



What Your IT Guys Aren't Telling You About IT Controls, Storage and Access

George Fallon, CDP, CISA, CPA, CGFM

Clifton Gunderson LLP

Virginia GFOA Annual Spring Conference, 2010





What We Will Cover

- Short history of hacking
- Identity theft
- Vulnerabilities
 - Windows
 - Applications
 - Networks
- Cloud computing





Short History of Hacking

- **1960s:** The Dawn of Hacking
- **1970s:** Phone Phreaks and Cap'n Crunch
- **1980:** Hacker Message Boards and Groups
- **1983:** Kids' Games
- **1984:** Hacker 'Zines
- **1986:** Use a Computer, Go to Jail
- **1988:** The Morris Worm
- **1989:** The Germans and the KGB
- **1990:** Operation Sundevil
- **1993:** Why Buy a Car When You Can Hack One?





Short History of Hacking

- **1994:** Hacking Tools-R-Us
- **1995:** The Mitnick Takedown
- **1997:** Hacking AOL
- **1998:** The Cult of Hacking and the Israeli Connection
- **1999:** Software Security Goes Mainstream
- **2000:** Service Denied
- **2001:** DNS Attack
- **2007:** FBI Operation Bot Roast finds over 1 million botnet victims
- **2007:** TJ Maxx
- **2008:** Around 20 Chinese hackers claim to have gained access to the world's most sensitive sites, including The Pentagon. They operate from a bare apartment on a Chinese island





Hacking For Fun And Adventure/ Not-for-Profit

- Defacing websites for bragging rights; show the world their skill
- Hacker magazines sold in stores with articles about breaking into police computers, libraries and phone systems
- Script Kiddie-built tools and exposes weakness, but not real harm





Hacking For Fun And Adventure/ Not-for-Profit

- Caused company's internal IT administrative time to correct the problem that was exposed
- Embarrassment
- No direct financial loss





Cybercrime / For-Profit Identity Theft

- 90% percent of our *Identity theft* cases deal with *drugs*
- “**phishing**” is a process of attempting to acquire sensitive information such as user names, passwords and credit card details by masquerading as a trustworthy entity





Hackers Are Organized

- Intrusions Conducted by Attackers:
 - Well funded and Organized Groups
- They are not “Hackers” → Professionals
 - Systematically Compromising U.S. Government and Commercial Entities
- Motivation Behind These Attacks
 - Economic, Financial and Political Advantages
 - Research and Development
 - Internal and External State Security
 - External Image





Types of Identify Theft

- Medical Identity Theft
- Criminal Identity Theft
- Children & Identity Theft
- Financial Identity Theft
- Seniors and Identity Theft
- SSN Identity Theft





Medical Identity Theft

- Medical Identity Theft is one of the fastest growing forms of identity theft in the United States today
- Effects of Medical Identity Theft include the following, and in addition to the possibility of receiving incorrect treatment due to medical identity theft:
 - False medical and pharmaceutical bills
 - False health insurance claims
 - Denial of health insurance claims
 - Denial of health insurance coverage
 - Denial of life insurance claims
 - Denial of life insurance coverage
 - Denial of employment based on false medical history
 - Time and expense correcting false patient records
 - Time and expense correcting false insurance records





Criminal Identity Theft

- Criminal Identity Theft is everyone's worst nightmare
- Criminal identity thieves commit crimes while using your identity
- Because law enforcement officials believe you are the actual criminal, you could be arrested and jailed for a crime you know nothing about





Children & Identity Theft

- There is a growing trend of identity thieves stealing the identities of children – even infants.
- In particular, the Social Security numbers of children are considered very valuable by identity thieves as parents are unlikely to check the credit reports of their children.
- After all, very few children are going to be involved in any type of credit transaction until sometime between the age of fourteen and eighteen at the earliest.





Financial Identity Theft

- Four significant numbers contribute to the understanding of how large a problem we face when we examine financial identity theft. The numbers are 50 billion; 15 million; 3.5 thousand; and, 25.
- Each year, approximately:
 - 15 million Americans are identity theft victims
 - \$50 billion in financial losses to the country
 - \$3,500 is the average amount lost
 - 25 hours is the time each victim expends recovering from the consequences of identity theft





Senior Citizen Identity Theft

- Unfortunately, as long as there have been identity thieves, they have always targeted senior citizens.
- Many identity crimes, crimes of deception and financial crimes are traditionally aimed at our senior population.
- Criminals believe seniors may be:
 - more susceptible to crimes of deception, and
 - the amount of money that can be stolen from a senior may exceed that of other segments of the population.





Social Security Number Identity Theft





Social Security Number Identity Theft

- Statistically, every American's Social Security number has been lost or stolen in just the last few years.
- The majority of these lost or stolen Social Security numbers are a result of corporate and government database security breaches.
- The most frequent forms of database security breaches are lost and stolen laptops and the successful hacking of computer databases.
 - Often these databases contain sensitive personal information – including Social Security numbers.
 - Unfortunately, breaches involving millions of Social Security numbers have also occurred on a relatively frequent basis.





Vulnerabilities

- **“Vulnerability”** is a weakness or flaw which allows an attacker to reduce a system integrity, availability or confidentiality.





Are Passwords Working?

- 20 character passwords?
- Complex passwords – (upper case, numeric and special characters)
- As password lengths gets longer and more complex, the more the tendency to write it down
- Computers are getting faster, so the time to crack a password is decreasing





Are Passwords Working?

- Common password weaknesses
 - No password
 - Username is the same as the password
 - The username or the username concatenated with itself
 - Passwords such as “password,” “passcode,” “admin,” and their derivatives
 - Service accounts





Are Access Controls Working

- Most widely reported problem areas
 - Overly broad access, not periodically reviewed
 - Undocumented access granted
 - Poor ID and password management
 - Improper implementation of software controls
 - Inadequate monitoring of user activity





Is Windows Safe?

- When windows was first designed in 19xx, security was not an issue. The culture of the industry was trusting and have all open code.
- New windows products must be compatible to older versions, so security flaws are brought forward to newer versions.
- Since Windows is the largest install base in the world, it is a target for hackers.





Are Your Web Applications Safe?

- Undisciplined testing procedures
- Unauthorized software and software changes
- Inappropriate access to software
- Security not considered





Are Your Web Applications Safe?

- HTTP requests from browsers to web apps
 - URL, Query string, Form Fields, Hidden Fields, Cookies, Headers
 - Web apps use this information to generate web pages





Are Your Web Applications Safe?

- Hacking Applications is stunningly prevalent
- Easy to exploit without special tools or knowledge
- Little chance of being detected
- Hundreds of thousands of developers, tiny fraction with security





Are Your Web Applications Safe?

- Corruption or disclosure of database contents
- Root access to web and application servers
- Loss of authentication and access control for users
- Defacement
- Secondary attacks from your site





Are Your Web Applications Safe?

- Remote code execution
- SQL injection
- Cross Site Scripting (XSS) Username enumeration





Are Your Web Applications Safe?

- Web and Application Server Misconfiguration
 - All web and application servers have many security-relevant configuration options
 - Default accounts and passwords
- Unnecessary default, backup, sample apps, libraries
- Overly informative error messages
- Misconfigured SSL, default certificates, self-signed certs
- Unused administrative services





Are Your Networks Safe?

- Poor Server Configurations
- Patches not Applied
 - Microsoft and non-Microsoft
- Open ports





Are Your Networks Safe?

- All web and application servers have many security-relevant configuration options
 - Default accounts and passwords
 - Unnecessary default, backup, sample apps, libraries
 - Overly informative error messages
 - Misconfigured SSL, default certificates, self-signed certs
 - Unused administrative services





Are The Devices You Use Everyday Safe?

- Memory Sticks
- Discarded or Lost Thumb Drives
- Discarded Computers
- Copiers and Printers
- Discarded Copiers and Printers





Cloud Computing

- Cloud computing is a general term for anything that involves delivering hosted services over the Internet.
- These services are broadly divided into three categories:
 - Infrastructure-as-a-Service (IaaS)
 - Platform-as-a-Service (PaaS)
 - Software-as-a-Service (SaaS)





Open Forum – Questions?





Thank You!

George Fallon
Partner, Information Technology
Clifton Gunderson LLP

888.778.6688

George.Fallon@cliftoncpa.com

