Data protection

Safeguarding critical enterprise data is not a simple task, but new technologies can assist.

ebook

An SC Magazine publication

Sponsored by

nCircle

Data scrutiny

Finding, classifying and safeguarding critical and sensitive data in the enterprise is not an easy task, but there are technologies to help, reports Beth Schultz.

Enterprise IT security professionals have long recognized the need for a defense-in-depth strategy, starting at the corporate edge and layering in one protection mechanism after another. Of late, they've been zeroing in on the very center of the bull's eye.

"Companies are getting really specific," says Emily Mossburg, a principal with Deloitte's security and privacy practice. "They want to be able to understand and protect particular data elements and, in some cases, specific instances of these data elements."

So when people today say "data security," she adds, "that really is what we're seeing in the marketplace right now – an emphasis on the data itself and how to put some level of protection on each of those data elements."

Developments which push corporate data outside the perimeter – such as use of mobility technology, external social networking and public cloud services – have heightened the need for data-specific security, not to mention concerns over it, says Jeff Falcon, senior security solutions specialist at CDW, a Vernon Hills, Ill.-based computer reseller.

"The pace at which things are changing seems to be a bit unsettling for many organizations and their pain points are consistent," he says. "They're asking themselves questions such as 'What intellectual property and regulatory data do I have? How is it being used, and where on the network does it reside?'"

Then when – or if – an organization has the opportunity to obtain visibility into the processes of where the data is and how it is ultimately being used, the big question is 'How do we protect it?,' he says. "And, from a process perspective, another question arises: 'Do we need to make changes in the way we allow access to and delivery and storage of information?'"

The trouble is, he says, that the data elements in need of protecting range from obvious, regulated bits – such as Social Security or credit card numbers – to amorphous blobs of intellectual property, the worth of which can be highly subjective and vary from one company – if not department – to the next.

"It is clear what a data element is as it relates to a law or regulation, and what protection is needed to be in compliance," Deloitte's Mossburg says. Much harder is figuring out data elements from an intellectual property perspective and determining how to put together a view of intellectual property so tools can recognize it.

Wrapping up the corporate goodies

That's where many enterprise IT security organizations are now focused, trying to get as good a handle on protecting intellectual property as they believe they have on keeping regulated data safe, she adds. "Once you can define your intellectual property, you can better find it, and once you can find it, you can better understand the risks and, of course, the value and how it should be protected."

A focus on intellectual property is growing among enterprise IT security organizations, agrees Bill Phelps, executive director and North America security practice lead at Accenture, a global management consulting, technology services and outsourcing company.

"Organizations over the last year and a half have become more focused on intellectual property as something they're protecting from an information security standpoint, not just PII [personally identifiable information] and credit card numbers and other discrete information," he says. "They're finding that they have other classes of data, much of it unstructured, that needs to be protected."

Processes and procedures that allow an organization to identify and evaluate data's significance are hugely important, Phelps says.

1

in every 10 laptops will be stolen within the first year of purchase.

– NewSoftwares

"Technology capabilities – such as digital rights management, data leakage prevention [DLP], encryption, database security, identity management linked to particular types of data – presume that you have a data classification model," he explains. "It also presumes business rules about who in an organization has access to what types of information, about what information needs to be protected at different levels and that you have information about where the data sits. But in many cases, these strategic prerequisites don't exist."

IT security professionals are figuring out that just watching for a Social Security number leaving the organization doesn't achieve a whole lot, he adds. "They need to step back and better analyze the information in the organization."

Mapping out corporate data

Understanding where data sits in the organization involves mapping the data lifecycle or, put another way, creating a business process data map, Mossburg says.

"You want to understand the infrastructure that the data is flowing over – the servers, applications, repositories and warehouses and so on," she says. "But you also need to understand how it flows from a process perspective. This helps point out threats to consider that are outside the obvious and provide an understanding of the value of and risk to the data – where should and shouldn't it be, how should and shouldn't it be used.

"Then based on all that information, you can put together a patchwork quilt of security that aligns to the data as it moves through the organization," Mossburg says.

IT departments can get their hands on many excellent data mapping tools, but they must complement those with manual work, she cautions. "A tool isn't going to give you the context you need. For that you need a manual effort."

To get that context at International Rectifier (IR), a global power management technology company in El Segundo, Calif., James Tu, director of information security, says he tops off monitoring via DLP tools from McAfee and Websense with business user interviews.

"In setting the companywide data classification policy, the security team has to work with the business units to figure out how critical data is processed," Tu says. "It is the data owners who understand that, not the security people. But while business users can tell you in generic terms what kind of information is critical and where they think the data is stored, they're not really sure."

> "The more automated and preventative the tools are, the better."
>
> *– Derek Brink, VP and research fellow in IT security at Aberdeen Group*

"But using DLP in monitoring mode, before we go into a business unit, we know exactly how those people use the data, where they access data, how they store data and where they send it to," he adds. "Armed with that data, plus interviews on how they use data inside and outside the company, we can put together a policy for how we handle, use and control data."

With data mapping in his arsenal, Bruce Phillips, CISO at Fidelity National Financial (FNF), a provider of title insurance, specialty insurance and claims management services in Jacksonville, Fla., says he knows firsthand the strategic importance of such projects.

"Our challenge, and it is not unique, is that we've grown by acquisition," Phillips says. "As we go through the mergers and acquisitions, we need to understand the thought processes going on within different cultures as they built or bought applications, where they put them, so we know where the data lies. We can do a data map to understand first where the data is, what the sensitivity is, and then drill down to regulatory require-

512m

records have been breached in the United States since 2005.

–Privacy Rights Clearinghouse

ments and see where controls are in place and where we can mitigate risk."

That process isn't without pain, he says. "If anyone tells you that doing a data mapping project takes one person and a couple of months, I would seriously have him checked into a facility," he adds. "It is extremely painful to go through a data mapping exercise."

In FNF's case, he says, the company's aggressive acquisition strategy has added to the challenge. "As we bring in new organizations, we have to indoctrinate them to the process of identifying data sources and repositories and stewards, and classify the data, at least in a simple manner, to get us to a starting point," he says. "That's always a challenge because no one wants to do it – it is extra work, and it isn't easy."

> "The security team has to work with the business units to figure out how critical data is processed."
>
> *– James Tu, director of information security, International Rectifier*

Mossburg recommends creating a visual picture of the data flow and then mapping threats against it. "Then you can lay technology and controls on top and, getting back to the patchwork quilt idea, cover those risks you've identified," she says. "When you can see this visually, you get a powerful picture and more of an understanding of your situation."

Similar to any security-risk assessment, this is not a trivial undertaking, Phelps says. "But, companies just have got to bite the bullet and go through data discovery, classification and cleanup," he says.

He advises Accenture clients, which tend to be global companies with revenues in excess of $10 billion, to plan on spending anywhere from 18 to 24 months on such a project, and sometimes longer, Phelps says.

"Organizations have to understand how big of a challenge this is," he says. "They have to figure what types of information they believe are most important to be protected and determine whether that information is relatively well understood and controlled today or highly distributed with uncertainty around how well it is controlled."

Phelps equates the corporate challenge to one a longtime homeowner might face if suddenly told to clean up the attic, garage and other places that junk has accumulated over the decades. "They'll have information all over the place, stuck in SharePoint, on people's laptops, a lot of it unstructured in Word documents and Excel spreadsheets, and physically scattered around in data centers and server rooms and – whether management realizes it or not – in the cloud," he says.

Organizations can start by looking at relevant regulatory frameworks, of which there are an ever-increasing number, and establish a lowest common denominator. From there, they need to identify their business-critical data. For technology companies, that might be software code or product designs, while for mutual fund companies, trading strategies.

"There are few organizations that don't have something that they'd call an important trade secret, most of which is now electronic in some way, and would be valuable to competitors, cybercriminals and other adversaries," Phelps says.

FNF's Phillips recommends starting at a high level – classifying data by intellectual property, and customer and brand protection, for example. "If you get too granular at the beginning, you're going to bury yourself," he says. "So keep it broad at first and then start digging down as you move along."

Enterprises should think of it as a maturity model, he adds. "Ask yourself, 'Is there anything in this application I can learn about from a regulatory standpoint?' That's the first driver. Then look at risk and brand protection and things that fall under that."

95

to 97 percent of lost and stolen notebooks are never returned to their original owners.

– NewSoftwares

Three data classifications – public, restricted and confidential – serve Boeing Employees' Credit Union (BECU) well, says Randall Jarrell, information protection analyst at the Seattle-based nonprofit financial institution. Marketing materials and other benign information fall in the public class, while data intended for internal use only is considered restricted, and data available only on a need-to-know basis falls in the confidential class, he explains.

All member data is restricted and confidential. "Member data definitely won't be leaving the credit union unencrypted or unauthorized," Jarrell says.

No matter how IT security classifies data, corporate boards increasingly are seeking reassurances that data of a critical nature is understood and well protected.

"I've started to hear the expression 'data spill,'" says Phelps, noting its play on the colossal mess BP recently made of containing the Deepwater Horizon oil spill. "Boards are starting to take a greater interest in critical information and the potential consequences of losing it, and they want to be sure there's a common understanding of all this."

> "You want to understand the infrastructure that the data is flowing over..."
>
> *– Emily Mossburg, principal with Deloitte's security and privacy practice*

It is the general lack of understanding about data classifications and policy enforcement that makes protecting data so difficult, says IR's Tu.

"You go to a company and ask different people for the same piece of data, and some will say it is important, some will say it is not, and some will come in somewhere in between," he says. "If nobody knows the data critical pieces, how are you going to control the data?"

That is the big question, with no one set answer. Data protection mechanisms that work for some companies aren't even a consideration at others.

"What we see a lot of is, 'I've got a tool in place, but I don't think I'm getting the most out of it,'" says Deloitte's Mossburg. "So now they're asking, 'How can I appropriately tune my configuration, my policies, so I'm really getting something more out of what I have?"

Jarrell at Boeing, which uses RSA security tools, agrees. "As an IT guy, I can always use more tools, but that's not necessarily the best solution. What I need to do is use the tools I have more effectively, and have tools that talk to each other."

Next steps for DLP

At IR, DLP has long been a mainstay data security technology, but lately Tu says he has taken that protection up a notch. Protecting the company's trade secrets, of which it has many, has been a driver, he says.

"For trade secrets, you can't pull down a tab file that says 'This is important' or 'This isn't important,'" he says. "Trade secrets are difficult to protect because the content isn't as well defined as, say, a Social Security or driver's license number."

So, IR now classifies data based on location tags available with McAfee's DLP product, Tu says. As the name suggests, location-based tagging allows users to tag content from any particular file share, storage drive or other location for protection.

"Older DLP technology either indexes the documents or opens each file and looks for a combination of keywords," he says. "To me, this content-based tagging isn't very useful or effective when dealing with intellectual property or trade secrets. But location-based classification is very, very useful."

For example, IR knows the finance group uses particular folders to store documents, so whenever somebody pulls data from that location to the desktop, it can apply data classification and determine the policy for

3

days: how often a security breach is reported in the United States.

– NewSoftwares

controlling the data, such as monitoring or blocking its use, Tu explains.

Beginning in monitoring mode, as was the case at IR, is the wise first step with DLP, says Derek Brink, vice president and research fellow in IT security at Aberdeen Group, an IT research firm.

> "Having this type of technology would let us set thresholds..."
>
> – Jason Luttrell, security engineer, Express

"A best practice is starting DLP under the covers and transparently – without implementing any policy, stopping anything or causing friction to the business – but gathering insight into the data and where it flows before taking proactive steps," Brink says. "Otherwise, if you turned on enforcement from day one, you'd bring the business to its knees, and you certainly wouldn't be very popular."

Brink, who authored a research brief, *Putting the P in DLP*, which Aberdeen issued in July, anticipates that security companies increasingly will integrate DLP capabilities with content-aware technologies aimed at email and web use.

"The monitoring and filtering engines underneath those are similar to ones we see with DLP, so we expect to see a convergence among them," he explains. And that's a good thing, he adds. "The more automated and preventative the tools are, the better."

And tuning is critical, too, Mossburg adds. "You can start with just monitoring and flagging data, but ultimately DLP needs to be tuned to the point that it understands which data should be leaving and when," she says.

Tying DLP output into security information and event management (SIEM) platforms and identity management tools is a key effort, too, says Accenture's Phelps. "You want to be able to see events and correlate those," he says.

"For example, one of the patterns for insider threat is an employee doing things that are permissible, but in unusual volumes or frequency," he adds. "So, if someone as part of doing a job has access to source code, but over the course of a week has downloaded a gigabyte of information to a local drive, you want to see that occurring, have it feed into the SIEM for correlation and watching rules from an identity management standpoint."

Enterprise IT security professionals need to make tool integration a greater priority, he adds.

Better log management

"With the right DLP product, you can have a good chance to put solid protections in place, but that has to come with logging of data," agrees Larry Whiteside, CISO at Visiting Nurse Service of New York (VNSNY), a non-profit home health care organization serving New York, Westchester and Nassau counties. "Logs are the most fundamental, rudimentary piece to any security program," he says. "That's where you have to start."

At VNSNY, DLP technology from Websense integrates into a log management platform from LogLogic, Whiteside says.

"Being able to identify data, know where you've put it, and put some controls around it while you're logging who has access to it, who is accessing it, and at what time, is an extremely important move forward in our industry," he adds.

Layering intelligence into the SIEM is critical for improved data protection, agrees Jason Luttrell, security engineer at Express, a clothing retailer based in Columbus, Ohio.

Toward that end, he says, Express has begun using the geolocation technology available in LogRhythm's log management system. With the technology, the LogRhythm platform looks at each incoming log to see if it contains a public IP address. If so, it does a database lookup for that and adds location information to the log.

"This is huge for us," Luttrell says. "We can see how many VPN logins we had that didn't originate in the United States, for

$6b

a year: total cost of breaches at America's hospitals.

–Ponemon Institute

example. That's just more intelligence being integrated with log data coming in to help us identify what might be some abnormalities. Otherwise, we're manually looking that up and that's lots of wasted time."

Along these same lines, Express also is eyeing LogRhythm's correlation capability that would let it create event baselines and run comparisons. "Having this type of technology would let us set thresholds and say, 'If the change in activity – say failed login attempts – increases by 15 to 20 percent from one day to the next, alert us and show the baseline difference,'" he explains. "That way, we can identify spikes and peaks and valleys on a day-to-day basis and more easily understand why a baseline might have changed and whether it bears digging into to look for malicious activity or improper configurations."

> "Maybe log data isn't as critical as PII, but it is still important to think about encrypting."
>
> *– Larry Whiteside, CISO, Visiting Nurse Service of New York*

For VNSNY, figuring out a way to better compress and possibly even encrypt the log data while it is in motion are critical next steps when it comes to log management, Whiteside says. "Maybe log data isn't as critical as PII or personal health information, but it is still important to think about encrypting," he says. "If I have faulty information in my log management system and you act on that, how badly can that affect your corporation?"

Encrypting everywhere

If DLP and log management have become de facto data protection technologies within the enterprise, so too has encryption. Federal and state privacy regulations have made it so. DLP and encryption often make a good tag team.

Phoenix-based Apollo Group, for example, is implementing McAfee's Data Loss Prevention 9 suite to stop users from writing sensitive data, such as Social Security and credit card numbers, to external media, says Scott Carlson, principal security engineer at the global private education provider for working adults. If they absolutely have to place sensitive data on a takeaway device, the DLP software will only write to a McAfee-branded encrypted USB, he says.

That's a situation that's familiar at BECU. There, should the company's RSA DLP software see account or Social Security numbers, for example, it sends the data to an encryption add-on from Voltage Security, Jarrell says.

At FNF, encryption of sensitive data begins at the source, within its Oracle and SQL databases, using SafeNet DataSecure encryption appliances, Phillips says.

"The encryption is transparent to the application, and we can centrally manage the keys and encryption and what's in the database and what's protected, obfuscating all that information away from the database administrators and application developers," he says.

"The nice thing about doing the encryption at the database is that we can granularly control by column level what you can or cannot do, by user," he adds. "Database administrators, for example, don't have decrypt capabilities on any of our databases. They're working with ciphertext, and business analysts who need to extract and manipulate data, say in Excel, can pull ciphertext data into a spreadsheet, and can work with what they need."

What's more, the data isn't decrypted as it is backed up onto tape. "So if you lose a backup tape, you lose a tape," Phillips adds. "It is not a data security issue."

That's also the case with lost laptops at Lone Star College System (LSCS), a 14-campus community college serving the greater Houston area. "If somebody calls me and says they've had a laptop stolen, I'm like,

50

to 55 per cent of companies surveyed have reported laptop theft.

– NewSoftwares

'OK,'" says Link Alander, associate vice chancellor for technology services at LSCS. "I know it is encrypted so I don't have to worry about data security. But before, the first thing I had to ask was, 'Was it encrypted?'"

That dreaded question came prior to the mobility craze that has LCSC allowing any administrative, faculty and staff member to receive a laptop and, along with that, Symantec Endpoint Encryption technology. "All of a sudden, I don't know what data I've got out there," says Alander. "I don't know what they might have downloaded onto their laptops," adding that to date he's distributed about 2,400 laptops using endpoint encryption.

Ultimately, he says, he expects encrypted laptops to comprise one-third of his installed base, for a total of about 4,000 machines. "Each year, as desktops expire, I hear a constant, 'Yeah, I want a laptop instead,'" he says. Given that trend, "endpoint encryption is my biggest win yet."

The people matter

Other enterprise IT organizations might find their biggest data protection gains in any number of other technologies – identity management, database monitoring, digital rights management, file integrity monitoring. But no matter where a company might stand on data protection, it must remember that it is somewhere, says Aberdeen's Brink. "And, it can still get better, even if it is best in class – of which only 20 percent of organizations are," he says.

But that means accounting not only for the technology, but people and processes, too, Brink says.

"That's trite, but true," he says. "We can find companies using the same exact technology and one of those companies will get excellent results and the other will struggle. So, clearly, people and process make a difference."

For example, Aberdeen has found that enterprises with best-in-class data protection strategies have formulated standardized responses to security events. "They don't wait for an exception and then say, 'Uh oh, now what do we do?'," Brink says. "Instead, they've thought through potential scenarios and have plans for what to do when something goes wrong. Because it will. It always does," Brink says.

Also on the process front, best performers seek to eliminate root causes rather than simply prevent an action, he adds. "It is a great to be able to catch your dog when it gets out and runs loose around the backyard. But it is much better if you can prevent the dog from getting out in the first place."

Having an executive in charge who has overall accountability and ownership of the data security initiative turns out to be always correlated with top performance, Brink adds. "I refer to it as the 'one-throat-to-choke principle," he says.

Executive oversight is certainly a must for a meaty data classification project, adds CDW's Falcon.

FNF's Phillips agrees. "I'm coming in and making people do more work, but telling them things will turn out easier for them in the long run," he says. "And they're like, 'Yeah, right.' Data mapping in itself is such a challenge, it has to be sponsored at a fairly high level."

At the other end of the spectrum, don't shortchange user awareness, Brink says.

"We find in our research that making users aware by giving them documentation and issuing regular reminders of what's appropriate use and what their obligations are to protect the company's data correlates with best results." ■

For more information on SC Magazine *ebooks, please contact Illena Armstrong, editor-in-chief,* SC Magazine, *at illena.armstrong@haymarketmedia.com.*

$3.8m

the mean corporate loss owing to IT breaches last year.

–Ponemon Institute

Sponsor

nCircle

nCircle is the leading provider of automated security and compliance auditing solutions. More than 4,500 enterprises, government agencies and service providers around the world rely on nCircle's proactive solutions to manage and reduce security risk and achieve compliance on their networks. nCircle has won numerous awards for growth, innovation, customer satisfaction and technology leadership. nCircle is headquartered in San Francisco, Calif., with regional offices throughout the United States and in London and Toronto. Additional information about nCircle is available at www.ncircle.com.

Masthead

EDITORIAL

EDITOR-IN-CHIEF Illena Armstrong
illena.armstrong@haymarketmedia.com

DEPUTY EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com

MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION

ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com

SENIOR PRODUCTION Krassi Varbanov
krassi.varbanov@haymarketmedia.com

U.S. SALES

EASTERN REGION SALES MANAGER Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*

WESTERN REGION SALES MANAGER Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

NATIONAL INSIDE SALES EXEC. Brittany Thompson
(646) 638-6152 *brittany.thompson@haymarketmedia.com*

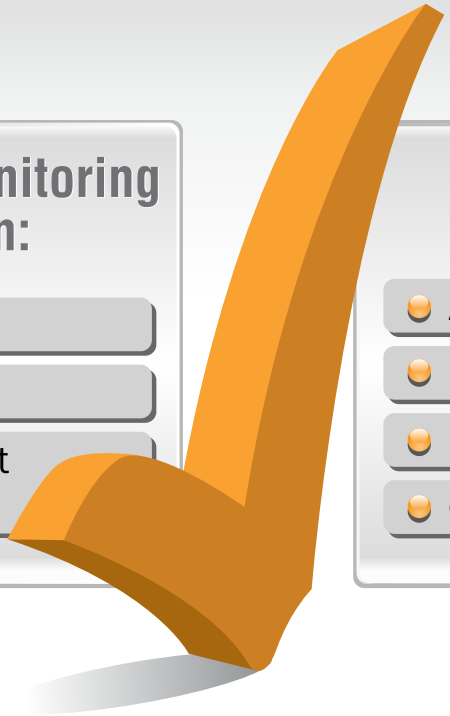
Three critical questions...

- How can I monitor files on *all* my critical assets?
- How can I automatically detect unauthorized file changes?
- How can I ensure file changes are authorized?

One Suite answer.

File Integrity Monitoring Required In:

- PCI DSS
- NIST 800.53
- Consensus Audit Guidelines



nCircle

- Agentless monitoring
- Low cost of ownership
- Deploys in hours
- Complete network coverage

nCircle File Integrity Monitor™

Get started with file integrity monitoring
www.ncircle.com/FIM

nCircle