

# Baseline

## Is Your Information Really Safe

By Ericka Chickowski

2009-03-20

Here are 10 ways to protect your company's data.

As more organizations realize that using perimeter and anti-virus technologies alone is like locking their doors but leaving their windows open, it's become evident that enterprises must upgrade their security practices in order to prevent huge data breaches like the one announced by Heartland Payment Systems this past January.

The consensus among security veterans is that enterprises must take an information-centric risk management approach. The following 10 steps can provide a strong foundation for your organization's information security strategy.

### 1. MESHING YOUR COMPANY'S SECURITY AND COMPLIANCE EFFORTS

First and foremost, your enterprise should approach the security problem with a comprehensive risk-management strategy that prioritizes information based on its importance to your organization and on regulatory requirements that necessitate its protection. This prioritization should then inform your company's decisions about where IT security will concentrate its efforts.

"We look at the information across different forms and in the different places that it calls home," says Adam Hansen, director of information security for Sonnenschein Nath & Rosenthal, a national law firm with more than 800 attorneys and 15 offices in the United States and Europe. "So we start looking at how we can protect that information and what level of protection we can afford. If the information is of no value or is valued at less than the cost to secure it, why would we throw money at a problem that doesn't exist?"

Compliance will play a part in this risk prioritization because the risks of noncompliance are very real. However, most security experts agree that you shouldn't make compliance concerns the be-all and end-all driver of security initiatives.

Most IT security experts will tell you that compliance does not guarantee that an organization is secure. Nevertheless, if compliance is baked into the strategy without holding too much influence, it can be a great tool for building consensus and support among executives who might otherwise be reluctant to open the purse strings.

"The auditor is one of my best friends," says Brian McPhedran, associate vice president of IT risk management for Aegon Canada, part of Aegon, an international provider of life insurance, pensions and investment products that's headquartered in The Hague, the Netherlands. He explains that in one case he was able to score more funds to implement database security due to an auditor's recommendations to the company's executives.

Governance, risk and compliance (GRC) tools can definitely play a big role in ensuring that you have a healthy compliance and risk management program and can point out where your program needs work.

"It falls on management and the IT department to ensure that there are comprehensive security measures in place and that an internal audit will validate the assumptions of the controls," says Josh Golden, director of internal audit for Kulicke & Soffa Industries, a Fort Washington, Pa.-based semiconductor manufacturer that uses the BWISE Enterprise GRC platform to aid internal auditors in this process. "Having a software application that is going to assist in the testing protocols is a tremendous help. It's really a give and take that needs to take place—and is taking place within Kulicke & Soffa—to optimize how we go about complying with a regulation. In addition, we want to translate that into value for the investors and management."

### 2. POLICY DEVELOPMENT, MONITORING AND ENFORCEMENT

Once you start developing a risk management program and prioritize your risks, you should translate that into actionable policies that control the systems that house your information. Without policies, the implementation of security technology is a waste. Many companies continue to throw technology at the problem in a shotgun approach and then wonder what happened when they have a security breach.

"A lot of it is about policy, process and procedures," says Jeremy Bowers, security coordinator for Sequoia Retail Systems in Mountain View, Calif., which provides retail software to college bookstores. "In most cases, there's not a silver bullet: You can't say, 'We're going to buy this product, and it's going to save us a ton of time.'"

There are various tools that can help automate the enforcement of policies. In fact, the next eight categories describe ways to effectively control policy enforcement at different layers within the IT infrastructure. At the top of the stack are security information and event management tools that can help tie all these tools together to help you track activity across systems for compliance purposes and to automate policy enforcement.

#### Resource Library:

Mike McDanell, security information officer with the Pasadena Credit Union in California, says TriGeo Security Information Manager was initially deployed to help the credit union aggregate all the security logs he was monitoring across systems. He later started using it to monitor and enforce policy actions.

“It’s helped me find out when employees are doing something they’re not supposed to do,” he says. “For example, when something happens—such as when employees plug in something they’re not supposed to use, like a digital camera—I get a little kickback from TriGeo telling me that they’ve done something against policy.”

### 3. ENDPOINT MANAGEMENT

In the past, discussions about the protection of endpoints, such as PCs and laptops, have revolved around anti-virus software. Recently, however, the focus has shifted to policy-based enforcement that offers more complete protection. Policy-based endpoint management should cover configuration management, patch management, access management, application management and even anti-virus applications.

“If you start to control your endpoints from a policy perspective, then suddenly you’ve got the ability to manage your endpoints much more effectively than you can with a single technology or a couple of technologies,” says Scott Johnson, business line executive for host solutions at IBM Internet Security Systems (ISS).

Sonnenschein’s Hansen says protecting endpoint systems is a cornerstone to his approach because once you prioritize information, you’ll likely realize that much of it is stored on these systems. That’s why it’s critical to ensure that endpoint devices are a safe place to house data.

“If you think about it, this is where more of a systems security approach comes in,” says Hansen, who makes use of IBM ISS technologies to carry out that approach. “I think we’re obligated to look at the systems that we can manipulate and manage.”

### 4. APPLICATION WHITELISTING

As hackers continue to develop more sophisticated techniques to evade detection and flood anti-virus technology with thousands of variants of the same malware in order to get past signatures, you might want to consider changing your protection models.

Some enterprises find that application whitelisting is a good alternative to the traditional anti-virus model. The idea is that instead of blocking the known bad elements, you will allow only the specified good applications to run and will block everything else.

According to Josh Corman, principal security strategist for IBM ISS, whitelisting can be appropriate in some use cases, but in other instances, it will drive up operational costs so high that it will become untenable. The best cases are in static environments in which workers will not need to install applications on the fly to get work done. He mentions call center environments as an example.

“One of the best applications we ever saw for application whitelisting was a retail environment with Windows XP-based cash registers,” Corman says. “They modified the image only once every six months, so anything new had to be bad.” In that case, whitelisting was so effective that there wasn’t a need to install anti-virus protection on those machines.

### 5. IDENTITY AND ACCESS MANAGEMENT

One of the key components of any security program is the control of information access based on individual rights and responsibilities. As your enterprise establishes access policies based on identity, you need to institute technologies that ensure people are allowed access only to the information they’re entitled to see or manipulate.

“You need to have a rigorous process in place to allow you the opportunity to manage access to the maximum extent,” says Mark Ford, a principal in Deloitte & Touche’s Security & Privacy Services practice. He adds that too many application silos across IT infrastructures have resulted in a disordered environment for access control.

“It’s been one of the least looked-at aspects of IT environments for many years,” Ford says. “Identity management is really pulling those pieces together. And by allowing you to start to manage it centrally, it gives you the opportunity to take out some of the bad parts.”

For example, one of the “bad parts” is simply relying on the antiquated user name and password setup that’s so prevalent in IT. Second-factor authentication—biometrics, tokens and the like—is a good place to start. And single sign-on technologies can help you tie together the silos Ford mentions.

It’s also important to find a way to handle identity across different organizations and infrastructures when you’re partnering with other enterprises. For example, at the New York-based pharmaceutical company Bristol-Myers Squibb, Shailesh Patel, senior advisor for identity and access engineering, is responsible for making sure BMS can share information safely with other pharmaceutical companies without allowing those partners access to sensitive intellectual property.

Bristol-Myers Squibb uses CA Federation Manager and CA SiteMinder to control and manage identities on either side of a Web portal. This ensures that only the data the company identifies will be shared and that when BMS employees sign on to partner applications, their credential information will not be compromised.

“This prevents a lot of issues, such as man-in-the-middle attacks and denial-of-service attacks,” says Patel. “Plus, with this sort of implementation, you’re not just making sure information is exchanged securely. You’re also making sure that the identity information is created very easily, and that saves time.”

## 6. SECURING THE MOBILE ENTERPRISE

As BlackBerry phones, iPhones and other smartphones advance their data-access capabilities, they obviously become more important tools for road warriors and executives. However, at the same time, they become a huge IT liability. Smart management of these devices must be treated as an important piece of the information security puzzle. Be wary, though, of locking down the smartphones to the point that it becomes impossible to use them for business applications.

One major challenge is that the IT department often doesn’t “own” these devices, and IT never owns the network over which these smartphones ultimately transmit information, says Steven Ferguson, senior network engineer for the Technical College System of Georgia in Atlanta. The college uses a security service called Purewire to institute policy-based controls over its end users’ smartphone activities on the Internet.

“We’re able to stop access to a bad Web site before there’s even an opportunity to infect one of our devices,” Ferguson says. “Our approach is to lock down appropriate employee devices with policies so they don’t have access to certain types of data or certain types of abilities to spread data. The service itself protects against internal threats by blocking access to known data mining sites and things of that nature.”

## 7. DATA LEAK PREVENTION

One way a number of organizations are trying to apply an information-centric security approach is through the use of data leak protection (DLP). According to Rich Mogull, founder of Securosis and former Gartner analyst, a DLP product is defined as one that’s based on central policies that identify, monitor and protect data at rest, in motion and in use through deep content analysis.

The DLP sweet spot so far has been with structured data that regulations have mandated must be protected. “Initially, people who are deploying this are more focused on things like protecting credit card numbers and Social Security numbers,” Mogull says, “because that’s where they perceive their biggest risk.”

Some experts believe that DLP may be a bit of a one-trick pony in that aspect, though. For example, Sonnenschein’s Hansen says his company has looked into DLP but decided against the technology because it was very expensive and couldn’t protect the firm’s unstructured intellectual property information that floats around in Word and Excel documents. He believes the future is in digital rights management technology, which he thinks will offer security managers more control and flexibility.

## 8. DATABASE SECURITY

Corporate databases are the biggest treasure trove of sensitive information, yet database security is often neglected by organizations more concerned with network defenses, endpoint management and the like. This is made even more dangerous by the fact that many enterprise databases are run by legacy applications that were developed in a time before open systems and constant information sharing across networks.

Organizations need a way to monitor who has access to information stored in databases and what these employees do with the data. Many enterprises are using database monitoring and security tools to accomplish this task.

“We have some legacy applications [for which], because of performance reasons, the actual database logs were not turned on,” says McPhedran of Aegon. The company uses a product called Imperva SecureSphere to monitor database activity, look for anomalies in use patterns and flag flagrant policy violations.

As McPhedran puts it, it’s a matter of trusting employees while simultaneously verifying that they are doing the right thing. At first, he got some pushback from executives and human resources managers who said, “We trust our employees.”

“Well, that’s an interesting statement,” McPhedran responded, “but do you want to bet your salary and bonus on it?”

## 9. WEB APPLICATION AND BROWSER SECURITY

Exploitation of Web application vulnerabilities is quickly becoming most hackers’ favorite method of breaking into corporate data stores. Many organizations spend tons of money on firewalls and network security, only to undo it all by opening up holes in the network via Web application portals. Unfortunately, most of them are not doing a good job of baking security into the code of these applications.

Fundamentally, Web application security must be approached by properly training your developers in how to code securely. But that will take time, and mistakes can still crop up, which is why many organizations, such as Sequoia Retail Systems, are also using Web application firewalls as a stopgap measure.

“What it gives us is an ability to stop a threat or prevent a threat until the software can actually be fixed,” explains Bowers, who says Sequoia uses Breach Security Web Defend. “With a Web app firewall there are things you can do with prevention. You can do TCP resets and blocking and use other methods of preventing access to that vulnerability so that you’re actually securing the Web site until you can fix the code.”

And organizations aren’t the only ones that suffer from Web-based attacks. A company’s customers can also be victimized by identity theft through a combination of user error and browser-side vulnerabilities.

Rob Weaver, head of IT security for ING Direct, believes that many security problems in the banking industry stem from customer-side attacks, such as phishing. The company, a unit of ING in Amsterdam, the Netherlands, adopted a third-party product from Trusteer to protect the machines of customers who choose to opt in. The product ensures that every time a customer attempts to log in to ING’s site, that individual is really logging in to ING and not to a phishing site

“Without your customers, there is no company,” Weaver points out. “What greater resource do we have to protect?”

## 10. ENCRYPTION

Encryption of high-priority information should be an integral part of any full-fledged information security program. Many of today’s biggest breaches could have been relegated to the “non-event” category if the affected organizations had implemented encryption to protect their data.

While encryption implementations can sometimes be costly and complicated, you can start simply by instituting whole disk encryption of laptops. Unencrypted mobile devices are one of the biggest culprits of data breaches: The Department of Veterans Affairs’ breach a few years back is a testament to that. Most importantly, though, you should be encrypting based on the risk assessments and prioritizations outlined earlier.

“I think encryption is another area that goes back to the information-centric philosophy,” says Sonnenschein’s Hansen, who employs numerous encryption products for data at rest and in transit. “I think encryption does protect the information, so I’m not going to cut corners on what I spend on encryption.”

Encryption may be a less expensive option in the coming years, as technology vendors make improvements to open standards for key management, which has long been an obstacle to across-the-board encryption implementations. Most recently, a coalition of vendors including EMC, Hewlett-Packard and IBM banded