

12 STEP SECURITY PROGRAM

BRENTWOOD COOL SPRINGS CHAMBER

MAY 8, 2012

DR. FREDERICK SCHOLL,
PHD, CISSP, CISM, CHP, ITIL

2011: THE YEAR OF THE DATA BREACH

- ▶ 368 Million records breached
- ▶ Intellectual property theft = ?
- ▶ Company reputation



RISKS TO SMALL/MEDIUM BUSINESS

- ▶ “Smaller businesses are the ideal target for such raids, and money-driven, risk-averse cybercriminals understand this very well” (Verizon 2011 Breach Report)

and other
deal, but
're using
vn.” (See

findings
erring to
at as you
) of this
meeting

Table 2. Organizational size by number of breaches (number of employees)

1 to 10	42
11 to 100	570
101 to 1,000	48
1,001 to 10,000	27
10,001 to 100,000	23
Over 100,000	10
Unknown	135

CFO.COM

CFO Magazine

You are here: [Home](#) : [CFO Magazine](#) : [January/February 2012 Issue](#) : Article

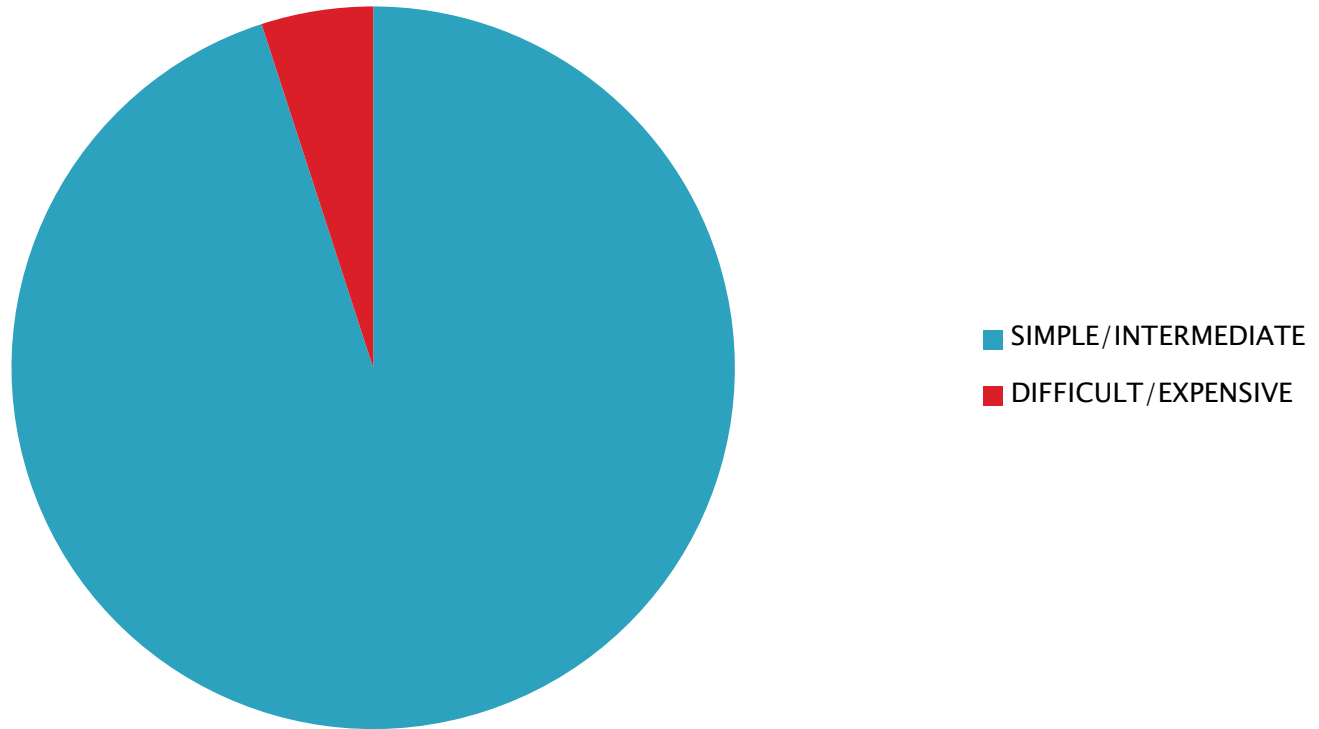
Where the Money Is, and the Security Isn't

Cyber thieves are increasingly targeting small and midsize businesses, and why not? Most SMBs do little to protect themselves.

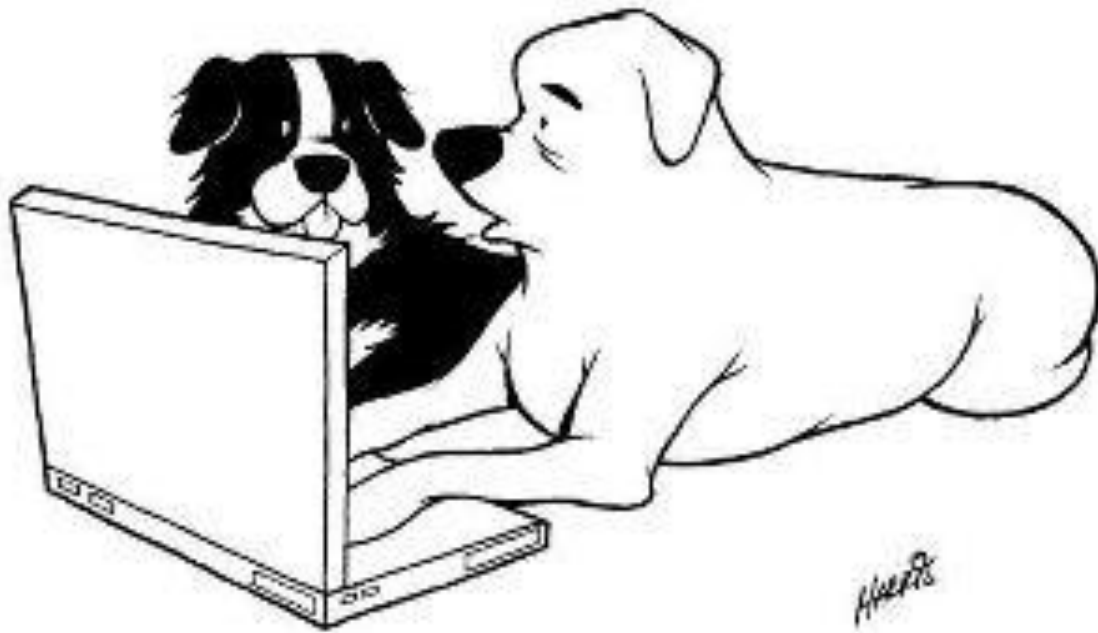
Russ Banham - CFO Magazine

February 1, 2012

CAUSES OF BREACHES (VERIZON)



MORE DATA BREACH CAUSES



"And then I just hit delete. I haven't actually eaten any homework for years."

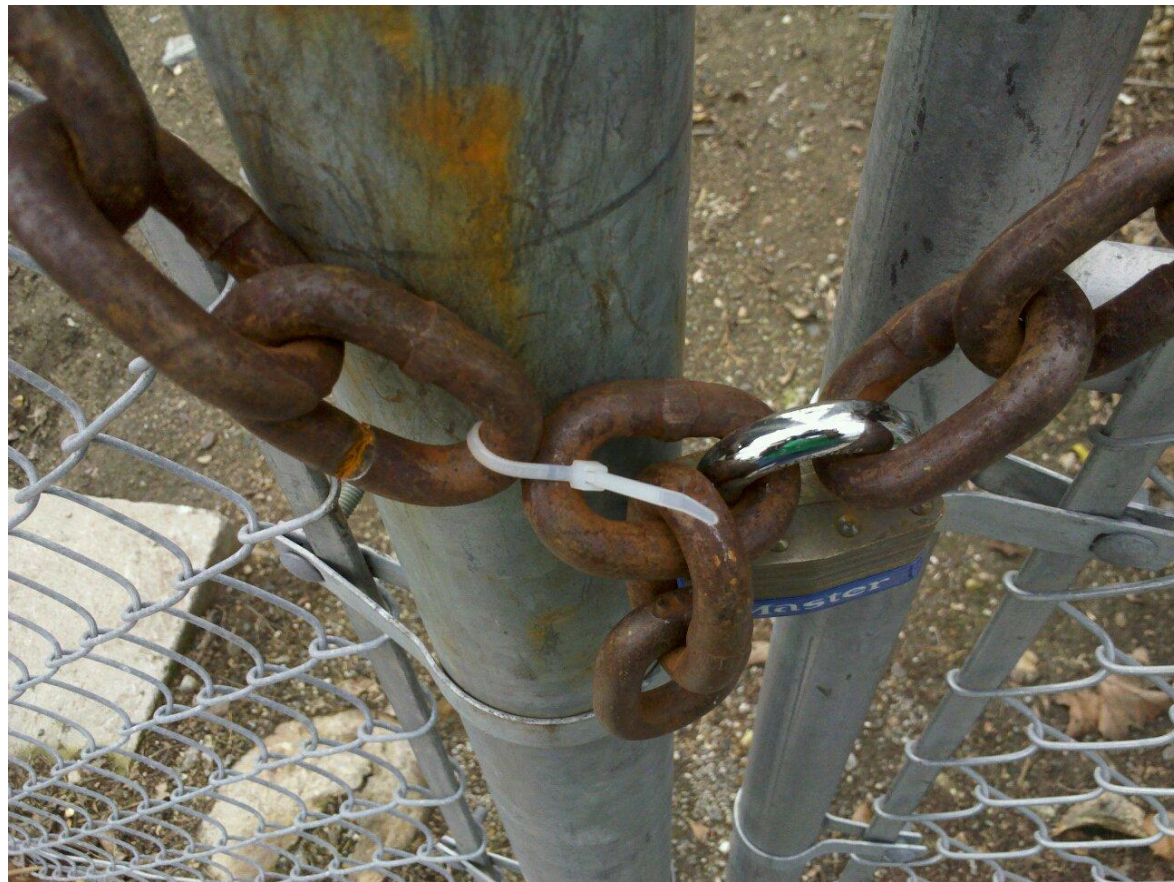
WRONG SECURITY FOCUS LEADS TO...



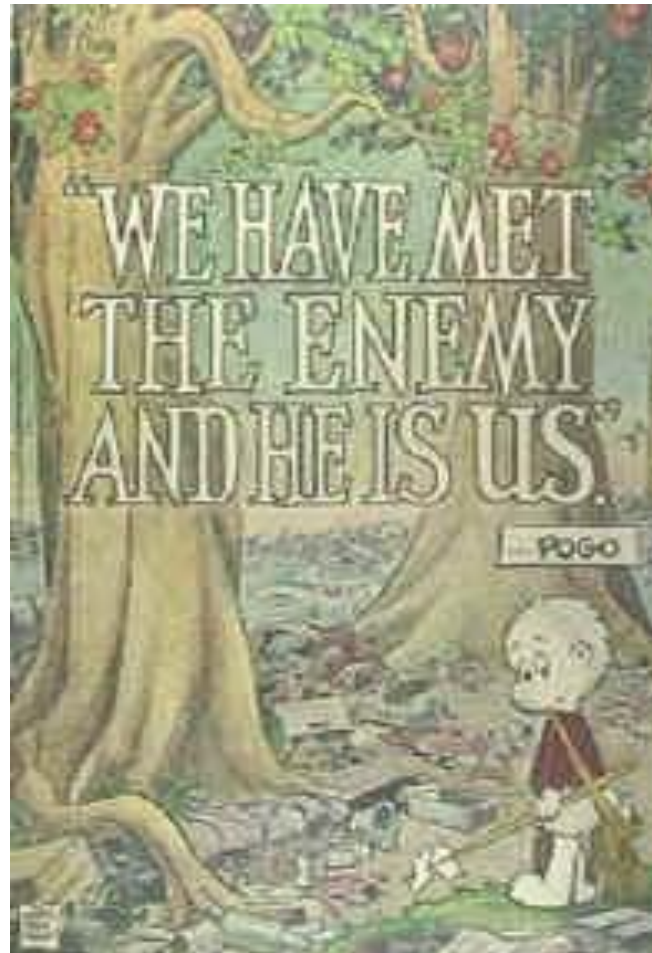
THE WRONG CONTROLS



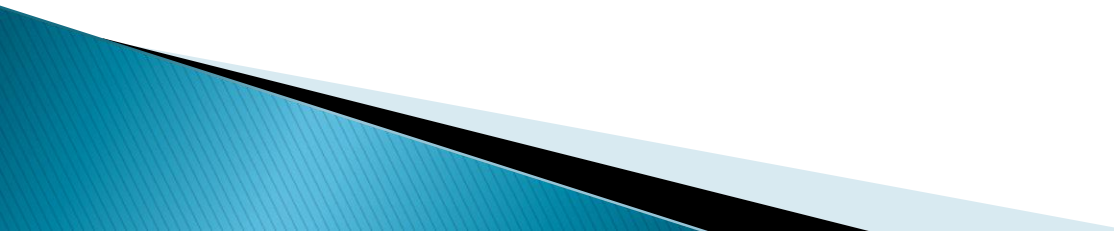
SECURITY IS BROKEN



WE ARE THE PROBLEM



SECURITY FAILURES 101: HB GARY

- ▶ Breach at company's custom website (**not tested for security**)
 - ▶ Hackers cracked **easy to guess passwords**
 - ▶ Used **same password** to break in to second machine
 - ▶ Privilege escalation on **unpatched** system
 - ▶ Gained access to company email system
 - ▶ Used **social engineering** to gain further access
 - ▶ Post mortem: HB Gary acquired 4/2012
- 

BAKER'S DOZEN OF SECURITY TIPS



RISK MANAGEMENT

WHAT CAN GO WRONG?	WHAT IS LIKELIHOOD?	RECOMMENDED FIX
Loss of laptops	High	Encrypt data
Rogue contractor	Medium	Mandate background checks at contractors

HARD PART: TRACKING AND EXECUTING

LEANKIT: SOFTWARE FOR IMPROVING PRODUCTIVITY
BOOK: "PERSONAL KANBAN"

PEOPLE ARE SECURITY

- ▶ Engage workforce: regular quarterly *security awareness training* sessions
- ▶ Social engineering in the Facebook era
- ▶ Background checking (Kroll and others)
- ▶ Needed: good awareness wiki covering current security events and practices of interest to chamber companies
- ▶ Best for now:
 - HIPAA: (“*new* HHS breach notification site”)
 - www.datalossdb.org

EMAIL BEST PRACTICES

- ▶ DON'T CLICK ON ATTACHMENTS
- ▶ DON'T CLICK ON LINKS
- ▶ BEWARE OF PHISHING ATTACKS

CRITICAL: There has been a change to your TRANSUNION score

Fraud Monitoring [creditreportoptions@clatwhata.com]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Sent: Mon 5/7/2012 11:34 AM

To: Fred Scholl

ALERT: THERE MAY HAVE BEEN CHANGES TO YOUR CREDIT SCORE

freds@monarch-info.com

View all 3 reports instantly at NO COST. Receive score monitoring at all three major bureaus and avoid credit fraud. To retrieve your score [Click Here](#)

To unsubscribe please [Click Here](#)



EMAIL SECURITY: TLS



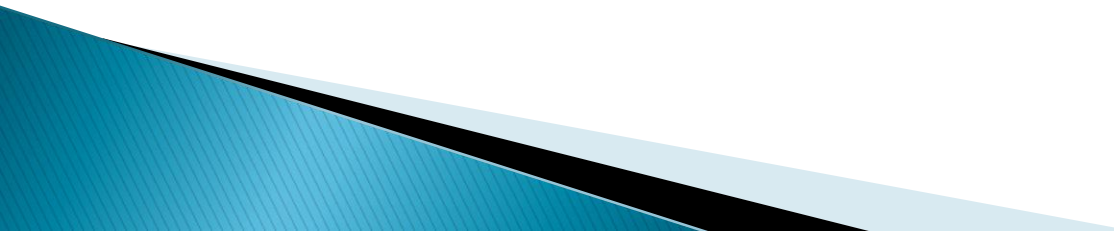
ENCRYPTED
AES 256



[CHECKTLS.COM](https://checktls.com)

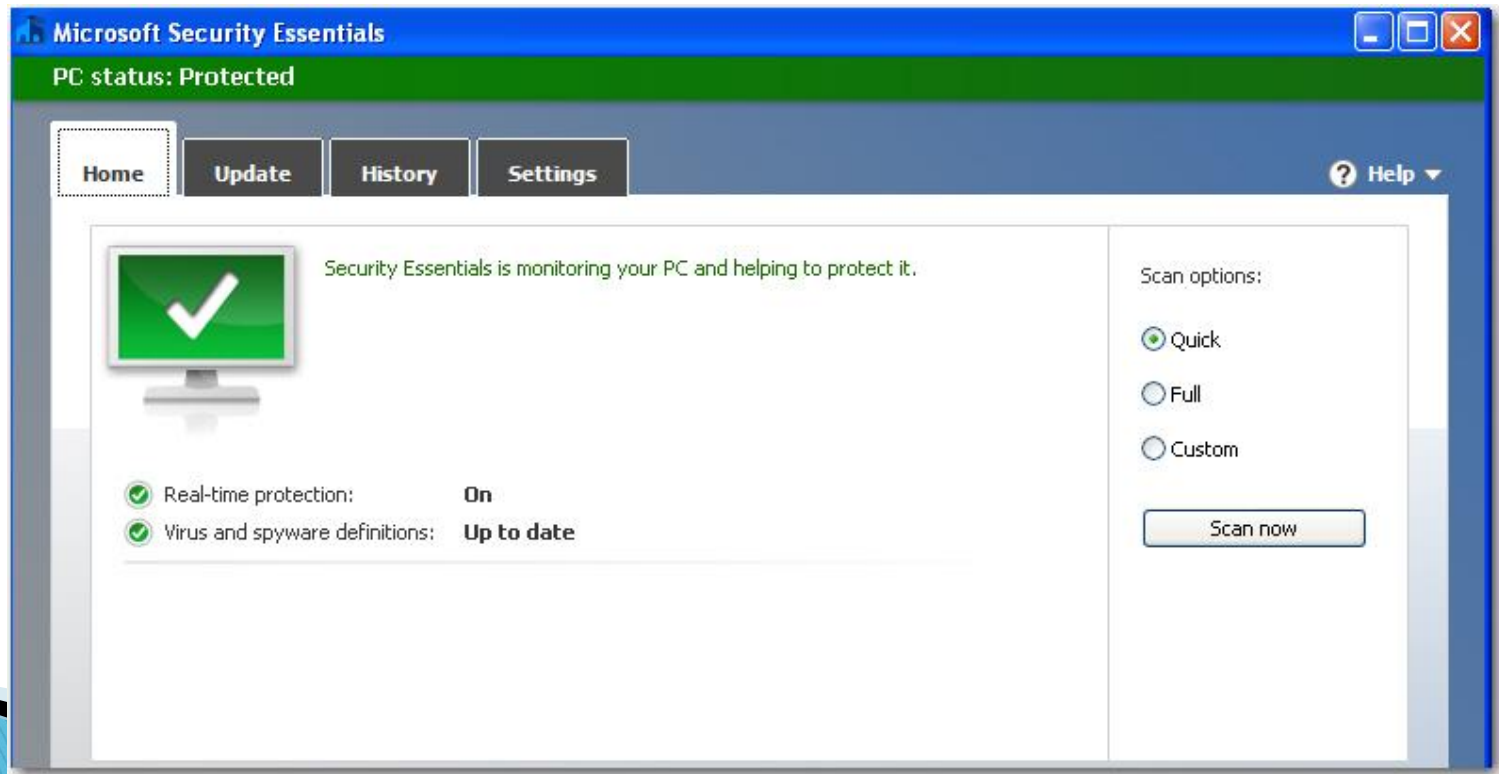


END TO END ENCRYPTION OPTIONS

- ▶ Use Word or PDF to encrypt the attachment; send secret key by separate email
 - ▶ Implement TLS as described
 - ▶ Use public key method for repeated emails to same person
 - Deadbolt (\$9.95)
 - ▶ Join security email group such as offered by Zixmail, LuxSci and others
- 

KEEP ANTI-VIRUS UP TO DATE

- ▶ MICROSOFT SECURITY ESSENTIALS (FREE)
- ▶ NONE OF THE AV PROGRAMS CATCH EVERYTHING
- ▶ REMOVING MALWARE: CHECK [HERE](#) OR [HERE](#)



BANKING SECURITY



USE SEPARATE COMPUTER
FOR ONLINE BANKING, OR
USE BOOTABLE DISK

CHOOSE COMPLEX PASSWORDS

- ▶ Avoid words in any dictionary!
- ▶ Don't reuse passwords
- ▶ Do use complex passwords (8 OR MORE A,3 #)
- ▶ Use password managers: LastPass (\$1 /month), Key



DATA DISPOSAL



ASSET CLASSIFICATION AND
MANAGEMENT



PHYSICAL SECURITY

- ▶ LAPTOPS: will be lost
- ▶ USB memory: will be lost
- ▶ Windows 7 upgrade: implement Bit locker encryption



MANAGE CLOUD SERVICES CAUTIOUSLY

- ▶ Data backup
 - What level of restore do you need?
 - *Can you restore the data? Have you tested it?*
 - LAPTOP + DROPBOX + LOCAL FILE BACKUP (CRITICAL WORK)
- ▶ Look for certifications
 - ISO 27001
 - SSAE 16

ARE YOU SECURE?



FREEDOM FROM WORRY



VIGILENT & PREPARED

REAL SECURITY



CONTACT:
FRED SCHOLL
615-739-1039
FREDS@MONARCH-INFO.COM

MONARCH INFORMATION NETWORKS
104 EAST PARK DRIVE
BRENTWOOD