

No.1 / March 2011

**MEDIA
PLANET**

INFORMATION SECURITY & DOCUMENT MANAGEMENT

3

TIPS TO

BEING MORE
BUSINESS EFFICIENT

Working faster
NASCAR
winners inspire
us all to work
smarter

Security
Anatomy of a
cyber crime

Data protection
Cost saving
tips for your
business

PROTECTING YOUR FAMILY AND BUSINESS

Howard Schmidt, the White House Cyber Security
Coordinator, explains how to stay safe online

PHOTO: OFFICIAL WHITE HOUSE PHOTO



Securing
Our
eCITY

an ESET led initiative

Your best defense
against cybercrime?

Knowledge.

Sign up for a free
cybersecurity workshop at:
www.securingourecity.org

Your smarter antivirus software?

ESET.
Faster. Easier. More effective.

Visit www.eset.com for a free trial.

eset
Internet Security

CHALLENGES

As information shifts to computerized records and as we enter an age when cyber crime is expected to overtake conventional crime, effectively securing your business information is more important than ever.

Management of business information and its impact

Cyber thieves in the Ukraine stole more than \$400,000 from the bank account of a small business

in Redondo Beach. Other cyber thieves broke into the website of an online retailer in Whittier and stole money from the company's customers. A manufacturing company in Los Angeles spent more than six months and countless thousands of dollars in an extensive FTC inquiry following the inadvertent disclosure of employee social security numbers. A dishonest employee in a distribution warehouse in Van Nuys embezzled \$375,000 right under the nose of company management while an angry employee in Beverly Hills permanently deleted 15 years of information from the company's servers.

The increasing risk of cyber crime

The 250,000 businesses, not-for-profits and government units in Los Angeles are at increasing risk of cyber crime. So are Los Angeles' 3,000,000 families. Cyber criminals want our credit cards, our bank account numbers and our identities. Even our children are at risk from the sexual predators who troll the Internet.

We cannot defeat the scourge of cyber crime with technology alone.



Stan Stahl, Ph.D.
Los Angeles chapter of the Information Systems Security Association

Every business, not-for-profit and government unit must proactively manage the security of its information. Every family must manage the security of the information in its computers, lest it fall into the wrong hands. The time for action is now.

As president of the Los Angeles Chapter of the Information Systems Security Association, I applaud Mediaplanet and the Los Angeles Times for publishing this special insert on cyber crime.

Providing community leadership

Our organization, ISSA-LA, is partnering with other organizations such as OWASP-LA, ISACA-LA and the LA chapter of InfraGARD to provide the community leadership required for us all to meet the challenge of cyber crime. Our motto is it takes a village to secure the village and our mission is to be the catalyst for action.

I encourage you to read this special section. More importantly, I encourage you to act on the valuable information you will find within its pages.

We are about to enter an era as fundamental in its

impact on businesses and organizations as the shift to computerized records from paper systems or the shift from paper brochures to web sites.

Social technologies—think in terms of using tools like Facebook and Twitter for marketing, but also in terms of using these kinds of technologies inside your organization as a replacement for email—are about to revolutionize the management of company information.

This revolution creates challenges—and opportunities—for organizations of all sizes. Here are some tips to avoid being left behind.

Start experimenting

1 There are people in your organization—take my word for it—who are way more knowledgeable than your IT people about how to use social technologies. Set them free.

Provide guidance on what's acceptable

2 Set some guidelines on how you expect employees to behave in the social world. But don't go nuts; this isn't a 30 page document. IBM's social policy is one page long.



John Mancini
President and CEO of AIIM

Revise email methods

3 Start thinking about replacing as much of email as you can with a structure more friendly to cooperation. Sending countless emails around your organization with meaningless cc's and bcc's and repetitive attachments is not a way to tap into the intelligence in the heads of your employees. Get going on an alternative.

Listen to your lawyers, but don't let them tie you in knots

4 Lawyers for the most part hate the implications of social media, particularly when it comes to the possibility of discovery. They have valid concerns that need to be heard, but don't let them play a "NO" trump card.

As social technologies take root in the culture and in organizations, they will begin to become something that is not only "interesting," but also critical to the transformation of the business process. And to also the competitiveness and profitability of companies. Don't be left behind.



WE RECOMMEND



NASCAR champions tell us how they took speed to another level using document solutions

PAGE 6

"It made everyone work smarter."

Save money with document management **p.4**

How you can benefit from document management solutions

Protecting your business **p. 10**

How you can secure your business before it's too late

MEDIA PLANET

INFORMATION SECURITY & DOCUMENT MANAGEMENT

1ST EDITION, MARCH 2011

Managing Director: Allan Chiu
allan.chiu@mediaplanet.com

Editorial Manager: Jackie McDermott
jackie.mcdermott@mediaplanet.com

Responsible for this issue

Publishers: Tonika Miller & Allison Moore
tonika.miller@mediaplanet.com
allison.moore@mediaplanet.com

Business Developers:
Rebecca Ramgren & Elba Flamenco
rebecca.ramgren@mediaplanet.com
elba.flamenco@mediaplanet.com

Designer: Missy Kayko
missy.kayko@mediaplanet.com

Contributors: Janice Chaffin, Doug Chansky, George Grachis, Anthony Hymes, Barry Hartzberg, John Mancini, Michael Mascioni, Will Menaker, Stephen Rahl, Stan Stahl, Judith Vanderkay, Carmela Wong

Distributed within:

Los Angeles Times, March 2011
This section was written by Mediaplanet and did not involve Los Angeles Times News or Editorial Departments.

TOSHIBA
Leading Innovation >>>

Which is
easier, cutting
document
costs or
cutting jobs?

In about 30 minutes, we can help you save up to 40% on document output costs. And there's no telling what or who that might help you save.

To learn more, call
1-866 -24-IOTEC or
visit iotecdigital.com

IOTEC

printworks



NEWS



DON'T MISS!

Money saving tips and facts

- ➔ Migrate to the cloud. It will significantly reduce your business' equipment and operational costs.
- ➔ Automate business processes to reduce unnecessary paper usage.
- ➔ Digitize your documents. It is estimated that it costs \$20,000 to fill a five drawer filing cabinet with paper documents.
- ➔ Automate data capture and forms processing with optical character recognition. This will reduce the labor hours spent manually entering in information.
- ➔ Implement a document management solution. This can lower your operational costs by 25—65 percent.

Question: How can businesses become more efficient?
Answer: By utilizing document management systems to cut down on waste and costs.

Save money with document management

Traditional printing for businesses, usually an ad-hoc system put together by an IT department that is not looking at the whole picture, means heaps of extra documents, printing multiple versions for different people, and an overflowing bin by the water cooler labeled "recycling."

Different departments often buy printing supplies from different vendors on a one-off basis. This is extremely costly. It digs into the productivity of workers. Workers must then source supplies and that extends the downtime to other workers who are in need of something printed, such as engineers.

Old-fashioned document management is not much better, which

is apparent in the way that employees handle physical documents. According to NowDocs, 15 percent of papers are lost by work groups, and 7.5 percent of papers will never be found again. They reckon that 90 percent of documents are merely shuffled when handled, and that it costs an average of about \$120 to track down a missing document.

Becoming more efficient

Fortunately, new solutions are emerging that look at document and print management as a complete picture with many overlapping parts. By analyzing the costs and needs involved for each part, efficiency as a whole is improved. For example, individual print stations were proving very costly, so new systems emphasize group printing.

"Fortunately, new solutions are emerging that look at document and print management as a complete picture with many overlapping parts."

These improvements are also thanks to better technology and access to the cloud, essentially online computing power and storage space. Documents can be printed remotely to save time and can be edited in the cloud, with more devices such as smartphones, reserving the printing

for only the final version of a document or report.

Implementing solutions

Skipping this printing step until it is absolutely necessary is great news for productivity, but going entirely digital is even better. While it will never be possible to be completely paperless (certain documents require a physical signature), digitizing records makes for easier reference and is actually more secure than leaving physical records that could be destroyed by fire or flood.

Putting all of this together adds up to a big cost saver. According to HID, a print management system can save up to \$220 per employee per year.

ANTHONY HYMES

editorial@mediaplanet.com



Manage your business; we'll corral your information

www.satory.com • info@satory.com



NEWS

A personal guide to staying safe online

Cybercriminals steal your sensitive personal information by taking control of your computer.

This control also lets them install rogue programs on your computer, turning your computer into a zombie under their control—the cyber-equivalent of Night of the Living Dead. These control programs make money for the cybercriminals by sending spam, displaying pop-up ads, and committing sophisticated computer crime. How do they do it? Cybercriminals take control of your computer by exploiting four weaknesses:

- Every computer program running on your computer has subtle programming errors (vulnerabilities) that cybercriminals exploit to take control of your computer.
- Legitimate internet web sites often fail to prevent cybercriminals from installing malicious programs on their websites. When you visit these sites, these malicious programs silently install Trojan horses and other malware on your computer.

- Default settings for many computer programs make it easy for cyber criminals to take control of your computer.
- Users often don't know what they need to do to minimize the dangers and risks of cybercrime, particularly the need for defense-in-depth.



SECURE YOUR WIFI. If you have a wireless network, encrypt it with WPA2 encryption. PHOTO: ISTOCKPHOTO.COM

In order to keep cybercriminals off your computer, here are some defense strategies:

- **Keep systems patched:** Software manufacturers issue program updates containing patches to fix known vulnerabilities. Set Microsoft Windows and Office to automatically update. Manually update other programs like Adobe Acrobat, iTunes, Flash and Java.
- **Limit exposure:** Create separate accounts for all family members. This will make it harder for cybercriminals to install malware on your computer.
- **Protect your desktop:** Install a reputable antivirus/antispyware product and keep it up-to-date. Sophisticated cybercriminals can get past basic antivirus/antispyware software. Antivirus is necessary but not sufficient.
- **Secure your WiFi:** If you have a wireless network, encrypt it with WPA2 encryption. Otherwise anyone near you can eavesdrop on your communications and piggy-back on your connection.
- **Beware of scams:** Don't click on web-site ads or pop-ups offering to

scan your computer for free. Cybercriminals love to take advantage of people's fear of getting a virus. Instead of scanning your computer, these programs will infect it.

- **Always be wary:** Don't follow links in unfamiliar or unusual emails, especially those requesting your user names, passwords, or financial information. A SPAM filter can help you avoid these e-mails but you must be on guard for emails that get past your SPAM filter.
- **Defense strategy:** Be careful with your financial information on-line. Use a credit card rather than a debit card when shopping on-line. Link PayPal to your credit card, not your bank account. Federal law limits your credit card exposure to \$50. There is no corresponding limit if you use a debit card (even though many banks cover debit card fraud).

Remember, always think about the information you are giving out and when in doubt, don't.

STAN STAHL, PH.D
editorial@mediaplanet.com



The Internet is today's home away from home; it is the playground for our imaginations; it is society without the need to be out in world physically; it is the new community we live in. So the same as we lock our cars and houses, we need to safe guard the 'e-ME' or electronic version of our individual information. Neglecting to not do this or failing to take the topic seriously is just as crazy as pinning up our debit card with PIN number to the tack board at the local community shop with a note saying, "if needed use this, it's on me, you're welcome."

It is our personal responsibility to protect ourselves—understanding that concept, understanding our own Internet presence, and wanting to take steps to secure it is the first line of defense.

DOUG CHANSKY,
CONTOUR DATA SOLUTION

black hat
BRIEFINGS & TRAINING

USA + 2011
EMBEDDING SECURITY

JULY 30 - AUG 4
CAESARS PALACE
LAS VEGAS NEVADA

50+ TRAINING COURSES
8 TRACKS OF SECURITY RESEARCH
OVER 6000 SECURITY PROFESSIONALS

REGISTER BY APRIL 30 WITH THE CODE [BHUSALA80]
TO RECEIVE 10% OFF OF BRIEFINGS:
WWW.BLACKHAT.COM

INSPIRATION

The organization behind five NASCAR Championships in a row,
Hendrick Motorsports is driven by new technology that enables their staff to work smarter.

Even the fastest can work faster

HOW WE MADE IT

Formed in 1984 by Rick Hendrick, Hendrick Motorsports knows a few things about success. Winning five NASCAR championships in a row is an extraordinary feat; no other major sports organization has done anything like it, not even great teams like the Celtics, Yankees, or Red Wings.

But with 550 employees, a massive 600,000 sq ft facility, and new technology, Hendrick Motorsports is also succeeding at business. Chris Newsome heads the IT department at

Hendrick and talks about how their print management system slashed their printing costs and revved up the way employees work.

Why did you go with a document management system?

“We grew so fast that print management was getting out of control. We performed an Encompass Document Analysis to see where we could increase efficiency and save money. Right away it was obvious that we were overloaded with hardware, and not printing in a very smart manner.”



“It made everyone work smarter.”

Chris Newsome,
Head of IT,
Hendrick Motorsports

“In the first year we saved approximately \$110,000. Plus we got everyone working smarter across the campus, using group printing, taking high-cost printers off of people’s desks, and using Re-Rite to transform paper documents into PDF, Word and Excel, which we use often.”

How did it help to make Hendrick go faster?

“It made everyone work smarter. We have a lot to do and need to work fast. Any time we can save 15-20 minutes, that’s a bonus. By combining the latest multifunction products

with great software, we streamlined workflow—saving hundreds of productivity hours monthly.”

What were you able to do with the savings?

“We put the savings right back into racing. We have a budget, but when you partner up and can see the money, it’s easy to put it right back into winning more championships.”

ANTHONY HYMES
editorial@mediaplanet.com

indus has been providing turnkey document management solutions since 1985.



We are a major supplier of planetary and robotic book scanners, with software solutions tailored for university libraries, county governments and other organizations that have volumes of bound materials to be digitized.

Consult with us to determine the best solution for your records management needs.



Call us at 1-800-843-9377 or visit us at www.indususa.com

indus International, Inc. 340 South Oak Street West Salem, WI 54669

INSIGHT

The high priority assigned by the **Obama administration to cyber security** is no secret. Howard Schmidt, the White House appointed cyber security coordinator explains the federal government's comprehensive initiatives aimed at raising awareness.

Federal government ramps up cyber security awareness campaign

This strategy is partly driven by the changing nature of cyber attacks, which seem to be more concentrated on “end users and consumers,” who tend to be “less sophisticated” about cyber security, according to Howard Schmidt, the White House's Cyber Security Coordinator.

A cornerstone of the federal government's cyber security awareness campaign is its National Initiative for Cyber Security Education (NICE) program, which is designed to integrate various federal cyber security efforts, and develop a broader range of cyber security experts beyond technologists, including business, legal, and international relations personnel. One of the key NICE initiatives is Stop.Think.Connect., which was

launched last October, and was designed to equip citizens with resources and tools to meet cyber security challenges, including tips on cyber security. So far, 5,000 citizens have signed up as friends of the campaign, reports Schmidt.

The Cyber Awareness Coalition, one of the largest government cyber security awareness efforts, is helping promote a number of government cyber awareness initiatives, including Stop.Think.Connect. Currently, members of the coalition include such agencies as the Department of Justice, Department of State, Department of Education, NSA, and FBI's InfraGard.

In another significant initiative, the federal government is holding Cyber Citizen Forums to raise public awareness about cyber security in a number of U.S. cities, including San Diego, Mem-

“Stop.Think.Connect. was designed to equip citizens with resources and tools to meet cyber security challenges.”



Howard Schmidt
White House Cyber Security Coordinator

phis, and Detroit, in conjunction with colleges and universities.

Beyond that, the federal government is organizing Cyber Security Campaign Roundtables to “bring together non-profit organizations and the private sector” to develop “best practices” in cyber security and help convey the federal government's prime cyber security messages, says Schmidt.

Reduce the risk

Ultimately, these programs are designed to “reduce the risk” of cyber attacks, anticipate potential cyber security threats, and afford all parties, including “end users,” a “shared” role in cyber security, points out Schmidt. These efforts and others are paying off in a number of ways, according to him. For example, the significant rise in e-commerce transactions indi-

cates greater public trust in the security of the e-commerce infrastructure, Schmidt asserts.

Simulations are serving as a key training tool in federal cyber security efforts, he says. One of the government's main simulation initiatives is Cyber Storm, led by DHS, which simulates response to not only “specific threats,” but also “cascading effects” of such cyber incidents. The government is employing these kinds of simulations to help “reduce the duration of particular cyber security threats, recover from the threats, and reconstitute” so that the country can “return to business” as usual, explains Schmidt. He notes that these tools are being used to train both current “cyber security experts” and “future cyber security officials.”

INSPIRATION



DON'T MISS!

National Cyber Security Events

The ISSA-LA 3rd Annual Information Security Summit Wednesday, June 15, 2011 7:30 am – 6:00 pm UCLA Campus

→ ISSA-LA- The Information System Security Association is the largest international association of security specialists. Membership ensures that you are on the cutting edge of innovation and adhere to the highest standard of ethics. ISSA helps you stay abreast with technological advances, develop professionally, and build relationships with professionals.

Infosec World Conference & Expo (April 17-21, 2011) in Orlando, FL

→ This conference will offer 70 sessions covering all areas of information security. It is attended by 1,500 IT leaders. Speakers will cover topics such as next generation firewalls, securing content in Sharepoint, and hard drive forensics. Key-note speakers this year include Roger W Cressey Counterterrorism Analyst, NBC and former presidential advisor and Bob Sullivan, Senior Technology Correspondent, MSNBC. For more information please visit <http://www.misti.com/default.asp?page=65&Return=70&ProductID=539&LS=infosecworld>



PHOTO: ISTOCK.COM

TIP

2

ATTEND
CONFERENCES
AND EVENTS

Anatomy of a cyber crime

Over just the last ten years, the range and scope of cyber crime has become even broader than the range of physical crime. Who is this community of cyber criminals? And what organizations exist to counter this growing threat?

The ISSA (The Information Systems Security Association), a non-profit organization that provides community-based education, awareness and training in effectively managing cyber crime and the President of its Los Angeles chapter, Stan Stahl—one of the country's leading experts on cyber security—are at the forefront of a movement that is closing the gap between the people with the means and motivation to commit these crimes, and both their victims and the law.

Cyber crime is in many ways the natural evolution of any other kind of organized crime, and the crimi-



nals run their operations in a similar way. "Like Tony Soprano, there are bosses," says Stahl, "but instead of sending out their goons, these guys have their geeks," highly specialized experts who look for and exploit vulnerabilities in the code of commonly used programs. Cyber crime is a global industry. "For example, a cyber-criminal in the Ukraine is planning a job where money will need to be transferred out of the country. He will call up a buddy in China and say 'I need 80 money mules to move \$700,000 next week.'"

"Like Tony Soprano, there are bosses," says Stahl, "but instead of sending out their goons, these guys have their geeks."

Stan Stahl

Cyber crime is, "run like a business," and it is becoming big business.

The cyber criminal

Where there is a will there is a way, "and the way," says Stahl, "is like shooting fish in a barrel, because businesses are woefully unprepared." The creativity of the cyber-criminal in terms of how to monetize information is virtually limitless. "If you can imagine it, it can happen," everything from stealing people's identities, medical insurance to, "honest to goodness dollars

from the bank accounts of businesses," says Stahl, "and what's worse is that when the company that's been victimized calls their bank, the bank is not obligated by law to give the money back."

According to Stahl, a big part of the problem is a denial of how serious the problem is, but "a critical piece of the solution requires that businesses, banks, information systems security professionals, and associations like the ISSA, all get involved and come to the table and deal with this issue in a way that's practical and workable. So much could be done just by sharing information and the collective wisdom of the community." Having a conversation among the right people is the first step in building a community that is able to effectively defend itself from today's cyber criminal.

WILL MENAKER

editorial@mediaplanet.com

PANEL OF EXPERTS



George Grachis

District Information Security Analyst; Brevard Public Schools; Board Member ISSA, ISACA & InfraGard; Keiser University Advisory Board



Janice Chaffin

Group president, Consumer Business Unit, Symantec



Doug Chansky

Senior Technology & Security Consultant, MCP, VCP Contour Data Solutions



Question 1:

As many people find cyber security to be a confusing topic, what do you believe are the main misconceptions regarding internet security?

That if you use antivirus and update your operating system patches or have a Mac you are safe from cybercrime and malware, malicious software. The reality is user education and awareness is becoming more important as cyber criminals exploit technologies like Anti-virus and firewalls, making them less effective. In my book "OMGClickHereToGetScammed," I mention, we all learn and get licensed to drive a car, why not get trained to be a responsible cyber citizen?

The Norton Cybercrime Report shows that 65 percent of Internet users globally have fallen victim to cybercrime, and many feel powerless against it. Cybercrime has therefore become a silent digital epidemic. The reality is people can fight cybercrime with the right protection and knowledge about online threats.

Speaking with people about this topic I always get a similar response, "if I secure my computer then there will be nothing left." Most feel that being security conscious means they have to keep everything to themselves and not share anything. The second is that their machine will run slow.

Question 2:

The attacker community is constantly evolving. How have you noticed these changes and how have you dealt with them?

I spend a lot of time reading Internet RSS feeds, websites and participate in three professional information security and audit organizations; Information Systems Security Association (ISSA), ISACA and InfraGard. I use this timely information and apply it to our enterprise environment. In essence we then look at how a given threat or vulnerability impacts our organization

Cybercriminals now run sophisticated schemes to steal financial information. Norton has responded with technologies that automatically block new threats. As consumers depend more on their mobile devices, we've also expanded our offerings to include mobile security.

The attacker is becoming more personal. Attackers are getting closer to you or are even people close to you. They are using social networking as a scouting utility allowing them to be more convincing. This can be controlled by computer security controls and carefully reviewing your Internet activities and partners.

Question 3:

How can individuals avoid leaving themselves vulnerable to cyber threats? What's the biggest obstacle they can face and how can they overcome it?

I believe user education and awareness is the biggest obstacle we now face. My father's generation created the Internet and my generation built it. We have since placed everything we value, including our identities, onto a system that was never designed for security. To make matters worse we neglected to train anyone on how to safely navigate in this newly connected world.

Security software that protects against a variety of threats is essential. It's not enough to use basic protection, like free antivirus solutions. People need comprehensive protection against phishing, identity theft, and more. Consumers should also stay up-to-date on threats with the Norton Cybercrime Index, which tracks and warns people about daily cybercrime risks and provides actionable steps on how to stay protected.

There are a few key concepts to remember and they seem to do a good job against most attackers. First, know who is on the other side of your activity. Second, look for web sites that display a secure connection. Third, pay attention to warnings the computer software displays.

INSIGHT


**BEST TIPS FOR
BUSINESS & DATA**
Educate your workforce

Make sure your employees know a simple fact: no business is 'too small' to be targeted by cyber crime.

Loose clicks sink ships

It's a sad truth, the majority of cyber-incidents can be traced back to a single mistake made by an unsuspecting person.

Close vulnerabilities

Make sure your workforce is equipped with current software, and convey the importance of accepting software updates when prompted.

Make sure to backup

The time you spend setting up a data backup system is a pittance compared to the monumental hassle of retrieving data from a broken hard-drive on an employee laptop.

Make sure the cure isn't worse than the Problem

Too often, very-small businesses will purchase software designed for much larger enterprises. This can eat-up your time, making the total cost of securing your business much higher than you bargained for.

GARY MULLEN

Question: What's the most effective way for a small business owner or employee to combat cyber crime?

Answer: Simply being aware of the nature of these crimes and the specific behaviors that increase one's risk of exposure is an important first step in protecting yourself and your business.



Protecting your business

Today's sophisticated cyber criminals employ a two-phase attack to take over business and home computers.

These attacks combine getting the user or employee to open the door to the outside, and then delivering a payload in the form of a malware program or Trojan Horse that will allow the cyber criminal to take control of your network and information, often completely undetected. Successful defense starts with a combination of training staff and using technology.

Getting the door open can involve a criminal who looks for holes in the security of popular websites, which allow them to insert their own code, thus causing any visitor to that site to run the attacker's code on their computer. Or, those who create their own website and try to entice users to come to them, often



"First and foremost, make sure that every program that you use for your business is running the most up-to-date version."

in the form of spammed e-mails or pop-up ads. Once the door is open and the malware or Trojan Horse installed, the cyber criminal can do almost anything: read all the files on a hard drive, copy and record every key stroke—including passwords to bank accounts or customer's credit card information—or even use your computer to launch attacks on other targets.

There are no "silver bullets" that can keep cyber criminals off a computer. But there are a few basic things that go a long way towards keeping

the casual cyber criminal at bay. First and foremost, make sure that every program that you use for your business is running the most up-to-date version. Often cyber-crimes are committed by exploiting systems in which a new update or "patch" has been available for weeks, or even months without the user noticing.

Second, make sure every computer is protected with an effective anti-virus/anti-spyware program. Even better, upgrade to a Host Intrusion Prevention System. While more expensive than basic anti-virus solu-

tions, they also are more effective at blocking today's advanced cyber attacks. Information is valuable. This is not the time to be penny-wise and pound-foolish.

And finally, train your people. Make sure they know the danger signs. Make sure they understand their role in keeping cyber criminals away from sensitive or critical information.

For any business, large or small, the best security starts from the bottom up with the awareness and understanding of the individual user or employee, but is led and managed from the top down by those who understand that cyber security is a fundamental aspect of business governance.

WILL MENAKER
editorial@mediaplanet.com



ENSURE THE SECURITY OF YOUR ENTIRE IT INFRASTRUCTURE.

CYBER CONTROL
CYBER MONITORING
CYBER FORENSICS

Proactive control of your critical IT infrastructure
Real-time detection and analysis protects against cyber threats
Detailed, auditable security intelligence provides actionable evidence

Watch our cyber security video series at
www.tripwire.com/data-protection



PANEL OF EXPERTS



Bill Melo

Vice President, Marketing, Services and Solutions, Toshiba America Business Solutions Inc.



Ryan Duguid

Senior Product Manager, Microsoft Corporation, Inc.



John Mancini

President and CEO of AIIM



Question 1:

What are direct benefits businesses will incur upon implementing an effective document management solution?

Reduce the cost of doing business by automating document workflow. Documents (paper and electronic) are the lifeblood of any business. Unfortunately, most organizations don't have a formal system for how they capture, manage, store and deliver documents, so the process becomes very labor intensive. A document management system allows an organization to 'tame the chaos' and bring order by creating formal processes and workflows.

The most effective document management strategy can be found at the intersection of traditional document management, collaboration, social computing and search. By deploying a collaborative platform that provides these core capabilities in a way that is natural and intuitive, businesses will be able to amplify the impact of their people, improve process efficiency and reduce risk.

Document management will help your organization operate more efficiently, be more responsive to customers because you can actually find things, and speed up your processes. Failure to manage your documents will create an undecipherable digital landfill that will slow everything down.

Question 2:

What should businesses keep in mind when purchasing a document management solution?

Scalability and ease-of-use. The ideal solution is one that will grow with your company. Ease of use is very important for employee buy-in. Is the system easy to use and integrate with other business applications? If the solution is too complicated to use relative to the value it brings and the problems it solves, then there is little benefit.

Key decision makers need to carefully balance business requirements, IT objectives and end user acceptance when choosing a document management solution. Historically, purchasing decisions have been made based on the requirements of a small set of information custodians who focus on specific problems without considering wider business objectives, the need for IT rationalization and the fact that end user adoption is critical to a successful implementation. As we move in to an era of consumerization of IT, decision makers need to seek out solutions that provide document management as part of an extensible platform that delivers collaboration, social computing and search while showing end users clear value in their daily work.

There is no single right solution; only a solution that is right for our organization. There are a wide variety of solutions, ranging from simple, inexpensive point solutions to complicated enterprise solutions. Take the time to find the appropriate one.

Question 3:

How can document management solutions address compliance and security issues?

As previously mentioned, security and compliance are some of the most important benefits, of a document management system. The ideal solution should include a Records Management feature. This allows you to create a policy by document type, stipulating how long the documents should be retained and when and under what conditions they should be destroyed. This feature is critical from a compliance perspective. On the security front, document management systems can include policies for users and groups that allow a company to determine what documents or document types users have access to and what they can do with them (view, edit, print, copy, etc.). Organizations looking at document management should investigate an enterprise digital rights management (DRM) solution. This can integrate with and compliment your system by ensuring documents are secure within your company, and even when they leave your organization.

Document management solutions offer a wide range of capabilities to control access to information, prevent unauthorized dissemination of information and provide full audit history of all user and system activity. Of course technology is only part of the solution when it comes to compliance and security and no document management deployment is complete without an effective governance strategy that defines users permissions, rights management policy, retention rules and metadata capture requirements. In addition, no system is foolproof without clear policy and process that dictate user responsibility for information handling and management.

The first step toward compliance is the step of getting things under some element of control, even if it's not perfect. Don't allow the worry about finding a perfect solution keep you from doing something. The sooner you tackle the digital landfill, the sooner your business will be competitive.

Accept a friend request

accompanied by a digital picture
of a scantily clad female

even though you don't know her
from Adam (or Boris),

which, coincidentally, happens to be
"her" real name,

increasing your virtual friend count

while granting him/her access

to your online savings account.

Allow

Deny



Deny digital dangers (and their unfortunate outcomes) with Norton Internet Security 2011.
Ranked #1 in both Protection and Overall Performance.*



*Source: norton.com/passmark2011, norton.com/dennislabs2011
© 2011 Symantec Corporation. All rights reserved. Symantec and Norton are registered trademarks of Symantec Corporation.

everyclickmatters.com