

# Information Security

“Key Points to Ponder”

# Information Security Session Outline

- Data defined
- Technology, applications and how they affect you
- Security issues surrounding Information Technology
- How does this affect me?
- How does this affect my work place?

# Data Defined

- Simply put, data is any information used electronically.
- Can be:
  - Stored – Disk, thumb drive, CD, DVD, Phone, PC, Tape
  - Shared – Social Networking, Online
  - Transferred
  - Printed
  - Copied
  - Texted
  - Emailed
  - Faxed

# Data Defined

## Data theft culture 'flourishing,' survey finds

[Tash Shifrin email](#)

Tuesday 21 November 2006 14:42

A culture of data theft is flourishing in UK workplaces, security experts have warned.

A survey of more than **1,000 UK workers** carried out by research company Tickbox.net for security firm Prefix IT found that **60% admitted to theft of confidential documents, customer databases, business contacts or sales leads.**

But the survey found that managers were unaware of the scale of the problem. **Just 7% of managers believed their companies had been affected by data theft, while 29% of managers said the issue was not recognized at board level.**

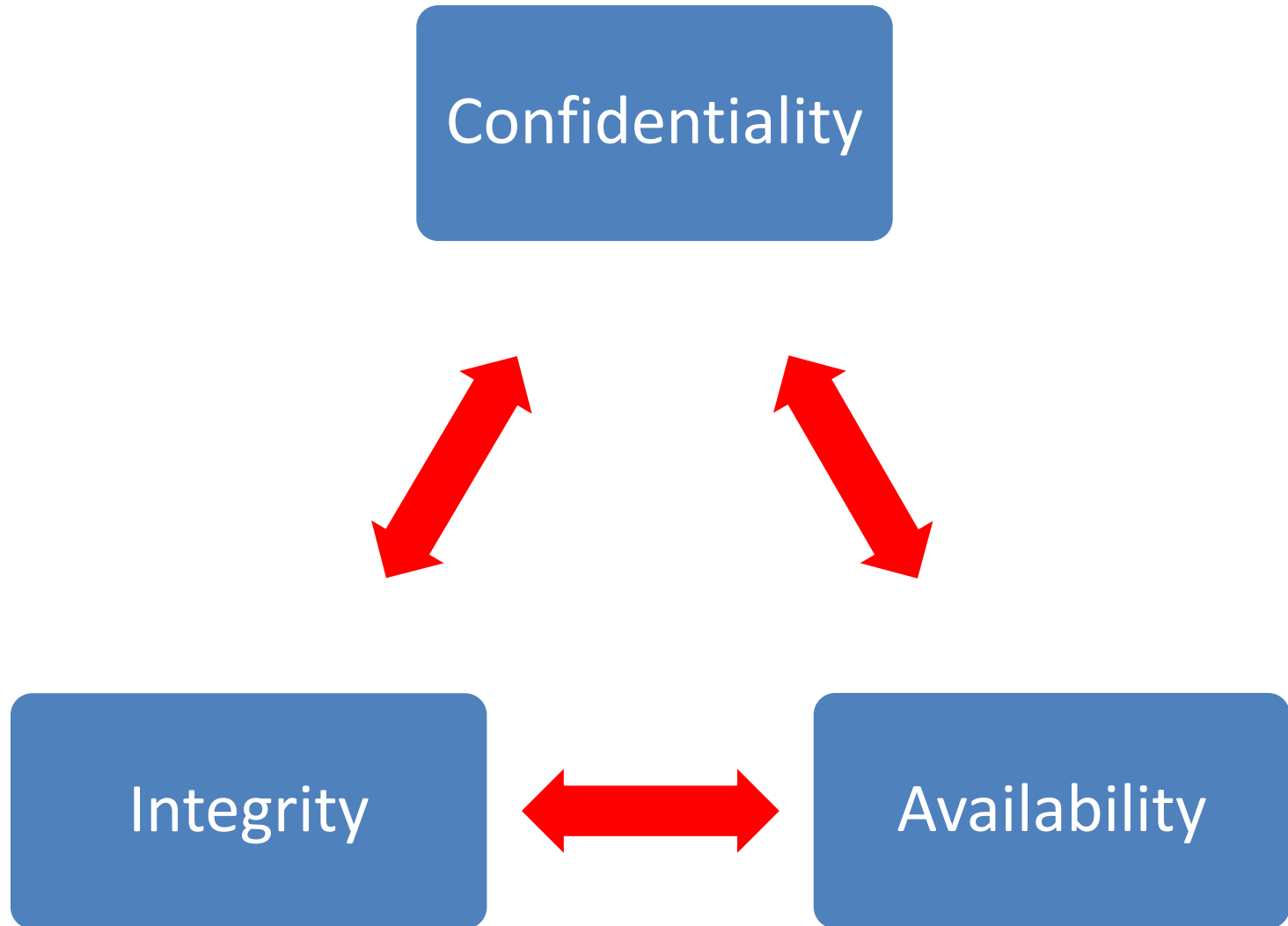
The survey revealed that **73% of workers were not aware of any special security measures to prevent workplace data theft and 44% were unaware of policy explaining what could and could not be taken home.**

Nearly two-thirds of those surveyed - **63%** - **said there were no restrictions on using personal portable devices such USB memory sticks in the workplace, while the same proportion believed that staff "think nothing of taking things from the workplace".**

Prefix IT chief executive Graeme Pitts-Drake said, "While trust in staff is laudable, it is professionally negligent not to protect company assets appropriately through policy and technical means. Failing to communicate with staff about un-acceptable activities is tantamount to endorsing theft."

Comment on this article: [computer.weekly@rbi.co.uk](mailto:computer.weekly@rbi.co.uk)

# C.I.A Information Security Triangle



# Data Retention and Disposal

- How long should you keep online access to your Data? How long should you keep your archived Data?
- What type of media do you use to archive your offline Data? What is its “shelf life”? Do you have a plan to transfer archived Data from obsolete media formats to current media formats?
- Who has physical and/or read access to archived media and its Data?
- How do you properly dispose of the media that contains sensitive Data?

# Data Security

## Data security lessons from Russian spy ring

July 9, 2010 by Sam Narisi **Posted in:**

[In this week's e-newsletter](#), [Latest News & Views](#), [Security](#)

You'd think a gang of spies would know a lot about document security — after all, it's their job to exploit security holes to gain access to sensitive info. But it turns they make many of the same mistakes as your company's users.

While looking into the Russian ring accused of spying on the U.S., federal investigators found the gang had plenty of security holes of their own — and their lack of IT support and know-how has been a big help in the feds' investigation.

Among the errors:

**A lack of an effective password policy** — One of the alleged spies used a disk protected with a strong, 27-character password to hold confidential documents — but left it written down on a Post-It note stuck to the computer, which officers found when they searched the suspect's home, [Network World](#) reports.

**No network security** — Another suspect regularly used unsecured public wireless networks to communicate with Russian government officials. U.S. agents tracked the spy and saw her using the free WiFi offered in book stores and coffee shops.

**Poor help desk support** — Some laptops used by the gang took months to troubleshoot, and one spy was so frustrated with her computer that she turned it over to an undercover U.S. agent who promised he could repair it.

# Technology Applications

The question is not “do you use” it is, “which do you use?”

## Business Applications

- HRMS
- Budget
- Email
- Financial
- MS Office
- PowerPoint
- CRM
- ERP
- Facebook
- Twitter
- Google
- LinkedIn
- YouTube
- Skype

## Personal Applications

- Facebook
- Twitter
- YouTube
- Google
- MySpace
- Skype
- Texting
- Ebay
- Amazon
- Interactive Video Gaming
- Movie Download
- Music Download
- Video Games

# Issues with Application Security

- True or False, Application Development Programmers are taught secure coding techniques in school.
- True or False, All applications developed for business purposes are secure.
- True or False, All Facebook and Smart Phone applications are “vetted” by the vendor.
- True or False, A secure application frees the user from vulnerabilities in the operating system.

# General Building/Office Access

- Do you know who has or should have access to your work space and/or mission critical equipment?
- If you had an “emergency” or “loss” event, could you provide proof who was in the work space at the time of the event?
- Do you, your staff and/or co-workers know how to “challenge” an unknown person found in a sensitive area.

# Printing Security, Really?!?

## HP printer hack risk prompts update

Firmware update guards against file snaffling

By [John Leyden](#) Posted in [Enterprise Security](#), [9th February 2009 13:35 GMT](#)

Users of HP LaserJet printers need to apply a firmware update following the discovery of a potentially troublesome [vulnerability](#). The security bug creates a means for hackers to gain access to files sent to printers via the web administration console on vulnerable machines. A security [advisory](#) from HP explains various versions of its HP Digital Senders as well as HP LaserJet printers and HP Color LaserJet printers are all potentially vulnerable.

Users of HP LaserJet 2410, 2420, 2430, 4250, 4350, 9040, and 9050 series all need to upgrade their printer's firmware software to a secure version. HP Color LaserJet 4730mfp, HP Color LaserJet 9500mfp and HP 9200C Digital Sender users also need to update.

PCs and servers are the main focus for security updates, but embedded systems and devices (such as printers) also pose the occasional security risk. That's because printers and photocopiers have grown in sophistication to become document processing hubs instead of single-function boxes. Digital copies of scanned or printed documents are often stored on such devices, which are becoming more and more like other computing devices, and therefore subject to much the same security risks.

Printers can become the conduit for hacking attacks as well as a possible (though not especially potent) agent for spreading malware, as worms such as Code Red have illustrated. "Printers tend to be low on the priority list of systems or devices to be patched - this one will likely linger for years to come," [notes](#) SANS Institute security researcher Adrien de Beaupre. "The impact might not seem severe, as in the attacker can view the printer configuration - however, viewing cached versions of printed documents can be [serious]." ®

# Printing Security, Really?!?

## Are these 5 mistakes compromising your printer's security?

August 11, 2009 by Sam Narisi

Posted in: [Security](#), [Special Report](#)

MFPs are constantly getting smarter and more “computer-like” — which makes them more vulnerable to the security risks that affect other devices. With networked MFPs, security breaches are possible at every step of the printing process — on the user’s computer, on the server, between the server and the printer, and on the printer itself. Last but not least, there’s a low-tech risk that’s been around as long as shared printers: a co-worker or other passer-by taking someone else’s pages out of the printer’s output tray. That problem’s apparently widespread — **56% of employees have seen sensitive documents left in the printer unattended**, according to a recent [survey](#) by Samsung Electronics.

Here are five common mistakes businesses make that compromise printer security:

**Printing off an unsecured disk** — If your device prints off its own disk, you can probably set it to erase the disk after every job (sometimes you need to buy add-on software from your vendor). Alternatively, some printers let you bypass the hard disk and print straight from RAM (which is more secure but takes longer). Finally, you can buy a model without a hard disk — that’s an option you may not even need.

**Not requiring authentication where it’s needed** — A common mistake of setting up shared printers is treating every department the same — even though some deal with more sensitive documents than others. Though it may be too big a hassle in some places, for departments that regularly print confidential documents, consider getting a printer that requires a user to enter a password into the machine before it prints. Some models also use swipe cards, or even biometric fingerprint readers.

**Keeping the reprint option** — Some printer models let users hit a button that prints another copy of the previous job. Obviously you don’t want that capability when someone’s printing a secure document.

**Ignoring virus protection** — Printers and MFPs usually get the least attention when it comes to viruses, but there’s still malware out there than can take control of a printer or steal the documents being sent to the device. One way to reduce risk: Get a model with a proprietary operating system.

**Failing to train users** — Like any security issues, the risks associated with MFPs contain a significant human element. It’s important for employees who regularly print sensitive docs to be aware of the risks and know what they can do to minimize problems.

# Printing Security, Really?!?

## [4 steps for secure printing](#)

April 15, 2009 by Sam Narisi

Posted in: [In this week's e-newsletter](#), [Latest News & Views](#), [Solutions](#)

Printing poses a variety of security risks, whether it's the theft of digital data on the printer's hard drive or paper printouts falling into the wrong hands. Here are some ways to keep both digital and physical documents secure during the printing process, from a story in [eWeek](#):

**Require authentication:** In departments that regularly print confidential documents, consider getting a printer that requires a user to enter a password into the machine before it prints. Other models use swipe cards, or even biometric fingerprint readers.

**Overwrite data:** If your device prints off its own disk, you can probably set it to erase the disk after every job.

**Check the OS:** Some printers use a proprietary operating system, making them relatively safe from virus attacks. But others use a common OS and are therefore vulnerable. Find out what's on your devices and plan accordingly.

**Print from memory:** It takes a little longer, but some printers let you bypass the hard disk and print straight from RAM. Or, buy a model without a hard disk — that's an option you may not even need.

# Printing Security, Really?!?

- Overwrite the Hard Disk at the End of Life
- Overwrite Data Immediately
- Encrypt the Drive
- Encrypt it – Really
- Print from Memory
- Secure Print, with Passwords
- Secure Print, with Cards
- Secure Print, with Biometrics
- Securest Print
- Secure Everything Else
- Timeout the User
- Turnoff the Reprint Command
- Timeout on Secure Print Jobs
- Scan Encryption
- Unauthorized Copy Control
- Secure Mailbox Print
- E-mail and Fax Destinations
- Who Sent the E-mail
- Tracking and Activity Logs
- Virus Protection

# Copier Security, Really?!?

- As of 2010, how long has the copier been around? 40, 50, 60 or 70 years?
- Since 2002, what do all digital copiers have in common?
- What is the number one thing that identity thieves look for in a used copier?
- What Data is at risk from today's multi-function and/or networked copier?
- What role, if any, does data encryption play regarding today's copiers?
- What makes up "due diligence" at a copier's "End of Life"?
- What are some Physical Security measures regarding copiers?

# Copier Security, Really?!?

## Copier Hard Drive Security

### Your Copier's Hard Drive Can Open the Door to Identity Theft

By [William Deutsch](#), About.com Guide

- Be careful what you copy. Avoid copying personal information on work or public machines. Especially if you have no control over how those machines are administered.
- If you're leasing a machine, discuss end of life security with your service provider to ensure that copy machine hard drives will be completely erased when the machine is removed.
- The other alternative is to destroy or erase the disk yourself before selling the machine or allowing it to be removed from your business.

# USB Devices

## IT Security

### U.S. military compromised by removable media malware: Five ways to avoid the same fate

By Chad Perrin

August 27, 2010, 11:08 AM PDT

Takeaway: Defense Secretary Lynn has been discussing a 2008 compromise of U.S. military network security by a foreign intelligence agency. The DOD is taking measures to protect itself. You should do the same. *Defense Secretary Lynn has been discussing a 2008 compromise of U.S. military network security by a foreign intelligence agency. The DOD is taking measures to protect itself. You should do the same.* The Washington Post reports in [Defense official discloses cyberattack](#): The most significant breach of US military computers was caused by a flash drive inserted into a US military laptop on a post in the Middle East in 2008. A foreign intelligence agency managed to place malware on a USB flash drive that was later plugged into the US military laptop, infecting it. From there, the infection made its way onto a U.S. military Central Command network. According to Defense Secretary William J. Lynn III: “That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control.” “It was a network administrator’s worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.”

With the growth of widespread network-delivered malware infections in today’s almost universally connected world, it can be easy to forget that sometimes the old methods are still effective. In the 1990s, people who used computers on a regular basis were much more cognizant of the potential danger of viruses that could move from computer to computer via removable media like floppy disks. The threat has not gone away just because it is often easier to infect many computers over the network instead. In fact, if your organization is very well-protected from network threats, a determined attacker may well take advantage of the relatively low level of protection used for other means of infection like removable media. Even for those of us who may not be likely targets of such attacks, the development of malware that uses removable media as an infection vector can also catch many of the rest of us in the crossfire, if we are not careful. There are a number of measures that can be employed to reduce your vulnerability to malware that infects MS Windows computers via USB flash media and other removable media.

## How to avoid removable media malware

- . **Disable AutoRun**
- . **Implement restrictive removable media policy**
- . **Check all removable media on a secure system before use**
- . **Choose to ban all removable media**
- . **Implement the basics**

# USB Devices

- Do you allow USB or “Thumb” Drives to be used in your Organization? Do you have Policies, Standards, Guidelines and/or Procedures in place governing their use?
- Are these devices required to be password, encrypted, biometric etc... protected? Are they required to be checked periodically for “malware”?
- Are these devices issued by the organization or provided by individuals? If by individuals is who owns the Data?

# External Media Security

- Is your media encrypted?
- Do you use “Off-The Shelf” (OTS) backup software and media?
- Are your backup routines audited on a regular basis to ensure that all mission critical Data is being backed up to media?
- Is your media Write-Protected immediately or A.S.A.P after the backup procedure is complete?
- Is your media rotated off site? Do you have at least a 5 Day, 1 Month, 1 Quarter and 1 Year End rotation schedule?
- Is your media transported in an industry approved transport container?
- Is your media assigned a unique tracking number? Is there a media log or inventory?
- Is your media transported and stored in an industry standard environment i.e temperature, humidity, media case, magnet free, impact resistant?
- Is your media tested periodically to ensure Data Integrity?

# External Media Management

- What if your backup media was lost or stolen?
- Is your media encrypted? If so, how do you manage your encryption keys? What encryption method and level of encryption are you using?
- Do you know where your media is and who has it at any given time or day?
- How often do you clean or maintain your media drives?
- How many uses re-writes or uses before media is retired?
- In business or disaster recovery situation, does your recovery site have the ability to read and restore your data?

# Work PC

- What about your work PC? Why is it important to keep its access to a minimum?
- Do you “lock” your work PC each time you leave your desk? Does your PC automatically “lock” your PC after a no activity for a period of time?
- Does your PC automatically check for operating system software updates or patches?
- Do you have Anti-Virus; Anti-Malware; Anti-Spyware; Anti-Spam etc... software? Is it updated daily? Is the license current?
- Do you keep your password in written form on or near your PC i.e. On the Keyboard, On the Monitor, Under the Mouse Pad? Does anyone besides you know or use your User ID and Password? Do you change your password periodically?
- Is your PC and/or Data backed up or imaged on a regular basis?
- Do you have sensitive or mission critical data stored on your PC?
- What are arm’s length transactions and why are they important in your day to day business?

# Home Desktops

- Who has access to your home PC? How do you know that only “those” people have access? Does it matter if someone gains access?
- Do you give your credit card information out to strangers? If the answer is no. What makes you think you can buy something online securely? What do you look for in order to verify that your transaction is secure?
- Who actually has a right to your social security number?
- Does your PC automatically check for operating system software updates or patches?
- Do you have Anti-Virus; Anti-Malware; Anti-Spyware; Anti-Spam etc... software? Is it updated daily? Is the license current?
- Do you use your Home PC to work from home? If so, how do you connect? What are your organization’s Policies and Rules regarding your PC?
- True or False, if you connect from your Home PC using VPN you are protected against Viruses, Malware, Spyware etc...?

# Mobile Device Security

## Cell Phones, Smart Phones

How many people have information on their phone that they wouldn't want just anyone to have access to?

How many people have their phone password protected?

By Georgina Prodhan of Reuters 02/08/2011

<http://www.msnbc.msn.com/id/41471308?gt1=43001>

- Reuters reports, Cell phone security threats rose sharply last year as a proliferation of Internet-enabled mobile devices like smart phones and tablets provided new opportunities for cybercriminals, security software maker McAfee said.
- In its fourth-quarter threat report, released on Tuesday, McAfee said **the number of pieces of new cell phone malware it found in 2010 rose 46 percent over 2009's level.**
- "As more users [access the Internet](#) from an ever-expanding pool of devices — computer, tablet, smart phone or Internet TV — Web-based threats will continue to grow in size and sophistication," it said.
- McAfee, which is being bought by Intel for \$7.68 billion, said it expected PDF and Flash maker Adobe to remain a favorite of cybercriminals this year, after it overtook Microsoft in popularity as a target in 2010.
- It attributed the trend to Adobe's greater popularity in [mobile devices](#) and non-Microsoft environments, coupled with the ongoing widespread use of PDF document files to convey malware.
- McAfee said Google's Android, which last quarter overtook Nokia as the maker of the world's most popular smart phone software, had been targeted by a Trojan horse that buried itself in Android applications and games.
- And politically motivated hacking was on the rise, it said, with the highest-profile protagonist being the ["Anonymous" activist group](#) that targeted the websites of organizations it perceived to be hostile to controversial site WikiLeaks.

# Mobile Device Security

## Microsoft Laptops, Tablets, Smart Phones

- Do you keep sensitive Data on your Laptop?
- Do you encrypt your Data? Use biometric access?  
Have you considered “Lo-Jack” for your Laptop?
- Do use a physical locking device or carrying case?  
Is your carrying case shock resistant?
- How often and where do you backup your Laptop?
- Do you have games or use your work Laptop for personal use? If so, what rules apply?

# Mobile Device Security

## iPods, iPads and iPhones

### **Vatican: Catholics cannot confess via iPhone**

'Confession: A Roman Catholic app' walks Catholics through the sacrament

iTunes Confession: A Roman Catholic app, thought to be the first to be approved by a church authority

is not designed to replace going to confession.

By Catherine Hornby

VATICAN CITY — Catholics cannot confess via iPhone and technology is not a substitute for being present when admitting sins to a priest, the Vatican spokesman said on Wednesday. The statement by Father Federico Lombardi follows the launch of an iPhone application aimed at helping Catholics through confession sanctioned by the Catholic Church in the United States. "One cannot speak in any way of confessing via iPhone," Lombardi said on Wednesday, adding that confession required the presence of the penitent and the priest. "This cannot be substituted by any IT application," Lombardi added.

Confession: A Roman Catholic app, thought to be the first to be approved by a church authority, walks Catholics through the sacrament and contains what the company behind the program describes as a "personalized examination of conscience for each user. "The application is not designed to replace going to confession but to help Catholics through the act, which generally involves admitting sins to a priest in a confessional booth. Some reports on its approval by the Catholic Church in the U.S. suggested confession would now be possible via iPhone.

*Copyright 2011 Thomson Reuters*

# Mobile Device Security

## iPods, iPads and iPhones

### Hackers only need six minutes to reveal your iPhone passwords

By Rosa Golijan Posted on TECHNOLOG on MSNBC.com

Thursday, February 10, 2011

Discovering that your iPhone has been lost or stolen can be a terrible experience. Not only do you have to deal with replacing the device, but you also have to worry about someone accessing all the personal information you've got on the gadget. That's why you always remember to password-protect your iPhone — to keep all your data safe if something goes wrong. Too bad that only slows hackers down for about six minutes. [PC World reports](#) that researchers at the Fraunhofer Institute Secure Information Technology in Germany [published a paper](#) which describes how someone with malicious intent can easily reveal most of the passwords stored on an iPhone — whether the device itself is password-protected or not — using a process that takes barely more than six minutes to complete.

The first step in the method is to jailbreak the device — which basically means circumventing some iPhone security measures and installing software not authorized by Apple. This can be accomplished using one of many freely available software tools and allows for the installation of an SSH server — which in turn allows for access to the device's password management system, better known as the keychain. At this point there's a tricky step in which hackers face a keychain database which is encrypted with a key that can't be extracted from the iPhone.

The solution? Use the key from software within the device. Ta da! A few clicks later the iPhone will happily share its stored secrets. MS Exchange accounts, LDAP accounts (Lightweight Directory Access Protocol that allows for access to all sorts of directories, generally for corporate use), voicemail, VPN passwords, WiFi passwords and some app passwords are all easily viewed. The only things safe for the time being are passwords for web sites, and that's only because they are stored in a different protection class.

Scary, no? The good news is that the researchers who discovered this particular password revealing method will not be revealing the exact scripts they used to accomplish the task. The bad news? It shouldn't take long for someone else to figure the method out. So what can you do? Not very much. There doesn't appear to be any preventative measures you can take to keep your data safe. All you can do is rush to change your passwords the instant you notice your iPhone is missing:

Owner's [sic] of a lost or stolen iOS device should therefore instantly initiate a change of all stored passwords. Additionally, this should be also done for accounts not stored on the device but which might have equal or similar passwords, as an attacker might try out revealed passwords against the full list of known accounts.

## Social Media Security: Facebook, Twitter, YouTube, Google

- In whom do you put your Trust?
- What happens when you post a picture of your child on Facebook? Can you simply delete it and it go away? What if that wasn't the case? Would that matter to you?
- When is a "Friend" NOT a "Friend?"
- TMI?
- Can you assume any privacy?

# Social Media Security:

## Facebook, Twitter, YouTube, Google

### What 13 Things Should You Not Post On Facebook:

1. Your Birth Date And Place
2. Your Mother's Maiden Name
3. Your Home Address
4. Your Long Trips Away From Home
5. Your Short Trips Away From Home
6. Your Inappropriate Photos
7. Confessionals
8. Your Phone Number
9. Your Vacation Countdown
10. Your Child's Name
11. Your 'Risky' Behavior
12. The Layout Of Your Home
13. Your Profile On Public Search

# Social Media Security:

## Facebook, Twitter, YouTube, Google

### Twitter security loophole can expose users' direct messages

By Suzanne Choney Posted on TECHNOLOG on MSNBS.com

October 5, 2010

A security loophole in Twitter can give website developers easy access to users' private direct messages, messages that are exchanged between two people and not meant to be shared on Twitter or with anyone else, according to a report.

Search engine and security specialist Gary-Adam Shannon writes on [SearchEngineWatch.com](http://SearchEngineWatch.com) that "worries" about such access "have been floating in the Twitter streams of late. Many have voiced concerns about privacy breaches by applications that log users in to Twitter or access their account. Turns out, those fears are well founded. The Twitter API can be exploited quite easily and let anyone [with access to website code] gain access to your direct messages."

The access can be granted when a user logs into Twitter or a site (such as a blog) that uses Twitter and requires your Twitter user name and password.

Twitter's API (that is, application programming interface) "allows developers access to lots of neat information," Shannon wrote. "You can send messages, update statuses and do whatever you so please. Sure, there are some permission settings available for developers (read vs. read/write), but few users read this stuff anyway."

Twitter has not yet responded to questions about the loophole from msnbc.com.

"Personally, I don't care to read direct messages. However, I can see it being useful for list harvesting," Shannon wrote. His recommendation on how to deal with the loophole? "Don't let applications log you in. Average users really don't know what they're doing and it's really easy to automatically hit the big 'accept' buttons online or during a software installation. But in this case it could be the equivalent of hitting 'Install' on a spyware application. "To be fair, even the geeks do it. How many of you actually read the terms and conditions to the last application you installed, or website you signed up to?"

"Bottom line: Be aware of what you're granting access to, whether it's on Twitter, Facebook, or any other site. Be smart about what you give access to, or else your private data will no longer be private."

# Email Retention Issues

- Confirming a trend that other software security companies have reported, McAfee said spam levels had decreased sharply, especially in the second half of the fourth quarter, with **62 percent less** by the end of the year than at the beginning.
- The company said, however, that spam's hitting its lowest level for years simply represented a transition period with several botnets — collections of computers harnessed to act in concert — going dormant at an usually busy time of year.
- Do you use your email for personal contacts and accounts? Do you use your personal email account for business purposes?
- What are your company's privacy and harassment policies?

# Policies, Guidelines, Standards, Procedures

- What is a Policy?
- What is a Standard?
- What is a Guideline?
- What is a Procedure?

## Consulting, Auditing, Architecture

- What do you should look for in a Information Security Consultant, Auditor and/or Architect?
- Does “one size fit all”?
- What are HIPAA, SOX, GLBA, FDIC, SEC, FISMA, PCI-DSS, CoBIT, Best Practices etc..? How do they affect my approach to Information Security?
- What is ISC(2)? What is ISACA? What is a CISSP? A CISA? A CISM? How do they fit into the mix?

# Consulting, Auditing, Architecture

## Understaffed IT departments threaten data security

January 19, 2010 by Sam Narisi

Posted in: [In this week's e-newsletter](#), [Latest News & Views](#), [Security](#)

A recent poll warns businesses about the security dangers of working with a too-small IT staff.

According to a year-end survey by security software developer [Symantec](#), half of corporate IT managers state that their data center operations are understaffed, 18% said that their data centers were extremely short of staffing — and upper management is crying for even bigger cutbacks.

The annual survey was conducted with IT and network managers at over 1,7000 companies worldwide. More than 30% of the companies reported cutbacks in IT over the last year, even as the mission for the department has gotten bigger, with such issues as mobile computing and cloud computing.

The big problem here is that routine data security policies will be neglected as IT and network staffers get more and more loaded on their plates. In part, the war with would-be data thieves and hackers keeps escalating even as the resources for the defense are decreasing. The irony is that the Symantec story comes just as another survey by accounting firm [Ernst & Young](#) declares that most firms have increasing concerns about data security.

# **(ISC)<sup>2</sup> CISSP Information Security Domains**

- **Access Control Systems & Methodology**
- **Applications & Systems Development**
- **Business Continuity & Disaster Recovery Planning**
- **Cryptography**
- **Law, Investigation & Ethics**
- **Operations Security**
- **Physical Security**
- **Security Architecture & Models**
- **Security Management Practices**
- **Telecommunications & Network Security**

# (ISC)<sup>2</sup> Code Of Ethics

Compliance with the preamble and canons is mandatory. Conflicts between the canons should be resolved in the order of the canons. The canons are not equal and conflicts between them are not intended to create ethical binds.

## **Protect society, the commonwealth, and the infrastructure**

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

## **Act honorably, honestly, justly, responsibly, and legally**

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

## **Provide diligent and competent service to principals**

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

## **Advance and protect the profession**

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

# Where do we go from here?

- Do nothing and hope for the best.
- Depend on existing internal IT resources to develop an Information Security structure on their own.
- Hire additional IT Security Resources to develop, implement, monitor and maintain an Information Technology structure and keep you current in an ever changing IT World.
- Partner with Certified Security Professionals and Information Technology Solutions Provider to develop, implement, monitor and maintain an Information Technology structure and keep you current in an ever changing IT World.