Hopefully, Melissa Hathaway's findings will be made public, and hopefully she delivers a dynamic message, because it's going to have to be dynamic to be heard about the din caused by the depressed economy.

As Kurtz rightfully pointed out: "This is going to require a sustained effort in this economic environment, but that doesn't mean we shouldn't focus on this."

Michael S. Mimoso is Editor of Information Security. *Send feedback on this column to feedback@infosecuritymag.com.*

VIEWPOINT

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

Notification Acts Notify, Not Secure

I read Face-Off (State Data Breach Notification Acts: Have They Helped? January 2009); Marcus Ranum and Bruce Schneier are under the common misconception that breach notification laws have anything to do with security at all. They are simply that—notification laws.

They do potentially encourage good behavior (encryption can get you an exemption in most cases) but they do not mandate security nor reward good behavior (there's no tax credit for buying a firewall, for example). They simply require certain breaches to be made public.

In fact, any legal penalties are not for having the breach, but are for failing to report the breach. The peanut paste salmonella fiasco and food safety reporting is a good analogy. There's no reward for good behavior but plenty of downside for bad behavior, i.e., not reporting the presence of salmonella. Speeding tickets are another good example—you don't earn rewards (except in some states and for insurance purposes with some companies) for safe driving, but you suffer if caught speeding.

To argue that data breach notification laws have not improved security misses the point of the laws—which is to notify—and to let market and litigation forces act to bring the better behavior into being.

The payment card industry has contractual clauses that require compliance with the Payment Card Industry Data Security Standard (PCI DSS); there's no reward for compliance but plenty of downside for not complying. The Heartland Payment Processing breach, for example, rightly points out that PCI DSS does not, per se, require encryption in certain key places. That does not make PCI DSS ineffective, and, PCI DSS does require additional layered controls (antivirus, patching, etc.) which can work to counteract other shortcomings.

Notification laws are just another form of layered controls, none of which are 100 percent effective.

–Roger Nebel, director, FTI Consulting

Digital INFORMATION SECURITY magazine: Thumbs Up

I used to work for a major publisher now struggling to make a profit as readership of its print products has declined. Economics and environmental considerations make conversion from print to digital transmission of knowledge imperative. Publishers and readers have to make it work.

The conversion will drive further innovation in display devices leading to a richer reader experience. Press on!

–Name Withheld by Request

COMING IN APRIL

Effective Log Management

We'll focus on the policies and processes for effective log management when complying with regulations. In this article Stephen Northcutt, CEO of the SANs Technology Institute, will explain options in the market, how to build a review process, outline who is accountable and create proper documentation.

Data Loss Prevention in the Real World

We'll explain what happens when real organizations deploy DLP, and what lessons can be learned. In this feature, Rich Mogull partner of Securosis, will outline three DLP deployment scenarios designed to cover the most common uses, emphasizing those that are most effective.

Leveraging Identity Management Investments

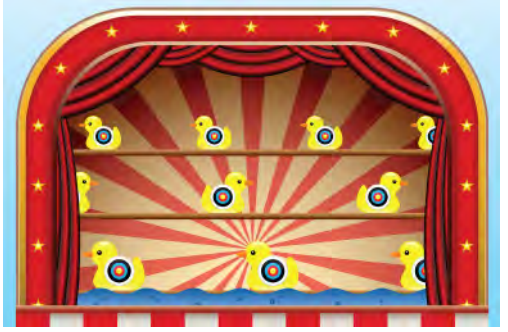
While large enterprises have deployed a mix of identity management products – from provisioning and authentication technologies to entitlement management and virtual directories –few have enjoyed the synergies that these products bring when they are fully integrated. In an era of limited IT budgets, Mark Diodati senior analyst for the Burton Group, will explain how to fully leverage your identity management investments.

Also:

Table-top Exercise

Read about how the state of Delaware last year tested the readiness of its incident response program.

MUST READ!



Bad Things Come in Threes

Third-party scrutiny is a priority as companies outsource more data and services. BY DAVID MORTMAN

AS THE ECONOMY worsens and corporate budgets tighten, there will be an increased pressure on CIOs and their staffs to use third-party service providers for various IT services. This will include everything from existing outsourcing of HR services, payment processing and CRM services to more cloud-based services such as Amazon Elastic Compute Cloud and Microsoft's Azure. Additionally, we will undoubtedly see an increase of privacy and security compliance regulations. Combine the increased flow of data outside the traditional corporate perimeter with the additional compliance needs, and the result is a much sharper focus on the security of third-party service providers.

But how are CISOs supposed to verify the security of a service provider meets their needs? This isn't exactly a new problem, yet it's not one we've had a good solution for in part because it's a moving target, especially in the case of many of the new cloud-based offerings that aren't built with security in mind. In the end, what a security manager needs to do is perform a risk-based assessment of the business utility of the offering versus the security risk.

In order to do a full-on risk assessment, the first step is to understand the security posture of the service provider.

In order to do a full-on risk assessment, the first step is to understand the security posture of the service provider. At a high level, you can generally get a feel for whether or not the vendor has the right mindset through interviews with its security staff and by reviewing its security and privacy policies to see if they are in line with your company's policies. When reviewing vendors in the past, I've used Request for Information (RFI)-style questionnaires to allow me to compare and contrast similar vendors when it comes to security. Ultimately, though, you will either need to audit the provider yourself to see if reality matches the vendor's claims or have a trusted third party perform that audit.

Now audit is a loaded word. Vendors hate to do them but love to use standardized ones as proof that they are secure. Just keep in mind that standard audits only cover specific domains, so if you need a vendor to be PCI compliant, it doesn't help if they pull out proof that they are HIPAA compliant or vice-versa. If you are going to just accept audits that the vendor has already done, be sure that those are actually in line with your needs and don't assume they're sufficient.

In particular, it is very important to remember that SAS 70 is not now, nor has it ever been, a security audit or proof of any real level of security. SAS 70 is a financial

controls audit but has become popular due to the Gramm-Leach-Bliley Act (GLBA) of 1999. As a result of GLBA and similar legislation, most insurance companies are requiring SAS 70 audits from their financial services customers and also requiring those customers make their vendors perform SAS 70s.

The vendors now have a situation where for one reason—customer demand from financials—they have spent a large sum of money on one special type of audit such as a SAS 70. Audits quickly get expensive so they want to minimize the number of audits they perform and need to keep track of, which means that they try to use existing audits as much as possible. Be strong; don't accept only a SAS 70 unless what you are concerned with are the vendor's financial controls. Otherwise, demand that vendors provide the necessary proof of security so you can either have the comfort level you need or implement additional security controls to achieve it.

David Mortman is CSO-in-residence at information security research and consulting firm Echelon One. Send comments on this column to feedback@infosecuritymag.com.

Analysis | CONFICKER WORM

Microsoft Issues $250,000 Bounty

Coalition forms to attempt to catch the cybercriminal and stave off copycat attacks. BY ROBERT WESTERVELT

SO FAR IT HASN'T RUINED any machines or pilfered any data, but the Conficker worm showed so much potential for widespread damage that it rallied a number of different groups together to defeat it.

A coalition formed Feb. 12 to go on the offensive and shut down the hundreds of command and control servers that the Conficker worm uses to receive its marching orders. The group is led by Microsoft and consists of antivirus giants, security vendors, Internet registries and DNS providers such as ICANN and NeuStar. Microsoft issued a $250,000 bounty for anyone who gives information about the cybercriminal responsible for the worm if it leads to their arrest and conviction.

Experts say the worm attracted too much attention. The longer a worm stays undetected, the more lucrative it is for the worm author or the cybercriminal gang behind it. With no antivirus signatures detecting the worm, those responsible for it can harvest as much data as possible and sell it on the black market. The coalition's biggest fear is the possibility of a massive distributed denial-of-service attack if the worm's author decides to send out orders to use the hoard of infected computers to shut down Internet access to companies or certain networks. But now experts admit that those orders are unlikely.

"Its propagation was too successful," said Vincent Weafer, vice president of Symantec security response. "The longer we go with no payload the more it becomes unlikely we'll see one."

Conficker, also known as Downadup, attracted attention when it quickly spread by exploiting a Microsoft remote procedure call flaw. It began spreading just days after the software giant rushed out an emergency patch to address the issue in late October.

IT administrators who were too slow to deploy the patch were the most frustrated.

Countries where software pirating is rampant saw the largest infection numbers. In all an estimated 10 million machines were infected at the peak of Conficker's spread. Today antivirus researchers estimate that number to be considerably less since tools were available to allow victims to easily remove the Trojan.

"Largely we've seen a movement away from self propagating worms to things like Web exploit toolkits in the last few years," said Thomas Cross, security researcher for IBM ISS X-Force research team. "In many respects it's like the threats of yesteryear."

The coalition, however, may be more about highlighting a public image of cooperation to stave off future worm attacks than about stopping the present one. History has shown that in times of economic crisis, cybercriminals increase their development of worms and other malware. Shortly after the dot-com bubble crashed, the Code Red worm was unleashed, infecting hundreds of thousands of machines in 2001. The Nimda worm followed, latching on to back doors left behind by Code Red. Sobig soon infected millions of machines, successfully spreading through email attachments. Blaster infected 48,000 computers and caused an estimated $1.2 million in damage when it spread in August 2003. Shortly after, the Sasser worm infected computers worldwide, causing them to crash and reboot.

"Largely we've seen a movement away from self propagating worms to things like Web exploit toolkits in the last few years. In many respects it's like the threats of yesteryear."

–THOMAS CROSS, security researcher, IBM ISS X-Force research team

"In times of crisis the good guys want to band together and this time everyone's sort of fed up in the current environment," said Pete Lindstrom, research director at Spire Security. "With economic times weighing down on us, this gives everyone something specific to do. It's something we can try to control."

Recognizing the need to stop copycats, Microsoft took a hard line on malware authors in 2003 when it allocated $5 million to create the antivirus reward program to arrest and convict those responsible for the malicious programs. It was seen as largely successful. Those responsible for Blaster and Sasser were arrested and convicted. Two German men shared the $250,000 reward for the information that helped identify the 19-year-old responsible for Sasser.

"The idea of working together against a common foe has pulled whole nations out of crisis," Lindstrom said. "This [coalition] reenergizes the whole security community and is something that was really needed."

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

The Pressure Is On

THIS MONTH HACKERS have been targeting security vendors for their latest attacks as Kaspersky Labs and F-Secure disclose hacks. Meanwhile the Health and Human Services agency cracks down on HIPAA compliance fining CVS for violations.

—*Information Security* staff

$2.25M

The amount CVS Caremark paid because of a HIPAA violation where pharmacy employees threw items such as pill bottles with patient information into the trash.

$105M

The amount Research In Motion (RIM) paid for Certicom's encryption software and defeated VeriSign in an ongoing bidding war for the encryption vendor.

$250,000

The reward Microsoft is offering for information leading to the arrest and conviction for the cybercriminals responsible for the fast spreading Conficker/Downadup worm.

25,000

The possible number of activation codes that a Romanian hacker got when breaking into a custom built, U.S.-based Kaspersky Lab support website. F-Secure was also hacked.

SOURCE: SearchSecurity.com

OVER-HEARD

"Virtualization gives IT the opportunity to challenge traditional security concepts and secure the technical business infrastructure more cost effectively. These security benefits can be realized from the greater control IT has over configuration of application environments, easier processes for vulnerability management, and rapid delivery of pristine application images to all points of the organization."

–ERIC OGREN, founder and Principal Analyst, Ogren Group

LAYER 8

Classification Blues

Simplicity is the key to ensuring effective data classification in the enterprise. BY JAY G. HEISER

THE PROCESS OF DATA CLASSIFICATION is not something that comes naturally to us. So why even bother to do it at all? Because it just makes no sense to treat all information as if it has the same security significance (or integrity significance or availability significance). Without making a conscious decision to perform different levels of control on different types of data, you inevitably either treat all data as if it were nuclear waste, carefully securing it to such a degree that nobody can get any work done, or apply no controls whatsoever, ensuring that proprietary and regulated data will get into the wrong hands.

A classification scheme is a mechanism to optimize the level of security effort, maintaining the maximum possible flexibility while ensuring a proportionate level of control for sensitive data. But how do we do choose a model that is practical and useful?

A classification scheme is a mechanism to optimize the level of security effort, maintaining the maximum possible flexibility while ensuring a proportionate level of control for sensitive data.

Given that classification is a practice we borrowed directly from military organizations, it's illuminating to examine what they've learned over the last century. The U.S. had no formal scheme until World War I, when the French and British forced use of a three-tiered scheme. By the start of World War II, the allies somewhat reluctantly accommodated a more complex and information-rich world by extending classification to four levels, and then the U.S. demanded that a fifth level be added for the Manhattan Project. Because of the significant global threat presented by thermonuclear weaponry, NATO continued, albeit grudgingly, to use a five-level scheme.

The military always avoided additional complexity to their schemes because of the difficulty of applying classifications compounds with each added level. I am aware of some commercial organizations that use one more level than NATO. That probably doesn't make sense, even if they are dealing with nuclear bombs. My experience has been that anything above three levels is too abstract to be practical.

Ten years ago, I was introduced to the idea of a simple low, medium, high scheme through the National Security Agency's Information Security (INFOSEC) Assessment Methodology course. The NSA, traditionally not an organization that shies away from abstract and impractical computer security concepts, has been promulgating this low-

granularity concept for a decade. The International Security Forum (ISF) also has been recommending a low, medium, high scale.

Ultimately, a scheme that is "too simple" is superior to one that is "too complex." Simplicity is especially important as it becomes increasingly clear that the lines of business need to not only determine the sensitivity of their own IT assets, but they also need to "own" the associated risk. A complex scheme that requires business managers to become data classification specialists is a non-starter.

Increasingly, we're going to be offering security in the form of service levels, aligning the degree of protection with business needs and budgets. The baseline level of protection is suitable for the majority of business information, which is of low sensitivity, but special information requires special care, and that costs extra. Our service catalog has to be easily understandable, offering specific benefits for higher costs.

Of course, to be effective, a data classification scheme requires processes and technology to provide the correct level of security specific to each level. And data owners and users must be willing to follow the processes and use the technology, even when it means extra work or reduced system performance. However, a growing number of organizations are learning that low, medium, and high make a very practical starting point for service level offerings.

Jay Heiser is a London-based research vice president at Gartner. Send your comments on this column to feedback@infosecuritymag.com.

what drives *your* approach to IT security?

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

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

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

- ISO 17799/27002 Compliance
- HIPAA and PCI DSS Compliance
- Application Vulnerability Testing
- Security Audits and Assessments
- Security Architecture and Design
- Identity Management
- Penetration Testing
- Security Best Practices and Policy
- Emergency Incident Response
- System Hardening
- Technology Strategy
- ASP Assessments

SystemEXPERTS
LEADERSHIP IN SECURITY & COMPLIANCE

HOW TO Secure Cloud Computing

On-demand computing services can save both large enterprises and small businesses a lot of money, but security and regulatory compliance become difficult.

BY NEIL ROITER

CLOUD COMPUTING is attractive, seductive and perhaps irresistible. The benefits are compelling, particularly the pay-as-you-go model that has been likened to buying electricity (or, if you, prefer, buying your drinks by the glass rather than the bottle).

There's a powerful business case for buying computational power, disk storage, collaboration, application development resources, CRM, on demand. Rather than buying more servers and disks or expanding or deploying expensive infrastructure and programs, cloud computing is flexible and scalable. It can meet short-term initiatives and requirements and deal with peaks and valleys in business cycles.

But where does security fit into all this? Security analysts and practitioners generally say proceed, but proceed with caution. All the risks to sensitive corporate data associated with outsourcing apply to cloud computing, and then some. Enforcing security policy and meeting compliance requirements are tough enough when you deal with third parties and their known or unknown subcontractors, especially on a global scale. Add the blurry characteristics of the cloud and the entry of non-traditional vendors into the technology market, and some caution flags go up.

In an IDC survey of 244 IT executives/CIOs published last fall, 75 percent of the respondents cited security as a significant or very significant challenge with cloud computing. Compare that with 63 percent cited for the next two concerns—performance and availability. So, you'd better get ahead of the risks of cloud computing before your business colleagues get ahead of you.

"I recommend security people get some exposure to it," says Craig Balding, technical security lead for a Fortune 500 company who also publishes a blog on www.cloudsecurity.org. "Because the CFO, attracted by the numbers, or the CIO who is told by the CFO, is going to come knocking on the door and ask 'What's this cloud thing all about? What can we do in the cloud?'"

Let's examine some of the risks versus the benefits of cloud computing, and what your company can do to mitigate those risks and reap some of its benefits.

Security Isn't a Vendor Priority

Not surprisingly, cloud computing providers are not talking much about security today. That's pretty typical whenever "The Next Big Thing" in technology bursts upon the business landscape.

Most of the public discourse is coming from security experts and analysts pushing vendors to take the initiative. Amazon, for example, doesn't have much of a security presence on their Amazon Web Services (AWS) Web site, and the same is true for Google Apps, says Balding. There's no obvious procedure or clear commitment, for example, to deal with a researcher who wants to report a vulnerability.

"Google and Amazon have very smart security people," Balding says. "But, when you talk to the Amazon evangelists who are prominent at every cloud conference about security, there's not much of a conversation. It would be great if they put people into the community who could talk about security."

The question is not whether cloud computing vendors are indifferent to security—clearly, they are not. Rather, how important is strong security to their business models and how far they are willing to go and how much are they willing to spend? Does the business model, for example, support a security program that is not only strong but flexible enough to meet unique customer security and compliance requirements, especially large multinational companies?

"Cloud computing is optimized for performance, optimized for resource consumption, and optimized for scalability," says Forrester analyst Chenxi Wang. "It's not really optimized for security."

"Cloud computing is optimized for performance, optimized for resource consumption, and optimized for scalability. It's not really optimized for security."

–CHENXI WANG, analyst, Forrester Research

At this early stage of the market, you have to be concerned with where security is now and whether vendors can bake it into their services from the start or try to bolt it on under pressure from customers. It's a new market in which companies have to be especially diligent about

security before jumping in.

"Right now, it's not cut and dried," says Gartner analyst Mark Nicolett. "It's an early adopter type of situation. You can't assume any level of security practice any more than you can assume a certain level of security practice with a traditional outsourcer."

Cloud's Heightened Risks

What you can assume with cloud computing is that you have to deal with all the risk factors you expect to face in "normal" outsourcing. But cloud computing also brings its own inherent set of security problems, which make it not only difficult for your company to get the assurance it needs to meet its obligations, but in some cases difficult for the service provider to meet all your requirements.

"What's different about cloud is control," says Balding. "To have control implies visibility. You can't control something if you can't see."

Consider three cardinal requirements of data security: availability, integrity and confidentiality.

The first is core to your business and your service provider's business. A data breach is bad enough, but if the service goes down, the business is down. Amazon's Simple Storage Service (S3) went down twice last year for several hours, for example. If your first requirement is near-100% uptime, then it's a good bet that almost every vendor will make that its number one priority.

> "What's different about cloud is control. To have control implies visibility. You can't control something if you can't see."
>
> –CRAIG BALDING, technical security lead for a Fortune 500 company

Data integrity and confidentiality are another matter. Integrity requires that only authorized users make authorized changes. Confidentiality means that only authorized users can read the data. One would expect to apply strong controls to enforce policies over authorized user access, authentication, segregation of data etc. With traditional partners and service providers who handle your sensitive data, you can extend those controls. But with cloud computing, you don't know and, as a practical matter, can't know where your data is. You don't know what server is computing for you, where it's transiting over which network, even where it's stored as the providers' systems respond dynamically to your rising and falling requirements and those of thousands of other customers. The flexibility and scalability that makes cloud computing attractive makes it unpredictable.

"Going to Amazon, or IBM or Dell or Microsoft in cloud isn't much different than outsourcing to AT&T," says Jeff Kalwerisky, chief security evangelist at Alpha Software. "The difference now is you literally don't know where data is."

Furthermore, it's difficult to assure data segregation, because those networks and servers are sharing data from thousands of customers. So you have to be concerned that your service provider's personnel *and* someone from another organization may be reading it because of improper authorization or authentication.

A related issue, says Forrester's Wang, is transitive trust because cloud computing vendors have to rely on third-party suppliers to provide computational and infrastructure resources. So, how can I extend that trust even if I have a trusted relationship with my provider?

"These third-party infrastructure resources touch my confidential data," says Wang.

"Do I allow this trust I've established with, for example, Amazon, to be carried over to a third party, and how do I even evaluate that? The transitive trust question does not have a clear answer."

So, your vendor doesn't know where your data is going to be at any given time, and that makes it difficult to determine if your data is being handled in a way that assures confidentiality and privacy.

COMPLIANCE

Cloud Blurs Auditors' Vision

IF SECURITY CONTROLS are obscured in the cloud, it follows that regulatory compliance can be problematic as well. How do you perform an on-site audit for example, when you have a distributed and dynamic multi-tenant computing environment spread all over the globe? It may be very difficult to convince auditors that your data is properly isolated and cannot be viewed by other customers.

Compliance presents cloud providers with a business problem: Meeting particular compliance requirements of each customer takes away some of the economies of scale that allow them to offer inexpensive services and still realize nice profit margins. But it's one they need to address if they want large, heavily regulated companies as customers.

"There are conflicting requirements," says Forrester analyst Chenxi Wang, "between specific compliance regulations, between specific security requirements of a client and the need to amortize resources and amortize consumption across different clients. Achieving compliance becomes a little more difficult."

Since your data can be anywhere, data location can be particularly tricky, especially when it spans international borders. For example, says Gartner analyst Mark Nicolett, European privacy laws restrict movement and cross–border access of certain types of data.

"You have to be aware of any restrictions in this area," he says, because cloud providers typically don't provide any type of location gating or guarantees about compliance on your behalf with privacy laws of that sort."

Nevertheless, don't assume that you can't outsource regulated data and operations into the cloud. You'll need to work with auditors and prospective service providers to determine if cloud computing supports your compliance requirements.

"It depends on the regulations," says Craig Balding, technical security lead for a Fortune 500 company. A lot of people waving the regulation flag and saying, I can't do this in cloud."

Much depends on what type of audits are required to satisfy the data and process control requirements. Does the auditor need to see change control logs; do you need to run security tools against the cloud computing provider's infrastructure (which is, as a practical matter, *everywhere*)? Is a paper audit sufficient or does it need to be more hands-on?

"Those are questions that will get fleshed out over time," Balding says but it's not terribly clear right now."

–NEIL ROITER

Ascend to the Cloud with Caution

None of this means that your company should dismiss the idea of doing business in the cloud; nor should you compromise security.

"The only thing you can do now is good contractual thinking before you go in," says Alpha Software's Kalwerisky. Large customers can leverage major cloud providers to assure better security and transparency, he says. After all, there are choices.

"If one provider won't play ball, I can go to others," he says. "The market will drive it."

Gartner recommends that you adhere to strong security requirements for engaging outsourcers, even though the cloud computing environment is more problematic. The risks to your data are still there.

In its report, "Assessing the Risks of Cloud Computing," Gartner strongly recommends engaging a third-party security firm to perform a risk assessment. It cautions that even large and sophisticated organizations, such as major financial institutions, which are used to conducting their own assessments, are better off hiring a third party to evaluate cloud computing partnerships.

The distributed nature of cloud computing makes this kind of assessment more difficult. And, unlike traditional outsourcing partners who have come to view good security as a competitive value, cloud computing providers may be more reticent about outsiders auditing their operation, or at least limit their access. They may be less likely to allow auditors and assessment teams to lay hands on their data centers, but performing log reviews and reviewing audit trails should be negotiable.

> "The only thing you can do now is good contractual thinking before you go in."
>
> –JEFF KALWERISKY, chief security evangelist, Alpha Software

"Obviously, auditing cannot be as detailed," says Forrester's Wang. For example, a vulnerability assessment scan of Google [is not reasonable]. They won't let you do that. You have to see if it is possible to do some level of external auditing. Today, that is very difficult."

Large enterprises certainly shouldn't settle for the providers' standard service level agreements, but smaller companies are another story. They typically lack the expertise to adequately assess the security of the services, so they are more apt to rely on providers who have that expertise.

"Most small companies I talk to, unless they are highly regulated, tend to put performance, reduction of resource overhead ahead of security," says Wang. "But that doesn't mean that cloud computing vendors shouldn't do more to satisfy their needs and be more transparent."

The most important consideration, regardless of company size, is the sensitivity of the data that's exposed to the service provider. If the service does not put sensitive data at risk or jeopardize your operation, security requirements for the vendor can be less stringent. On the other hand, companies shouldn't compromise security if confidential customer information, intellectual property or other sensitive data is at risk.

"What companies need to do is evaluate risks against business benefits, identify workloads where business benefits are high relative to risks," says Gartner's Nicolett. "Those workloads are the ones that are most appropriate for cloud computing at this time."

Companies can also insist on encrypting data, both in transit and at rest. Encrypting data in motion is pretty much a given; all service providers are using SSL or some other strong encryption. Data at rest is more complex, and you may have to rely on your own resources to encrypt it. The key question is…who holds the keys?

Encryption is less reassuring if the provider controls the keys. It gets back to a question of trust and verification that the provider is following strict policies regarding who has access to the keys and under what circumstances. The mechanics are more intricate if your company holds the keys, but the security is obviously in your hands, since only your personnel can decrypt the data.

Gartner's Nicolett cites vulnerability management service provider Qualys as a good model. Customers' data is commingled, but it is encrypted, and the customer controls the decryption keys.

"It is the capability that makes companies feel comfortable to have their sensitive security data hosted externally," he says.

Stick to Policy

Easy accessibility is one of cloud computing's strengths—and also one of it's risks. It's trivial for a department, workgroup or even an individual to jump onto the cloud on their own. Just whip out that corporate credit card.

It's the downside of democratization from security point of view," says Balding. "Unless you have fantastic DLP in place, you may not even know a cloud is being used."

Consider a group of developers who can circumvent their company's policies and processes—maybe things move a little too slowly for their liking. They're not the bad guys; they're just trying to get their jobs done and do what they love doing: creating first-rate software for their company.

Or a business unit can make the decision to contract for application development or perhaps CRM, such as salesforce.com. They get the job done, but bypass all the policy controls they should adhere to.

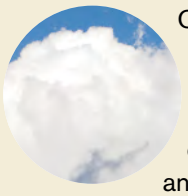
"It's probably a valid business decision, but the worry is it's an unconscious decision," says Gartner's Nicolett. "Then there is no evaluation of security, compliance and risk level, because the people that understand those risks aren't involved in that decision."

There are operational risks as well, he says. Workflows can be damaged or disrupted because the links between the applications moved into the cloud and internal processes aren't clear, and process integration may be degraded.

You can still migrate the application to the cloud, he says, but you need to make a conscious, well-planned decision that addresses these kinds of potential problems up front.

PRIVATE CLOUDS

Get Off of My Cloud



ONE WAY TO maintain control of your data in the cloud is to own it, says Craig Balding, technical security lead for a Fortune 500 company.

Large companies are heavily invested in data centers already, he says, so business agility and new business initiatives may be more compelling drivers for cloud computing than saving on hardware costs, at least at this stage. Hence the notion of private clouds, which can be completely internal for large companies (call that an "enterprise cloud"), but would more likely involve third-parties, such as one of the hosting providers that are trying to move into cloud-based services.

The difference is the private cloud wouldn't be open to the public. The enterprise customer reaps most of the on-demand benefits of cloud computing, but can exert the same security and compliance controls they do with more conventional outsourcing. Since hosting providers typically segregate data by sector—defense, financial services, for example, and are accustomed to maintaining strong access controls over each customer's information, they would be well-positioned to support this type of cloud.

"With a private cloud, there's less of an attack surface," Balding says, because not everyone in the world can sign up with a credit card." ›

—NEIL ROITER

The solution is straightforward. If your company has good governance in place, employees follow policy and procedure for risk assessment, planning and review before signing on for services. The message from the top should be that yes, outsourcing policies apply to cloud computing. So, put the credit card back in your wallet, at least until you've thought this through.

Standardization—the Next Step?

One of the major impediments to evaluating cloud computing providers is the lack of standards by which you can compare them. There are no standards for how data is stored, access controls, performance metrics, etc.

This raises business *and* security issues. For example, if I outsource my sales system to one provider, but want to contract another for accounts receivable, how do I share data between them? Is it even possible?

Vendors, analysts and security leaders are discussing the need for standardization, as an example, for SLAs.

"My clients have trouble understanding one SLA against others because the language is different; the properties they promise are different," says Forrester's Wang. "You really have to spend a lot of time making sure you are comparing apples to apples."

The next step might be agreement by an industry consortium, and eventually by some recognized standards organization. Getting competitors to agree on standards is historically a tough sell, and this probably will be no exception.

"None of the vendors will want to change to some other vendor's standard," says Alpha Software's Kalwerisky. "But once we have standards about how data is stored and security issues and many other things, then cloud computing becomes an unstoppable option, because you'll have everything you have in your data center with a lot less hassle and less capital investment."

"My clients have trouble understanding one SLA against others because the language is different; the properties they promise are different. You really have to spend a lot of time making sure you are comparing apples to apples."

—CHENXI WANG, analyst, Forrester

Neil Roiter is senior technology editor for Information Security. *Send your comments on this article to feedback@infosecuritymag.com.*

What Can You Entrust to the Cloud?


Adrian Seccombe, CISO of Eli Lilly

Jericho Forum outlines a cloud collaboration model. BY RON CONDON

NOT LONG AGO, a researcher at the pharmaceutical company Eli Lilly needed to analyze a lot of data fast. If the results turned out as he believed, the company could have a world-beating drug on its hands.

The only trouble was that he would need 25 servers to crunch the huge volume of data, and he knew it could take up to three months to get approval for the investment. In an industry where the cost of delaying a product is estimated at $150 per second (yes, per second), that three months' wait would be very expensive indeed.

Adrian Seccombe, the company's global head of security, explains: "He went to a tame IT guy who'd been playing around in this thing called 'The Cloud'. The guy got out his credit card, plugged it into Amazon Web Services, and had 25 servers up and running in the cloud within an hour."

They then realized they'd built the servers incorrectly so they had to take them down and start again. The second time, it took them 40 minutes to get the servers up and running.

"Within two hours they were crunching the data. The research time had suddenly collapsed from three months to two hours," says Seccombe.

And there is more. When they realized the analysis would not be complete by the time they wanted to go home, they were able to crank up the power, and bring on more servers to speed things up. "They wanted to get the data back from the cloud as they felt a little uncomfortable leaving it out there overnight."

They completed the task, and were given a bill from Amazon for the princely sum of $89. At $150 per second, a three-month wait would have cost more than $1 billion.

The cost comparison is mind-boggling and demonstrates the sheer power of the cloud computing concept. But for Seccombe, the example also underlines some of the problems with the model too.

"They repatriated the data results, and did it securely over a secure line that goes end-to-end into the Amazon cloud. It was secure and quick."

Or was it? How could they prove there was no trace of their data left in the Amazon cloud? They had to take Amazon's word for it.

It is just one of many questions that are now being raised with the advent of cloud computing, software-as-a-service, and the new collaborative model that relies on companies sharing their digital assets.

And it is why Seccombe, wearing his other hat as a member of the Jericho Forum, a security think-tank, has been working recently with others in the group to come up with some kind of framework to chart how it can be done effectively and securely.

The result of this work, due to be unveiled officially in March, is a three-dimensional cube that attempts to map out in graphic form the key decisions that companies will have

to make when deciding which tasks could be safely consigned to the cloud, which should be kept under lock and key, and how you tie all the various ways of working together.

For the last five years the Jericho Forum has been challenging conventional thought about information security and mapping out the requirements of a "de-perimeterized" world where solid boundaries are replaced by mobility and collaboration between organizations.

Last year, Jericho laid out its Collaboration-Oriented Architecture, which defined how systems could work together without jeopardizing security. Now it is going further to map out the security requirements of cloud computing. The results of this latest exercise raise some challenges for the security industry, but also outline some interesting opportunities for those with the vision to seize them.

The main message of the group is that the cloud can incorporate a variety of approaches, according to the level of control you need over a process.

The cloud collaboration model looks like a Rubik Cube with four faces on each side–thereby creating eight separate sub-cubes that represent different types of working.

The three dimensions of the cube are:

- Open/ proprietary
- Perimeterized/ deperimeterized
- Internal/external

The model is intended to help companies categorize their business processes and ultimately to plan the kind of systems architecture they are going to need going forward.

"It's a mistake to see the cloud as one thing," Seccombe says. "You can have internal proprietary perimeterized clouds, and you can have external, open, deperimeterized clouds.

"It's a mistake to see the cloud as one thing. You can have internal proprietary perimeterized clouds, and you can have external, open, deperimeterized clouds."

–ADRIAN SECCOMBE, CISO, Eli Lilly

"Inside Eli Lilly, we are trying to decide where we want to do what business processes. For example, bringing together the ingredients for a pill–we probably wouldn't do that with an open, external deperimeterized cloud. That is more likely to be proprietary, perimeterized and internal, still using cloud technologies possibly, but I need more control over it."

The key, going forward, is to build efficient and secure interfaces between the various sub-clouds so that business in the cloud can work in a seamless way, and create the necessary services to make it happen.

One of these, for example, could be an independent service to check the repatriation of data from the cloud once a task is finished. "It's not that we don't trust Amazon, but it is a question of separation of duties," he says. "You don't want the auditor to be the one who's providing the service."

Working up the 'cloud layers'

Given the huge advantages of working in the cloud, the goal now is to see how much work you can safely entrust to the cloud as a whole.

Jericho envisages this potential as a series of layers as follows:

- Value/Outcomes
- Process
- Software
- Platform
- Infrastructure

As companies move up the stack, and entrust their infrastructure, platform, software, and so on, to a cloud-based service, they can achieve what Seccombe describes as 'abstraction': "Abstraction means that you don't really care what's going on beneath, because somebody else is looking after it for you, and will deal with it in a responsive manner."

He admits that most cloud activity is down at the infrastructure and platform level (as with Amazon Web Services) or with software (as with Salesforce or Netsuite). But he cites one example of value-as-a-service, which came from personal experience.

When looking for a new battery for his Blackberry, he clicked on the Amazon website, which brought up five shops that were selling the battery. He chose a shop and ordered, and the battery quickly arrived in an Amazon box. "Amazon brought to me the value experience of getting that battery, but I can't remember which shop I bought it from. This was my first experience of value as a service. I did one click and got the battery delivered the next day."

The example underlines the move towards customer-centric computing supported by increased collaboration in the cloud. And it is not just about shopping.

Seccombe cites the www.patientlikeus.com website where people with various complaints can compare notes. For a drug company, something like that would present huge opportunities to get patient feedback, but only if the right controls are in place.

And here's the rub. The cloud is very appealing, but diving in without the right level of security in place is a recipe for disaster. As Seccombe says, you can't bolt on security after the fact. "If you enter the cloud naively, then you lose sight of your data. You lose control," he says. "That's why we are trying to get this done up-front."

> "If you enter the cloud naively, then you lose sight of your data. You lose control. That's why we are trying to get this done up-front."
>
> –ADRIAN SECCOMBE, CISO, Eli Lilly

What's next?

Cloud computing could have a huge bearing on how we do IT. Even if companies continue to run their own systems in-house, they might develop and test applications in the cloud rather than buy their own systems for the purpose.

Off-site disaster recovery centers will also start to look like a waste of money when cloud-based services can offer the necessary back-up without the huge up-front cost.

But the services need to be easier to use. For example, the Eli Lilly researchers had to configure their own servers manually, but in future that kind of service could be automated with new servers coming on stream automatically to cope with the demand.

Identity and access management will also take on a new importance as more collaboration takes place in the cloud, and where collaborative activities may be very short, lasting minutes rather than years.

"The old model, which assumes that everyone inside your silo is trustworthy and where you build an Active Directory for those players to use resources inside your organization, is dead or dying. We have to find ways to change it," says Seccombe.

Ron Condon is UK Bureau Chief for SearchSecurity.co.uk. Send your comments on this article to feedback@infosecuritymag.com.

The Security IT Downloads library on SearchSecurity.com contains the most comprehensive resource of free commercial security software titles available on the web. Plus, benefit from our editor recommended security tools and valuable shareware every security pro needs in their back pocket. View the library at: **www.SearchSecurity.com/itdownloads**

SearchSecurity.com

FIVE CONSIDERATIONS WHEN SECURING A MIDSIZE COMPANY

Smaller organizations need to be more resourceful and we'll explain how risk management, automation and managed security services, among others, can help.

BY MARCIA SAVAGE

GET CREATIVE.

That's the most important step for anyone in charge of securing a midsize business, says Tony Meholic. He should know. Meholic went from managing the ethical hacking team at JP Morgan Chase, a huge worldwide enterprise, to leading security at Republic First Bank, a 300-employee regional bank based in Philadelphia. At JP Morgan, buying a $100,000 tool was a simple matter of some paperwork and signatures. At Republic First, asking for a $25,000 tool got him a pat on the back and a vague promise of "maybe sometime."

"You have to get more creative as far as maintaining security, because certainly the requirements don't change," Meholic, vice president and information security officer, says.

Just like their large counterparts, midsize companies with 100 to 1,000 employees face regulatory compliance pressures. They also face the same kinds of threats and can't afford a reputation-destroying and costly data security breach. But unlike big enterprises, midsize businesses don't have the luxury of ample resources and large security teams. They rely on ingenuity to figure out ways to secure their data assets on sometimes shoestring budgets and are well-versed in the resourcefulness the recession requires of companies of all sizes.

For Meholic, security on a tight budget led him to automate and streamline manual processes. Security officers at other midsize companies and industry experts cite automation as a key tactic, along with other strategies, including wringing more security value out of existing equipment and outsourcing certain security services. Some point to core strategies applicable to businesses of all sizes like risk management. We've compiled their advice into five essential considerations for securing a midsize business.

#1 Risk Management

For many companies, including midsize ones, smart security starts by analyzing and assessing risks.

"Step one is to figure out what your risks are," says Matt Roedell, vice president of infrastructure and information security at TruMark Financial Credit Union, 300-employee firm with $1 billion in assets based in Trevose, Pa. "You need to perform a risk assessment."

Once a company does a detailed risk assessment—either on its own or with outside expertise—it can analyze which risks impact its business the most, research what tools and services can mitigate them, and how much those solutions cost, he says.

"It's very easy to put a proposal on a desk and say, 'We need this.' It's different when you put it in terms of risk to the business."

–MATT ROEDELL, vice president of infrastructure and information security, TruMark Financial Credit Union

"It's very easy to put a proposal on a desk and say, 'We need this.' It's different when you put it in terms of risk to the business," Roedell says. Along with a proposed purchase order, he recommends presenting business executives with what he calls a "risk acceptance document" in the event they don't want to fund the risk mitigation. No one will want to sign it, he says.

Business managers aren't IT or security experts; they just want to know what will negatively affect the company and its bottom line, he says: "So tell them what it will do to the bottom line."

Indeed, midmarket information security managers must take the time to understand their company's business, especially in these tough economic times, says Khalid Kark, principal analyst at Forrester Research.

"You need to pick your battles. You have to prioritize," he says. "To do that, you need a clear idea of what the business priorities are and what your existing capabilities are."

Instead of creating a laundry list of security actions, those in charge of security at midsize companies should step back and look at what parts of their business are most critical, e.g., if it was lost how much revenue the company would lose, says Jack Phillips, co-founder and CEO of IANS, a Boston-based infosecurity research firm.

"You can't cover all your risks. You have to make an educated guess as

to where your highest risks are and focus on them," he says. "Prioritize is the key word."

In a down economy, companies need to view their business processes from a risk perspective and look at ways they can reduce risk by re-architecting the process instead of buying more products, Phillips says.

Jay Arya, a vice president and information security officer at Short Hills, N.J.-based Investors Savings Bank, which has about 500 employees including three focused on security, says any business must take a holistic approach to information protection. For example, email security can't be implemented without taking into account its impact on business processes; if it winds up blocking email to customers it would hurt the business. At the same time, sensitive information needs to be protected, he says.

"You have to look at the whole company … what the business needs are and focus security based on that," he says. "The last thing you want is your business to suffer because of security. It's a fine line between effective security and operation of the business."

#2 Automation

Midmarket companies often rely on one person to manage security, and in many cases, that person juggles security responsibilities with other work. Limited manpower can make automation critical in the midmarket.

"You have to get creative about the use of resources," Meholic says. "The more you can automate the better."

"You have to get creative about the use of resources. The more you can automate the better."

–TONY MEHOLIC, vice president and information security officer, Republic First Bank

Forrester's Kark says some midsize businesses actually are a little more advanced in their use of technology compared to big companies, so they take advantage of the automation it can offer. "They don't have a lot of resources and typically technology and automation of some tasks would enable them to keep that low level of resources and still be able to do at least adequate security."

One particular area where automation can help is compliance; there are a slew of tools that gather, analyze and report on compliance activities holistically instead of doing each activity individually, Kark says.

Arya at Investors Savings Bank says his firm's regulatory requirements include FDIC, SOX, GLBA, and state rules, making compliance a huge task. He's evaluating a tool that would provide automatic compliance reports.

"To comply with all the different regulations, you need to understand them and understand how they affect customers and the business," he says. "An automated tool makes it easier to set a preset model, feed the data into it and it provides reports, which makes the auditors happy."

The governance, risk and compliance (GRC) tools he's looking at don't

come cheap; they range in price from $20,000 to $100,000. Depending on what a firm wants to achieve, spending $30,000 on a product to automate compliance makes sense if it means it doesn't have to hire additional personnel, Arya says.

For Cimarex Energy, a tool from Guardium provides automated database security monitoring that goes beyond the ability of a human. The Denver-based independent oil and gas exploration and production company, which counts about 850 employees, has an ERP application that processes about a million database transactions an hour.

"At that rate, there's no way you could have a human doing any kind of monitoring," says Ann Auerbach, manager of IT compliance at Cimarex. "Auditors always ask how you know the IT staff isn't going in at night and changing the data…Without the tool, I don't know how we would prove to the auditors that unauthorized transactions were not entered into the database."

The tool also helps IT staff at Cimarex locate problems such as infected PCs by tracking unusual activity such as invalid database logins, she adds.

NETWORK SECURITY

All-in-One Security

UTMS CAN STREAMLINE SECURITY BUT AREN'T A CURE-ALL.

FOR MIDSIZE BUSINESSES without a staff devoted to security, unified threat management (UTM) devices can be a good option. These products combine security functions such as antivirus, intrusion detection and firewall protection, forming something of a security Swiss Army knife.

"It's less costly to manage and it usually has a single interface, so there's less training required. One person can manage it," says Jay Arya, a vice president and information security officer at Investors Savings Bank.

While an all-in-one device can streamline security, it can have its drawbacks – namely that it may not do everything well, he adds. "It may not have the correct features to enable the tight security some users may need."

A UTM is a good fit for certain situations, depending on what security problem a company is trying to solve, he says. The multi-function appliances can be helpful with certain functions, such as antivirus, anti-spyware and firewall protection. At Investors Savings Bank, a UTM from Sophos, Sophos Endpoint Security and Control, allowed it to combine those functions onto a single platform, making them more efficient and easier to manage, he says.

Tim Richardson, security products manager at IT services firm Akibia, says the power of technology has increased over time, making it possible to do more on a single device. Having a firewall, IPS and antivirus on one device is easier to manage but has the potential to complicate troubleshooting, he says.

"You have to make sure your troubleshooting tools are robust enough so whatever happens, you can pinpoint it," he says. ›

–MARCIA SAVAGE

DEPLOYMENT

One Step at a Time

PHASED APPROACH TO IT PROJECTS POPULAR IN MIDMARKET.

AN INCREASINGLY POPULAR strategy for some midsize companies is a phased approach to technology deployments, says Khalid Kark.

"They're forcing vendors to provide them with modular solutions," he says. "So identity and access management could be a multi-year project. They're asking vendors to provide a step-by-step, modular approach."

This approach allows a company to break up large projects that require a lot of time and money into chunks and periodically re-evaluate the project's status, he says. "So every year, they go back and re-evaluate where they are and where they need to go from there."

For example after the first year, a business could decide the investment is too much and hold off on taking additional steps, Kark says. "They want the flexibility to be able to change course when necessary." ›

–MARCIA SAVAGE

For Roedell at TruMark Financial Credit Union, the automation offered by security information management (SIM) technology is essential; his company uses a SIM product from TriGeo. What makes an infosecurity program effective is the ability to analyze all the security data in the environment in real time and take action, he says, adding "the only way to do that is with a SIM."

In some cases, automation doesn't have to require extra investment in technology. For example, Microsoft Excel spreadsheets can be customized and programmed to automate a lot of tasks, Meholic says.

He leveraged Excel when he automated and integrated several manual processes at the bank. User access reviews, IT risk assessments, GLBA assessments and other processes were all tediously manual, he says. He conducted a data flow examination to identify assets that interacted with confidential information; applications could then be assigned a "confidential data footprint" or CDF value. Those values are used across the various processes, so that employees don't have to start from scratch with each process and also for rating consistency. A change to a CDF is automatically made in spreadsheets for all the processes, reducing maintenance time and improving resource efficiency.

"It doesn't have to be anything really elaborate," he says. "There are a lot of things like that that can make life easier."

#3 Leveraging Existing Infrastructure

Figuring out ways to get more security from existing technology is a money-saving measure that many companies have started to consider in order to weather the recession, but the tactic can be essential for perennially resource-strapped midsize companies.

"There are so many things you can do to reduce risk by just using what you already have," says TruMark's Roedell.

For example, organizations can simply turn on the built-in port security in Cisco switches, he says, explaining that port security is critical for preventing just anyone from walking into the office and plugging in a laptop. "It doesn't cost anything but labor to turn it on," Roedell says.

Tim Richardson, security products manager at IT services firm Akibia, says the company focuses on educating customers about leveraging their technology investments in order to get the fullest benefit. Westborough,

NUMBERS

Small and Midsize Business Security Priorities

FORRESTER RESEARCH'S SURVEY OF NORTH AMERICAN AND EUROPEAN COMPANIES HIGHLIGHTS TOP ISSUES FOR SMBs.

87 percent deem data security as important

61 percent say other organizational priorities taking precedence over security is their top challenge

31 percent cite demand for specialized skills as the top driver for using a managed service

58 percent have deployed personal firewalls

19 percent plan to adopt or pilot a host intrusion prevention system this year

SOURCE: FORRESTER 1,206 respondents

Mass.-based Akibia serves a client base that is about 50 percent mid-size businesses.

Data leak prevention is one area of security that can cost a lot depending on what a company wants to achieve, but businesses can reduce their risk of data loss substantially by simply using the Transport Layer Security (TLS) encryption feature that's included in most email gateways, he says.

"Where is most of your data coming and going? That's email. Chances are the bulk is between you and partners … You probably already have a contractual relationship in place with them. You just need to make sure the email between the two organizations is encrypted," Richardson says.

"The technology is there, it's just a matter of taking time to validate it works," he adds.

With security technologies such as firewalls maturing and becoming integrated parts of the network infrastructure, companies are more willing to have one vendor provide multiple functions, says Forrester's Kark.

"Midmarket companies are a lot more open to that," he says. "Many infrastructure vendors are adding on security components and midmarket companies are more open to adding the security components as opposed to buying something new," Kark says.

IANS' Phillips says another strategy that can be effective for midsized companies is one large enterprises are using: turning vendors into partners.

"If you have an incumbent security software provider, alert them that your expectations will go up …that you will expect the best thinking from them on not just how to lock down firewalls, but how to reduce the risk exposure for the enterprise," he says. "They can be a free resource to draw upon. Their incentive is to help you because they don't want to lose your business."

And of course, organizations can reap a lot of security benefits with simple policy implementations, such as preventing users from acting as local administrators on their PCs, Roedell says. Acting as a local administrator allows an employee to install programs on a machine, which can lead to a host of security problems.

#4 Managed Services

Over the past year, Kark has seen a sharp shift towards managed security services. While the economic downturn may have accelerated this trend, managed services can be a good option for companies with limited security expertise on staff, he says.

"I'm seeing a lot more midmarket companies moving to outsourcing of security operations and services. It's pretty useful for a company that's resource constrained to hire an outsourcing company," he says. "It won't save money but what you get is a lot better protection and 24x7 support."

The biggest value from outsourced security is the expertise, which is in short supply; companies pay a premium to have that knowledge in-house, Kark says.

Arya agrees that expertise is the top benefit of a managed service, but adds that outsourcing can also eliminate hardware costs and streamline reporting.

"Midsize companies don't have all the resources to handle every single aspect of security," Arya says. "For those, managed security is not only a viable but necessary option. These companies have the tools, the resources and the expertise."

Kark says some managed security services such as firewall management, vulnerability management and antispam filtering are more mature; it's easier for a midsize company to know what it's getting with those services and their associated costs when it shops for an outsourcer.

But outsourcing doesn't mean entirely hands-off. Vendor management is important, Meholic says.

"It's pretty useful for a company that's resource constrained to hire an outsourcing company. It won't save money but what you get is a lot better protection and 24x7 support."

—JAY AYRA,
vice president and information security officer, Investors Savings Bank

For instance, when Republic First uses outsourcers for vulnerability assessments or penetration tests, he makes sure the way vendors rank vulnerabilities matches with the bank's criteria, he said. Vendors can have a tendency to rank the severity of a vulnerability a bit higher than an organization will, he adds.

"They are working for you, so you need to make sure you control how they do it and how they report it," he says.

Other midsize organizations prefer to rely on their in-house expertise. Cimarex's Auerbach says the firm is very selective when it comes to outside vendors for IT projects; preferring to use the knowledge of its 40-member team of seasoned IT professionals. The small size of the team also facilitates cooperation, and makes it easy for employees to pick up the phone and call a colleague to analyze potential problems.

"If it looks like we're getting a lot of unsuccessful login attempts, it's easy to respond because we have such a small group," she says. "You can

easily pick up the phone and ask, 'Can you take a look at this?' and get to the root cause in very short amount of time."

#5 Security Awareness

No matter a company's size, training employees about information security is critical. The human element is by far the biggest risk in an organization, says Mike Helinsky, director of information technology operations at Brooks Health System in Jacksonville, Fla.

"The person who leaves their user name and password on a sticky note attached to their monitor…That is by far the weakest link in the entire security spectrum," he says.

For midsize companies, it's particularly important to educate not just the rank and file about security but also executive management, Kark says. The recession—which can increase the potential for insider misuse of systems but also lead businesses to take on more risk to save money—makes this education more critical, he says.

He's seen several cases in which those in charge of security at midsize companies have made convincing arguments to executive management about the need for security by pointing out the costs of a breach and how they could potentially put the company out of business.

One of Arya's first steps when he took the security leadership role at Investors Savings Bank was to roll out an online security awareness tool for employees. Awareness is key for all users, no matter their position, he says.

"These days, in any business, if everyone doesn't get involved, security is not going to work," he says.

Republic First puts a priority on security awareness training for employees as well as its customers, Meholic says, noting that the federal Red Flag rules require financial institutions to provide security training for employees and customers.

Moving forward, though, he'll have more help in securing the organization. Late last year, Pennsylvania Commerce Bancorp acquired Republic First Bancorp, the holding company for Republic First Bank. The newly merged company will be called Metro Bancorp, and counts more than 1,200 employees. Meholic expects it will have a staff for information security. While the basics of his job will remain the same, there will be some challenges, he says.

The first challenge will be making sure the bank's established infosecurity program meets the needs of the new, more complex environment, Meholic says. To that end, the infosecurity team's main focus will be identifying any deficiencies and developing new policies and processes to address them. The next challenge will be to have a well-defined role for the team.

"Once established and integrated with the other departments of the bank, performing information security related tasks should be easier," Meholic says.

Marcia Savage is features editor at Information Security. *Send your comments on this article to feedback@infosecuritymag.com.*

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.

It's Everybody's Web

How much information is too much information, and how will you monitor and manage the use of Web 2.0 inside your organization?

BY MICHAEL S. MIMOSO

YOU DON'T WANT to become the Pete Hoekstra of your company.

Not that Pete's a bad guy. In fact, Rep. Hoekstra of Michigan has a distinguished legacy of service in politics and business, including a 2004 appointment as chairman of the House Permanent Select Committee on Intelligence, where he is the ranking Republican and still leads oversight on intelligence issues. He's a connected guy.

And that's his problem.

Early in February, Hoekstra flew into Iraq as part of a Congressional delegation's trip there, and to Afghanistan. Upon his arrival, he posted to his Twitter page that he'd just landed in the Iraqi capital of Baghdad and was stunned he had BlackBerry service for the first time in his 11 trips to Iraq. He later made posts about moving through the "Green Zone" via helicopter to the U.S. Embassy.

So much for what was supposed to be a secret trip, and so much for keeping the sanctity of the delegation's itinerary. Hoekstra has close to 3,500 Twitter followers, and theoretically, each one knew of, and could share, his whereabouts in an instant.

Such is the viral nature of social networking, and a prime example of the risk to sensitive corporate and private information presented by, what is for many, today's primary means of small talk.

Tweeting, for instance, is becoming part of the professional lexicon, whether you work in the public or private sector. People are ever more connected socially via networks such as Twitter, LinkedIn, Facebook and countless others. People who Twitter in their personal lives, for example, also tend to bring those 140-character Tweets into their professional lives, and the line can become blurred as to how much information becomes too much information.

Paranoia? Not really.

Take LinkedIn, for example. LinkedIn, for the uninitiated, is a professional networking service, a place where people are able to make business contacts, join others in similar industries in informal information-sharing groups, and ferret out new job prospects. It's also a haven for mining competitive intelligence. Threats expert Lenny Zeltser wrote recently for the SANS Internet Storm Center that attackers are checking out company profiles for title changes that would indicate strategy or organizational shifts. New hires show up on company profiles too; they're fresh meat for attackers because newbies aren't up to speed on company policy or security culture. Sophisticated attackers can also map organizations via these profiles in order to target attacks.

Web 2.0 has radically messed with the way information and even marketing material is disseminated and consumed.

Web 2.0 has radically messed with the way information and even marketing material is disseminated and consumed. Twits (the affectionate nickname for folks on Twitter) scooped CNN.com on the January crash of USAir flight 1549 into the Hudson River. Blogs, RSS feeds and Craigslist have pushed newspapers and their day-old analysis of news to the brink of extinction. Many companies are building their brands via social networking, going as far as disseminating press releases and product announcements via Web 2.0.

It's an immediacy not even email can offer. But like any business implement, there must be controls and finding a happy security balance between policy and technology is tricky. Banning social networking—and by extension, Web 2.0—in the enterprise is akin, as expert Marcus Ranum likes to say, to complaining after a horse has left an unlocked barn. The next-generation workforce has Web 2.0 neatly packed away in their backpacks and intends to use it at their desks; it's up to the security industry to work with business management to contain the threat of its side effects: information leakage, malware infestations and productivity drain.

MALWARE AND DATA LEAKAGE ARE SERIOUS RISKS

User generated content is what separates today's Web 2.0 from yesterday's online experience. People love to share the most innocuous things with their online friends, download silly applications and manage what they believe to be their private space on the Internet. The companion truth is that attackers have followed their prey to social networking platforms, and are laying down phishing snares, infecting machines with ad-generating software and logging keystrokes.

In the business world, the dangers to corporate secrets are growing. As business embraces these new mediums, the odds grow that someone could inadvertently spill secrets on a blog or collaboration portal, or follow links in a Facebook app to a phishing or malware site and either lose personal information or afford an attacker unfettered access to a corporate network.

"In the old days, you put up content on a website and people can browse it. Hopefully, the website is under the control of one party and it's easier to inspect content and make sure it's legitimate," says Chenxi Wang, principal analyst at Forrester Research. "Now with social networking, you're involving a large number of parties who are all uploading content; it's very difficult to attain the same level of assurance."

WORKAROUNDS

You're the Last to Know

USERS ARE AHEAD OF IT WHEN IT COMES TO SIDE-STEPPING WEB 2.0 RESTRICTIONS.

DO YOU REALLY know the extent of what Web 2.0 sites are visited, or what tools are being installed on machines in your network? Your perception is probably counter to reality.

While more organizations are making a business case for the capabilities found in Web 2.0 applications, users for the most part aren't waiting for you to iron out your acceptable usage policies or lay out a list of permitted apps. They're forging ahead and using and installing a glut of Web 2.0 tools and applications such as peer-to-peer file sharing, Web conferencing and anonymiziers such as Tor, in addition to downloading user-generated applications from Facebook, MySpace and LinkedIn. These end-arounds are increasingly exposing companies to data loss and malware infections.

Face Time Communications recently asked IT and security managers at more than 80 enterprises how many and which Web 2.0 apps they believed were running in their networks. Their estimates are far lower than reality. For example: 60 percent believed users were actively doing social networking; 54 percent thought P2P apps were installed and 15 percent were confident of the presence of anonymizers; when in fact there was 100 percent, or close to it, penetration of all of these tools and more, including Internet Protocol TV (IPTV), which streams mainstream television programming.

"Hackers are following people, and moving to Web 2.0," says Face Time VP of product marketing Frank Cabri. "Threats are moving in parallel."

And even when IT puts barriers in place–sites are blocked or restricted, or size limits put on email files–users find other ways around them with the use of anonymizers or proxy servers such as Ultrasurf that bypass the corporate networks and policies banning visits to certain sites. Users wanting to move restricted data off a network can upload their hard drives to a Web-based storage service such as Dropbox or Megaupload. These services also support encryption.

"The problem is, IT is always the last one to know," says Palo Alto Networks VP of marketing Steve Mullaney. "The lack of visibility is the problem. You think you're stopping things by blocking MySpace, but younger people especially are going to be stopped for about two seconds. They're going to fire up Ultrasurf or use some encrypted proxy avoidance app that lets you do what you want." ▸

–MICHAEL S. MIMOSO

Wang says companies are getting less Draconian about social networking use inside the firewall. If there is a business purpose, it is allowed, even if it is restricted somewhat; it's also a useful in helping attracting younger workers. She points out that in some heavily regulated industries, such as financial services and health care where communication must be logged, policies are stricter on content that leaves over the Web. Webmail, such as Gmail and Yahoo, is a concern there, as are peer-to-peer file sharing resources and online storage containers such as Megaupload; knowledge workers could use these resources to circumvent policies on what types and how documents are allowed to leave the network *(see "You're the Last to Know," p. 37)*.

"I think companies need to be judicious about Web 2.0 adoption and usage; don't use anything the business doesn't call for," Wang says. "Really take a close look at the security treatment of new technology and whether it opens you to risk and whether you're prepared to handle or accept it."

Jamie Gesswein wasn't willing to accept the risks that accompany social networking—not entirely any way. Gesswein, network security engineer for Children's Hospital of The King's Daughters in Norfolk, Va., says only a handful of public relations and marketing employees have access to social networking sites; the business case being that they need such access to monitor blogs and the like for mentions of the hospital.

"The biggest concerns were downloading malware and data leakage too," Gesswein says. Hospital staff aren't the only people with Internet access at the hospital; its young patients are allowed to bring in their laptops and access the Net via a guest wireless network. But even then, MySpace, Facebook and the like are blocked.

"We get a lot of calls from nurses and administrators asking us to allow access to kids to Facebook and MySpace, but we've stuck to our guns and not allowed it," Gesswein says. "I don't need a 7-year-old in the hospital accessing MySpace."

> "We get a lot of calls from nurses and administrators asking us to allow access to kids to Facebook and MySpace…I don't need a 7-year-old in the hospital accessing MySpace."
>
> —JAMIE GESSWEIN
> network security engineer, Children's Hospital of The King's Daughters

Organizations need to train users about which of their actions online pose the biggest risks.

"Don't click on links in Facebook, or on wikis or blogs," says Tim Roddy, senior director of product marketing at McAfee. "There's a real danger is you don't know who posted the content there. Most organizations have data security policies, but those need to be updated to include whether you can use web-based email to send information, or you can post to a blog. It's an awareness issue for employees because most data leakage isn't deliberate. Look at what's being posted; people shouldn't be blogging about their company—period."

A bigger driver is federal and industry regulation; for Children's Hospital of the King's Daughters, it's HIPAA compliance. With stringent watch on patient privacy in the health care industry, compliance helps drive the message home to upper manage-

ment of the importance of data protection and get their backing to shut down as many egress points as possible.

Still, deny-by-default isn't going to work forever. *Information Security*'s annual Priorities 2009 survey tends to back up this trend. More than 660 responded to a question about social networking, and 42 percent say they ban it entirely. Of the 58 percent that don't, only 9 percent said they allowed unrestricted access *(see "Banned," below)*.

"In general, things are loosening up," Forrester's Wang says. "More people are saying it's useful for business purposes. And more people are allowing them to attract younger workers. It really depends on the company culture."

Clearly, a mix of technology and policy is the most sensible road to travel for many companies. Web security gateways that address not only antimalware, but URL and content filtering are being turned on social networking sites in order to catch private data such as credit card or Social Security numbers, or certain keywords that would indicate a corporate secret could be heading through the pipes onto the Web.

"The better weapon is to have the technology in place, but without policy, it would be moot," says Gesswein, who has a Sophos WS 1000 Web appliance installed on the hospital's network. The appliance, and others like it, inspects inbound and outbound traffic and compares it to policy, allows granular control over Web content and also includes an anonymizing proxy detection technology that sniffs out proxy servers more savvy users could use to sneak out confidential data through, for example, personal webmail accounts. "We have the ability to show the management what is going on in the network, what is being protected and how."

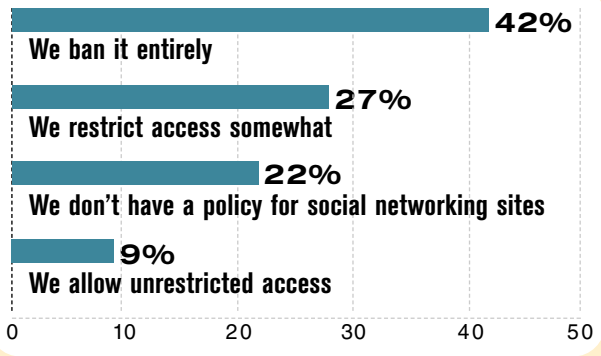
SOCIAL NETWORKING POLICIES

Banned?

DOES YOUR COMPANY HAVE A POLICY FOR THE USE OF SOCIAL NETWORKING SITES?

Q

Which best describes your policy for the use of social networking sites, e.g., Facebook and MySpace, for business?



SOURCE: *Information Security*'s Priorities 2009 Survey; 662 respondents

Gesswein struggles with that balance of providing access and enforcing policy. Doctors, like others in many industries, can collaborate online with peers via social networking sites. Medical collaboration sites and message boards, blogs and wikis are invaluable tools in speeding up patient care. Gesswein acknowledges that more staff members are also accessing information via personal devices such as BlackBerries and iPhones.

"The hardest thing is to have to keep telling myself that there has to be a balance. In a perfect world as a security person, everything is blocked, nothing is allowed. But in reality, we have to make money to stay alive. In order for them to make that money more efficiently, they need this technology in place, have access to information and be able to send and receive and talk to people more effectively. That balance between security and giving them this ability is tough. If you have to have this type of access and technology, let me work with you to figure out how I can protect the information and also at the same time, get you what you want."

MONITOR OUTBOUND CONTENT

Web 2.0 security isn't just about social networking and leaking secrets inadvertently on a blog post. Online productivity suites such as those afforded by Google apps are attractive no-cost options for organizations seeking free email, word processing, spreadsheets and document-sharing capabilities. Problems arise on these platforms from the lack of oversight, especially when they're used departmentally, or even by select individuals on a project.

Greenhill & Co., a small investment banking firm in New York, needed to get a handle on users accessing and moving documents on webmail services such as Gmail, Hotmail and others. John Shaffer, vice president of IT, says Sarbanes-Oxley auditors were looking at this risk and how it was being mitigated. Worse, he didn't want to see documents such as compensation spreadsheets leaking outside his organization via Gmail or Google docs.

While Gmail and Google docs are free applications, enterprise versions provide some management and security capabilities that enterprises could use to rein in users via policy controls.

"We had two choices: capture HTTP mail, or block it. We blocked it as opposed to archiving external email," Shaffer says, adding that users were hurdling port-blocking firewalls by using SSL. The organization moved in Palo Alto Networks' PA series firewalls that consolidated threat protection and content filtering into one box. Shaffer had the visibility he needed to satisfy auditors and learn exactly what users were up to, especially over Gmail. He could also then set blocking policies per user via Active Directory.

"Data leakage was a big concern. We wanted to make sure people were not attaching spreadsheets," Shaffer says. "There are a number of ways to get data out of a network. We're at least making a best effort to get out to some. When we get audited and go through the whole Sarbanes-Oxley process, that's one of the things they're looking at."

While Gmail and Google docs are free applications, enterprise versions provide some management and security capabilities that enterprises could use to rein in users via policy controls.

"If we are talking about a vendor that is providing collaboration services for corporations, you have to expect a very stringent policy control interface for me to say this type of document can be shared to this group, but not outside. Or, this document lives on a server for this long, but then is deleted," says Wang. "I haven't seen a lot of collaboration sites that offer this type of elaborate policy control interface to users. People like Google have to work on it. If they are trying to break into the enterprise, policy control is important."

Wang acknowledges that monitoring outbound content is difficult, but sees that trend spiking in a positive direction as more content security vendors acquire data leak prevention tools.

"There's a lot more going on around outbound data filtering," Wang says. "In the old days, it was all about filtering inbound email. Today, content filtering and webmail filtering is taking on more of a business context. We want to look at outbound content; what kind of mail you're sending out, attachments too, as well as Facebook and MySpace and what you're posting there. A lot of secure Web gateways have primitive abilities to recognize structured data. They're not as sophisticated enough to block corporate secrets, for example. That's in a fairly early stage. But that's the direction vendors are working hard toward."

The good news is that, yes, vendors and CISOs are looking at Web 2.0 security and the consequences of user behaviors online. Social networking presents security and productivity issues that run counter to growing business uses for these tools. Enterprises see a marketing value in Web 2.0 outlets such as Facebook, Twitter and LinkedIn. Younger people entering the workforce are used to having these sites and this kind of connectivity at their disposal, and expect it as part of their professional existence.

CISOs, as with any new online phenomenon, have to find that precious balance between security and productivity. Risk must be offset with a mix of policy and technology, and users must be educated so that important information isn't inadvertently leaked online and the next Pete Hoekstra doesn't work within your company's four walls.

Michael S. Mimoso is Editor of Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

Security Topics Tailored to Your Needs

You rely on *Information Security* magazine every month for original, in-depth information and analysis on the security of your enterprise. But as you know, to secure your data and network you need to be well informed every day. Stop scouring the web; become a member of SearchSecurity.com and receive tailored messaging delivered right to your inbox with the latest news, current threats, expert advice, white papers, webcasts, and much more on the security topics that YOU select including:

Network Security
Intrusion Defense
Identity and Access Management
Email Security
Web Security
Current Threats
Application Security
Compliance
Security Management
Platform Security

Stay informed 24/7. Activate your free SearchSecurity.com membership at www.SearchSecurity.com/join today.

SearchSecurity.com
The Web's best security-specific information resource for enterprise IT professionals

CHOOSING THE RIGHT WEB APPLICATION FIREWALL

PCI DSS is requiring companies to buy Web application firewalls. We'll show you how to pick the WAF that's right for you, and how to use it so your company is compliant–and more secure.

BY MICHAEL COBB

ENTERPRISES RUSHING to meet PCI DSS compliance requirements may find themselves in a quandary when it comes to choosing a Web application firewall (WAF).

How do you know what to look for? How do you deploy and manage the appliance or software effectively? How do you fit it into your existing infrastructure? We'll highlight the key considerations when evaluating products so your company is in compliance.

A Web application firewall or application-layer firewall is an appliance or software designed to protect web applications against attacks and data leakage. It sits between a Web client and a Web server, analyzing application layer messages for violations in the programmed security policy. Web application firewalls address different security issues than network firewalls and intrusion detection/prevention systems, which are designed to defend the perimeter of a network. But before you rush to buy, you'll need to understand that this is not a plug-and-play

check box compliance item and requires more than just putting an appliance in front of your application servers.

What You Need to Know

Whenever new legislation or security requirements are introduced, those tasked with ensuring compliance often tend to rush the decision-making process. Many system administrators base their decision on a single vendor's sales pitch or a particular requirement or feature they've picked up on.

The result, more than likely, will be inappropriate or less than optimal security. Even a tight deadline doesn't absolve you of due diligence. To choose a security device such as a Web application firewall, you need to answer the following questions:

- What does it need to do based on your security policy objectives and legislative requirements?
- What additional services would be valuable?
- How will it fit into your existing network—do you have the in-house skills to use it correctly and effectively?
- How will it affect existing services and users and at what cost?

New compliance requirements such as PCI DSS require you to update or at least review your security policy before you can answer the first question. A good security policy defines your objectives and requirements for securing your data. That foundation allows you to define what security devices are appropriate to meet your requirements. Since each Web application is unique, security must be custom-tailored to protect against the potential threats identified during the threat modeling phase of your secure lifecycle development program. Review which of these threats the WAFs under consideration safeguard against—such as analyzing parameters passed via cookies or URLs and providing defenses against all of the OWASP Top Ten application vulnerabilities—as well as any additional requirements mandated for compliance.

Since each Web application is unique, security must be custom-tailored to protect against the potential threats identified during the threat modeling phase of your secure lifecycle development program.

Choosing Your WAF

To ensure a WAF is suitable for PCI DSS compliance purposes you should compare its capabilities with those recommended in the *"Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified"* [https://www.pcisecuritystandards.org/pdfs/infosupp_6_6_applicationfirewalls_codereviews.pdf] issued by the PCI Security Standards Council.

They must be able to inspect and handle Web page content such as HTML, Dynamic HTML (DHTML), and cascading style sheets (CSS), as well as the protocols that your application uses, such as HTTP and HTTPS.

Also, check how quickly the vendor has adopted new protocols in the past.

TECHNICAL TIPS

Choosing a Web Application Firewall

FOLLOW THESE BASIC STEPS IN SELECTING THE APPROPRIATE WAF FOR YOU APPLICATION:

1. **Use** security policy objectives to define what controls your WAF must have.
2. **Review** the types of risk each product covers.
3. **Test** performance and scalability.
4. **Evaluate** the vendor's technical support.
5. **Assess** whether you have the required in-house skills to maintain and manage it.
6. **Balance** security, throughput, and overall cost.

Review their development and support policy to determine if they will support custom protocols or protect a set range of application protocols. In addition, a WAF must be able to inspect Web services messages, typically SOAP and XML. Ask the WAF vendor about their processes for auto-updating and applying dynamic signatures. Such conversations will help you assess their technical support and help services.

Lastly, ask about the additional cost of specific features. For example, some applications may require FIPS hardware key store support. A WAF vendor may support this requirement but at a dramatically higher price.

As you work through the list of requirements, take the time to understand the technical approaches and depth of treatment that each WAF uses to provide coverage of one or more security areas. Can you white list data types and ranges and create rules combining both white and black lists? How strong is the WAF against attack on itself? For example, it should run on a hardened OS, probably with components running in a non-privileged and closed runtime environment. If the product's security isn't rock solid, you should probably end the discussion right there.

Software vs. Hardware

The PCI Information Supplement states that a WAF can be implemented in software on a standard server running a common operating system or an appliance. It may be a stand-alone device or integrated into other network components. So, you can choose from the full range of WAFs on the market.

Software WAFs are usually cheaper and more flexible. Appliances are typically easier to install and configure, partly because their operating system has already been hardened, whereas a software firewall will require you to harden it. (A WAF won't protect you against poor configurations or vulnerabilities in your servers.)

If you opt for a software-based product, choose one that works on a platform with which your IT department is familiar. Either way, check out what type of training and support is provided by the firewall vendor—and at what cost.

There are, of course, open source software WAFs, such as ModSecurity [http://modsecurity.org] and AQTRONIX WebKnight [http://www.aqtronix.com]. If they meet your requirements you can greatly reduce your costs, but you will still need staff to learn, install, configure, and maintain it. Many open source projects have excellent support forums but unlike a purchased product you won't be able to call a help desk in an emergency.

Performance and scalability are other important considerations when evaluating hardware or software options. Some devices may be limited as to how many transac-

tions per hour it can handle. Other appliances may have bandwidth limitations. You will need to choose a scalable and flexible firewall if you're planning on increased Web activity or adding applications in the near future.

Software products often provide an easier upgrade path than appliances, but hardware WAFs are better suited for high-volume sites, which require high throughput.

If you are running a large-scale application, which requires more than one WAF, then centralized management may be a critical feature so firewall policies can be deployed and managed from a single location.

Our advice is not to get hung up on whether the WAF is hardware or software, as long as it can meets your objectives and you have the in-house skills to configure and manage it.

Help is on Hand

Plan on devoting plenty of time to fully evaluate WAF products. Once you have narrowed down your choices to those that meet your basic requirements, how do you compare the different options?

The Web Application Security Consortium (WASC) [http://www.webappsec.org/] creates and advocates standards for Web application security. They have developed the Web Application Firewall Evaluation Criteria (WAFEC) [http://www.webappsec.org/projects/wafec/] for comparisons. Their testing methodology can be used by any reasonably skilled technician to independently assess the quality of a WAF solution.

APPLICATION ASSURANCE

What's Next?

WEB APPLICATION FIREWALLS ARE JUST THE START.

INCREASING SOPHISTICATION OF application attacks, the protection offered by WAFs should be integrated into application assurance platforms. This structure, promoted by vendors such as F5 and Barracuda, combines WAFs, database security, XML security gateways and application traffic management to provide more holistic security coverage.

The benefits include the ability to compare information across these devices to accurately determine if traffic is potentially malicious. This makes traffic control, analysis and reporting far more effective. Administrators can configure one set of policy rules and parameters, rather than trying to enforce each policy across several different devices, greatly reducing administrative overhead.

Looking into the future, it is essential that WAFs or whatever supercedes them gain the ability to interpret inbound data the same way as the application it is protecting. This will entail some form of script engine to remove any obfuscation, so that the security device will view the request in the same form that the browser will. This will make it far easier to assess whether or not the code is malicious. Let's hope we will see this form of dynamic analysis in the next generation of security devices. ›

–MICHAEL COBB

Use their criteria as part of your evaluation process. Follow WASC's recommendation to pay close attention to the deployment architecture used, support for HTTP, HTML and XML, detection and protection techniques employed, logging and reporting capabilities, and management and performance.

WAF Deployment

Congratulations, you've chosen, purchased and installed a WAF with the necessary compliance capabilities. But that doesn't mean that you're compliant. Proper positioning, configuration, administration and monitoring are essential.

Installation needs to follow the four-step security lifecycle: Secure, monitor, test and improve. This is a continuous process that loops back on itself in a persistent cycle of protection. Before any device is connected to your network, you need to ensure that you have documented the network infrastructure and hardened the device or the box it will run on. This means applying patches as well as taking the time to configure the device for increased security.

Configuration will stem directly from the business rules that you've established in your security policy (such as allowed character sets). If you approach firewall configuration this way, the rules and filters will define themselves. WAFs can expose technical problems within a network or application, such as false positive alerts or traffic bottlenecks.

Careful testing is essential, particularly if your site makes use of unusual headers, URLs or cookies, or specific content that does not conform to Web standards. Extra testing time should be allowed if you are running multi-language versions of your application, as it may have to handle different character sets.

The testing should match the "live" application environment as closely as possible. This will help expose any system integration issues the WAF may cause prior to deployment. Stress testing the WAF using tools with Microsoft's Web Application Stress and Capacity Analysis Tools or AppPerfect Load Tester will also help reveal any bottlenecks caused by the positioning of the WAF.

WAF Management

Once you're up and running, assess how any future Web application firewall changes may impact your Web applications, and vice versa. You must, of course, document the changes you make to your network infrastructure for future reference and troubleshooting. This involves tracking any changes made to their configuration now and in the future.

Changes to the production environment should always occur during a monitored maintenance window. Make sure all affected parties throughout the organization are advised in advance of the timing and scope of the changes. To ensure that configurations aren't changed unintentionally or without due process, you must control physical as well as logical access to your security devices. Strict adherence to change control, business continuity, and disaster recovery policies will all play a part in protecting the WAF and your business.

Because application-layer firewalls examine the entire network packet rather than just the network addresses and ports, they have more extensive logging capabilities and can record application-specific commands. So, don't let this capability and infor-

mation go to waste. Log file analysis can warn you of impending or current attacks. Ensure that you define what information you want your firewall to log—preferably the full request and response data, including headers and body payloads. Make sure your staff have the expertise—and adequate time—to review and analyze it.

Web applications will never be 100 percent secure. Even without internal pressures to deploy Web applications quickly, there will be vulnerabilities that are open to threats. By having a Web application firewall in place as part of a layered security model, you can observe, monitor and look for signs of intrusion. It can also mean the difference between scrambling to fix a vulnerability or having the breathing room to repair the vulnerability to your own timetable. ›

Michael Cobb, CISSP-ISSAP, is the founder and managing director of Cobweb Applications Ltd., a consultancy that offers IT training and support in data security and analysis. He co-authored the book IIS Security *and has written numerous technical articles for leading IT publications. Cobb is the guest instructor for SearchSecurity.com's Messaging Security School and, as a SearchSecurity.com site expert, answers user questions on application security and platform security. Send comments on this article to feedback@infosecuritymag.com.*

PRIMER

PCI DSS 101

HERE ARE THE REQUIREMENTS AND SOME GOTCHAS.

The Payment Card Industry Data Security Standard (PCI DSS) was developed by the PCI Security Standards Council, an open forum launched in 2006. The council is part of PCI, a joint industry organization set up by a group of the major credit card companies, and is responsible for the ongoing development, management, education, and awareness of the PCI DSS.

However, it doesn't enforce the PCI DSS, nor does it set the penalties for any violations. Enforcement is left to the specific credit card companies and acquirers. PCI DSS does not replace individual credit card company's compliance programs but has been incorporated as the technical requirements for data security compliance. The PCI DSS must be met by all merchants that accept credit and debit cards issued by the major credit card companies.

Under the PCI DSS, an organization must be able to assure their customers that their credit card data, account information, and transaction information is safe from hackers or any malicious system intrusion by adopting various specific measures to ensure data security. These include building and maintaining a secure IT network, protecting cardholder data and maintaining a vulnerability management program and information security policy.

The standard's compliance requirements are ranked in four levels, and the level of compliance required of a merchant is based upon the annual volume of payment card transactions it processes. Level 1, the highest level, can also be imposed on organizations that have been attacked or are otherwise deemed as high risk. A single violation of any of the requirements can trigger an overall non-compliant status, resulting in fines, and, possibly, suspension or revocation of card processing privileges until the merchant is PCI compliant.

For more details, visit the PCI Security Standards Council Web site [https://www.pcisecuritystandards.org/]. ›

—Michael Cobb

ADVERTISING INDEX

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.