BETWEEN THE LINES

TAPPING THE POTENTIAL OF
21ST CENTURY DOCUMENTS

by John M. Kelly

11

Mitigating Risk, Maximizing Protection

Let's start with a mystery.

Carol, a call center rep, is having a hectic morning. One call barely ends before another begins. As Carol warmly greets the next customer, she remembers it's her sister's birthday. She reminds herself to call her sister later that night. A note would help, but Carol's company has a "clean desk" policy. Carol's work surface has no pens, pencils, papers or other means of capturing confidential information.

The customer, a friendly woman named Lorraine, provides Carol with her basic transaction stats—name, account number, Social Security number. Carol's fingers fly across the keyboard, completing a secure e-form. Fortunately, Carol's system masks Lorraine's information so it doesn't appear on screen for long. Carol explains to Lorraine that all customer data must be verified and places her on hold.

During those free seconds, Carol considers leaving herself a voice mail reminder about her sister. She dials her own cell phone number, rattles off a message and returns to finish the customer transaction. A few weeks later, money begins disappearing from the customer's bank account and fraudulent charges cram her credit card bills.

So whodunit?

One of our clients was forced to ask the same question when a similar situation actually occurred. Like most companies with support centers, the client recorded its inbound calls. As an extra precaution, they also taped outbound communication.

The client discovered that when "Carol" called her cell phone, the message she recorded was Lorraine's name and social security number. Because of that, Carol now makes her phone calls from behind bars.

This situation is frighteningly common. According to a 2010 security report from Verizon and the U.S. Secret Service, 48 percent of data breaches are caused by insiders.[1] While Carol didn't officially hack into her company's system, her actions were emblematic of one of the most significant issues facing today's businesses—protecting the organization, its information and its customers.

Vulnerability in 3-D: Digitization, Distribution, Devices

There are a number of factors contributing to the vulnerability of today's enterprises. In his best-seller, *The World is Flat*, Thomas L. Friedman enumerates several, including the PC revolution, connectivity and outsourcing.[2] Any reasonably informed Internet search will reveal countless others.

To keep things simple, I've boiled it down to three. The first is digitization. There's no doubt that digital documents provide greater efficiency and flexibility. Information can be processed easily. Access can be expanded. Workflows can be streamlined. But those benefits yield a higher security risk. When you make something digital, in a sense, it lives forever. The minute you forward an electronic form or post a note on Facebook, you've relinquished your control. Without the proper precautions, you're practically inviting others to make your information their own.

In addition, because so much information is now digital, the responsibility for enterprise protection has shifted from areas like the legal department and security personnel to the IT group. This transition makes security more of a proactive endeavor, less about "How do we address what happened?" and more about "How do we stop it from happening?"

Factor number 2 is aptly summed up by Friedman—an open, distributed world that keeps "flattening." Business operations today expand far beyond the border of a single building. Or region. Or country. Whereas in the past, "pieces" of work might have been outsourced, the modern workflow is frequently a seamless global stream stretching across cities and continents.

It is not unusual for a supply chain to start in California, jump to New Zealand and wind its way through China before ending in London. These far-reaching walls of business are diaphanous at best, which makes it easier to peek inside or quickly slip out with trade secrets.

Finally, as an effect of flattening, endpoints are migrating outward and multiplying. No longer tethered by wires, digital devices such as laptops, phones, tablet PCs and multimedia systems can be used virtually anywhere by almost anyone. And it's a rare individual who possesses just one. The closer these devices get to the edge, the farther they are from your control.

What's more, endpoints keep getting smarter, offering more apps and therefore, more access. Up until the first commercial camera cell phone was introduced in 2000, phones that took photos only appeared in James Bond films. Now, 76 percent of adult cell phone users snap pictures of friends and family.[3] Or, in some cases, of confidential business information.

Clearly, the pre-Internet days of hardwired terminals linked to a secure internal network alongside landline phones are over. Business boundaries—and correspondingly, security

perimeters—have vanished. Meanwhile, content at the edge continues to explode, ignited by trends such as cloud computing and social media.

As a result, your enterprise must work harder than ever to protect its assets and customers. But where do you begin? The whirlwind of information—product information, business information, social information—never ceases. How do you assess it for risk? Or determine who has access to your information if you can't tell where it is? Or ensure that your clouds of data aren't obscuring a smoking gun?

Documents: Where the Treasures are Buried

In one of the most famous of all U.S. security breaches, Deep Throat helped Woodward and Bernstein solve the Watergate puzzle by encouraging them to "follow the money." Today, he might say, "follow the document."

Why? Because documents are the primary business vehicle for capturing and managing information.

At the first Xerox security summit, one of our speakers recounted three real-world examples of corporate espionage:

- A researcher at a large medical firm working on the DNA model for Alzheimer's disease was secretly providing data to a foreign neurological center.
- A mole at a global adhesives enterprise entering the Asian market was stealing information for almost a decade.
- A disgruntled employee at a multinational energy conservation company was faxing research to competitive firms.

In all three cases, documents were at the core of the crisis. Documents are just as central to identity theft, which would be virtually nonexistent if identities weren't initially captured in documents.

Safeguarding documents and their content is mandatory. But the protection of the processes that surround documents is no less critical. Without both, you're locking the crown jewels in a safe without installing a castle-wide security system.

By tracing the flow of a document—including its multiple stops and starts—you can begin to discover the potential for leakage. You need to understand every step in a document's creation and routing, as well as its content owners and reviewers, storage locations, access trajectories, surrounding events (such as Carol's call center conversation) and so on.

For a recent, disheartening example, look no further than the quarter-million U.S. diplomatic cables involved in the WikiLeaks scandal. Although many of the documents were classified—

including 11,000 designated "secret"—over 3 million government employees had access to the information.[4]

Which leaves you wondering—if the U.S. government can't put the right security measures in place, what chance do the rest of us have?

Recognizing the Weak Spots

Contrary to what you might think, data breaches at U.S. companies are actually decreasing. That's the good news out of the latest PGP-Ponemon Institute study.[5] However, companies are becoming more reluctant to report a breach, so whether the decrease reflects incidents or incident reporting is up for debate. Regardless, the bad news is that costs per incident are going up, reaching an average of $6.75 million.

These costs represent everything from initial detection to customer defection, plus considerable legal fees. The most expensive breach in the study consumed nearly $31 million. The least expensive wasn't exactly a bargain, coming in at $750,000.

"U.S. businesses can't afford to ignore protecting the valuable, sensitive data they have been entrusted with," says Philip Dunkelberger, president and CEO of PGP Corporation. "Companies whose data is not protected are not only facing expensive direct costs from cleaning up a data breach, but also a loss in customer confidence that has long-lasting ramifications."[6]

The impact of a breach can result in devastating short and long-term consequences. It's not just your information and balance sheet that are at risk, it's your reputation. And reputations can be a lot harder to restore than data files.

Therefore, it's a rare company that doesn't have some form of document-related security in place, usually antivirus software at a minimum. But it's equally rare to find a company with a truly comprehensive security solution, from strategy and tools to education and governance.

When we audit the technology and workflow of new clients, we uncover many recurrent security vulnerabilities. Here are four of the most common, along with the combative measures being deployed by visionary enterprises.

Weak Spot: Underestimating Output Devices

Weapon: Device and Document Controls, Both Basic and Innovative

Most firms don't think twice about securing their PCs and network, yet they overlook their copiers, faxes and multifunction printers. When that happens, these—and other—output devices represent a triple threat to security. First, many are actually servers, linked to a company's network. Second, some house hard drives, which store electronic images of their

output. Third, a good number are called upon to generate hard copies of highly confidential information—sometimes legally, sometimes not.

From a network perspective, these devices look like every other powerful computer node. Therefore, the first step toward addressing their security issues is to view the devices as network endpoints, demanding the same protection as any other node. Employees should be required to enter user IDs and passwords just as they would with any network computer.

The second is to leverage device security technologies, such as removable hard drives, internal firewalls and tools for overwriting or erasing data. Some are built-in, others are purchased separately, often at a moderate price. When leasing or buying output devices, it's critical to insist on such features. It's equally essential to inquire about the vendor's own security procedures as well as their compliance with IT security standards such as CCC, Common Criteria Certification. For example, a leasing vendor may let you purchase a device's hard drive upon termination of your contract. Or the drive may be crushed and replaced.

Device vendors like Xerox also offer innovative technologies specifically designed to make hard copies more secure. For instance, our DataGlyphs® symbology encodes machine-readable data into the gray areas of photographs and our GlossMark® technology embeds a hologram-like image onto the surface of printouts to prohibit reproduction.

While these tools may sound like something out of *The Matrix*, they've been available for a number of years, as have features like audit trails, which provide a detailed record of device use. More recent advances include embedded Radio Frequency Identification (RFID), which makes it difficult to remove a document without triggering an alarm, and "intelligent redaction," which keeps documents accessible, but limits sensitive content to those with a special passcode.

Another protective measure involves outsourcing document production and management to a trusted vendor. Through this strategy, you're able to benefit from the latest security technologies without a major capital investment. You can also implement a consistent set of enterprise-wide controls.

Equally valuable, outsourcing firms offer a big-picture view of devices and workflows, keeping you apprised of who's using which devices at what time and for what reason—crucial information in the event of a breach.

Weak Spot: Incorrect Assumptions and Inadequate Protection

Weapon: Thorough Assessment and Expanded Security

It's amazing how many organizations believe they're well protected because they have anti-virus software. Even when they have outdated antivirus software.

A continual review of your security solution to ensure currency isn't a "nice to have." It's a "must have." Just as the flu virus changes from season to season, so, too, do computer viruses. But computer "seasons" shift in a nanosecond. Without updated virus protection, you're fighting this year's influenza with last year's vaccination.

To continue the analogy, keep in mind that a flu shot alone won't protect you. You need a sensible diet, a good night's sleep and, if my Irish grandmother is to be believed, a hand-knit hat and gloves. In the desktop security world, that translates into protection against viruses and malware, spyware, spam and other potential network intrusions. In fact, in the most recent CSI (Computer Security Institute) Computer Crime and Security Survey, malware infection was the most commonly seen attack, reported by 67.1 percent of respondents.[7]

Of course, any solid assessment of document security should look beyond the desktop to the network itself. Are servers patched and up-to-date? Are demarcation points shielded? Are employees using Skype, instant messaging, peer-to-peer communication and other firewall jumpers? Applications must come under equal scrutiny, whether off-the-shelf or proprietary. If a hacker cracks an application, he or she could gain route access to a database, which is the electronic equivalent of handing over the keys to the kingdom.

During our assessments of client infrastructures, we'll often attempt external penetration of the network as a normal course of events. Sometimes, we'll even replicate the attempt in the physical world.

We're also able to provide clients with a risk-based ranking of potential threats. Our analysis incorporates general information—data from U.S. security agencies, patterns we see emerging across our clients' networks, hacker trends—plus client-specific information, such as the company's technology, education programs and C-level commitment to security. As a consequence, the client receives a predictive profile that details the likelihood of each security event as it relates to an organization of their size, in their industry, with their particular infrastructure and issues.

Ten years ago, network attacks in the U.S. may have numbered around 10,000 each year. Today, ACS, A Xerox Company sees about 100,000 a month, with 25,000 new vulnerabilities identified in that same time period.[8] Many can be prevented. 85 percent of the attacks referenced in the Verizon/Secret Service report were not considered technically difficult. 96 percent of the reported breaches could have been avoided with simple or intermediate-level controls.[9]

Now is the time to reexamine and fortify your security solution. Fighting back may be less difficult than you think.

The Attack of the Zombie Computers

You gotta ask yourself, are you a fighter … or are you zombie food?
From the 2003 film, Undead

Zombie computer attacks are not like zombie attacks in the movies; they're not after blood. They want to disrupt your entire business. These remote-controlled hijackers can flood business websites causing denial of service for legitimate customers. They can spread spam and viruses and conduct other maleficence—all without a computer's owner ever realizing it. These frightening adversaries are relentless and innumerable.

Fighting these attacks is analogous to opening the front door to millions of zombies while armed only with a rifle. You have to dispatch them one-by-one while the zombies are all around you, seething in the dark.

That's essentially what ACS did when the website of a major client was attacked. It was part of an assault on the automobile industry. ACS fought through the swarm, established barricades and dispatched every threat. But as fans of the genre know, new strains of zombies are certain to rise up. And that's the real horror in the online battle theatre.

Weak Spot: Lack of Phishing Knowledge

Weapon: Authentication Layers and Employee Education

By now, you've probably heard the term "phishing." If you haven't, imagine a wide net being cast over thousands of network users, then tightening. Now imagine that the net is squeezed with such force that money pops out of the victims' wallets. Here's a typical example:

You—and countless others—receive an email from a bank telling you to update your account. The email has a link. The link leads you to a page that looks exactly like your bank's website. You're asked to enter your password, Social Security number and other account information. Feel the net closing in?

The site is fake, of course, an exact replica of your bank's Web presence, right down to its logo and tagline. Sometimes called "spoofing," it's the old Nigerian letter scam wrapped in a

cloak of bits and bytes. Recently, a more targeted version called "spearphishing" has emerged. Spearphishing uses a smaller net that is harder to detect. With spearphishing, you receive a highly specific email that appears to be normal. For example, it might replicate your company's email format or include co-workers' names in the distribution list.

Sometimes, phishing is used simply to terrorize a network. We recently helped a client address a major phishing crisis caused by a disgruntled outsider. Employees received an email informing them that a document awaited on a sharepoint site. All they had to do was click the embedded link. 25,000 did. Their actions released a Trojan that penetrated the client's network, invaded email lists and spread like an electrical fire, quickly bringing the network to its knees. We carefully brought it back up.

One way institutions—particularly those managing personally identifiable financial information (PIFI)—are fighting phishing is by building multiple layers of authentication that are difficult to replicate. The first screen asks for your name. The second requires approval of a familiar photo. The third requests your password. The fourth asks for your oldest sibling's middle name. It's like surrounding a moat with barbed wire behind a brick wall inside a mountain range. Or, as the security pros call it, defense in depth. Confidential information remains protected and users are "trained" to expect a security sequence.

User responses to phishing scams can be difficult to predict. Therefore, it's best to prepare. We always recommend formal programs for educating employees about phishing and its consequences. Security tools can aid in limiting an attack, but ultimately, it is the user who decides whether to click. User training needs to be a major component of any security solution, particularly in light of the next menace.

Weak Spot: Insider Threats

Weapon: Data Loss Prevention Technologies

"Most security breaches happen from inside the organization." We've all heard the claim. But it's a myth. As mentioned earlier, inside attacks account for less than half of all breaches. However, they're responsible for the majority of enterprise data theft. Why, if fewer in number, do they have a greater impact? Because they're insidious and internal.

You can brace yourself for the attack of an angry stranger, but how do you prepare for the betrayal of an ally? Even Julius Caesar was caught off guard.

One answer lies in Data Loss Prevention (DLP) technologies. DLP tools operate like sentinels, surveying your network for unusual actions and typical fraud-related behaviors. This is particularly useful for protecting intellectual property and defending against identity theft.

For example, a DLP system might:

- Highlight suspicious actions, such as an employee making excessive copies or sending volumes of email to himself before leaving the company for a new job.
- Call attention to behaviors that don't align with corporate authorizations or to patterns that are indicative of fraud, like an operations manager repeatedly accessing corporate financial data at 2 a.m.
- Release a trigger when sensitive document content—a bank routing number or a key engineering spec—is included in an email.
- Create an audit trail of device usage, including user name, date and time.

More than simply activity monitors, DLP technologies can also spring into defensive action. For example, they can automatically encrypt confidential information left unsecured by a user. Or block network traffic.

But technology can only address part of the problem. The ultimate endpoint is a human being. The value of employee awareness and education cannot be overstated. As one security expert once said to me:

"You can't run a business without trusting somebody. Trust is key to success. So we trust, educate and verify."

---

8 Ways to Immediately Improve Your Security

1. Assess the comprehensiveness of your endpoint security (desktop devices, smartphones, flash drives) by reviewing your protection against viruses, spam, malware, etc.

2. Assess protection at the network layer. You should have either an intrusion prevention system (IPS) or at the very least an intrusion detection system (IDS), along with basics such as firewalls and network authentication.

3. Review the security and vulnerability of your output devices, including physical components (hard drives), security features (data erasure), usage, network connections, compliance and, if leased, vendor security procedures.

4. Make sure your complete security infrastructure—from antivirus software to document technologies to network pathways—is updated.

5. Educate your employees about threats like phishing through formal training and internal awareness programs. And remind them about the importance of internal compliance in protecting against inadvertent security breaches.

6. Create a checklist of crucial security program elements, including reporting, accountability, policies, technologies/processes, controls, awareness programs, physical components, reviews and incidence response.
7. Open up the C-level conversation. CIOs and CISOs should talk to their peers about dollars and risk, not terabytes. CEOs, COOs, and CFOs, in turn, should take an active role in security and not view it as "IT's job."
8. Monitor your security strategies and solutions on a constant basis. Security isn't a destination, it's a journey.

Compliance: The Other Side of the Risk Coin

> *You have two groups of individuals you really need to worry about—the criminally minded … and the loyal, law-abiding employees who on a day-to-day basis are handling your sensitive information in a way that makes it vulnerable to inadvertent disclosure.*[10]
>
> Dan Verton, Executive Editor, Homeland Defense Journal

Security is about people trying to steal from others or wreak havoc across a network. But there's a harder-to-quantify threat that causes comparable harm: noncompliance. Enterprises don't realize just how potentially dangerous a document can be when it's an integral part of a compliance process.

As regulations continue to increase and the lure of litigation shows no sign of waning, it's more important than ever for organizations to comply with government and industry mandates. Not doing so can expose an enterprise to litigation and risk, especially in industries that deal with personally identifiable information (PII) or health data. But virtually all industries are affected.

According to Ernst & Young's most recent report on the top 10 global business risks:

> The most important business risks for 2010 are concentrated in the areas of regulation and compliance. Many of these threats are related to the aftermath of the global financial crisis. Asset management, banking and to a lesser extent, insurance are facing a political backlash and regulatory overhaul following the global financial crisis.
>
> Oil and gas, real estate and mining and metals are contending with efforts by cash-strapped governments to gain revenues. And public sector organizations must cope with knee-jerk decisions made by political leaders under pressure.[11]

The culprit behind an information security breach knows exactly what he's doing. But the employee that creates a compliance issue may be completely unaware of his actions. In some ways, that's more dangerous. We all admit that mistakes can happen and delays are sometimes unavoidable. But the consequences of the inadvertent can be just as costly as those of the intentional:

- Failure to adhere to COBRA's provisions costs $100 per person per day ($200 if more than one person is affected), with the maximum penalty of $2 million per year.[12]
- Failure to comply with HIPAA will cost you $100 for each violation, with wrongful disclosures leading to a $50,000 penalty, imprisonment or both.[13]
- Failure to report the public health risk of a chemical substance to the U.S. Environmental Protection Agency results in a $32,500 fine for each violation.[14]
- Failure to follow Sarbanes-Oxley can result in multimillion-dollar fines, the loss of your exchange listing and imprisonment (up to 10 years if you're a CEO or CFO who submitted a wrong certification; up to 20 if submitted willfully).[15]

These fines represent noncompliance, but there are costs involved in compliance, as well, such as legal fees and document processing expenses. Not to mention the cost of delays and mistakes—the consequences of a missing form bearing confidential information or the inability to produce regulatory documents in a timely manner.

For instance, even a one-day delay in the production of the instructions for a new biomedical device can cost a company thousands of dollars. If the IFU (Instructions for Use) is rife with mistakes, it might also cost the company its CE (Conformite Europeene) mark or FDA approval. The same holds true for the approval of new drugs—every lost day equals lost dollars.

Using Documents to Ensure Compliance

Where do documents fit with all this compliance madness? Pretty much everywhere. Compliance management is information management—and we all know where most information resides.

Yet most managers and employees don't view documents as a risk. Documents need to be thought of as almost radioactive—incredibly destructive if not handled properly. Here are four simple document compliance scenarios that help illustrate the point:

Your company's annual report is ready to be released. The CEO rewrote his letter five times and the CFO made some last-minute adjustments. Were their changes made in the same document? Did they both approve their updates? Did anyone access the document who shouldn't have?

Your sales reps are on the phone processing credit card transactions. Are their actions compliant with the payment card industry's security standards? Can employees print sensitive data? Does information remain on-screen if a rep leaves to ask a co-worker a question?

The OSHA inspector asks to see your injury/illness log and questions some of the dates. Is the form current? Has it been filled out according to procedures? Does it have the proper certification?

You're sending patient records out for statistical analysis. Did you remember to include the Medicaid patients? Was everyone's personal identification information blocked or removed?

These are just small, individual examples. Project them in great numbers throughout the enterprise and the magnitude of documents' compliance influence becomes apparent. Documents are the core of compliance (e.g., secure PIFI content) and they fill the edges (credit card application forms). They provide proof of adherence (OSHA injury/illness logs), plus the source of the proof (employee medical records). The greater your control and management of documents, the tighter your compliance.

Enterprises in all industries should be sensitive to the fact that document compromise presents a true compliance risk—one that's heightened by the vagaries of mobile and cloud technologies. Employees and managers need guidance, structure and tools to keep that risk as low as possible.

Picture the aforementioned annual report scenario with a tool like DocuShare® compliance software. DocuShare can track when and why changes were made, and by whom. It also enables simultaneous document review, with password-protected electronic signatures. So you can be certain that the CEO's changes were made by the CEO. And if the CFO wants to distribute AR earnings for a final look, DocuShare produces a read-only version of the content and tracks any attempts to inappropriately handle the material.

Or imagine the preceding health care scenario with the intelligent redaction feature mentioned earlier. If the employee had forgotten to hide sensitive information, the redaction tool would prevent statisticians from viewing that portion of the form. And with document tracking, the employee would know immediately whether he or she had included the Medicaid files.

Technology that lets you create document "chunks" can also be invaluable, particularly in insurance, financial services and health care. Let's say you're an investment firm making a major change to a mutual fund. The change needs to be communicated to a number of constituents—internal personnel, financial advisors, institutional investors, private investors. After multiple paragraph drafts, endless reviews and several compliance rewrites,

a final statement is approved by all. That content chunk can be locked in place, stored online and made accessible through a global portal to any authorized user.

As a result, the official description of the fund's changes never varies. The language in a letter to investors is exactly the same as that in a PowerPoint presentation to institutional customers, which mirrors the content in a client services newsletter.

Minimizing Risk in Different Ways

- One of our government clients is helping to reduce business and personal risk through a Therapeutic Consultation Program. By closely monitoring patient documents such as drug claims, the program identifies patients who are out of compliance with treatment guidelines and helps prevent duplicate drug therapy. This not only aids personal health, but also has helped save millions in tax dollars.
- One of our hospitality industry clients is leveraging the power of automation to reduce risks related to workers' comp. The company imaged all of its workers' comp documents and files, enabling the organization to respond more quickly to claims, improve their risk management and in some cases avoid litigation.

Motion to Produce: The Value of E-Discovery

In December 2005, the Federal Rules of Civil Procedure made a small change that impacted the world in a big way. They redefined the term "record" to include email and other electronic documents. Since that day, the discovery process in litigation has never been the same.

Whether you're a lawyer, plaintiff or defendant, you bear the burden of producing all records related to your case. As noted before, that means searching for all relevant materials (including voice mails and instant messages), organizing them, storing them and sharing them for review—quickly and in compliance with court orders. This task is not getting any easier. In February, 2011, U.S. District Court Judge Shira A. Scheindlin held that the federal government must include metadata in Freedom of Information Act production because it is an integral part of public records.[16]

Scroll through the legal headlines of the last few years and it is not unusual to find companies settling cases simply to avoid the burden and expense of producing documents. Not to

mention instances where firms lost their case or endured millions of dollars in fines because they failed to either preserve discovery materials or produce them in a timely manner. Better document management can keep you from adding your company's name to the list.

Many of the tools mentioned in these pages—digitized documents, workflow controls, BlitzDocs collaboration, intelligent redaction—can aid in e-discovery, helping locate, cull and manage volumes of complex legal data. Relevant documents can be isolated from nonrelevant. Files can be reviewed in tandem. Confidential information can be blocked from view in documents provided to the opposing side. And legal teams can spend less time grappling with documents and more time developing solid strategies.

Compliance without Trying (Almost)

As mentioned earlier, compliance comes down to one thing—information management. If you're terrible at managing information, you'll probably fail at compliance.

How do you stop that from happening? By implementing strong technologies, policies and governance at the departmental and enterprise levels.

If your documents and their processes are well controlled, efficient and accurate, you can sometimes achieve compliance without working very hard at it. You avoid issues like unknowingly violating privacy laws because of the way your information is organized and distributed. Or you circumvent the regulatory repercussions of product information that is inadvertently misleading. You also steer clear of the other potential catastrophes already discussed.

You no longer send out documents wondering if the content is correct and/or compliant. Employees no longer question whether they're legally allowed to share certain pieces of data. And compliance teams don't worry about missing pieces of information. Regulatory questions are asked and answered up front so that problems are minimized later on.

In the midst of increasing regulatory controls, it's hard not to view compliance as the bane of an enterprise's existence. However, it's also proving to be a boon to enterprise security. In order to adhere to standards such as HIPAA, the Payment Card Industry Data Security Standard and the U.S. state data breach notification laws, companies are being driven to strengthen their security processes and controls. In fact, in the CSI survey, more than half the respondents say that regulatory compliance "improved their organization" and half of them report that "upper management made security a higher priority."[17]

Whether you realize it or not, you may be locking more e-doors than ever before, simply because outside forces—both good and evil—are forcing your hand.

How Secure Are You about What's Ahead?

Perhaps the most frightening thing about the compliance and security risks of the modern business world is that they are destined to intensify.

New regulations, such as the recent Dodd-Frank Act, will bring new challenges. New technologies will arrive with new threats. Consumer access tools, like smartphones and iPads, will further penetrate the commercial world, unearthing new risk issues. What's more, an e-generation is storming the workforce demanding 24/7, open access. What impact will they have on the balance of freedom and security?

Regulations never stand still and technology is equally swift in movement. As recently as three years ago, security surveys like the ones referenced in these pages had no category for "social networks." Yet, 28 percent of the breaches in the Verizon/Secret Service report employed social tactics.[18]

Regardless of what's ahead, documents will remain key. Protect your documents and their processes and you'll protect the enterprise. To do so, you need to ensure that your organization has the right security solution. But don't get too comfortable in your security blanket. You need to remain agile and aware. Constant vigilance and nimble evolution are paramount. An independent Gartner, Inc. report on security sums up the first point well:

> There is no such thing as a perfect, universally appropriate model for security organizations. Every organization must develop its own model, taking into consideration major trends and practical realities.[19]

As for the second point—the importance of vigilance—few described it better than my grandmother when she quoted a famous Irish proverb, "It's no time to go to the doctor when the patient is dead."

Endnotes

1. Verizon RISK team in cooperation with the United States Secret Service, *2010 Data Breach Investigation Report,* http://www.verizonbusiness.com/
2. Thomas L. Friedman, *The World Is Flat,* Farrar, Straus and Giroux, 2005
3. Scott Campbell, *Most Cell Phone Users Not Using Apps*, CRN, http://www.crn.com/news/applications-os/index.htm
4. David Leigh, *U.S. Embassy Cables Leaks Sparks Global Diplomatic Crisis*, http://www.guardian.co.uk/world/2010/nov/28/us-embassy-cable-leak-diplomacy-crisis
5. *Ponemon Study Shows the Cost of a Data Breach Continues to Increase*, http://www.ponemon.org/news-2/23
6. Ibid.
7. *15th Annual, 2010/2011 Computer Crime and Security Survey*, www.goCSI.com
8. Based on monthly attacks against ACS networks, along with new vulnerabilities identified by McAfee
9. Verizon RISK team in cooperation with the United States Secret Service, *2010 Data Breach Investigation Report,* www.verizonbusiness.com
10. James McNair, "Computer Security Threats Multiplying," *Cincinnati Enquirer*, October 19, 2006, Cincinnati.com
11. Ernst & Young in collaboration with Oxford Analytica, *The Ernst & Young Business Risk Report 2010—The top 10 risks for global business*
12. Susan Smith, "The New Excise Tax Penalties: Compliance is Your Best Defense," *Washington Health Care News,* June 2010
13. Office of HIPAA Privacy and Security, http://www.med.miami.edu/hipaa/public/
14. Office of Civil Enforcement, U.S. EPA, *August 2008, Failure to Report Chemical Risks Can Result in Major Fines*
15. *Sarbanes-Oxley Basics*, http://www.sox-online.com/basics.html
16. *New Opinion by Judge Scheindlin on FOIA, Metadata and Cooperation*, 7 February 2011, http://e-discoveryteam.com/2011/1/02/07/new-opinion-by-judge-scheindlin
17. *15th Annual, 2010/2011 Computer Crime and Security Survey,* www.goCSI.com
18. Verizon RISK team in cooperation with the United States Secret Service, *2010 Data Breach Investigation Report*, www.verizonbusiness.com
19. Gartner, Inc., *Best Practices: The Information Security Organization*, March 12, 2010