Sponsored by tripwire TAKE CONTROL.

LOG MANAGEMENT IN A CYBERWORLD

As the world becomes increasingly digitized, we've witnessed the rise of myriad cyber attacks aimed at private and public sector organizations. Cybercrime, increasingly operated under well-muscled organized crime syndicates, has become a huge threat. With so many potential cyber villains poking around the gates, enterprises must have strong protections and pristine visibility into what's happening on the network. In these articles, *CSO* and its sister publications *CIO, Computerworld* and *Network World* explore the increasing importance of log management as cybercrime and other malicious threats grow.

eGuide

CIO COMPUTERWORLD CSO InfoWorld ITWORLD NETWORKWORLD®

IN THIS eGUIDE

2. Cybercrime: The Mega Threat

What threats to a company's sensitive and confidential data are getting worse, staying the same or actually becoming more manageable?

3. Organized Cybercrime Revealed

Criminal groups have discovered cyberspace—they're specialized, can create markets and above all, are entrepreneurial.

8. The Seven Deadly Sins of Network Security

Companies that suffer serious network security breaches have almost always committed one (or all) of seven deadly sins. Is your company guilty?

12. Are SIEM and Log Management the Same Thing?

A *Network World* tester answers the question.

13. University of Tennessee Finds 'Bonus Benefits' in Log Management

Log management can help with security and compliance.

15. Cybercrime Resources

Tips and tools to help your organization stay secure despite the mounting cyber threat.

Analysis

CYBERCRIME: THE MEGA THREAT

Dr. Larry Ponemon • CSO

What threats to a company's sensitive and confidential data are getting worse, staying the same or actually becoming more manageable?

Last year's Security Mega Trends Survey was conducted by Ponemon Institute and sponsored by Lumension to better understand if certain publicized IT risks to personal and confidential data are, or should be, more or less of a concern for companies. We asked 577 IT security practitioners to consider how 10 Security Mega Trends affect companies today and to predict their impact during the next 12 to 24 months. The opinions of these experts, we believe, will be helpful to companies that are struggling to understand how they should allocate resources to the protection of data during these difficult economic times.

We selected the following mega trends for this study based on input from a panel of experts in IT security. They are: cloud computing, virtualization, mobility and mobile devices, cybercrime, outsourcing to third parties, data breaches and the risk of identity theft, peer-to-peer file sharing and Web 2.0.

The study examined the risks posed by mega trends that exist today and how the risk will change over the next 12 to 24 months. According to an overwhelming 77 percent of individuals in IT security responding to our survey, cybercrime will become a high or very high risk over the next 12 to 24 months.

The selection of cybercrime as the mega trend most likely to be a high or very high risk in the next 12 to 24 months can be partly based on the fact that 92 percent of respondents in our study reported that their companies have had a cyber attack. The biggest security risk associated with cybercrime is that such an attack will cause a business interruption followed by the theft of customer and employee data.

Other mega trends becoming more risky are cloud computing, malware, web 2.0 and mobile devices.

Organizations are faced with a plethora of security threats to their confidential and sensitive data assets. Forecasting the areas that pose the highest risk will help companies create an IT security strategy that is as cost effective as possible in times of tightening budgets. •

Dr. Larry Ponemon is the chairman and founder of The Ponemon Institute.

In-depth

ORGANIZED CYBERCRIME REVEALED

By Michael Fitzgerald • CSO

Criminal groups have discovered cyberspace—they're specialized, can create markets and above all, are entrepreneurial.

As if CSOs don't have enough on their plates, they now need to beat back made men, capos and the other elements of the Mafia. Yes, the Mafia is formally involved in cybercrime, or so alleges the U.S. attorney for Florida, who filed charges against associates of the Bonanno crime family that included pilfering data from Lexis-Nexis.

The Mafia engaging in cybercrime might sound like your grandmother joining Facebook. In fact, "the majority of data breaches are the result of organized crime," says Nick Holland, an analyst at Aite Group in Boston. That doesn't mean it's the conventional Mafia pulling the strings—though it can be. In fact, it's hard to tell just who is in control sometimes. For the most part, cybergroups that become notorious, like the Rockfish or the old Russian Business Network, do so because very few cybercrime groups publicize themselves, says Steve Santorelli of Team Cymru. (Cymru, pronounced cumri, is the Welsh word for Wales.)

In fact, observers sometimes disagree on just who's behind a crime. Take 2008's RBS Worldpay scam, which saw hackers not only make off with 1.5 million records from the electronic payments processor, but make fake ATM cards used to withdraw more than $9 million in 49 cities around the world in a one-hour period. Frank Heidt, CEO of Leviathan Security in Seattle, thinks this was a case of an extremely well-organized group with roots in Russian organized crime. Peter Cassidy, director of research at Triarche Consulting Group in Cambridge, Mass., says it looks like a franchise-style operation in which the data and details on how and when to use it was sold to groups operating in different regions.

Either way, it's organized crime. Just a few years ago, most hackers either acted for the glory of spreading a virus they'd written, or handled all aspects of an operation, from phishing to building fake websites to cashing in on the fraud. Since then, cybercriminals have discovered Adam Smith. They specialize, they create markets and above all, they're entrepreneurial. And because of the Internet, "you get radical distribution of labor and a radically fast ability to recruit skills," says Cassidy.

These organizations adopt various structures. The crime family model obviously still applies when the Mafia is involved. Some groups that seem independent of the Mafia, like the people who ran Carder's Market—an underground site for buying and selling

credit card information—also use a Mafia-like structure and terminology. Phishing groups tend to work like Japanese keiretsu, says Cassidy, who is also secretary of the Anti-Phishing Working Group. Cybercriminals sometimes use a hub-and-spoke model, where a criminal mastermind puts together various tools and people needed to pull off a job. Want a botnet? A Symantec study found that on average, you could gain use of one for $225. Need a keystroke logger? Average price: $23. Want someone to host a phishing scam? That can be had for as little as $2. A specific vulnerability in financial sites might cost $3,000.

You can even get specialized versions of malware, websites, etc.—the Verizon 2009 Data Breach report found that 59 percent of the malware it saw was customized. Sometimes the criminals adopt models that look like the software business. You can literally buy "fraud as a service," where criminals subscribe to hosted services—a story first illuminated in CSO's September 2007 article, "Inside the Global Hacker Service Economy."

Between 70 percent and 80 percent of malware now comes from organized groups, estimates Bogdan Dumitru, CTO at BitDefender, an antivirus firm based in Romania. Lone hackers still break new ground: Dumitru says Twitter malware that's popped up recently was "developed by a kid. But in the next two months we'll probably see organized entities taking advantage of it."

Dark Market

The fluidity of cyberorganizations can make them more difficult for law enforcement to penetrate than their real-world counterparts. But it's not impossible. DarkMarket, a spam and phishing forum, eventually was taken over and hosted on FBI servers. J. Keith Mularski, the supervisory special agent at the FBI assigned to the National Cyber Forensics and Training Unit, ran this site undercover, posing as a spammer named MasterSplynter.

DarkMarket started leading to arrests of prominent spammers and phishers in May 2007. It eventually closed in October 2008, after the arrest of DarkMarket's boss, a Turkish hacker whose handle was Cha0, leaving Mularski as the last leader standing. Ultimately, sixty people—most of them the most powerful members of DarkMarket—were arrested in at least four countries: Germany, Turkey, the U.K. and the U.S. The FBI also got six complete malware packages and may have prevented $70 million in losses at financial services firms. Plus, it arrested Cha0 and his seven-member gang in Istanbul before they could ship out about 1,000 ATM skimmers, which prevented an additional $33 million in losses.

"Sure, they'll reorganize, but with every law enforcement action, it's a little bit harder to regroup," says Mularski.

The DarkMarket operation has at least temporarily driven many cybercriminals off of Internet Relay Chat and bulletin boards, says Team Cymru's Santorelli. They've opted instead for private instant messenger groups that they control, says Santorelli.

DarkMarket involved law enforcement groups working together across borders. That's a good step in what remains a challenge. Cybercriminals "are good at finding cracks in international law," says Yuval Ben-Itzhak, CTO of security firm Finjan. A group might be based in one country, use servers in a second and commit crimes in a third.

This problem has led to calls for better international law. For instance, Brazil has become a hotbed of bank fraud, phishing and Trojan activities since the penalties there are very light. Some are even calling for a group that can force Internet service providers to cut off servers that obviously house phishers.

More countries may be taking cybercrime seriously. While Eastern Europe is seen as a kind of Wild Cyber West, in 2008 Romanian police arrested 20 people in Ramnicu Valcea and Dragasani, towns known for organized eBay scams (one tried to auction off a Romanian city hall). Florin Talpes, BitDefender's CEO, says joining the European Union in 2007 has changed attitudes in Romania and in Bulgaria, which have created stronger legal frameworks for fighting cybercrime.

Mularski, however, cites Romania as a country where traditional organized crime clearly has become involved in cybercrime. The FBI arrested 35 Romanians running a phishing and ATM skimming scam in Los Angeles, and Mularski says they were connected with Romanian organized crime. He concedes that the FBI did work with Romanian law enforcement to make 80 arrests in the two countries in a separate case. At least there are arrests in Romania. That rarely happens in a place like Russia, although two unnamed Russian hackers were recently indicted in the Heartland and Hannaford hacking cases—along with U.S.-based alleged mastermind Albert Gonzalez.

Still, even cybercrime groups suffer from market forces. They've so flooded the cyber black market with credit card data that prices are falling. Organized crime has shifted its targets. They're after medical records, which are valuable. They target company CFOs, aiming to get access to corporate bank accounts and wire money out of them. That tactic has had success: In late July 2009, *The Washington Post* detailed how stealth Trojans had been used to infect a PC used by a county treasurer, a school district and the head of a small business. Hundreds of thousands of dollars were wired to money mules who then sent the funds on to bank accounts in the Ukraine and Russia.

Targeted industries are also shifting. While financial firms make the juiciest targets, Borenstein says that RSA is seeing more activity around the healthcare, manufacturing and government sectors.

Also on the rise are call center scams. Organized criminals may get access to someone's bank or brokerage account but be unable to transfer money because of Web protections put in place by financial firms. So the criminals call customer service to complain and even bully, hoping to get help in transferring money out.

Meanwhile, social networks "are gold mines to social engineers, to someone who wants to get to the CFO of an organization to attack them," says Joshua Corman, principal security strategist at IBM Internet Security Systems. Corman says CSOs need to tell employees not to answer things like those "25 Questions" surveys that run rampant on sites like Facebook because the answers often include information used as hints for account passwords.

Organized Crime Bookshelf

Organized Crime
By Howard Abadinsky (9th Edition - 2009)
A comprehensive look at organized crime origins, methods and impact.

Retail Crime, Security, and Loss Prevention
By Charles Sennewald and John Christman (2008)

The Mafia DVD Set
A four-disc documentary on the mafia in America, from Prohibition to John Gotti.

Battling Back

Even as cybercriminals get more sophisticated, the best ways to stop them are often the simple ones. Verizon's report said that many credit card breaches occurred at firms with minimal PCI compliance. It also

found that 51 percent of firms breached had never changed the default vendor passwords for equipment.

Equipment itself gets overrated by CSOs and CISOs, says Michael Levin, former deputy director of the National Cyber Security Division of the Department of Homeland Security. "They are wasting money on hardware and software," he says. Instead, they should do things like tell employees not to click on e-mail attachments and other basics. Levin has cofounded the Center

CITING CYBERCRIME, FBI DIRECTOR DOESN'T BANK ONLINE

Robert McMillan • IDG News Service

The head of the U.S. Federal Bureau of Investigation has stopped banking online after nearly falling for a phishing attempt.

FBI Director Robert Mueller said he recently came "just a few clicks away from falling into a classic Internet phishing scam" after receiving an e-mail that appeared to be from his bank.

"It looked pretty legitimate," Mueller said in a speech at San Francisco's Commonwealth Club. "They had mimicked the e-mails that the bank would ordinarily send out to its customers; they'd mimicked them very well."

In phishing scams, criminals send spam e-mails to their victims, hoping to trick them into entering sensitive information such as usernames and passwords at fake Web sites.

Though he stopped before handing over any sensitive information, the incident put an end to Mueller's online banking.

"After changing our passwords, I tried to pass the incident off to my wife ... as a teachable moment," he said. "To which she deftly replied, 'Well, it is not my teachable moment. However, it is our money. No more Internet banking for you.'"

Mueller said he considers online banking "very safe" but that "just in my household, we don't use it."

Phishing has evolved into a big problem, not just for banks, but for online retailers and even providers of consumer Web applications such as Facebook and Yahoo.

In June 2009—the latest month for which figures are available—the Anti-Phishing Working Group counted nearly 50,000 active phishing Web sites, the second-highest number it has ever recorded.

Late last week, criminals posted tens of thousands of passwords belonging to Microsoft Live Hotmail, Gmail, and Yahoo accounts online. They are all thought to have been stolen via phishing.

Mueller's FBI has had some success in going after phishers. It recently announced it had arrested 33 people in the U.S. in connection with an international phishing operation. Egyptian authorities have charged 47 in connection with the same scam.

"They targeted American financial institutions and also approximately 5,000 American citizens here in the United States," Mueller said. Dubbed Operation Phish Phry, "it is the largest international phishing case ever conducted," he added.

"Far too little attention has been paid to cyber threats and their consequences," Mueller said. "Intruders are reaching into our networks every day looking for valuable information. Unfortunately they're finding it. "

FACECROOKS?

Social networks are "gold mines to social engineers, to someone who wants to get to the CFO of an organization to attack them."
— Joshua Corman, principal security strategist, IBM Internet Security Systems

for Information Security Awareness in Fairfax, Va., which has prepared the free, online awareness training offered through Infraguard, the FBI's regional effort to work more closely with private companies on cybercrime.

CSOs should get involved with groups like Infraguard or develop relationships with regional FBI or Secret Service agents and local law enforcement. They should also regularly assess their risk levels. "You have to assess every record and every piece of data in the place for its value to criminals," says Cassidy.

CSOs should also be prepared to do much of their own forensics work before going to law enforcement. Levin says once law enforcement is involved, they may need a search warrant or even a grand jury subpoena to do things like explore company computers for malware, slowing the process.

Above all, talk to people outside of the security department or IT, and talk to peers at other companies, especially financial firms, which are on the front lines of the corporate cyberwars. The cybercriminals don't cloister themselves, and CSOs can't either. •

In-depth

THE SEVEN DEADLY SINS OF NETWORK SECURITY

By Bill Brenner • CSO

Companies that suffer serious network security breaches have almost always committed one (or all) of seven deadly sins. Is your company guilty?

Anyone worth their salt in information security will tell you a solid defense is built upon multiple layers of technology, policy and practice. That's defense-in-depth.

The technology layers are a critical piece of that puzzle—of course. But companies that suffer a major network breach have frequently failed on a more fundamental level. Here are the deadly network security sins experts say are rampant in the corporate world. Avoid these sins and you will have taken a critical step toward a secure network.

1 Not measuring network security risk

This sin typically involves a failure to take a thorough measurement of the company's most important assets and network configurations surrounding those assets. As the saying goes, you can't protect the crown jewels without first knowing what they are and where they are.

Chuck McGann, manager of corporate information security services for the U.S. Postal Service, is among those who cited the "failure to have a network topology diagram or discovery software to identify what is on your network and what it is doing."

When a company fails to take an accurate measurement of risk, the powers that be are often lulled into the false sense of comfort that comes with simply having antivirus software and a firewall, says Michael Leigh, senior information security manager at Cisco Systems. The bad news here is that some of that technology can become the very problem the organization sought to prevent.

"I find that a number of organizations believe their security appliance/devices (routers, firewalls, switches, etc.) are secure and do not layer their defenses around these devices," Leigh says. "Too often these devices are the toe hold into an organization."

Ken Smith, a security solutions architect at Forsythe Technology, says implementing security controls and policies without first understanding business needs and requirements is a problem he has witnessed many times. "It's the primary reason that security practitioners are often thought of as rigid or not adding value to the organization," he says. "When this is the case, users will come up with workarounds that could be worse than the problem you are trying to prevent in the first place."

2 Thinking compliance equals security

Typically the sin committed by upper management, this is the case where a company has invested a lot of time and treasure on meeting the requirements of government regulations and industry standards like HIPAA or PCI DSS, then dropping the ball once all the boxes on a compliance checklist have been checked off.

Experts unanimously say that, while these regulations can provide a good start on network security, by no means do they include all the requirements necessary to protect data.

The compliance-equals-security view is similar to the flaw of looking at security as a project rather than a process, says Timothy Brush, an independent security consultant based in Canada. Upper management looks at security as a project that must be dealt with, typically because of compliance concerns, then loses interest.

"The security landscape—technologies, vendors, attack vectors, vulnerabilities, etc.—is constantly changing," Brush notes. "The latest technology—firewall, IDS/IPS, identity management systems, vendor-driven technology du jour—or procedure—policy, standard, framework, business process—may increase an organization's security posture for the moment," but probably not a year or five down the road.

Daniel Blander, a CISM, CISSP and president of Techtonica Inc. in Los Angeles, has seen this sin committed over and over again, and mentioned it in a recent report on post-PCI audit troubles.

"Having worked on two PCI projects, the biggest challenge is typically management's view, 'Well, we're compliant, so we're done.'" he says. "Some parts of management understand the 'why' of PCI, but don't understand overall risk management. Maintaining attention after the fact is the biggest challenge."

3 Overlooking people

A similar thread in all the sins mentioned is a tendency of organizations to look at security as a mostly technological issue, ignoring that the biggest dangers emanate from the people using the machines without really understanding what they're doing—or that unwary employees can be exploited through common social engineering tricks.

"Too many focus on tools for the infrastructure within their organization and budget," says Matt Polatsek, a senior security engineer at Hughes Network Systems in the Washington D.C. area. "The people and/or employees are so often overlooked in either purposeful sabotage or inadvertent disclosure."

Firewalls, VPNs, IDS/IPS, SIEM tools, remote access, encryption, switches, and routers are all great and fun to play with, he says. But in the end, too few see the value in security awareness among the larger workforce and often lack a viable, enforceable policy on what users can and can't do on company machines, he adds.

Gary Bahadur, a Miami-based operations and security technology executive and a former vice president at Bank of America, cited the problem at the top of his personal list.

"Not educating/training the end user in basic security measures is a problem," he says. "All the security and money spent is useless if the end user continues to click on e-mail links, tape the password to the computer and surf porn sights. The biggest bang for the security buck is user education."

4 Too much access for too many

Most respondents agreed a lack of access control is the sin that has sent many a company down the road to trouble.

"The biggest failure I've seen is the lack of management support for the necessary expenditures and for the ongoing need to have a clear, working policy on who has authority to do what, who's responsible for granting or denying access, who's responsible for vetting changes, and having it all done in such a manner as to not be too cumbersome on the operations of the company," says Toivo Voll, a network administrator for an educational institution in the southeast.

George Johnson, chief security officer at the National Center for Crisis and Continuity Coordination (NC4), says IT shops often assign everyone administrative access to reduce the workload tighter controls involve. This, he says, is a recipe for a massive compromise.

But the opposite practice of allowing only executives administrative access while locking everyone else out is fraught with danger as well.

"Hackers are targeting execs—a tactic called 'whaling'—so this is a huge risk," Johnson says. "It also severely damages the credibility of the security mission when it is obvious that the boss doesn't care about it. Culture springs from the top."

The 2008 incident in San Francisco provides another illustration of the risks of putting too much control in one person's hands. A network administrator for the city was able to lock everyone else out of a critical system.

5 Lax patching procedures

A common security failure often stems from a company's inability to keep up with all the patches needed on the network's various devices. Proof of this problem was offered in a recent study from Verizon showing that 90 percent of successful exploits these days involve vulnerabilities for which a patch has been available for six months or longer.

"For the overwhelming majority of attacks exploiting known vulnerabilities, the patch had been available for months prior to the breach," Verizon says in its *2008 Data Breach Investigations Report*. "Also worthy of mention is that no breaches were caused by exploits of vulnerabilities patched within a month or less of the attack."

The bad guys know a lot of companies are slow to patch, and so they continue to cook up exploits for the older vulnerabilities, experts say. In fact, security experts say, worms like Blaster and Sasser—launched five to six years ago against vulnerabilities for which patches were made available around the same period—are still in wide circulation today.

Dan Ward, an IT security analyst at Acxiom, cites this as one of the major sins on his personal list. This problem, he says, extends not just to poor operating system patching, but also middleware, application and even device driver security updates.

6 Lax logging, monitoring

The final item on the list involves the failure of many organizations to keep an eye on all the activity logs coming out of the various devices on the network. As McGann points out, a company must know what's going on in the network in order to secure it.

Ward agrees. "Log management is one of those issues that no one really likes to deal with," he says.

"But since we're security professionals, we really need to dig into our log data and understand what's happening at all levels of the end-user chain."

7 Spurning the K.I.S.S. principle

It has been said that in the art of network security one must observe the K.I.S.S. principle—"keep it simple, stupid," or "keep it simple for security." Unfortunately, networks are getting increasingly complex as companies bolt one device onto the next, often configuring things badly along the way.

Add the failure to segment certain parts of the network from other parts and you have a recipe for disaster.

"What can I say? Complexity is bad, very bad," Brush says.

Nick Puetz, director of data security at FishNet Security, says trusted networking is one of the founding concepts of IT security. However, while most companies will spend millions of dollars to secure their perimeter, "they don't take any time to segment their internal network."

As a result, it becomes impossible to get a grip on where sensitive data is flowing from one part of the network to the next. If you can't be certain where all the data is on the network, protecting it is exceedingly difficult. It's also the type of thing compliance auditors frown upon. •

Opinion

ARE SIEM AND LOG MANAGEMENT THE SAME THING?

By Greg Shipley • Network World

Like many things in the IT industry, there's a lot of market positioning and buzz tossed around regarding how the original term of SIM (security information management), the subsequent marketing term SEM (security event management), and the newer combined term of SIEM (security information and event management) relate to the long standing process of log management.

The basics of log management aren't new. Operating systems, devices and applications all generate logs of some sort that contain system-specific events and notifications. The information in logs may vary in overall usefulness, but before one can derive much value out of them, they first need to be enabled, then transported and eventually stored. It is here that the first challenge of log management is presented: How does one gather this data from an often distributed range of systems and get it into a centralized (or at least semi-centralized) location?

There are varying techniques to accomplish centralization, ranging from standardizing on the syslog mechanism and then deploying centralized syslog servers, to using commercial products to address the log acquisition, transport and storage issues. Some of the other issues in log management include working around network bottlenecks, establishing reliable event transport (syslog over UDP isn't exactly the most robust of models), setting requirements around encryption, and managing the raw data storage issues.

So the first steps in this process are figuring out what type of log and event information you want to gather, how to transport it, and where to store it. But that leads to another major consideration: Once you have it, what do you want to do with it? It is at this point where basic log management ends and the higher-level functions associated with SIEM begins.

SIEM products typically provide many of the features required for log management but add event-reduction, alerting and real-time analysis capabilities. They provide the layer of technology that allows one to say with confidence that not only are logs being gathered but they are also being reviewed. SIEM also allows for the importation of data that isn't necessarily event-driven (such as vulnerability scanning reports)—hence the "information" portion of SIEM.

In watching the market mature over the past 10 years, we believe there is room for both traditional log management tools and the real-time analysis capabilities provided by SIEM tools, but we suspect that organizations would prefer to go to a single vendor for both. Clearly organizations have to solve the first problem (log management) in order to address the second (analysis and monitoring), but the wise purchaser will know that after the first problem is addressed the second will become immediately apparent. Plan accordingly. •

Shipley is the CTO of Neohapsis, an information risk management consulting firm.

Case study

U OF TENNESSEE FINDS 'BONUS BENEFITS' IN LOG MANAGEMENT

Linda Musthaler • Network World

Log management can help with security and compliance.

I recently talked with James Perry, the information security officer at the University of Tennessee about his use of log management. His department has been using ArcSight Logger since July 2008, and he's still finding interesting use cases. Here's a look at some of them and how his organization is benefiting from log management.

In many ways, a university environment is much more complex than a corporate environment. Perry's team has responsibility for security and operations at five campuses. He says they act almost like an ISP because they can't dictate what products, technologies and applications are used by students, professors and campus departments. For a university network manager, there's a strong need to balance student freedom with network security.

At the same time, the environment can't be a free-for-all. The university network serves 159 merchants such as bookstores, coffee shops and other sales operations. This means there is a requirement for PCI compliance. Two of the campuses work with medical data. That means HIPAA compliance. There's financial data, meaning GLBA compliance, and so on. As you can see, the need to log and monitor all activities for compliance purposes was a big driving factor in the university acquiring a log management product. What's more, like most organizations today, the university is experiencing budget cuts, so Perry was forced to improve security and operations with fewer resources. Log management has helped to achieve the latter objective as well.

Perry's team selected ArcSight Logger as their tool for two reasons. First of all, they were already using the ArcSight SIEM Platform to collect filtered security event information. Using the log management product from ArcSight meant that the two tools could easily use the same data for different purposes. Second, ArcSight Logger allows the university to collect data from many different types and brands of devices, bring it together in one place and normalize it for detailed reporting and alerting mechanisms. He calls ArcSight Logger "a syslog-type tool on steroids."

Prior to installing the log management tool, the university just had the SIEM solution. This tool would filter out extraneous data and look only for security events. When they added the log manager, the "extraneous" data that used to be discarded began to reveal lots of very useful compliance and operational information. For example, Perry says they can now see the signs of a pending device failure by reading specific events. These events trigger an alert to a technician who can tend to the device's needs before a complete failure.

Log management has helped with security, too. If there is a security breach from within, the log data helps pinpoint the source within minutes. Previously, security analysts could spend upwards of 45 minutes to find the source. That time is now down to two to three minutes.

Perry expected they would address their compliance requirements with the log management system. He's pleased to see there are "bonus benefits" that are making his team more efficient, and he expects they will find more uses for log management as time goes by. •

Musthaler is a principal analyst with Essential Solutions Corp.

Tips and tools

CYBERCRIME RESOURCES

Hassle-free Compliance

Does your organization treat compliance as a set of check boxes designed to meet the auditors' requirements? If so, you are wasting a lot of time, money and precious IT resources. This white paper is a roadmap for making compliance a painless, efficient, and routine part of your IT processes.

Download >>

Pulling the Plug on Legacy Log Management

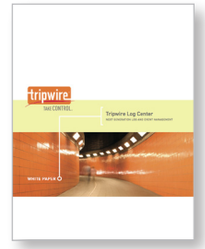
When it comes to log management today, CSOs have been left in the lurch. According to a new IDG Research Services survey, organizations are poised to "rip and replace" legacy technology to get a better handle on compliance and security.

Download >>

Proactive Visibility: IT Security Without Business Disruption

For IT security, determining how to gain visibility into systems without disrupting business operations is a key challenge. Some approaches use passive data collection, but do little with that data to promote security. Yet others, like vulnerability penetration testing, are capable of exposing vulnerabilities, but in doing so may take down a critical business system.

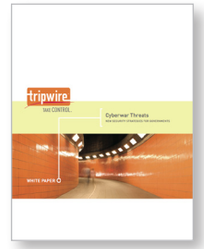
Listen >>



Tripwire Log Center: Next Generation Log and Event Management

Managing event logs was once seen as a job to be avoided, but IT compliance regulations have made it a necessary practice. Now, IT and security managers are also discovering the value embedded in those logs to help them improve their organizations' security. What's missing are integrated solutions that provide the performance, scalability and flexibility to match the needs of the modern enterprise.

Download >>



Cyberwar Threats: New Security Strategies for Governments

Threats posed by cyberwar cannot be defended using the traditional all-or-nothing security that's aimed solely at keeping attackers out of the government enterprise. Learn why Tripwire's solutions provide the real-time awareness necessary to fight cyberwar.

Download >>