INFORMATION SECURITY®

ESSENTIAL GUIDE TO THREAT MANAGEMENT

Your organizations are under attack from organized groups that are after the lifeblood of your company. We'll identify those attack vectors and tell you how to best secure your critical digital assets.

INSIDE

TechTarget
The Technology Media
ROI Experts

INFOSECURITYMAG.COM

Let them
roam
lose laptops
surf
audit
cut budgets

contents

ESSENTIAL GUIDE

THREAT MANAGEMENT

FEATURES

Beware the APT Hype Machine

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

BY MICHAEL S. MIMOSO

Vendor FUD is sure to follow China's advanced persistent attacks against Google; be discerning.

THE SECURITY INDUSTRY is filthy with acronyms, and most of them confuse and trivialize what they stand for.

APT, or advanced persistent threat, is the latest to poison our lexicon. Since China's attacks against Google and more than 30 other high tech and large enterprises were reported in January, experts and vendors have been going on about it and the FUD machine is revving up. Soon security companies will be marketing products around it. But you need to be discerning about APT and understand that this isn't about the attack per se, but more about the perpetrators.

APT isn't anything more than a sustained attack on an entity by a well-funded criminal or state-sponsored organization. These criminal or political entities have smart programmers at their disposal who use a blend of social engineering and malware including zero-day exploits to penetrate a company's defenses and quietly poke around.

It's a real threat, but not a radically new threat. And it's not something the can be countered with a shiny new 1U rack of the latest anti-x security defenses. But that's not going to stop the marketing machines of the leading security companies from hitching a ride aboard the APT bandwagon. Like compliance before it, you will soon have vendors promising that their solutions will head APT off at the pass. This is going to be the next disservice done to information security decision makers because executives are bound to ask silly questions such as whether APT can infect their precious BlackBerry.

You'd better have an informed answer because this one isn't going to go away.

The good thing about this is that Google was forthcoming about some details and was especially willing to point the finger at the Chinese. The attackers exploited a zero-day vulnerability in Internet Explorer 6 to gain access to Google's infrastructure in an attempt to access Gmail accounts of Chinese political activists. Malicious PDFs were used as well to launch attacks on more than 30 other IT and large American corporations, including big financial firms and defense contractors. There have been whispers that the Chinese had people on the inside at Google who helped facilitate the attacks. There have also been whispers that this is an act of cyberterrorism or cyberwar, but it's not. Let's get this out of the way right now: China's attacks on Google were espionage. Not cyberwar. Not cyberterrorism. Not even cyberbullying. They stole stuff—high value intellectual property.

APT, or espionage, shouldn't be news to you if you're Google, the military, the government, a manufacturer such as Boeing or Shell Oil, or if you run a large utility. You're being probed all the time and the dark dirty secret is that your secrets aren't secrets any more. Rival companies can employ APT to steal your secret sauce the same way foreign enemies can use it to steal jet fighter blueprints. But remember, APT isn't about the attack, but the attacker.

The only counter is a well thought-out security program, one that includes a thoughtful CISO at the top, detailed policies and processes acting as your framework, regular assessments of your assets and prioritized remediation of any problems. Your program has to be a living entity, not a regularly scheduled exercise; react when you have to, and always do your best to be proactive. Talk to executives about threats, but make it a realistic conversation. Talk about your business in plain English. Don't talk in acronyms such as APT; instead use terms they can relate to such as espionage. And explain the man-hours it would take to re-engineer your secret sauce from scratch if they don't support your well thought-out security program. Use facts instead of FUD.

And when Symantec, Cisco, and every other company that sells security widgets comes knocking on your door, remember, nothing they promise you will put APT out of business. ›

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

NEW WEB, NEW THREATS

The collaborative nature of Web 2.0 introduces myriad threats to data that must be proactively countered.

BY DAVID SHERRY

THERE IS AN old Chinese proverb that reads "may you live in interesting times." For security professionals, this does not ring hollow because a security career is always evolving and responding to emerging threats; "interesting" is our daily mission.

While our charge is broad, from architecture and policy, through awareness and compliance, much of what we do is defending against threats to the security of the information we protect. As the proverb tells us, this is where the interesting portion of our role gets defined. We have witnessed the evolution of threats migrate from attacking the vulnerabilities of the Web, through the weaknesses of messaging, on to data protection, and now into the realm of Web 2.0.

What exactly is Web 2.0? You would find myriad answers to this if you asked all of your security (and non-security) friends. It is the Internet as we now know it, and is known as the second generation of the World Wide Web. Web 2.0 refers to Web design, development and use that foster interactive information sharing, interoperability and collaboration on and via the Internet. Examples include Web-based communities, Web applications, social-networking sites, video-sharing sites, wikis, and blogs. A Web 2.0 site allows users to interact with other users, or even change website content, in contrast to non-interactive websites where users are limited to the passive viewing of information that is served to them.

With this next iteration come additional business opportunities, and security concerns. Chances are, your enterprise is either utilizing its power, or wondering how it can take advantage of it. Security needs to part of the conversation, no matter where you are in the process.

WEIGH BUSINESS NEED AGAINST WEB 2.0 RISKS

The collaborative, interactive nature of Web 2.0 has great appeal for business from a marketing and productivity point of view. Companies of all sizes and vertical markets are currently taking full advantage of social networking sites such as Facebook, Twitter and LinkedIn to connect with colleagues, peers and customers, or free online services such as webmail, Google Docs, and other collaborative platforms to share documents, best practices and message one another. "Ignore these technologies at possible business peril," says Diana Kelley, partner at Security Curve. "Not only are these technologies useful, but companies that don't adapt could well find themselves left behind the social revolution."

Companies are leveraging these sites for more than just communicating. Through Web 2.0 and social networking areas, enterprises are exchanging media, sharing documents, distributing and receiving resumes, developing and sharing custom applications, using social networks as a business strategy vehicle, leveraging open source solutions, and providing forums for customers and partners.

While all this interactivity is exciting and motivating, there is an enterprise triple threat found in Web 2.0: losses in productivity, vulnerabilities to data leaks, and inherent increased security risks.

CISOs must find the delicate balance between security and the business need for these tools, and enable their use in such a way that reduces the risk for data loss or reputational harm to the corporate brand.

I informally surveyed more than three dozen security colleagues across all verticals and found that 90 percent are concerned about these threats, and many have addressed (or are addressing) them through policy and technology. CISOs must find the delicate balance between security and the business need for these tools, and enable their use in such a way that reduces the risk for data loss or reputational harm to the corporate brand. While a sound security policy is a necessity in proactively responding to Web 2.0, policies must be enforced by technology.

The cost of dealing with a data breach continues to rise. In late January, the Ponemon Institute released its fifth annual study on the data breaches. The study reveals that the

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

average cost to an enterprise from a data breach rose from $6.65 million in 2008 to $6.75 million in 2009. In addition, the average cost per compromised record also went up to $202, from $204 the previous year.

With the increasing value to data, and the numerous conduits that it can be breached, it's no wonder that increasing regulatory mandates and constraints have been enacted. Enterprises now have a list of laws to comply with, including Gramm-Leach-Bliley, the Health Insurance Portability and Protection Act, Sarbanes Oxley, and the US Patriot Act to name just a few. Many states are also enacting stringent protection and encryption laws, such as California's SB 1386, and Massachusetts' 201 CMR 17.00, and businesses may be subject to these state-specific laws even if they are not based in either state.

The industry is starting to respond by developing and marketing standalone tools—or integrating protection into secure Web gateways, antimalware suites or UTMs—that filter for sensitive content and alert or block the action. Many have received excellent feedback, and industry analysts are quickly evaluating the tools and solutions available. One size does not fit all, however, and holistic thinking and documenting your expectations and success factors are critical.

NEW PARADIGM OF WEB 2.0 SECURITY THREATS

As with any evolution of a product or service, the old ways of performing a task or providing a solution simply may not work. This is also true in reducing and mitigating Web 2.0 threats. Time tested security solutions are no longer the key defense in guarding against attacks and data loss. Some characteristics of Web 2.0 security that are being discussed are:

- Traditional Web filtering is no longer adequate
- New protocols of AJAX, SAML, XML create problems for detection
- RSS and rich Internet applications can enter directly into networks
- Non-static Web content makes identification difficult
- High bandwidth use can hinder availability
- User-generated content is difficult to contain

Security teams must be aware of the need to address Web 2.0 threats in their desktop clients, protocols and transmissions, information sources and structures, and server weaknesses. While none of these attack vectors are new, how we respond to them may be.

Very rarely does a week go by where we do not hear news of the negative aspects of social networking sites and collaborative platforms. Whether it is violence and lawlessness, cyber-bullying and harassment, or legitimate breaches of confidential data, it is apparent that this brave new world poses risks to companies. Many of the threats that lead to confidential data loss hijack employee credentials without their knowledge. While there are obvious threats that would not surprise even the most casual user of the Internet, others are more subtle and benign, and need to be addressed in our enterprises.

Direct posting of company data to Web 2.0 technologies and communities is the most common. No vulnerability need be exploited or malicious code injected when employees (whether as part of their responsibilities or not) simply post protected or restricted information on blogs, wikis, or social networking sites. According to many security companies, the attacks on these technologies are on the rise as well, knowing that their growth and fast maturation can be a jackpot for insider information. Many of these attacks also come via malicious payloads, which are downloaded when spam and phishing scams are utilized. According to Sophos, 57% percent (an increase of more than 70% from the previous year) of people who use social networks report receiving spam and phishing messages. This number will surely continue to rise.

However, what about the risks posed by insiders who choose to utilize free webmail services, such as Gmail, Yahoo, Hotmail, and others? While allowing employees to access to these services during the workday most likely aligns with an acceptable use policy that allows "reasonable and limited personal use", the risk is what they are sending to these free mail services. They may be thinking that they are being good stewards of the company and sending data home to work on at night or over the weekend, but they are also placing the company at great risk. Not only are the transmission not encrypted, but the security of the servers may not be up to security requirements for the protection and value of the information. The data may be residing on several servers, and may not even reside in the country of origin or destination.

INCLUDE WEB 2.0 SECURITY IN ACCEPTABLE USE POLICY

Most enterprises already have a form of an acceptable use policy, which should govern the use of all resources in the enterprise computing environment. While it may be implicitly implied in your current policies that public Web 2.0 sites are covered (blogs, wikis, social networks), because of the nebulous nature of this technology, a more explicit rendering of the expectations and policies is necessary.

Critically read your current policy in a context of Web 2.0 technologies, and identify gaps that need to be addressed. For instance, because of the risks and inherent difficulty managing the use of social networking applications, many enterprises have made the decision to not allow access to social networking services and Web 2.0 powered sites from inside the corporate perimeter (often with the exception of human resources departments for recruiting purposes). This is an important decision because the information gained from these sites may be of corporate use. One security manager from a global manufacturer told me "there is no way we are going to design new ingredients for client products, and then prevent our employees from the public forums that enable us to gather the consumer experience."

> One security manager from a global manufacturer told me "there is no way we are going to design new ingredients for client products, and then prevent our employees from the public forums that enable us to gather the consumer experience."

Of greatest importance is a clear and unambiguous warning in the policy about sharing confidential corporate information. Enforcement of the policy can be made though analysis of Web logs for use during business time (if not allowed), or through automated searches of websites for corporate information. Many organizations have included Web 2.0 and data protection sections to their training on protecting corporate information. Ensure that the policy indicates the prohibitions against this, and clearly spells out the ramifications, including the levels of discipline that could occur. As always, when the acceptable use policy has been modified, ensure that all employees are made aware.

MAINTAIN YOUR TECHNICAL DEFENSES

Security success is all about combining the right combination of people, process, policy and technology. The same holds true when it comes to addressing Web 2.0 concerns. Utilizing this combination in a rapidly evolving area is difficult though. "This space is a reality and tough to fully monitor as there is a fine balance to levels of security rigidity and the inherent pervasive openness to Web 2.0", says Tim Young, vice president of information technology at Bright Horizons. Intrusion detection and intrusion prevention systems (IDS and IPS) need to be kept current to address the risks of this traffic, and bandwidth-shaping technology should be deployed in order to not only both maintain proper network speed, but also identify abuse or compromised machines.

AWARENESS

Leverage Risks to Teach Web 2.0 Security

REACH OUT TO BUSINESS UNITS TO BUILD AWARENESS AROUND WEB 2.0 THREATS.

Web 2.0 security risks may threaten confidential data, but smart security managers can also leverage them to enhance security awareness throughout an organization, and build convergence with key decision makers and leaders.

Web 2.0 and social networking are familiar terms, but may not conjure up risks to the enterprise. Many other areas of the corporation, while focusing on risk and some aspects of security, may need to be educated and consulted when creating a policy and modifying an appropriate use policy. Include senior representatives from human resources, risk management, privacy, physical security, audit, and legal in your preparations and response to these risks. A stronger partnership, and ultimately a stronger policy and process, will surely result from reaching out to them.

Establish a working group to meet periodically to discuss how this technology is emerging and evolving, and how the enterprise as a whole can address it. In addition, use formal training, newsletters, "lunch and learns," or any avenue possible to make employees aware of the proper and improper use of social networks, at work and at home.

As with many security issues and risks, a higher level of awareness points to a higher level of compliance. Use data protection as an essential teaching tool, and increase your education and awareness beyond passwords and acceptable use. Using your working group, encourage cross-functional responses for awareness, and speak with data. ›

—DAVID SHERRY

In addition, many popular Web-based social network services have an increasing number of applications available to download locally. While many are benign, a significant number of these small apps carry malicious payloads, hacking tools or marketing software. This can be combated by having a standard desktop image that does not allow local installation of applications, or changes to the registry keys or operating systems. Lastly, firewall rule sets can be granularly defined to monitor, catch or block social network traffic, and of course, always ensure that antivirus products are up to date as a last line of defense.

Finally, even with all of these controls in place, data and information will inevitably find its way to the Internet. Enterprises should remain vigilant in scouring the Internet regularly for any information that may be sensitive in nature. Using third-party reputation protection services, internal monitoring programs, or simply performing Web searches for keywords and phrases can be essential in identifying and addressing instances when company information is made available via social communities, either inadvertently or intentionally.

DATA PROTECTION VIA OUTBOUND CONTENT MANAGEMENT

There are many vendors and solutions that promise to mitigate and solve the threat of data loss in Web 2.0 environment. While this technology area has shown great promise, and continues to deliver, it is oftentimes misunderstood as a CISO reviews the morass of materials and reviews available.

A clearer definition can be simply stated as implementing an outbound content management program that reduces, mitigates, and eliminates data loss.

Data loss prevention, for example, is a solution, as well as a generic term that is an umbrella for many different technologies and strategies. Data loss can be prevented by encryption. It can also be mitigated or prevented by port blocking or content fiiltering. And there are software suites and appliances that can help in this area. Every security vendor of any size or maturity will gladly let you know of their DLP solution, and will use the term to cover just about all of their products. This doesn't make it any clearer.

A clearer definition can be simply stated as implementing an outbound content management program that reduces, mitigates, and eliminates data loss. The trick is how a company deploys systems capable of successfully detecting your highly sensitive information in the outbound mail system.

Also be aware of the types of DLP solutions, which fall into three broad categories: network based, host-based, and data identification. All three have their positives and negatives, and a CISO must remember that a performance hit will be observed on the network when a company runs any such solution inline. As with all security solutions, you need to strike a balance between speed, accuracy, and adequate coverage.

DLP solutions must be made aware of what a company lists as sensitive content if they are to be successful. Upon the sensitivity being listed, there are several ways in which the content can be identified, but first the solution must be able to open and understand numerous file types, and be able to detect content in nested and zipped documents as well.

Once the files are opened and reviewed by the solution, content analysis is begun to identify any sensitive data. Content analysis techniques include:

- Pattern-based searches using regular expressions
- Fingerprinting by searching elements of actual databases
- Exact file matching
- Statistical analysis to search for content that may resemble sensitive data, or contain pieces of it
- Document matching for complete files
- Analysis of lexicons (ex. employment opportunities, insider trading, harassment)
- Solution supplied categories, to address regulatory mandates such as HIPAA and GLBA

WEB 2.0 SECURITY STRATEGY MUST MIX TECHNOLOGY, POLICY

Security teams must be aware of the need to address Web 2.0 threats in their desktop clients, protocols and transmissions, information sources and structures, and server weaknesses. While none of these attack vectors are new, how we respond to them may be. Our enterprises ask us to eliminate malware and protect our company's data, all while allowing productivity, improving IT efficiency, and proving compliance. We should be encrypting our data and protecting our endpoints, but not hinder the process of how we do business. Add in the realities of an evolving Web and its use, and our task is a large one. The good news is, with preparation and process, we can be successful.

Our enterprises ask us to eliminate malware and protect our company's data, all while allowing productivity, improving IT efficiency, and proving compliance.

The first step is to embrace Web 2.0 and create a strategy and toolset to maximize its benefits. A CISO must proactively identify the risks, but use this information to increase awareness and inform the business of their possibility. Gone are the days of "fear, uncertainly, and doubt" because board level management now looks to security for business success.

Next, document a strategy that is based upon business objectives, and clearly indicate what to allow, what to block, and who should have access and when. New policy should be developed, or a current policy set be updated, and they should be clear and enforceable. Ensure that your policies address Web 2.0 technologies, and consider subjective policy setting, group level access, and productivity based sections to give your policy strength. Revisit your acceptable use policy, and look at it from a Web 2.0 lens, and be sure to cover new technologies such as anonymizing proxies. Include other groups for support such as HR, legal and audit.

After the policy set is in place, focus on data loss protection, and stopping any information from exiting your network before it happens. You need to protect and comply with regulatory mandates, all without disrupting the business processes. A solution that monitors, prevents, alerts, and encrypts, and quarantines as needed is necessary. Deploy a solution that is capable of stopping sensitive data from leaving via your outbound mail system. Your filtering system should analyze and act on outgoing email in real time, in order to not impact productivity, and be able to perform searches in nested and zipped files and attachments.

A DLP solution should be part of an overall, integrated security architecture that includes a vigilant anti-virus program, a robust anti-malware protection program, and the capabilities of an AJAX-aware analysis platform. In addition, make sure your browsers (and their plug-ins) are patched, and do not simply focus on the critical patches, because all vulnerabilities are targets in Web 2.0.

WEB 2.0: WITH PROGRESS COME RISKS

As with all emerging technologies, Web 2.0 and its related components are advancing rapidly, and security professionals need to remain aware of the risks and defenses associated with it. There is a generation entering the workforce ("digital natives") that assumes this technology will not only be available for their use, but is also essential to the way they communicate with colleagues and business partners. In addition, businesses are realizing the reach and depth they can achieve with a social media marketing strategy.

While there are many benefits that come with this new Web internally and externally, the policy, technology, people, and architecture to defend against the risks must be addressed proactively and not taken lightly. CISO's are the vanguard of their organizations in this regard, and through this effort, further solidify their value to the business.

Interesting times, indeed. ›

David Sherry is CISO at Brown University. Send comments on this article to feedback@infosecuritymag.com.

thawte™
it's a trust thing™

Building Trust Around The Globe

When you want to establish trusted relationships with anyone, anywhere on the internet, turn to *thawte*. Securing Web sites around the globe with:

- strong SSL encryption
- expansive browser support
- multi-lingual customer support
- recognized trust seal in 18 languages

thawte offers outstanding value on a full range of digital certificates. Secure your site today with a *thawte* SSL Certificate.

www.*thawte*.com

A Dangerous Delineation

Enterprises can no longer differentiate between insiders and external threats. That's such a 2003 paradigm.

BY MICHAEL S. MIMOSO

IF YOUR ENTERPRISE is drawing a figurative line down the middle of its network and divvying up security differently between insiders and outsiders, then honestly, you're so six years ago.

Get with it.

Outsiders are on the inside today. Customers, business partners, suppliers, contractors, and anyone else who tunnels in through your network or walks through your company's front door and has authorized access to systems or data is an insider—or is it an outsider? Either way, it doesn't really matter, the old paradigm is gone.

Get over it.

"Where the attack comes from is irrelevant," says blogger and senior vice president of strategy at eIQ Networks, Mike Rothman. "This idea of segmenting security defenses seems to be a marketing scheme and a very 2003 way to look at security. I always recommend to people that there is no insider. Everybody needs to be treated as an outsider. The old truism of trust-but-verify is absolutely critical."

The firewall used to be the great divide between insiders and outsiders, but third-party access over the Web has not only de-perimeterized the enterprise but forced businesses to dispense with separate defenses for each.

Problem is, not everyone has gotten the message.

IT'S ALL IN THE RISK ASSESSMENT

CISOs are probably leery of moving off the insider/outsider paradigm. Horror stories such as the fraud perpetrated by rogue trader Jerome Kerviel that cost French banking giants Societe Generale more than $7B US are enough to keep even the steeliest CISO awake at night. Yet those fears are statistically unfounded according to the acclaimed annual Verizon 2009 Data Breach Investigations Report [http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1353871,00.html].

The results come from evidence collected during data breach investigations by the Verizon Business investigative response team. The 2009 report revealed that 74 percent of breaches were caused by outsiders, while 20 percent by insiders (32 percent by business partners crossing the insider/outsider threshold). Only 22 percent of those breaches were directly related privilege misuse, while 64 percent involved hacking.

Organizations must understand that while insiders have the potential to do severe damage, those instances are few and far between. Regular and formalized risk assessments can help organizations visualize critical assets and where threats are mostly likely to cause costly damage, and prioritize security investments accordingly.

Horror stories such as the fraud perpetrated by rogue trader Jerome Kerviel that cost French banking giants Societe Generale more than $7B US are enough to keep even the steeliest CISO awake at night.

"Defining an insider is an important question," says Paul Kocher, president of Cryptography Research. "If you have a company with 10,000 employees, you know some of them are dishonest. But we've also dealt with a number of situations where there were compromises because of a failure to trust insiders; not giving the senior system administrators the privileges they need to monitor properly or not bringing in the proper people to do security reviews because there was a fear that by bringing somebody in to look at systems, that person would then know how to break them."

Privileged insiders [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1360496,00.html], those who set up and maintain critical databases, network segments and Web portals, hold a lot of power—no matter whether they're fulltime employees or contracted third parties. They configure systems, manage encryption keys and are often smart enough to quietly move sensitive data off a network. But there is a layer of trust with these people, some of whom are longtime employees who are invested in the well being of an organization. Dramatizing the risk associated with privileged insiders can be an en vogue marketing tactic you need to be wary of.

"I've never seen an intrusion as a result of a highly paid senior staff doing something wrong," Kocher says. "A lot of times you've got a situation where an ordinary user either through malice or ignorance compromises a system or enables somebody to compromise a system. In my mind, I differentiate between people trying to protect systems—they don't pose a threat despite having a lot of power."

WHO'S WATCHING THE WATCHERS?

That doesn't mean you ignore privileged insiders. It's just that your warm and fuzzy and cozy firewall, intrusion prevention system and antimalware aren't the best tools to combat the risks posed by those with privilege.

Enterprises that manage customer or financial data, or deal with intellectual property, have to rely on a mix of identity and access management (IAM) frameworks and processes such as provisioning, role-based access control, as well as database activity monitoring and a converged IAM and security information and event management system. It's about watching the watchers.

"Overall, I would say companies have done a very poor job monitoring privileged insiders," says Slavik Markovich, CTO of database security vendor Sentrigo. "A lot of times you have DBAs watching DBAs. Most companies don't have the correct tools to monitor privileged insiders. Companies are still focused on keeping outsiders out, rather than looking inside. It's a matter of time before we see companies create boundaries for insiders."

Most companies don't have the correct tools to monitor privileged insiders. Companies are still focused on keeping outsiders out, rather than looking inside.

Segregation of duties, and on occasion, even segmentation of systems, is critical to keeping privileged insiders within reach. The problem is that, especially in a recession, companies are resource-strapped and sometimes it's easier to dole out access rather than manage it properly.

"The joke is that if a person works for an organization long enough, they will eventually gain access to everything," says Ben Goodman, director of technology, Novell. "That concept that people are gaining rights and access as they go is a huge threat. Gaining too much access can break down checks and balances. If you keep accumulating access rights over time, we believe excess rights equal excess risk. If you have rights to things you don't need, it's just bringing unnecessary risk to your organization."

De-provisioning is the area where most companies fall down with trusted insiders. Not only is it important to assign roles and access as needed throughout a person's tenure with an organization and log and audit their activities, but once their responsibilities change or employment terminates, access must change or be shut off as well.

"It's one of the things organizations get banged on consistently in external audits, having legacy accounts still sitting around," Goodman says. "It's also one of the things that pose the greatest risk; intellectual property leakage, access to systems, it all comes down to not properly handling de-provisioning."

Companies at a minimum, if they haven't invested in identity management, need to look at permissions in Active Directory, for example, to look for orphaned accounts. Someone in finance who may have left the company could still have an ERP application account open, and if that account had, say, check-approval status, that open account would be enough to fail a Sarbanes-Oxley audit.

"They can't access it any more, OK, but someone may know that account is open

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

and could use those credentials to commit fraud," says Brian Cleary VP of marketing for enterprise access governance vendor Aveksa. Companies are stunned when a SOX audit finds that. Different classifications of users: super users; system admins; root-level access DBAs; all have the keys to the kingdom and need different controls because auditors are looking for shared accounts and shared passwords."

Role-based access controls, traditionally a difficult task for IT because of the diversity of roles within any organization, are becoming more critical. Experts urge organizations to grant access based on function and job role and port those roles into some kind of on-boarding framework so that regardless if an employee is a third-party temporary contractor or a fulltime employee, appropriate access is defined and consistently doled out.

The irony is that a privileged insider—a super user—is someone you trusted enough to hire or promote to give them the keys to the kingdom. Even if there is monitoring in place, chances are they set it up, or could manage a workaround.

> "Bigger companies, almost all, do background checks, especially companies that deal with sensitive data."
>
> –PAUL KOCHER, president of Cryptography Research

"It comes down to how much inefficiency you want to put in place," Kocher says. "For really large organizations, there are different problems. When you've got an administrator responsible for a particular system, a person with experience who is well compensated, all of those attributes are low risk. They're unlikely to be malicious or rogue; but you can never say never. It's inevitable you trust that individual and even put monitoring in place, but they often have the power to disable and work around those protections."

More companies, especially large enterprises, are getting better at screening potential employees before they're brought on board. That means background checks.

"Bigger companies, almost all, do background checks, especially companies that deal with sensitive data," Kocher says. "There are a number of things motivating that from liability concerns to the realization that people who lie on their resumes tend not to make particularly good employees. I've got friends who do background checks and they've been finding business is pretty good and business has not been letting up during the downturn."

Kent Anderson, managing director of consultancy Encurve and former director with PricewaterhouseCoopers, says smaller companies are terrible at background checks.

"In general, I don't see background checks done to a proper level of due diligence," Anderson says.

ONE SECURITY STACK TO SAVE THEM ALL

Outsourcing has done more to blur the lines between insiders and outsiders than anything else. Insiders, Anderson says, had certain attributes aside from fulltime employment, including authorized access to assets, knowledge of processes (and security controls) and opportunity. Classic outsiders, meanwhile, were removed from organizations, had no authorized access and limited opportunity and knowledge of processes.

The efficiencies introduced by outsourcing, coupled with the explosion of Web-based commerce and Web-based applications exchanging connections and data between disparate systems, have made traditional IT controls—set up to defend against outsiders—obsolete.

"The concept of the outsider, if it hasn't vanished, it's on its way," Anderson says.

Anderson says risk assessments lay the baseline for any development and implementation of security controls. It also helps to understand the classic triangle of criminal theory: mean, motive and opportunity. He adds a fourth, disenfranchisement, which he says is particularly important in a down economy.

"In this culture of layoffs, employees are no longer tied to a company through pensions and long-term employment," Anderson says. "Most employees under 30, if they stay on a job two years or more, it's unusual. There is no loyalty, and they possess a look-out-for-myself mentality. This is causing increases in insider risks."

Aveksa's Cleary cautions that in such an economic environment, if employees have access to information they don't need, they may misuse it.

"Think about the workforce reductions we've had; if you have no automation or visibility into access, you don't know what to de-provision. We've had reductions on a scale we've never seen before—10 percent to 15 percent reductions in two days sometimes. That leaves companies open to the potential for access-related risks."

Disgruntled or disenfranchised insiders lead to incidents. So do unintentional actions. In fact, the majority of insider-related incidents are not meant to be harmful. They're instead, policy violations or workarounds to technology barriers, such as using Web-based personal email to send sensitive documents to a home account to work on them after hours.

"There is no policy that protects against user stupidity," eIQ Networks' Rothman says. "A lot of the insider issues we have are accidental; they're not malicious. That's kinda why I stay to this concept of not thinking about an insider. If you don't have that delineation, what you're trying to do is protect the fundamental element of data and the systems that have access to that data against whoever may be accessing it at a given time. Part of what security has to do is protect us from ourselves, and we're trying to do the right thing. It's not like all employees are malicious. But, if you go back to the thinking that there really are no insiders, you never get confused about how to think about your protection stack. You have different layers of access, but you're always trying to verify what folks are doing."

> "There is no policy that protects against user stupidity. A lot of the insider issues we have are accidental; they're not malicious."
>
> –MIKE ROTHMAN, blogger and senior vice president of strategy, eIQ Networks

HOW TO BUILD AN INSIDER THREAT MODEL

Humans are frail and subject to temptation. You don't have to be Jerome Kerviel and steal $7B in fraudulent trades from a giant financial institution. You can be a DBA or a Web admin with too many privileges who is tempted to peek at the CEO's salary

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

that's tucked away in an HR database. Or you could work at a hospital and be a mark for someone at the *National Enquirer* who is willing to pay handsomely for a look at a celebrity's health records.

"IT security organizations are under an incredible amount of pressure to supply access where and when it's needed," Cleary says. "If you delay, the business gets frustrated and escalates the issue. Eventually, you compromise and give the business more access than they need and hope the business does the right thing."

Sometimes there are more sinister elements at work.

The CERT Coordination Center, based at the Software Engineering Institute at Carnegie Mellon University, studies the motivations behind insider attacks. Their researchers model insider behaviors to understand why incidents happen and how to mitigate the risk.

Dawn Capelli, senior member of the technical staff, explains that CERT/CC has built two new models of insiders to go along with previous work on IT insiders stealing intellectual property and IT saboteurs [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1340485_idx4,00.html]. One they're calling the entitled independent, where one person working alone on a project for a significant amount of time feels entitled to it. "They feel ownership and then something happens, either they don't get a raise or a promotion, and decide they're going to leave," Capelli explains. "They don't want revenge; they just leave. And because they feel ownership, they decide to take it with them (often to a competitor). The original employer loses a competitive edge to the new organization."

> "They don't want revenge; they just leave. And because they feel ownership, they decide to take it with them (often to a competitor)."
>
> –DAWN CAPELLI, senior member of the technical staff, The CERT Coordination Center, Carnegie Mellon University

The other pattern is what Capelli calls an ambitious leader. This usually involves an outside agent, a foreign government for example. The insider steals information on a project, not out of dissatisfaction with their employment, but a government or criminal organization making contact and negotiating for the information. "Typically, they have plans. They want to start a business or give the information to a foreign government," Capelli says. "Often, they need more than just what they were working on and start to recruit other insiders, making promises to take these people with them."

CERT/CC's research is based on actual case data culled from court records, media reports and interviews with organizations hit by insiders, prosecutors and investigators, Capelli says. She adds there are 318 cases in their database.

Capelli says organizations are hamstrung putting policies and practices in place to protect their sensitive data. Most insiders steal within a month of leaving an organization; problem is, for the most part, they're good at concealing their intentions and often don't put up flares that would make management suspicious of their activities.

"If HR tells information security that a person is going to leave and has turned in their resignation, can security look at what the person has been doing? There are bigger legal and privacy issues at play here," Capelli says. "If the person has not been doing anything wrong, you have no right to look at what they've been doing. That's really a big concern out there."

Tools such as DLP are incredibly useful for forensics and investigations, but aren't very proactive.

"By then it's too late," Capelli says. "You need to catch it as its leaving. Their hands are tied, and it's very frustrating for them. They come to one of our workshops, we do assessments, and it opens their eyes. It's very scary and frustrating to go back to do something and find out it's going to be hard to do."

TRUST-BUT-VERIFY ALWAYS APPLIES

Interestingly enough, when *Information Security* spoke to CERT/CC a year ago about its insider research, its definition of an insider did not include trusted business partners and third parties. That has since changed.

"We never did, but we're seeing more cases where third parties are involved," Capelli says.

Organizations still resting on this crutch of differentiating between insiders and outsiders are making a dangerous delineation, experts say.

"It doesn't really make sense to differentiate the two any longer," Novell's Goodman says. "It used to be when you would talk about IT security you were talking almost exclusively about firewalls and the hard shell, gooey center concept. There really is very little differentiation between what is an insider and outsider any longer."

> "We never did, but we're seeing more cases where third parties are involved."
> –DAWN CAPELLI, senior member of the technical staff, The CERT Coordination Center, Carnegie Mellon University

Pharmaceuticals, for example, look at their ability to bring in outsiders rapidly for clinical trials as a competitive advantage. In other instances, enterprises connect systems with vendors and suppliers and exchange data in order to keep business moving.

"If you're a manufacturer, you're exchanging a lot of data between suppliers," Kocher says. "Are their employees insiders? What are they? The usual mentality of putting strong walls all around doesn't apply well in modern business."

What does well is to escape the crutch of segmenting insiders and outsiders, assess where critical risks and vulnerabilities lie in your organization and minimize losses in those areas.

"I think we still have folks drawing that distinction," Rothman says. "We never have enough time, money or resources. It's about trying to, in an intelligent way, determine which three things you're going to do today that would have the biggest impact in reducing risk. It's hard, if it was easy, everybody would be doing it.

"We're in a new time. The way things are built today, it's really hard to understand who works for you now. If we can get out of this early-2000 timeframe of us versus them and adopt a trust-but-verify approach on anyone with access to your data, we'll be a lot better off." ›

Michael S. Mimoso is Editorial Director of TechTarget's Security Media Group. Send comments on this article to feedback@infosecuritymag.com.

Kiss your antivirus bloatware goodbye

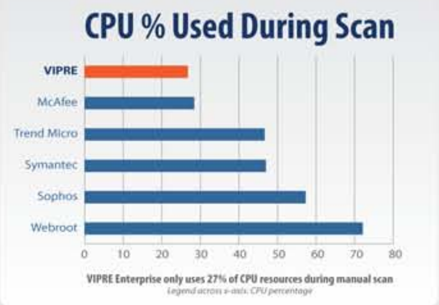
Special Competitive Upgrade: 50% Discount!

TEST DRIVE

VIPRE® ENTERPRISE

Next Generation of Total Malware Protection

The configurable Command Center puts all the information you need in one place. Manage individual agents, quarantines, threats, and more.



VIPRE Enterprise only uses 27% of CPU resources during manual scan

Legend across x-axis: CPU percentage

How does your current software compare? VIPRE Enterprise scans at a brisk 13.95 MB/sec and uses just 27% of CPU and 50 MB of RAM. In idle, it uses a mere 13.3 MB RAM with a disk footprint of just 113 MB. You'll hardly notice it's running!

Sunbelt Software

Until now, antivirus engines have been Frankensteins, bolted together from bits and pieces of different products. They're slow, full of bugs, and hard to manage.

VIPRE Enterprise is a revolutionary new approach. It's built from scratch as the all-in-one antivirus, antispyware, anti-rootkit solution that gives you complete endpoint malware protection ***without hogging resources!*** It's fast, powerful, and easy.

Plus, advanced anti-malware technology protects your system against the new wave of malware threats. No more juggling multiple programs. No more dealing with user complaints about slow workstation performance.

Compatible with Windows®7

- **COMPLETE!** All-in-one protection from today's malware.
- **FAST!** High-performance and low impact on system resources.
- **EASY!** Manage everything easily from one command screen.
- **RELIABLE!** Configurable, real-time monitoring technology.
- **AFFORDABLE!** Ask for a quote with our 50% competitive upgrade discount!

BEST IN TECH 2009 ADMINISTRATOR

Why struggle with slow resource hogs when you can manage ALL your malware threats with one fast, easy application?

WindowsIT Pro 2009 Community Choice GOLD

Curious? Download your FREE copy of VIPRE Enterprise and give it a test drive.

When you compare VIPRE Enterprise to Symantec, McAfee, Trend Micro or whatever antivirus program you're using, **you WILL want to switch!** Don't worry, though.You can get VIPRE Enterprise with a **50% competitive upgrade discount!**

vb 100 VIRUS virusbtn.com

Download VIPRE Enterprise today and get your own home version of VIPRE to keep FREE as our gift to you!

Download now: www.TestDriveVipre.com

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.SunbeltSoftware.com sales@sunbeltsoftware.com

Available on new licenses for a limited time. Subject to change without notice. See website for more details.

UTM Should NOT = Unnecessary Threat Management

Buying the right unified threat management appliance means knowing what—if anything—you actually need beyond a firewall.

BY NEIL ROITER

TABLE OF CONTENTS

EDITOR'S DESK

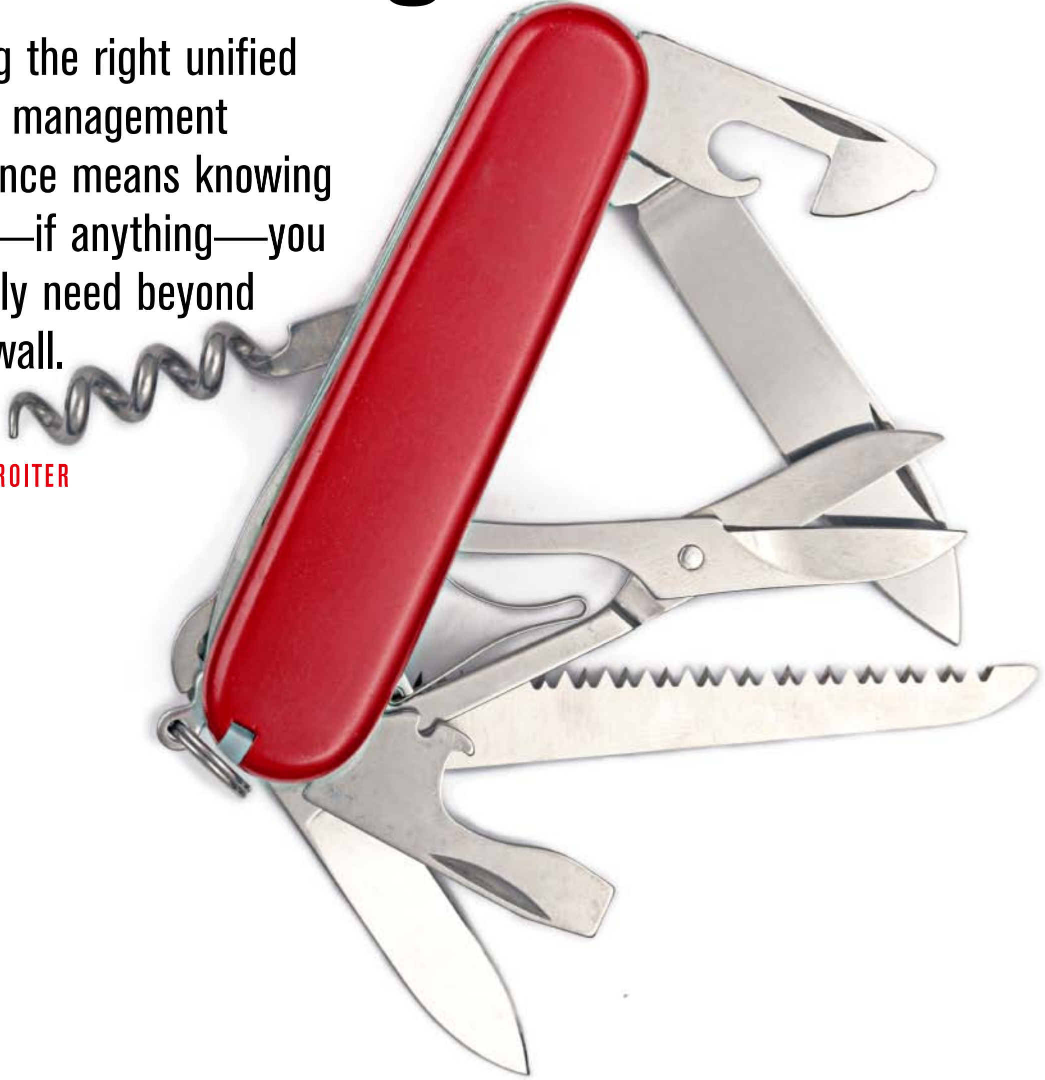
WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES



IF YOU ARE RESPONSIBLE for security at a small- to mid-sized business, if your current firewalls aren't unified threat management (UTM) appliances, then your next ones will be.

With the possible exception of a few low-end SOHO firewall products, every vendor offers a range of firewall/VPN appliances with options to add gateway antivirus, intrusion prevention, antispam, URL filtering and other security functions on a single box.

"The UTM space has essentially replaced the firewall space; at the low end, there are no firewalls that are not UTM," says Joel Snyder, senior partner at consultancy Opus One. "If you talk about what people used to buy for a small business in the $150-to-$1,000 range, I don't think you can find one that doesn't have UTM capabilities."

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

It can get confusing. Businesses are faced with complex choices: Extra security comes at a price, both in ongoing subscriptions and performance, so what do you really need and what are you prepared to pay for?

Most vendors offer an extensive line of appliances to accommodate traffic requirements and number of end users. Ready to choose? Not so fast. You'll take a performance hit when you start adding AV, IPS, and other security functions.

Small businesses have big security needs

Small businesses were starting to wake up to changing security needs when *Information Security* first covered "turnkey appliances" in 2004. Some had no firewalls at all, or first-generation firewalls that no longer supported the business. IT managers shopping for replacements from established firewall vendors found young companies that could offer firewalls plus additional security features packed into a single appliance—all at an attractive price.

Soon, this was christened the UTM market, and, eventually, everyone in the network firewall business was pushing unified threat management. Today, some vendors are pushing high-end appliances in what they claim is a nascent enterprise UTM market *(see "Is there an enterprise UTM?" p. 26)*.

For smaller businesses faced with growing security requirements, UTM made it easier to buy and manage a lot of security tools in a single appliance.

For smaller businesses faced with growing security requirements, UTM made it easier to buy and manage a lot of security tools in a single appliance. The alternative was more point products they could not afford. Or, worse yet, simply going with less security.

"Ten or 12 years ago, we had a firewall, but it wasn't a major piece of equipment—we thought, 'yeah, maybe we should get one,'" says Jason Omens of Seattle, Wash.-based marketing consulting firm BuzzBee, a WatchGuard UTM customer. "Now the number of threats has skyrocketed."

Omens has to be security conscious now, particularly because of the work BuzzBee does for Microsoft. Keeping precious intellectual property inside the organization is his biggest concern.

ZirMed, a Louisville, Ky.-based software-as-a-service provider for the healthcare industry, which has used SonicWALL UTM appliances since 2000, also raised its security profile as the years passed.

"It's not that we weren't focused on security—we had patient healthcare information to protect," says ZirMed CIO Chris Chirgwin. "But we've seen enactment of HIPAA, and since we added credit card processing, we fall under PCI. We've become a bigger business; now people want us to be SaS 70 audited."

Smaller companies can still have big security headaches. Law firm Sonnenschein Nath & Rosenthal LLP, an IBM ISS customer, is relatively small in employees numbers—but about 800 of them are lawyers, and the firm has a lot to protect.

"We produce hundreds of thousands of documents," says Adam Hansen, Sonnen-

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

DATA CENTERS

Is there an *enterprise* UTM?

SOME HIGH-END network firewall and UTM vendors say we're seeing the dawn of enterprise-grade unified threat management appliances. These, they say, are high-performance beasts that can process network AV, email security, Web security and perhaps other functions such as data loss prevention—in addition to network firewall, VPN and intrusion prevention in front of the data center without missing a beat.

While the rationale for UTM in the SMB world is adding affordable security on top of firewall/VPN in a single box, the argument in the enterprise is consolidation, as large companies look to save on capital expenses, management overhead, rack space and power.

Whether we'll see real UTM at the enterprise level is open to debate, but we are seeing IPS integrated into high-end firewalls with the muscle to keep traffic moving quickly enough for performance-sensitive applications.

"There are certain decision points where an organization reevaluates their security infrastructure," says Guy Guzner, Check Point Software Technologies director, security products. "There's a lot of restructuring of data centers, a lot of consolidation. When this happens, it gives us an opportunity to revisit some decisions that were made when integrated IPS wasn't mature."

But vendors, including Check Point, take this further. Guzner says that its UTM "software blade" approach is in the "early adoption phase" on its high-end Power-1line for things like gateway AV.

"The enterprise can realize an incredible ROI from a technology and cost perspective, says Anthony James, Fortinet vice president of products. "UTM gives them much more bang for the buck. They can move at the pace they want. They can replace a firewall at cost and add functions over time."

Greg Young, an analyst for Gartner—which prefers the term "multi-function firewall" to unified threat management—is more than cynical.

"There are lies, damn lies and UTM for the enterprise," he declares. "The physics works out, for doing inspection, so that you don't start running into problems until you hit the larger volumes of users, traffic and connections, and then the physics breaks down and then you really need separate products and processors for antivirus, for firewalling, for other deep inspections."

In effect, what vendors are talking about, Young says, are blades in a chassis, where the chassis becomes essentially a server rack. He cites Crossbeam Systems' blade architecture as a prime example.

He breaks the enterprise market into three silos: Next-generation firewalls, which include VPN and IPS; Web security gateways, which typically include URL filtering, and email security appliances.

Joel Snyder, senior partner at consultancy Opus One, takes a slightly different tack, defining Crossbeam as UTM, but otherwise agrees.

"I'm not saying there is one big UTM market," he says. "There are two: Crossbeam and everyone else that's SMB."

Enterprises *are* doing true UTM in the branch office, which have differentiated into separate product lines. The branch appliances generally don't need things like AV or antispam, because the mail is still centralized. But they do need other services, Young says, such as WAN optimization, and they will be managed by the same console as the enterprise firewall, because companies don't want to use two different consoles. For that reason, large firewall vendors tend to do well in the branch offices.

—NEIL ROITER

schein manager of information security. "Think about what lawyers print, what they transfer electronically. We protect information throughout its life cycle in whatever form it may take and be sorted."

Also, firms like Sonnenshein need the extra layers of security UTM can offer because they tend to stick with standard, off-the-shelf products. "That's great for support, Hansen says, "but not great in terms of mainstream vulnerabilities. The risk landscape is fairly broad. If they can run it through Word, we're vulnerable."

Growing into UTM

Years ago, it was fairly simple to choose the right-sized firewall for your business. Your bandwidth pipe was limited and your was traffic predictable.

Today, your choice of UTM appliance is a factor of business needs and the security features you choose to purchase and turn on. It's not just a purchase—it's a commitment. ZirMed found that out as it upgraded from a firewall to full UTM, then to a bigger UTM appliance.

"First, we said, let's embrace UTM—IPS, gateway AV, malware detection. Then we had to get more serious as we needed a chassis upgrade with considerably more horsepower," says Chirgwin. The next upgrade came when "we needed more horsepower, simply for more bandwidth. As we were committed to UTM and brought on more customers, the firewall was getting close to being a performance issue."

> "You need to balance, a box with more horsepower that doesn't break the bank. It's a fine line vendors walk down, a fine line users walk down, and the bar continues to be raised."
>
> —JIM FINN, CEO, eSoft

In general terms, you can plan to upgrade as your needs change, say every couple of years, or perhaps spend more initially to accommodate that growth down the line. BuzzBee's Omens, for example, faced with growing traffic as more customers have network access and transfer big files over FTP, is about to upgrade from a T-1 line to 10 Gbps Ethernet without changing appliances.

"It handles our small business needs as we grow," he says. "We want to be able to grow with what the company needs to do and know that these boxes can handle it."

He also looks for features like external ports on an appliance to accommodate his environment. For example, he uses one of the WatchGuard interfaces to link to an external NAS, so that traffic doesn't interfere with the internal network.

Even with planning, making the right choice isn't easy.

"Bandwidth growth is terribly hard to predict," says Gartner's Young. After you invest in the capital expense, if your throughput strains the appliance, vendors are ready to help you trade up. "That's how they make money."

"You need to balance a box with more horsepower that doesn't break the bank," says eSoft CEO Jim Finn. "It's a fine line vendors walk down, a fine line users walk down, and the bar continues to be raised."

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

Opus One's Snyder advises caution as you walk that line. High speed cable and DSL have brought fat pipes to small businesses. If you go beyond firewall and VPN and add gateway antivirus, you'll not only be paying a recurring cost for the subscription, but you'll also bump up your capital expense for a more powerful appliance.

"The costs can be non-predictable," he warns, "because vendors don't like to give good numbers for performance."

The wrong choice can be costly. If you don't have a good case for gateway AV, you're wasting money on the subscription and the box. If you find your box isn't fast enough, you have to upgrade. Or turn of the AV.

"And then you've wasted money and time," says Snyder.

Snyder, who has done extensive UTM testing, has written that transaction rates can drop in half with IPS enabled, and fractions of that with AV and IPS combined in extreme cases.

The recommendation is to plan ahead for your future needs, so you don't need to upgrade in six months or a year if you decide to turn on AV and/or other security apps because your security requirements change. Perhaps your compliance auditor says you need to improve security at the perimeter. Maybe you've had a data breach or your IT staff is spending too much time cleaning up/reimaging infected computers? Or those complaints to HR convinces management that you need to control visits to porn sites.

What's more, your changing business needs also impact your selection.

> "The big thing was to get the VPN working. The other things, like gateway antivirus, are good to have, since we're too small to have interest in another appliance. As BuzzBee grows, we'd like to be preemptive."
>
> —JASON OMENS, BuzzBee

As the economy improves and your business grows, you may hire more people, upgrade to a faster network or expand your online business. Save money and trouble ahead of time by testing the UTM appliance under stress on your network, and anticipate your needs to allow for growth.

UTM security options

Most SMBs aren't in the market for a UTM. They are shopping for a better firewall, perhaps or more robust VPN.

BuzzBee's Omens went to a UTM appliance because he was having difficulty setting up a VPN using PPTP on his old firewall.

"The big thing was to get the VPN working," he says. The other things, like gateway antivirus, are good to have, since we're too small to have interest in another appliance. As BuzzBee grows, we'd like to be preemptive."

"I don't believe most small business or even midmarket IT managers—think I want UTM versus I want a firewall, Snyder says. "But, the features are now so ubiquitous they are not surprised to see them. They hit a stumbling block of 'do I want them, do I have to pay, and does this help me in any way?"

Antivirus and other security applications are what make UTM a UTM. As a result,

TABLE OF CONTENTS

EDITOR’S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

you need to consider the value to you versus the cost.

AV is probably number one on the list. Small businesses are accustomed to buying it for their PCs and servers. And they worry about malware, in part because they are finding their endpoint AV isn’t sufficient—PCs and servers still get infected.

You pay a performance premium for turning on additional capabilities, particularly AV and IPS, which have to closely inspect traffic. You may not want everything or everything at one time, so set your sights on a low bundle price for the entire package. That way you can cherry pick and turn on a security service when you are ready or the need arises.

For example, you may not use URL filtering initially, but perhaps your HR department starts enforcing acceptable use policies, or wants to keep your employees off sites that eat up their work time. You may not feel you need network intrusion prevention now, but might when the business grows or you begin hosting Web sites.

Snyder again raises a yellow flag on IPS, saying the quality varies widely.

Don’t expect any of these security apps to be as robust as stand-alone products or services, but they may be “good enough,” or simply add a layer to your defenses at a reasonable price.

For example, antispam is a good addition if you are not using a stand-alone product or hosted service.

URL filtering is a good fit for UTM appliances, Snyder says—the firewall is a logical place to put it. The same goes for SSL VPN, which some UTM vendors offer as an option along with the more traditional IPsec. In either case, don’t expect either to have the kind of granular policy and management controls of their full-featured counterparts.

A UTM version of URL filtering is likely to be pretty basic. It will work off a URL database, but will not give you dynamic evaluation based on content. Nor should you expect access control integration with your directory, or the ability to set exceptions for groups or individuals who have legitimate access to certain types of sites.

> “The DLP is very rudimentary; it’s not full enterprise DLP. But if your requirements are low, it’s perfect.’
>
> —GREG YOUNG, analyst, Gartner

In addition, some new options such as data loss prevention are appearing. but again, manage your expectations.

“The DLP is very rudimentary; it’s not full enterprise DLP,” says Gartner’s Young. “But if your requirements are low, it’s perfect.’

So, if all you want to do is watch for credit card numbers or Social Security numbers, this is almost surely good enough DLP at the right price.

We’re starting to see Web application firewalls (WAFs) in UTMs as well, but this seems like even more of a reach. WAFs have become very popular since they became an option for the application security requirement for PCI DSS. But WAFs aren’t plug-and-play tools, and simply turning on this option in front of your Web apps will neither make you more secure nor PCI compliant. Plan to invest some care and feeding if you are going to deploy a WAF as part of your application security program and investigate the WAF’s capabilities before you decide it will be a checkbox PCI solution.

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

UTM Products

REPRESENTATIVE LIST OF UNIFIED THREAT MANAGEMENT VENDORS AND PRODUCTS.

COMPANY	PRODUCT(S)	DESCRIPTION
Astaro Internet Security www.astaro.com	Astaro Security Gateway	Appliances ranging from low-mid-sized companies to 10,000 users. Firewall, IPSec/SSL VPN, AV, Web filtering, email security
Calyptix Security www.calyptix.com	Access Enforcer	Appliances for 10 to 100 users designed to work with Microsoft Small Business Server 2008. Firewall, VPN, AV/antispyware, antispam, Web filtering, IPS IM management
Check Point Software Technologies www.checkpoint.com	UTM-1, Power-1	UTM-1: 12 appliances ranging from 400 Mbps to 4 Gbps firewall throughput. Firewall, VPN, AV, IPS, Web filtering, antispam-email security. Power-1: High-end network firewall appliances up to 25 Gbps firewall throughput; same security options plus IM control, VoIP security, SSL VPN, and networking features such as load balancing, HA, clustering and QoS
Crossbeam Systems www.crossbeam.com	X-Series	Blade architecture for mixing and matching third-party firewall, VPN, IDS, antivirus, URL filtering, content filtering. C series: 380 Mbps to 6 Gbps firewall throughput; X-Series: adds load balancing, IPS, Web application firewall; two 10 Gbps and 10 1 Gbps ports
Cyberoam www.cyberoam.com	Comprehensive Internet Security System	SOHO up to 6 Gbps firewall throughput appliances featuring identity-based UTM with include firewall, VPN (SSL & IPSec), AV and anti-spyware, anti-spam, IPS, content filtering, bandwidth management
Cymtec www.cymtec.com	Sentry	Appliances for small offices, branch offices; firewall, URL filtering, AV, application control
DeepNines Technologies www.deepnines.com	Security Edge Platform (SEP)	Software–based UTM up to 1 Gbps; firewall, IPS, AV, content filtering
eSoft www.esoft.com	InstaGate	SMB firewall/VPN, Web and email security
Fortinet www.fortinet.com	Fortinet FortiGate	Appliance ranging from small businesses to the FortiGate-5000 series for large enterprises, service providers and carriers; IPS, AV, Web filtering, antispam, application control
Funkwerk Enterprise Communications www.funkwerk-ec.com	Packetalarm UTM	10-250 user appliances; firewall/VPN, IPS, AV, antispam
Global DataGuard www.globaldataguard.com	Global DataGuard All-in-One Security Module for Enterprise UTM	IDP, NBA, AV, NAC, content filtering in medium-to-large enterprise appliances
Halon Security www.halonsecurity.com	SX series	800 Mhz to 3200 Mhz appliances; firewall/VPN, AV, antispam, content filtering, Web access control, IDS
Juniper Networks www.juniper.net	SSG	160 Mbps to 1 Gbps firewall throughput; VPN, IPS, AV, antispam, and Web filtering
McAfee www.mcafee.com	McAfee UTM Firewall (formerly Secure Computing SnapGear)	25 Mbps to 180 Mbps SMB appliances; firewall/VPN, AV, IDP, URL filtering, email filtering
02 Security www.02security.com	SifoWorks	100 Mbps to 1650 Mbps firewall/VPN; intrusion prevention, antivirus, Web filtering
Panda Security www.pandasecurity.com	GateDefender	40 Mbps to 850 Mbps SMB appliances; Firewall/VPN, IPS, AV, content filtering, antispam and Web filtering
Reticorp www.reticorp.com	Reticorp RetiEdge	Firewall/VPN, IPS, AV
Smoothwall www.smoothwall.com	Smoothwall SmoothGuard	900 Mbps series appliances, firewall/VPN, Web filtering and VPN solutions with IDS, antivirus, antispam
SonicWALL www.sonicwall.com	SonicWALL E NSA, NSA, TZ series appliances	Wide range of 90 Mbps to 5.6 Gbps appliances; application firewall, IPsec/SSL VPN, AV, IPS
Untangle www.untangle.com	Gateway Platform	12 open-source security apps for SMBs
Vasco www.vasco.com	aXsGUARD Gatekeeper	Three gigabit interface appliances; firewall/VPN, AV, IPS, content filtering, antispam
WatchGuard Technologies www.watchguard.cm	Firebox X	50-1,000 user appliances; firewall/VPN, AV, antispam, URL filtering, IPS
ZyXel www.zyxel.com	USG100, 300	Firewall/IPSEC/SSL VPN for up to 50 users

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

If it fills the bill, however, says Young, you won't have to buy a stand-alone product or tinker with open-source tools.

UTM is here to stay. For organizations with up to 500, perhaps 1,000 employees, depending on the specific attributes of the business, it is the firewall of the present and at least the foreseeable future.

It's a winner for firewall vendors, Snyder says.

"The whole reason UTM exists is because of recurring revenue," he says. "The recurring revenue model is the salvation of firewall industry. That's why these boxes exist."

For SMBs, UTM offers a number of security services for the price of a single appliance to purchase and modest, though recurring subscription fees. If you're sure all you need is firewall and VPN, don't feel you have to buy the extra subscriptions, so you don't get stuck with added fees or a more expensive appliance than you really need. If you think you may need to turn on additional services in the foreseeable future and/or anticipate more users and traffic, make sure you buy appliances that will grow with your needs. ▸

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

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

THIS IS Only a Drill

Delaware's Dept. of Technology and Information conducts annual incident response exercises that test the readiness of state agencies to respond to attacks.

BY MICHAEL S. MIMOSO

IF YOU'RE AN NFL FAN IN APRIL, you're well familiar with mock drafts. These pretend exercises portend to make a best guess at whom your favorite football franchise will select on Draft Day. Granted, while teams may be worth hundreds of millions of dollars, the NFL isn't playing the same high-stakes game as the federal and state governments.

So when a state such as Delaware calls all hands on deck for a mock exercise simulating a coordinated attack on information systems and communications, there's more at stake than who will be taking snaps for the next 10 seasons. Lives, critical infrastructure and national security are on the line.

Delaware's Dept. of Technology and Information (DTI) [http://dti.delaware.gov/] had conducted tabletop incident response exercises since 2005 to great results. Year after year, new insight was gained into technology and processes that weren't up to speed or needed a tweak. But the tabletop format was losing steam and organizers feared what had long been an effective evaluation tool would lose its value. IT people in particular aren't engaged for long without the ability to bang on a keyboard, write scripts and see measurable results. That was incentive enough for the state last year to add a hands-on aspect to the drill.

"It's good to simulate attacks on the state's information resources so folks in various capacities of state government can play along and talk about response and what things we can put in place to perhaps prevent an attack from happening altogether," says the state's chief security officer Elayne Starkey. "It's good to practice—for the same reason you have fire drills."

PLANNING EVERY STEP OF THE WAY

Delaware's exercise is anything but fire drill. To the contrary, it takes six months to plan, and involves 125 people from federal and state agencies, including IT managers, law enforcement, the FBI and academics. Disaster recovery coordinator Lisa Wragg is the project manager who drafts the exercise's objectives, organizes a steering committee that reviews and approves those objectives, and then, using the Homeland Security Exercise and Evaluation Program (HSEEP) [https://hseep.dhs.gov/pages/1001_HSEEP7.aspx] as a model, plans out the sequence of events and milestones that must be met along the way.

There are four preliminary meetings under the HSEEP model: a concepts and objectives meeting where the exercise objectives are mapped out and where the decision to include a functional, hands-on component was made; an initial planning conference where the concepts and objectives are finalized and approved, the venue is approved and participants selected; a midpoint planning conference where the sequence of events is established; and a final planning conference, where the review of the day's scenario and logistics is approved. The steering committee is a partner at each milestone, and that was made up of the state's high tech crimes unit, state police and the Delaware Emergency Management Agency.

Delaware's exercise is anything but fire drill. To the contrary, it takes six months to plan the exercise, which involves 125 people from federal and state agencies, including IT managers, law enforcement, the FBI and academics.

"You have to create a scenario and put together an outline of the day's events. People need to have a reason why things are happening," Wragg says, adding that she used many of the lessons learned in DTI's three previous exercises to build this one.

"If you just throw people in a room and just start hacking them and not have a story to go by or understand why something is happening, it's kind of meaningless to them," Wragg says.

Last October's scenario had a timely script. Held a week before the presidential election, the plot involved a cyberattack by the fictional country of Dystopia on state agency websites, networks and states' voting infrastructure. The plot was hammered out months earlier, and reinforced last summer when attacks on the country of Georgia's state-run websites [http://itknowledgeexchange.techtarget.com/security-bytes/russian-cyberwar-yes-no-maybe-so/] were conducted prior to physical conflict during its war with Russia.

"That drove home the possibility of what could happen," Wragg says. "We needed to prepare for it. We needed the scenario to be a terror attack this time."

SIMULATED ATTACKS, REAL RESPONSES

Starkey says the attack scenarios are kept close to the vest with fewer than 10 people knowing what's about to take place. The added dimension of this exercise being a terrorist attack on the voting infrastructure required some careful treading. Starkey did not want to leave the impression on any of the participants—including the National Guard, Air Force, school districts, state police, FBI, Dept. of Transportation, Dept. of Labor, in addition to DTI—that the state's election system was vulnerable.

All of the players were present at the DTI emergency operations center on Oct. 29 for the exercise, and in her opening remarks, Starkey laid out the day's high-level goals: prevent cyberattacks, sharpen response procedures and recovery.

"One thing that was important to us, was that when we start the exercises, that we create an environment of trust, take away the threatening feeling in the room—dispel that right away," Starkey says. "In my opening comments, I stressed this was

STRATEGY

Three Keys To Success

UNDERSTAND THE THREAT LANDSCAPE AND PLAN YOUR TABLETOP EXERCISES ACCORDINGLY.

Motivated attackers are going to penetrate even the most ardent defenses. Companies that realize that this is the information security environment of 2009, are the ones realizing the need to run through functional and tabletop incident response exercises such as the one conducted by the Delaware DTI.

Lenny Zeltser, an incident handler with the SANS Internet Storm Center, says even enterprises with mature security practices find great value in these mock exercises. He defines three keys to success:

#1 **DEFINE YOUR SUCCESS CRITERIA.** "You need to define what it means to do well," Zeltser says. Have you responded to an incident within 30 minutes, and have a good sense for the scope of an attack either hours later? Or maybe you define success as learning within a pre-determined period of time what data was affected and whether the right people were notified and put in position to make decisions.

#2 **INVOLVE THE RIGHT PEOPLE.** "It's too easy to operate in a silo," Zeltser says. You might be one of 10 teams responding to an incident, and those nine other teams won't prioritize security the way you do. "That means you may have to have power or authority or good will to get them involved."

#3 **EVOLVE YOUR EXERCISE.** "Don't run through the same exercise every year," Zeltser says. Your incident response exercise should evolve just as your business changes, the economy grows or shrinks and security priorities change. ›

—MICHAEL S. MIMOSO

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

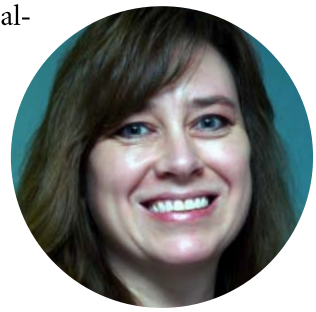
SPONSOR RESOURCES

not real. I wanted them to feel like this is safe haven, and that we understood they were all at different points of readiness."

"Don't feel badly about not having a policy in place that you should, or a procedure not defined completely. This is the place to kick all that around," Starkey adds. "One of my key objectives is for them to leave that day with a little to-do list of things they want to take care of in the weeks after the exercise. We want them to each year to go away with ideas of things to do to strengthen their infrastructures, and to improve their ability to respond and recover from an attack like this."

At an appointed time, programmers and network security engineers began releasing attack scripts against websites that were built in a development environment and set up on a segmented network. Responders in the EOC would need to recognize problems with a site such as defacements or denial-of-service attacks and take appropriate countermeasures, which were evaluated.

"It was like a little NASA—rows and rows of computers, screens up on a big wall where the participants were sitting, and behind the glass was exercise control where the injects and scripts were released," Wragg says.



"It was like a little NASA—rows and rows of computers, screens up on a big wall where the participants were sitting, and behind the glass was exercise control where the injects and scripts were released."

–LISA WRAGG ,
Disaster recovery coordinator, state of Delaware

Website defacements were the first wave of attacks, launched against the home pages of various state agencies. As word spread of the attacks, other agencies began to take measures to harden their Web apps to avoid being taken down as well. Several, Starkey and Wragg said, beat attackers to the punch.

"That was incredibly motivating to the other agencies," Starkey says. "We highlighted it in one of the breaks and congratulated them on the good work they did."

In another room adjacent to the EOC, a tabletop-style scenario was set up where people of similar function would work together. The service desk was also there taking incoming calls for trouble tickets. As soon as the attacks happened, calls flooded the service desk. High Tech Crimes officials were at one station, and working with law enforcement, they quickly began tracing the source of the attacks. Meanwhile, the state's Joint Information Center (JIC), which included public information officers from different state agencies, were at another putting out coordinated media releases and crafting appropriate public responses, alerting citizens that they should take caution using agency websites.

"It was pretty cool and interactive," Wragg says.

Once that segment of the exercise was complete, the DTI held a quick briefing on the importance of preserving evidence. Admins are initially more concerned with the availability of systems and getting them back online, but in this instance, they had to

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

tread lightly to preserve the integrity of the scene and assist in tracking the source of the attacks. The participants were also evaluated on how well they used the state's incident command system, prescribed by the federal government. The framework is built for emergency management agencies and represents a set of standard response procedures.

The next wave of the attack involved more website attacks, this time the target was sensitive personal data. Simulated FBI warnings were sent out that terrorists had launched cyberattacks against critical infrastructure, and soon thereafter, calls began flooding the service desk with citizens reporting possible identity theft after accessing services on state agency websites. The response involved assessing the cause of the breaches and reviewing data protection procedures. JIC also worked up statements directing citizens how to protect themselves online, and if necessary, report incidents to police.

The final phase of the exercise combined another hack with a physical attack. Denial-of-service attacks were launched against agencies' sites and services, while simultaneously terrorists were disabling lines used by service providers statewide. The offshoot was that these attacks could possibly impair the state's ability to vote in the upcoming elections. Steps were taken to rapidly move critical infrastructure to redundant facilities and keep services available until the service providers to could complete repairs.

LESSONS

Things to Remember

LISA WRAGG, DISASTER RECOVERY COORDINATOR FOR THE DELAWARE DTI, WAS THE PROJECT MANAGER FOR LAST YEAR'S INCIDENT RESPONSE EXERCISE. SHE LAYS OUT SEVEN LESSONS LEARNED.

1. Assign a project planner.
2. Secure an executive sponsor; CSO Elayne Starkey was her sponsor.
3. Follow a master event list and build your scenario around that list.
4. Stick to your scenario; what look like minor changes could have a big impact down the line.
5. Outline the details of your scenario, including attack scripts.
6. Address current threats in your scenario.
7. Get an outside agency to assess how you do; SunGard's Incident Management Exercise Service did DTI's assessment.

"The exercise creates a lot of interest in updating plans and going back and checking websites, making sure they're up to date and patched," Wragg says. "There is a lot of after-exercise activity. People want to do something."

MEASURABLE METRICS AND REVIEWS

Being the fourth such exercise, many of DTI's incident response processes are mature. Media and external communication are solid, Starkey and Wragg note, while adding that internal communication between agencies is an ongoing process.

"If we're looking for measurable stuff, some agencies quite frankly need help, and we're going to help them," Starkey says. "Quite frankly, I don't think we would have been able to identify who needed more help than others until we did the exercise."

Starkey says the agencies did well against the four stated objectives. All agencies identified vulnerabilities in their infrastructure leaving them susceptible to Web-based attacks. Each agency had a prescribed process for defending against attacks and rolled out those processes accordingly. Each addressed the preservation of evidence, with different levels of maturity in their respective processes. This was an area Starkey says ongoing education will be key going forward.

Business continuity [http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1330538,00.html] is also another area DTI will concentrate on going forward. The coordinated physical and cyberattack that played out in the final phase of the exercise stressed the importance of a continuity plan for critical services such as voting that must continue seamlessly should a key state network fail.

Breach notification was the final goal that each agency met with flying colors, much to Starkey's satisfaction since each agency information security officer was, in advance, given a procedure to follow on notification. Service desks were overwhelmed with calls; an indication the procedure was being followed.

In the end, Starkey says adding the functional component was definitely a game-winning touchdown, and that last year's participants would never go back to just a tabletop exercise.

"We have a catchphrase about this being a journey to compliance," Starkey says. "I recognize we're not there, we're not at 100 percent compliance across the board. We do see everyone moving different rates."

"If you look at the write-up after first year's exercise, the objectives were fundamental about increasing customers' awareness that cybersecurity was important. We've made incredible strides there to get them to pay attention, let alone comply with a 41-page security policy." ›

"Quite frankly, I don't think we would have been able to identify who needed more help than others until we did the exercise."

–ELAYNE STARKEY , CSO, state of Delaware

Michael S. Mimoso is Editorial Director of TechTarget's Security Media Group. Send comments on this article to feedback@infosecuritymag.com.

TABLE OF CONTENTS

EDITOR'S DESK

WEB 2.0 THREATS

INSIDER RISK

UTM

INCIDENT RESPONSE

SPONSOR RESOURCES

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Michael S. Mimoso

EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Marcus Ranum, Bruce Schneier,
Lee Kushner, Mike Murray

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

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

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

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

SITE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES DIRECTOR Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

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

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

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

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

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

TechTarget
The Technology Media
ROI Experts

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.

ArcSight, Inc.

See ad page **3**

- Managing Network-Centric Risks and Regulations
- Cybercrime Security Kit
- Combat Cybercrime, Demonstrate Compliance and Streamline IT Operations

Fiberlink Communications

See ad page **32**

- Learn More; The MaaS360 Visibility Service and Free Trial
- Are Your Laptops Secure? Be Confident! A MaaS360 Webcast
- Planning for a Pandemic: Turning office workers into mobile workers for business continuity. The MaaS360 ICE Service

Guidance Software, Inc.

See ad page **39**

- Avoiding PCI Non Compliance
- The Concise Guide to E-Discovery
- Understanding Data Location is Imperative for Data Loss Prevention

McAfee, Inc.

- The Security Paradox: The First Global Study that Quantifies the Cost of Reactive Versus Proactive Security in a Midsize Organization
- Mobile Security Report 2009
- Virtual Criminology Report 2009 — Virtually Here: The Age of Cyber Warfare

SOPHOS

Sophos Inc.

See ad page **1**

- How to protect your critical information easily
- High-performance protection at the network edge—what, why and how
- Not all malware detection is created equal

Sunbelt Software

Sunbelt Software

See ad page **23**

- Comparing Antivirus Scanning Performance and System Resource Utilization
- When Less is More: Why Small Companies Should Think Outside the Box for Protecting Endpoints
- Protecting Against the New Wave of Malware

thawte

Thawte

See ad page **15**

- Extended Validation - the New Standard in SSL Security
- Sign your Code and Content for Secure Distribution Online
- Get a Free SSL Trial Certificate from Thawte

websense® ESSENTIAL INFORMATION PROTECTION™

Websense, Inc.

See ad page **6**

- The Next Generation of Content Security Has Arrived! Learn More
- Understand Where the True Web Threats Lie in the Latest Websense Security Labs Report!