Advisory Services
Security

Automated.*

Security monitoring: the key to a successful compliance strategy

*connectedthinking

PRICEWATERHOUSECOOPERS

Table of contents

The heart of the matter

Are you listening to your company's log data? It has a lot to say about security.

Every second of every day, your organization's computer network busily generates a torrent of log data. This information details how and when each system, application, and security program is accessed.

It is tempting to think of this information as minutiae—but that would be a mistake.

Instead, think of log information as the least common denominator of data for tracking security events. This information can be used to reduce the complexity of data analysis and prove compliance with regulatory frameworks and internal policies. It can also be an essential tool to safeguard against data and identity theft, abuse of user accounts, unauthorized access, and fraud.

Although these system and network logs provide an advantage for monitoring and managing security, there's a catch. The hardware and software on a corporate network can generate a huge data volume, easily gigabytes a day. How can you possibly manage, analyze, and disseminate all that?

It's a big problem. Monitoring critical security events is one of the most effective ways to comply with regulations, but aggregating log information produces excess data that can easily overwhelm any company's resources.

What is needed is a risk-based, integrated, proactive solution to view and manage security events in real time. Although more companies have automated monitoring, many are still woefully unaware of their security profile.

For instance, 35 percent of chief information officers and other executives interviewed for our annual Global State of Information Security Survey[1] reported they did not know their number of security incidents for the past year, nor the most common avenue of attack. Forty-four percent of the more than 7,000 respondents could not say what security incidents presented the greatest threats to sensitive information, assets, and operations. Surprisingly, 42 percent did not know whether the most likely source of an attack was employees (current or former), customers, partners or suppliers, or hackers.

This startling uncertainty underscores the critical challenges organizations face. Given the broadly accepted reality that every network can be compromised, there are too many systems offering too many services and running too many insecure applications. No amount of code reviews, patching, or access control can safeguard against every attacker. When prevention does fail, how do organizations prepare for the likely intrusions?

Chances are they don't know how.

Clearly, companies need to reinvent their strategy for security and compliance. It takes a skillfully assembled combination of people, processes, and technologies to handle the risks.

[1] PricewaterhouseCooopers, 2008 Global State of Information Security Study, October 2008

An in-depth discussion

Data monitoring proactively guards against risks and helps prove compliance.

In today's business environment, organizations simply cannot operate confidently without an effective security monitoring program. One of the most basic yet successful approaches is to capture and analyze data at the system log level. Examining security events as they occur provides real-time transparency into what is taking place in the network and the effect of the events.

This type of monitoring empowers the security staff to deal with the inevitable consequences of too few resources and too many responsibilities. Security monitoring collects the data needed to generate better detection, assessment, and response processes. It allows key information about the risks to an organization's data and systems to go quickly from operations to the CISO. And it can help eliminate the harmful, costly impact from unauthorized access and activities.

The log data also proves compliance with external regulations and internal policies. Compliance, in fact, has traditionally been the driver behind enterprise security. Although the nature of security has broadened in recent years, CISOs continue to cite compliance with mandates such as the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI) as the primary motivator for security monitoring solutions. In fact, 75 percent of CISOs in our survey cite regulatory compliance as their main reason for security spending.

Yet the need to reduce, alleviate, and transfer risk is certainly not waning. New types of data threats have yielded new risks. We know, for instance, that a breach of a wireless network can cause devastating damage to a company. This type of data breach has been the topic of several high-profile articles in the press over the past couple of years.

But it doesn't stop there.

We have seen a slew of high-profile headlines announcing breaches of consumer information subject to protection under regulations such as HIPAA.

Exploits that take advantage of security weaknesses in smart phones and other mobile devices are on the rise. That's particularly troublesome because more workers are connecting to corporate networks with these devices. Today, 21 million people worldwide use smart phones, and that number is expected to increase exponentially in the coming years.

We are also seeing a groundswell in security threats as more companies work with—and share data with—third parties and partners. This type of arrangement calls for sophisticated vendor-risk management capabilities, yet 76 percent of companies do not keep track of all third parties using their customers' data, according to our 2008 security survey. In fact, only 41 percent of those surveyed say they require third parties, including outsourcing vendors, to conform to the client organization's privacy policies. Clearly, this is a challenge that will impact compliance and security in the near future.

What's more, we have seen an epidemic of credit card fraud—and with it a new way in which hackers can gain access to corporate databases. By making a structured query language (SQL) injection in an XML request, hackers are able to access data such as customers' credit card information, user access details, and privileges. When a company fails to protect customer data from SQL injections, it opens itself up to fines and outside audits, not to mention negative publicity and lasting damage to its reputation.

How risk can bring opportunity

Security monitoring enables organizations to potentially avoid a system compromise by capturing relevant information through sophisticated logging and tracking techniques. The logging capabilities can be configured to capture and respond to critical events—as defined by security risk assessments—that are conducted on applications, networks, systems, and security systems.

The resulting log data empowers organizations to identify and take action on the underlying activity that can impact compliance. But to do so, organizations must effectively collect, normalize, and archive security-related data across an array of devices throughout their enterprises. As we noted, the volume of log data can easily surpass companies' ability to manage and analyze it.
The idea of analyzing log data isn't new. In the past, though, organizations

Data monitoring proactively guards against risks and helps prove compliance.

could not use log data to enhance security because data analysis was done manually and could not be accomplished in real time. Because of this, the information was used only for postmortem or forensic review.

Today, more sophisticated log management tools, as well as increasingly robust computer systems, enable organizations to amalgamate and analyze events in real time. For instance, alerting mechanisms can immediately provide vital information on events such as log-on activity, security warnings, account management, and file access. And the very act of monitoring risks ensures that potential vulnerabilities have been properly identified and rated.

The advanced analysis available today enables organizations to take quick steps to respond to real-time attacks, examine historical data for investigative or audit purposes, and obtain reporting metrics. Analysis of data logs can provide around-the-clock visibility into the state of security across the infrastructure, enabling organizations to prioritize incidents and their management based on their severity and potential business impact.

When organizations begin to understand that these data logs contain the basic building blocks of information that compliance is built upon, they can more effectively design a strategy to comply with regulatory mandates with fewer resources. Prudent security monitoring will also make businesses less vulnerable to hostile attacks such as denial of service, as well as internal data breaches that can jeopardize the integrity of product or service delivery.

Additionally, tracking of data logs will enable organizations to avoid risks such as contract disputes or nonrepudiation. For instance, log management can protect integrity of data by proving that a message has been sent and received. The sender of a message confirming an order cannot later deny having sent the message, and the recipient cannot deny having received it.

A log management approach to security strategy can pay off in tangible benefits. Companies that analyze their data logs will be able to quickly mitigate vulnerabilities and protect themselves from malicious attacks. Security monitoring also helps shield organizations from financial losses, intellectual property theft, loss of brand reputation, erosion of shareholder value, and liability for fraud. And a successful security monitoring program will demonstrate to regulators that organizations are serious about addressing security issues in real time.

Overcoming the challenge of complexity

The benefits of security monitoring—both operational and financial—are compelling, yet many organizations have not made this approach a priority. In fact, companies face a variety of critical challenges that hinder implementation of a security monitoring program.

- Perhaps the biggest obstacle is that an enterprise security monitoring program can be difficult to plan, install, and manage. Creating a security program is research-intensive, requiring deep insight into the company's risks as well as precise analysis of processes and procedures. Once in place, without proper planning, security monitoring can be inefficient and/or ineffective.

What's more, the sheer volume of alerts and log entries—often many gigabytes a day—can challenge even the most technologically sophisticated organizations. But it's not only volume: Complexity is also a key challenge.

Log-correlation tools are built on an esoteric field of knowledge. Many types of log-correlation engines are available, but most organizations do not have the specialized analytical skills to identify a tool that meets their business requirements. The solution must be capable of employing sophisticated scripts to drill down and identify every device and component that produces a log, and then analyze all security events in these logs to determine their risk or severity.

Not only must a CISO help identify the right log-correlation tool, but he must also use his knowledge to convince the board that the security monitoring initiative will deliver business value to the company. Or he must try to, that is. This step is difficult for most CISOs because they often do not know how to quantify the value of the solution.

In the end, many organizations install a log-correlation tool, only to find that they lack the expertise to maintain and analyze the data. When that happens, they may shut down the logs or simply ignore them. To avoid this dead end, many companies could benefit by enlisting expert assistance to find a solution.

How to reinvent your security strategy

Implementation of a security monitoring solution is a big strategic step. As with any transformation, it requires a thorough analysis of the organization's risk appetite and business goals. We believe that the company should align any security initiative with business enablement to help produce better products and services.

Data monitoring proactively guards against risks and helps prove compliance.

During selection of a security monitoring program, much of the hard work revolves around a thorough analysis of the organization's risk exposure. First, security personnel must scrutinize the organization's risk landscape to ensure that security monitoring policies protect against potential risks. It is essential that business unit leaders and other stakeholders are engaged in identifying and classifying risks because they might have insight that the information technology department lacks.

Reaching out to other stakeholders also will help build buy-in for the initiative. If, for instance, you can demonstrate to the legal department that security vulnerabilities pose a potential risk and can clearly show how to mitigate that risk, you will prove the business value of security monitoring.

We believe that proven industry methodologies are key to determining the right processes for your company's program. Methodologies such as Information Technology Infrastructure Library (ITIL), Control Objectives for Information and related Technology (COBIT), and the International Organization for Standardization (ISO) provide a sound foundation upon which to build a security platform.

In addition, roles and responsibilities within the organization must be identified early in the process and used as a base. To guarantee the success of an implementation, security executives must decide who is responsible for which action and in what order. It is also essential to identify the critical applications that carry the highest risk, of course, but security staff must prioritize events, alerts, and incidents so that mitigation can be resolved effectively.

When it is time to determine the technical requirements for security monitoring, most companies turn to third-party partners with expertise in log-management applications. The right tool must offer sophisticated data mining and searches, as well as the capability to normalize results so that logs from different systems can be compared. The solution must be able to monitor the data as mandated by applicable regulatory requirements.

Selecting the right log correlation engines is complicated, and we have found that most organizations lack the expertise and analytical skills required to pinpoint the best solution. The expertise of a third-party specialist can be invaluable to these firms.

Technology is central to security monitoring, but you also need the right people and processes—and a trusted advisor.

Many companies approach their security monitoring solution as a technology initiative. Of course, technology is an important part of it, but planning and applying an effective security monitoring system is largely an analytical endeavor. It requires organizations to step back and objectively consider how their risks and business objectives impact security. This 360-degree vision is often difficult for companies to achieve on their own.

When they turn to outside partners, the biggest challenge may be finding a single company with the experience to provide a full view of security options and best practices. As a worldwide leader in security and compliance initiatives, PricewaterhouseCoopers can supply the technology and business knowledge, and then leverage our proficiency at solutions integration to offer the most effective system.

PwC has a long history of helping companies understand their risk appetite and meet compliance requirements. We take the time to listen to your situation, and our people understand sophisticated technology and how to optimize it for individual needs. Our global staff can coordinate among regional offices so that the biggest jobs are undertaken with the best care, no matter where they are located.

We do not consider providing an effective solution to risk-based security monitoring an insurmountable challenge. Rather, we see it as an opportunity to improve your organization's security and compliance. PwC can offer the support, advice, and assurance you need to set up your own customized security monitoring solution.

www.pwc.com/advisory

To have a deeper conversation on the topic mentioned, please contact:

Ciarán Kelly
Partner
ciaran.kelly@ie.pwc.com
01-7926408

Garrett Cronin
Partner
garrett.cronin@ie.pwc.com
01-7928807

Pat Kelleher
Director
pat.c.kelleher@ie.pwc.com
01-7927118

David McGee
Director
david.a.mcgee@ie.pwc.com
01-7928785

Deirdre Farrelly
Senior Manager
deirdre.m.farrelly@ie.pwc.com
01-7926706

Darren D'Arcy
Senior Manager
darren.darcy@ie.pwc.com
01-7928532

Liam McKenna
Senior Manager
liam.mckenna@ie.pwc.com
01-7928897

Kieran Mongan
Senior Manager
kieran.mongan@ie.pwc.com
01-7928632

Feilim Harvey
Manager
feilim.harvey@ie.pwc.com
01-7928631

Brían McSweeney
Manager
brian.mcsweeney@ie.pwc.co m
01-7928254

Robert Byrne
Manager
robert.a.byrne@ie.pwc.com
01-7926086

Eithne O'Riordan
Manager
eithne.oriordan@ie.pwc.com
01-7928109