Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Getting It In Writing

The Art of Policy Management

An e-Book publication sponsored by NAVEX GLOBAL™ The Ethics and Compliance Experts

COMPLIANCE WEEK

Founded in 2002, Compliance Week has become *THE* premier GRC resource for public companies and the organizations that support them.

Compliance Weeks' magazine, Website, electronic newsletters, databases, and live and virtual events are leveraged by tens of thousands of financial, legal, audit, risk, and compliance executives.

Our mission is to help our subscribers comprehend and comply with the constantly evolving global regulations and standards to which public companies must adhere, while focusing on critical regulatory and compliance issues related to financial reporting, regulatory enforcement, corporate governance, enterprise risk management, and related global issues.

NAVEX GLOBAL™
The Ethics and Compliance Experts

NAVEX Global™ is the trusted global ethics and compliance expert for more than 8,000 clients in over 200 countries. We provide the world's most comprehensive ethics and compliance ecosystem to manage governance, risk and compliance (GRC), helping protect organizations' people, reputation and bottom line.

Our array of GRC services help capture and respond to business risk, improving the economic and social value of organizations around the world. The company works with clients to manage ethics and compliance programs through an suite of solutions including case management, whistleblower hotlines, policy management, online training, risk & program assessments and expert advisory consulting. Our fully- integrated offering provides clients with key learnings and actionable data to inform change and protect their organization. More information can be found at www.navexglobal.com.

Inside this e-Book:

Policy Management: From Dilbert to Reality

By Jaclyn Jaeger

Ask any company how many policies it has and where they are located—from the corporate level down to the functional level—and chances are you won't get a straight answer.

A typical company will have some policies controlled by corporate headquarters, sure; but most tend to be created and managed independently by various business units, facilities, or locations, depending on each company's operations. Absent any sense of where those documents reside, most companies end up with hundreds of conflicting, redundant, or out-of-date policies.

"There are a lot of inefficiencies in such a system, because there is no sharing of knowledge or baseline information across the organization," says Ingrid Fredeen, vice president of the Ethical Leadership Group, the advisory services division of NAVEX Global. It also creates a lot of compliance and legal risks for the company, she says.

For multinational companies, those challenges are multiplied because policies need to extend across the entire enterprise, including subsidiaries, contractors, and consultants. "That adds a whole other level of complexity of how you deploy policy management," says Gaurav Kapoor, chief operating officer of MetricStream.

Enter the centralized policy management process: an effort to see a company's entire policy landscape, to ensure that each specific policy complies not only with the company's broad approach to policies and procedures, but also all relevant laws and regulations.

The first step is to determine which policies need to be centralized versus those that should remain local, Fredeen says—and no, that's not necessarily the contradiction in terms one might think. For example, unionized workforces often have specific rules that apply to individual facilities. "What is appropriate for local management and what is appropriate for centralizing?" she says.

Corporate headquarters does want enough oversight that it knows such policies exist, but the idea is not to have so much centralization that you infringe on local business practices. "You still have to allow people to manage their processes at the local level," Kapoor says. Central command only needs to know "what is being adhered to, and what is being managed and not managed."

What sort of policies *should* be corporate-wide, and obeyed by everybody? Codes of Conduct, anti-corruption policies, anti-competition policies, and harassment policies, to name a few. On the other hand, privacy policies can differ substantially from one nation to the next depending on each country's laws and culture.

POLICY MANAGEMENT CHECKLIST

Below is a checklist regarding how to determine if your policy management system enables effective policy implementation and enforcement across the policy lifecycle:

- Provide a consistent policy management framework for the entire enterprise.
- Manage the policy lifecycle of creation, communication, implementation, monitoring, maintenance, revision, and archiving.
- Deliver a system to document, approve, monitor, and review exceptions to policies.
- Consistent format for policy assessments and surveys to gauge compliance and understanding.
- Integrated eLearning and training quizzing and attestation.
- Provide easy access to policies in the right language and format for the audience.
- Gather and track comments to policies.
- Map policies to obligations, risks, controls, and investigations so there is a holistic view of policies and metrics.
- Provide a robust system of records to track who accessed a policy as well as dates of attestation, training, and read-and-understood acknowledgments.
- Provide a user-friendly portal for policies with workflow, content management, and integration to other systems.
- Provide a calendar view to see policies being communicated to various areas of the business, and ensure policy communications do not burden employees with too many tasks in any given time period.
- Provide links to hotlines for reporting policy violations.
- Publish access to additional resources such as helplines, FAQs, and forms.
- Enable cross-referencing and linking of related and supporting policies and procedures so users can quickly navigate to what is needed.
- Create categories of metadata to store within policies, and display documents by category so policies are easily catalogued and accessed.
- Restrict access to policy documents so readers cannot change them, and sensitive documents are not accessible to those who do not need them.
- Keep a record of the versions and interactions of each policy so the organization can refer to them when there is an incident or issue to defend the organization or provide evidence for.
- Maintain accountable workflows to allow certain people to approve policy documents, and move tasks to others with full audit trails.
- Deliver comprehensive metrics and reporting on the status, implementation, understanding, and enforcement of policies.

Source: Michael Rasmussen, GRC 20/20 Research.

Once a firm has identified which policies need to be centralized, it then establishes a corporate policy management repository. "It should be a policy management tool as opposed to a general document management system," says Lisa Hill, president of PolicyScape Consulting and OCEG Policy Management Group co-chair.

A policy management tool allows companies to create, approve, and share policies via a single system. That approach also lets the company establish an audit trail, by keeping track of when policies have been accessed or modified. (And, critically, who grants exceptions to which policies, for what reasons.) Some policy management tools even alert policy owners to changes in the law so they know when a policy needs updates.

While a policy management tool is not mandatory, a document management system like Microsoft SharePoint doesn't allow for the same level of control over policy access and it involves a lot more time and resources, Fredeen says.

Policies on Policies

Companies should also implement a roadmap for managing the policy lifecycle, from drafting and validating to approving and implementing, Hill says. That roadmap should be documented in the company's "meta policy," she says. In many circles, a meta policy is more memorably known as "a policy on policies."

Dilbert-like or not, the concept is important, Hill stresses. "Without a meta policy, it's difficult for companies to achieve the consistency and the governance they need for effective policy management."

In addition, the meta-policy and policy management lifecycle should be available to employees in case they need to create a new policy.

Hill advises corporations to establish a rule (oh, let's just say it: establish a policy) that says if a policy is *not* stored in that central repository, it isn't an official corporate policy. That reduces the company's possible legal liability should an employee refer to an out-of-date policy *not* stored in the central repository, "and a policy should not be able to get into the central repository unless it follows the meta policy, so you have that nice circle of control," Hill says.

How a policy is approved will vary from company to company. Some companies might prefer to establish a policy steering committee with representatives from all business units; others assign each new policy to an existing committee that has purview over the policy subject, says Hill.

Policy Owners

Because policy owners typically are dispersed across siloed functions without a corporate-wide view—that is, no single executive "owns" all policies—there is also a huge need for a corporate policy manager, Hill says. "It's not enough just to say, 'We have policy owners, and they're accountable,'" she says.

Freeden agrees. "Someone has to be given responsibility for managing the centralized process," she says. "It can't be an untended garden; it's a labor of love to do a great job managing policies."

> "A policy should not be able to get into the central repository unless it follows the meta policy, so you have that nice circle of control."
>
> Lisa Hill, President, PolicyScape Consulting

The centralized policy manager should also have responsibility to guide managers through the policy creation process, Hill says: reviewing and editing policies before final approval, ensuring they conform to the company's style guide, confirming they don't violate governance principles.

Another strongly recommended idea: close, and regular, oversight of policies by a legal adviser, since laws and regulation change rapidly. Some legal expert (outside counsel, in-house legal officers with the necessary knowledge) should review policies to ensure they reflect current law and regulation rather than fall out of date.

Along similar lines, policy owners themselves should review policies too, to be sure the policies stay current with the business and still solve the problems they were meant to address. Freeden recommends such reviews at least once a year.

Kapoor stresses that centralized policy management is "not a product; it's a process." Companies that have clearly defined policies in a central repository, with effective implementation procedures and proper oversight, are well on their way to having a well-run centralized policy management program. ■

The Art of Managing Policy Exception Requests

By Jaclyn Jaeger

Exception requests are often a thorn in the side of policy managers, and yet they are unavoidable for most.

An effective policy management process can ease the pain, which includes putting in place a "policy on policies" that describes a corporate policy, what it should include, and how policies get approved, reviewed, and trained upon, says Paul Liebman, a former in-house compliance and ethics attorney now in private consulting. Companies that manage policies well have a centralized policy management process and don't issue policy exceptions lightly, he adds.

At many companies, however, policies, procedures, and directives are generated in a decentralized way within a company's various business units or facilities. "Figuring out what a policy is—and what an exception to a policy is—is difficult, because companies don't have a lot of control over that process to begin with," Liebman says.

Compliance officers say writing good policies in the first place can minimize exception requests. "Good policies are written at a high level to provide guidance and direction and to define the principles upon which the policy rests, including references to appropriate regulations, industry standards, accounting standards, and other company policies," says David Frishkorn, chief compliance officer at business services provider Comverse Technology.

Too many exception requests can be a sign that the underlying policy has flaws. "When you start to make too many exceptions, the policies basically are no longer policies," says Ingrid Fredeen, vice president of the Ethical Leadership Group, the advisory services division of NAVEX Global. "They no longer serve their fundamental purpose if people believe that they'll be able to get away with something, or that the policy won't be enforced."

Granting a high number of exceptions can also expose the company to legal risks. If an employee bribes a foreign official, for example, and that employee is not disciplined or terminated, "you create a culture of condoning that behavior," Fredeen says.

Companies also want to avoid establishing exceptions that can undermine the policy if it sends the message that it doesn't always need to be followed. That's a common problem, says Fredeen, because favored employees always seem to test the waters of a policy exception first.

If a company has a policy against lying on a résumé, for example, and then finds out that its best salesperson violated that rule, it can be a mistake to grant an exception. If you don't fire that employee, Fredeen says you're faced with the predicament of making an exception for the next employee, who "invariably is somebody who may be of a different race, gender, or other protected party," Fredeen says.

"Policies are really about being fair, and they put employees on notice as to what is expected of them," she adds. "Most employee want to follow the rules; they want to do the right thing. Policies help them do that. Exceptions chew away at that sense of fairness."

Exceptions to Exceptions

That doesn't mean that there isn't a time and place for exceptions. If employees cannot get exceptions to a policy for reasons they deem valid, that will only encourage them to ignore the system or the policy owners—the outcome compliance officers want least.

EFFECTIVE POLICY MANAGEMENT

Below is an excerpt from Universal Weather & Aviation's presentation at CW's 2011 conference regarding the elements of effective policy management.

- Identify key policy stakeholders in the company (e.g. legal, HR, compliance, finance, ops & IT);
- Create a policy committee of high ranking vice presidents to align policies, procedures, and controls throughout the enterprise;
- Develop a policy committee charter to clearly identify roles and responsibilities;
- Publish a policy on policies;
- Develop clear management roles & responsibilities;
- Develop & use a clear, consistent, and concise writing style;
- Develop a standard policy template;
- Develop a formal communication, training, and attestation plan;
- Develop a continuous review, monitoring, and audit plan;
- NEVER write a requirement in your policy that either your management or employees cannot live up to or carry out.

Source: Universal Weather & Aviation.

In general, policy exception requests fall into two categories. The first is process and procedure policies, such as travel and expense costs and gift giving. "These sorts of policies are not necessarily driven by the law itself, but they're important policies for the organization to manage itself. The second category is compliance, ethics, and legal driven—harassment, wage and hour, bribery and corruption, anti-trust, and competition laws. So what then constitutes a valid exception request?

"Some policies are necessarily more granular, more transactional, or more employee-driven and lead to more exception requests," Frishkorn says. Examples include travel- and expense-related policies.


Frishkorn

Some aspects of a policy should be viewed as having no flexibility for interpretation, such as "any behavior that is designed to prevent death or serious injury or has the potential to create criminal liability," Liebman says. "The only situation that would trump these policies is if someone's life was at risk," he says.

"Another important lesson on policy management is to focus on the actual human behavior you're trying to encourage or discourage in the policy instead of simply parroting the law or regulation," says Liebman. If you think about the FCPA, for example, it's a much easier conversation to simply say, 'Don't bribe. Here is what we mean by bribery. Here is how we ensure that doesn't happen,'" he says. "When you present policies in that way, "exceptions become fewer and farther between."

"There needs to be a defined process for how exceptions are handled," says Bobby Butler, chief compliance officer and internal audit director for Universal Weather and Aviation, a global flight planning and flight support services provider.

Comverse, for example, "typically requires approval from a high-level manager—such as a senior vice president—and perhaps a functional expert approval from a relevant area like finance, HR, or legal," Frishkorn says.

According to Freedeen, companies should establish criteria against which to judge exception requests. Consider the following:

» Will you be able to maintain the exception going forward when the same exception request arises again?
» What risks—legal, cultural, and reputational—will this create by making an exception?
» Is the exception fair to employees and the corporate culture?
» Is there a valid business justification for the exception?
» What perception does the exception create?

Make sure exception requests are properly documented, too, says Liebman. "Everything should be very transparent not just out of respect for the process, and because you may have to explain your decision to others down the road."

Proper documentation enables management to judge future exceptions against what actions were taken in the past. "This process helps others in the organization understand those important business criteria, why these decisions make sense," says Fredeen, "and it helps them make better decisions."

Proper documentation is also important so that if the Justice Department or another regulator should ever come knocking, you can provide the proper paperwork quickly.

> "When you start to make too many exceptions, the policies basically are no longer policies."
>
> Ingrid Fredeen, Vice President, Ethical Leadership Group

"In a perfect world, everything is done electronically," says Butler. An electronic process also helps to gets things out of e-mail, hard drives, shared files, and mobile devices, he says.

Universal Weather and Aviation, for example, employs an electronic attestation tool, where employees have to certify that they've read, understood, and will comply with our policy. "We're working on trying to make the exception process just as streamlined," he says.

Another crucial component of a good policy management strategy is periodic assessments, which means revisiting policies to see how often exceptions occur. "If exceptions are occurring on a regular basis," says Butler, "you need to rethink and reexamine the limits that you're placing on employees, because they're not very realistic." ■

Business Case: The ROI of Policy Management

This article highlights the financial benefits of using NAVEX Global's PolicyTech policy manager by defining the investment in terms of:

- Faster retrieval. Saves time, as employees can access documents instantly.
- Resource reduction. Eliminates excess copying, distribution, and storage. Also enables compliance managers, hr directors, and document managers to reduce paper shuffle and focus on improving quality and compliance levels.
- Enhanced training. Ensures that employees have read and understood appropriate procedures without costly training staff. And authors need less training on company standardization.
- Automated management. Expedites the policy review and approval process.
- Proven compliance. Links regulatory guidelines to salient procedures.
- Lower redundancy. Saves time and confusion with updated and uniform documents.
- Increased productivity. Employees perform their job more efficiently.
- Heightened quality. Accurately followed procedures allow for continuous improvement.
- Risk prevention. Avoid costly litigation and prevent error and negative outcomes with accurate records of employee attestations and approved company policy.

The figures in the examples below are based on daily costs at an average company (hospital, business, government) with 500 employees where the average employee earns $18 per hour. While these figures will not fit the exact numbers of every organization, they show how savings are measurable and substantial.

Faster Retrieval

One of the principle ways companies save money using policy manager is through a decrease in the time employees spend finding documents.

Suppose that the average employee must find 1.5 policies, procedures, or forms per week. Assuming the document is correctly labeled and in the right spot and the employee knows exactly where to look, it will take an average of five minutes to locate the document. Each employee will spend 7.5 minutes per week looking for documents. If the average employee earns $18 an hour, the 7.5 minutes spent looking will cost the company $2.25 each week. Multiply that by 500 employees and 52 weeks and the cost to the company is $58,500 a year. Using the keyword search capabilities in policy manager, this employee can find the same document within 30 seconds—at one-tenth the cost of what it was before (a $52,650 savings).

Resource Reduction

The advantages of electronic policy management and storage go far beyond the ease of retrieval. By reducing the number of copies, you will also reduce the amount of paper, ink, and machine costs. Many mid-level organizations have around 2,000-3,000 policies and procedures with multiple copies of each and stored in multiple binders throughout the organization. If you have about 35 departments, with an average of 7 binders per department and an average of 250 pages in each binder, you will have around 61,250 pieces of paper. Even if you do not replace them annually, the copies made during the review and approval process on those that are reviewed or created could easily reach that number. On average, each copy costs $.05, and so the total cost could be at least $3,000 a year.

Many companies also require an employee handbook for each new employee. Printing handbooks, at minimum, probably costs around $2 an employee if you buy over 1,000. If you hire 2.5 new employees a week (about 125 a year) it will cost you about $250 a year. That doesn't sound like much, but remember if you make a change to the handbook, all of those copies are now useless. Using our software, you can make those changes easily, reconfirm the readership, and employees will have instant access.

Further, policies are electronically distributed to all appropriate employees with the assurance that the available policy is current and approved. These same policies and procedures often need to be approved or distributed to third parties, such as board members, contractors, and physicians at remote locations. Because our policy and procedure software is Web-based, those parties are able to access them from anywhere.

Enhanced Training

Anytime new training materials are added to the policy manager, each relevant party is sent an e-mail notification. Documents and material can be uploaded to the system in many document formats such as HTML, PDF, and video. This feature has two money-saving benefits; first, employees have 24-hour access to the training material and can refer back to it at will.

Typical annual cost and return on investment information:	
Current annual policy and procedure management cost (paper-based)	$168,912.50
Annual potential saving with NAVEX Global policy management	$116,632.50
Return on investment	
YR 1	69.05%
YR 2	86.04%
Payback period	3.71 months

NAVEX GLOBAL™
The Ethics and Compliance Experts

Second, there is no need for supervisors or trainers to travel and spend time training employees that can be just as easily reached via Internet. After the employee reads each document, passes a quiz (if required), and certifies they understood the document, their attestation and scores are permanently recorded in the system. Trainers now save time and can prove 100 percent readership of important documents. Employees can also send feedback to the trainer about any of the documents. Finally, when a new employee is hired, based on their assigned department and job title, they will automatically receive notification to read all of the documents required for that job title—no manager or trainer intervention needed.

Assume the average manager spends 8 hours annually training employees on policies and procedures. If you have 50 managers (10 percent of the workforce), the company will spend $7,200 a year on policy and procedure training. With PolicyTech, this training time may be reduced from 8 hours per manager to 2 hours per manager—an annual savings of $5,400.

Automated Management

Managing a company's documents can be unnecessarily time consuming and costly. One management challenge is keeping track of updating and archiving documents at appropriate times. On average, for every 100 employees, the company as a whole could spend 2 hours a day performing these tedious tasks. A 500-employee company could spend 10 hours a day costing $180, which equals $43,200 a year updating and archiving documents.

NAVEX Global actually keeps track of and notifies users when they must perform these management tasks—saving you thousands. Instead of spending 10 hours a day on document management, a 500-employee company will only spend 2 hours, costing you $6,480 a year as opposed to $43,200.

Another challenge, is getting employees to sign off that they have read and comprehend important documents, and then filing away these important reports. If each manager spent 10 minutes a day retrieving these signatures, it would cost $21,600 a year.

PolicyTech will send automatic e-mail reminders to staff to read and sign-off that they have read the appropriate document and passed a quiz if required. Reports can then be run to show who signed off and how well they comprehended it. Because PolicyTech does all the reminding and gathering, it will save you $21,600 a year.

Finally, managers and authors that create policies, procedures, and other important documents must get their work reviewed and approved before they are finalized. PolicyTech will reduce the amount of time it takes to get documents reviewed and approved. We have found that on average, customers cut this time in half!

Information above was calculated using the following data:

COMPANY INFORMATION	MANUAL	NAVEX GLOBAL
Number of employees who read policies and procedures	500	500
Number of employees who write policies and procedures	50	50
Average salary (per hour) of people who read and write policy and procedure documents	$18	$18
Retrieving and photocopying costs		
Average number of times per year each person searches for/retrieves a policy-type document	78	78
Average time taken to retrieve the paper document	5:00	0:30
Average time per person spent per month making copies of documentation (minutes)	5:00	0:30
Average number of employee handbooks printed for each employee per year ($2.00 each)	125	0
How many total binders of policies are there throughout your organization?	245	0
How many pages on average are stored in each binder?	250	0
How often per year on average do you replace those documents? (annual: 1, biannual: .5)	1	0
TRAINING COSTS		
Average hours spent per author, per year, on policy and procedure formatting training (hours)	5	3
Average time spent per employee/yr training employees on policies and procedures	8	2
POLICY MANAGEMENT COSTS		
Average hours spent per day by the company creating, editing, and producing manuals	10	2
Average hours spent per day by managers capturing/document policy attestations	.1	0
Average hours spent per day by authors following up with reviewers/approvers	.1	0
TOTAL	$168,913	$17,280

NAVEX GLOBAL™
The Ethics and Compliance Experts

Crafting an Effective Data Security Policy

By Karen Kroll

How concerned are companies about data breaches? In a recent survey, executives said they worried more about leaks of customer or employee data than natural disasters or investigations by the Securities and Exchange Commission.

The survey, conducted last year by Chubb, found that corporate executives rank "an electronic security breach of customer or employee data" as generating the greatest level of fear of potential lawsuits or financial losses. More than three-fifths of respondents said they were somewhat or very concerned about a data breach.

The concern is understandable. In 2011, the number of records compromised through data breaches hit 174 million, according to the Verizon 2012 Data Breach Investigations Report. It's a trend that shows no sign of slowing. During the past few months, bookseller Barnes & Noble, the South Carolina Department of Revenue, and Nationwide Insurance, to name just a few, all experienced significant data breaches.

Techonology companies, including Apple, Facebook, and Microsoft, have also announced that they have recently been the targets of concerted efforts by international hackers to get into their systems. And media companies, including the *New York Times* and the *Wall Street Journal*, have recently announced that they have been hacked, possibly by organizations connected to the Chinese government looking to monitor coverage by these companies of China. China's Ministry of National Defense has denied any involvement in the cyberattack at the *New York Times* or any other American corporations.

In short, there's been a rash of breaches into the systems of U.S. companies and no one appears to be immune from such attacks.

Moreover, the average annualized cost of a cybercrime in 2012 was $8.9 million, up about 38 percent from the preceding two years, Ponemon Institute reports. The price tag includes the cost of lost information, business disruption, and detecting and investigating the incident.

While no organization can completely insulate itself from a data breach, a relevant and effective data security policy is a solid starting point. Even if a company has an existing data security policy that hasn't been reviewed in the last year or so, the rapid pace of technology has likely rendered it obsolete.

As more employees access the corporate network from their own devices, for example, companies have to decide whether the current password policies should still apply. Failing to consider these and other developments may mean that companies are inadvertently "granting exceptions to policies without doing full risk assessments," says Joe Kurlanski, vice president at Sage Data Security.

New legislation also can necessitate modifications to organizations' data security policies. For example, earlier this year the U.S. Department of Health and Human Services announced new rules to protect patient privacy, including extending privacy requirements to health care organizations' business partners, such as contractors. Millions of entities need to update their policies based on the new regulations, says Rebecca Herold, an information security consultant.

Data security policies may require more frequent reviews than any other company policy, due to the rapidly changing technology environment and the requirements that govern it. That's not to suggest that developing an effective global data security policy is easy. For starters, organizations that operate internationally are subject to multiple, and at times competing, regulatory requirements.

Similarly, companies with product or service lines that cross industry sectors may be governed by varying sets of regulations, says Fred Cate, a professor at Indiana University School of Law and director of the University's Center for Applied Cyber-security Research. "It's not at all unusual for companies to have multiple data compliance requirements," he says.

In light of these challenges, a few principles generally apply when organizations are crafting data security policies. To start, a simple, broadly applicable and easily understood policy typically is more effective than one that attempts to detail all possible scenarios and responses. Overly detailed policies quickly become hard to follow. "The moment people say, 'I have to look it up,' it makes it harder to comply," Cate says.

Instead, the goal should be a global policy that outlines the organization's security objectives. For instance, a policy might state that the organization will ensure that access to critical systems can be restored within two hours of an outage, and with no more than ten minutes of lost data, Kurlanski says. This type of policy likely will be relevant in all the countries or industries in which the company is operating, he explains. Trying to draft separate policies for each region or market quickly can get unwieldy, since all the documents will need to be regularly reviewed and updated.

If some regulations apply only to a specific unit of an organization, they usually can be addressed in the procedures developed to implement the policy, Herold notes,

rather in the policy itself. For example, if one government body requires local businesses to retain documents for a certain period of time, supporting procedures can address the affected business unit's need to securely comply with this mandate.

The supporting procedures also can cover technical processes in more depth. They might outline, for instance, the steps needed to securely operate a company's POS systems in all its stores, Cate says.

Buy-in at All Levels

Essential to an effective security policy is support among both executives and employees. "You can't create a corporate policy without high-level buy-in," Kurlanski says. But if employees resist them, they won't work either. Most security policies impact employees' day-to-day jobs in ways that aren't always convenient—say, by limiting their ability to use their own devices when accessing the corporate network. Although not a panacea, broad support for the policies reduces the likelihood that employees will try to circumvent them. This is the thinking that led many companies to abandon efforts to keep employee-owned devices out of the workplace, for example.

> "How can you protect the information if you don't know where it is? Resolving this often requires documenting the lifecycle of the data."
>
> Rebecca Herold, Information Security Consultant

At the same time, employees need to understand and support the policies. Adopting an air-tight security policy does nothing if employees aren't trained on what it entails. "Good security awareness is based on changing behavior," says Ira Winkler, president of the international board of directors at the Information Systems Security Association and president of Internet Security Advisors Group. Winkler points out that many breaches occur as a result of employees' actions, such as unknowingly opening an email that introduces malware into the system. The goal is to foster a culture in which employees understand data security and the role they can play in enhancing it.

A solid security policy will require input from a range of departments. Depending on the company, this may include security, information systems, legal, compliance, human resources, and business unit representatives. Information security typically takes the lead, Kurlanski says.

Bringing together representatives from multiple departments not only tends to lead to better policies, but it also "helps re-forge relationships between departments," Kurlanski says. Too often, it becomes easy for the operating units to view security as a hurdle to overcome. Working as a team to draft a policy can mitigate this tendency.

Increasingly, effective security policies also need to account for an organization's outside business partners, such as IT service providers. For example, outsourcing the storage of electronic data doesn't relieve an organization from the obligation to make sure it's secure. "You want to make sure [your data] isn't sitting in Earl's garage around the corner," Kurlanski says.

Where Policies Fall Short

Experts also point to several mistakes that are easy to make when developing a data security policy. One is simply not knowing which information should come under the policy, says Herold. "What information do you need to protect?"

Similarly, some organizations have a difficult time determining just where the information resides, Herold adds. "How can protect the information if you don't know where it is?" Resolving this often requires documenting the lifecycle of the data, she says. Where is it created? Where does it go? Who has access? Finally, what's being done with it?"

Another potential trouble spot is developing a policy without having the resources to actually implement it, Kurlanski notes. Say an organization's policy states that it will regularly scan for rogue access points, but the organization lacks any practical way of doing this. Ignoring this provision can lead to legal troubles; if a breach occurs, regulators will want to know why the organization didn't do what it had stated it would to protect the data.

Finally, it's not unusual for organizations to focus on securing their data collection and storage processes, but then to overlook data disposal, Herold says. "A large percentage of data breaches come from poor or lacking disposal practices."

Avoiding these mistakes and putting in place solid policies can form a foundation for an effective data security program, reducing the risk that an organization falls victim to a breach. The Verizon report found that 96 percent of attacks were not highly difficult, and that 79 percent of victims were targets of opportunity. As the report states, "Most victims fell prey because they were found to possess an identifiable weakness rather than because they were pre-identified for attack." ■

A Winning BYOD Policy Balances Usability & Control

By Todd Neff

The idea of sensitive company data flying through the airwaves to computing devices the company doesn't own is enough to make most compliance officers' blood pressure rise.

Sooner or later, however, many of them will face this exact scenario. With the phenomenon of BYOD—bring your own device—most companies have had to make a decision to either let employees use their own tablets, mobile devices, and other personal electronic equipment for work or ban their use completely.

At some companies it might be too late to turn back the clock on prohibiting the access of business data on personal devices. "Honestly, a lot of organizations we talk to are not thinking, 'How am I going to set this up?' It's, 'How am I going to start managing this BYOD program that already exists?'" says Tim Williams, director of product management for Absolute Software, whose products focus on security and compliance around BYOD.

Employees have done company work on home computers since the dawn of the floppy disk. BYOD (also called BYOT, the "T" standing for "technology"; and also the less-snappy "consumerization") represents something deeper. It's the formal corporate recognition that user-owned hardware—in particular iPhones, iPads, and their Android equivalents, but also notebook computers—has become a fixture of modern organizations. In a recent research note, technology research firm Gartner described BYOD as "the single most radical shift in the economics of client computing for business since PCs invaded the workplace."

"Every business needs a clearly articulated position on BYOD, even if it chooses not to allow for it," the authors added.

That position, Gartner, Forrester, and many others agree, must be fortified by a combination of IT infrastructure and crystal-clear policy regarding what devices get the green light; what company data employees should or shouldn't be accessing and what apps and Web services they must avoid for security and compliance reasons; and what happens when an employee-owned device goes lost or stolen or leaves the company with its owner.

It's easier to just say no—and says David Remnitz, leader of Ernst & Young's forensic Technologies and Discovery Services, some perhaps should. At minimum, he said, companies whose BYOD-candidate employees are steeped in sensitive healthcare or financial information should institute "an extraordinarily well-defined BYOD program to ensure that any device introduced into the environment follows a very tight series of compliance-oriented functions."

Companies are increasingly looking for ways to make allowances for BYOD for several reasons; chief among them is the opportunity to cut IT costs. While the overall savings from BYOD depend on the organization, the amount can be substantial: Intel employees own 58 percent of the mobile devices they use, the company's Chief Information Officer Kim Stevenson recently told *InfoWorld*, generating an estimated $150 million a year in higher productivity and savings. BYOD

BLACKBERRY EXPENSE

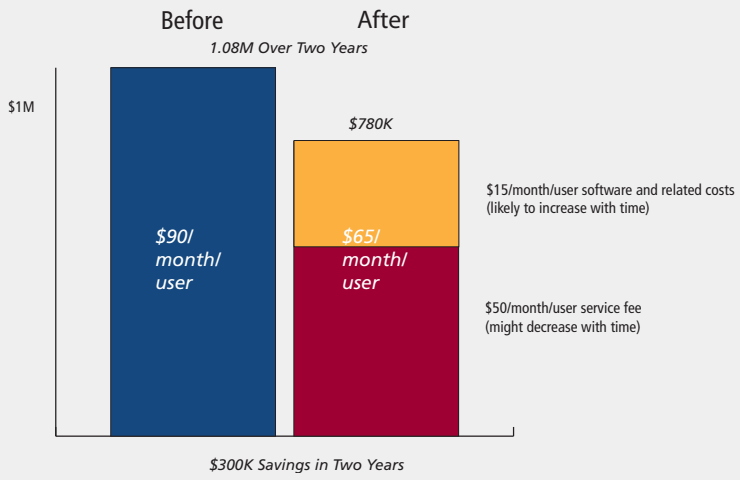
Below is a chart regarding BYOD From Gartner:

With the wide range of capabilities brought by mobile devices and the myriad ways in which business processes are being reinvented as a result, we are entering a time of tremendous change.

There are instances where current-state mobility costs can be cut, such as in the common case of replacing an existing BlackBerry device that provides mobile e-mail and calendaring. To take an example, moving a 500-person mobile workforce running corporate-supplied BlackBerry devices at a cost of $90 per month to personally owned devices results in a 29 percent reduction in hard costs, using a standard $50-per-month reimbursement rate, while investing roughly $360 per user in new infrastructure, software, and support.

Source: Gartner.

From Blackberries to Personal Smartphones: How Much Savings?



is also environmentally sound, saving the production and shipping of duplicate devices—all those people with separate personal and corporate cell phones—multiplied by thousands of employees in a single large company alone. Foremost, though, employees just want to use their own devices.

"The reality is, BYOD is being forced upon the major corporations we interact with," Remnitz says.

It's not just younger professionals who have grown up with mobile technologies and whose mobile-computing tastes are as particular as their tastes in music, food, or dress. It's also "the realization that technology is changing so fast and dynamically that one of the only ways to counter that is to have employees carry the technologies they prefer in their hand and pocket and briefcase," Remnitz adds.

While technology is instrumental to instituting compliant BYOD programs, policy is the key, says Bill Ho, president of Biscom, which specializes in secure document delivery.

"I personally feel that the policy and education side is more important than the technology," Ho says. "The technology is the easy part: you encrypt, you require PINs, you watch what apps are being installed, you put in encrypted containers and run corporate apps through mobile device management software," Ho said.

Usability should be the starting point, Williams says. Take the example of Dropbox, file-sharing software that boasts 100 million users. A recent survey by BYOD software firm Nasuni found that one in five employees used Dropbox for work-related files. The compliance-related concerns with Dropbox, Evernote, and their ilk range from the strength of authentication, levels of encryption, and other data-protection considerations, as well as traceability and auditability limitations. Among the leading scofflaws? Vice presidents and directors, the survey found.

"One of them said, 'Oh, I didn't know that policy applied to me,'" says Connor Fee, Nasuni's marketing director.

Education and training is part of the answer, he says. But the Nasuni survey found that half the employees using Dropbox were aware of the company policy forbidding it. Fee says that, facing a wave of BYOD, IT departments need to start thinking less like system architects and more like marketers: talking to end-user "customers" to understand what they want, explaining what can and can't be done and why. Simply blocking a BYOD device's access to Dropbox is easy. Companies need to ask what employees really want from Dropbox. "They're not using Dropbox because of a special brand loyalty to Dropbox," Williams says. They use it because they want to have their stuff."

Striking a Balance

Figuring out a middle ground means balancing corporate control with usability, Fee adds. "Lots of control is good for IT and bad for the end user. Anything bad of the end user in 2012 isn't going to survive very long," he says.

Indeed, usability must be the starting point for any BYOD program. It's the employee's phone, after all, and they're saving the company money, at least on the hardware side, by using it. "So it has to start with making it easy for the user to get e-mail and get the docs and the apps they need to access company documents," Williams says.

There also needs to be some perspective on where to draw the line. Employees e-mail files, copy sensitive data to thumb drives, forget their laptops in airplanes, write their passwords on Post-It notes stuck on their monitors, and commit other transgressions. These are the folks the company should be thinking about when designing a BYOD program. "You can't get too wrapped up in malicious employees, because they're going to find a way to circumvent you anyway," Williams says.

There are ways to sharply improve compliance while lessening IT-department headaches. First is establishing exactly what mobile devices can be part of the program and establish configuration rules such that they're part of a known inventory.

Policy and technology intertwine with the introduction of the aforementioned mobile device management (MDM) software. MDM systems can provide VPN-style conduits for secure e-mail; prevent copying or forwarding of sensitive files; remotely wipe all of a device's data or some portion thereof; provide secure Dropbox-style environments for mobile document sharing; and much more. Solutions abound, with vendors including IBM, SAP/Sybase, Symantec, Cisco, Citrix, VMware, Absolute, MobileIron, Zenprise, Airwatch, Fiberlink Maas360, Good, and Nasuni, among others.

MDM software can lessen the compliance headaches of BYOD with some creative solutions to balancing usability and control. Absolute, for example, has a government client that allows iPad viewing of certain classified documents only during a certain scheduled meetings, then locks them down to forbid copying into other applications or forwarding by e-mail, text message, or otherwise avenues. When the meeting is over, the iPad automatically deletes the file, Williams says.

Their software must go hand-in-hand with the employee's understanding of how MDM technology will affect their devices in good times and bad. Policies might include a reminder that the secure file-sharing solution in the confines of the MDM—and not Dropbox—must be used. They will make clear that password protection of the device itself is now required and that multiple password misses or a report of a lost or stolen device will trigger a remote wipe of art or all of the device's data.

"You have to be sure that you're overseeing the introduction and upkeep of these devices and can pull the trigger and clear the data off one when it's known to be outside your control," Remnitz says.

Employees may not like it, Ho adds.

"It's a tough balance to provide security and also make it easy to use," he says. "Add a couple of extra clicks and people complain loudly." ■