IT Audit Corner

Analysis of Strong vs. Weak Passwords


Data breaches are a dime a dozen these days. But when hackers steal databases full of customer info, login names and passwords, the passwords themselves aren’t usually sitting out in plain sight. Typically the passwords will be cryptographically hashed.

Hashing a password is the process of taking a string of any length (the password in this example) and producing a fixed length hash value. Password cracking tools can be used to try and guess that password that converts into these hashes. This leads to a need for strong passwords to make the guessing process time consuming and hopefully infeasible.

I asked a friend of mine, IT security expert Josh Kaldor, about what makes a good password and he had quite a lot to say on the subject. Josh did some research, creating hashes using various combinations of passwords with different attributes, then went to cracking them and comparing the results against a benchmark. Here are some of his conclusions:

![Hashing Example from Wikipedia](image)
**Phrase Methods**

Phrases are a great way to meet password requirement length and complexity requirements. A common problem here is that users will be apt to choose non-random (guessable / relatable) phrases or pop-culture references such as ‘TheHungerGames1’ which are subject to obvious dictionary attacks. The words have to be non-relational.

**Strong Example:** SpaceTrunk!=SeaElephant  
**Weak Example:** TheHungerGames1

**Acronym Methods**

Using acronyms to create a password is a handy way to hamper Dictionary Attacks on your password and creating a password hard to remember for the person who doesn’t know the acronym behind it. The issue here is that it’s hard to create a long string and if a user adds digits to the end, is incredibly weak (as crackers assume digits or modifiers at the start or end). Make these passwords stronger by combining with a phrase.

**Strong:** Iu2w4acw3e  *(I used to work 4 a company with 3 employees)*  
**Weak:** IgfHSi93  *(I graduated HS in 93)*

**Pattern Methods**

Like the acronym method, a pattern method is great for creating a seemingly illogical string that is hard to remember and will foil Dictionary Attacks. The issue in this case are people’s tendency to use similar patterns (like QWERTY), which in turn play right into the Dictionary Attack’s hands.

**Strong:** de3LO)Ptre  
**Weak:** qWERTY12345

**CONSIDERATIONS FOR THE AUDITOR**

PCI-DSS requirements for a strong password include the password being at least seven characters long and include uppercase, lowercase, numerical, special characters, and more. Other compliance standards require very similar sets of attributes.
Generic Active Directory Password Parameters.

As an auditor, you should look to go above and beyond by providing recommendations like educating end users on what makes a strong password, common characteristics of weak passwords and being sure other strong preventative controls are in place. Controls might include:

- Checking for the adoption of a Clean Desk Policy and adherence to it.
- Checking for passwords being passed in support tickets or emails.
- Verifying that new users are required to change passwords when they first login.
- Verifying that passwords are not stored unencrypted within databases.
- Verifying that even internal systems (such as ticketing and help desk systems) utilize encrypted communications since users on the network could be packet sniffing and capture passwords that might be passed in plain text.
Chapter Luncheons

JANUARY 2015

HOW TO AUDIT LOGICAL ACCESS CONTROLS

January 22, 2015
12:00 PM to 2:00 PM
AmericanWest Bank
110 S Ferrall St
Spokane, WA 99202

Stephen Hunt
Staff Auditor
AmericanWest Bank

Today’s information = POWER. And MONEY. What is the value of your institution’s information? What lengths would someone who has access to it go through to steal your information resources? Has your organization done enough to protect its information? Is anyone safe?

Recent cyber attacks, such as the attack on Sony Pictures, may have been prevented by adequate access controls. One team of computer security experts believes that Sony was attacked by its own people. Why did those employees have access to the information they did, and what could Sony have done to prevent the attack?

Join us to learn how to perform an Access Controls Audit as well as learn industry best practices and other standards. Bring your laptop, as this will be a “hands-on” training.

About the Speaker

Stephen Hunt is an Internal Auditor at AmericanWest Bank, where he is assigned information technology, operational, and financial audits. In addition to his audit duties, Stephen is also responsible for the administration of the Audit Department’s GRC system.

Mr. Hunt is a graduate of Eastern Washington University (EWU) with a Bachelor of Arts in Management Information Systems and Business Management. Stephen has a working knowledge of various computer programming languages such as VBA, SQL, HTML, PHP, JAVA, and others.

Stephen currently serves as the Newsletter Editor for the Spokane chapter of the Institute of Internal Auditors (IIA).

IIA Members-Only Webinars

Visit the IIA Members-Only Webinars web site for more information and to register for these FREE training events:

- COSO 2013 Update - Where Are You With Integration and Where Should You Be By Now? (01/08/2015)
- Building a Fraud-Resistant Organization (01/08/2015)
- An Outlook on the Internal Audit Landscape for the Year Ahead (01/20/2015)

1 Requires current IIA membership
<table>
<thead>
<tr>
<th>Month</th>
<th>Event</th>
<th>CPEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEPTEMBER</td>
<td>Excel: Intro to Macros</td>
<td>1 CPE</td>
</tr>
<tr>
<td>OCTOBER</td>
<td>IT Risk – Keeping Your Business Off the Front Page of the Newspaper</td>
<td>1 CPE</td>
</tr>
<tr>
<td>NOVEMBER</td>
<td>CANCELLED in lieu of the Annual ACFE Fraud Conference</td>
<td></td>
</tr>
<tr>
<td>DECEMBER</td>
<td>Joint Holiday Luncheon with the ACFE</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>JANUARY</td>
<td>How to Audit Access Controls</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>FEBRUARY</td>
<td>Date TBD</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>MARCH</td>
<td>Date TBD</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>APRIL</td>
<td>Date TBD</td>
<td>2 CPEs</td>
</tr>
<tr>
<td>MAY</td>
<td>Date TBD</td>
<td>8 CPEs</td>
</tr>
<tr>
<td>JUNE</td>
<td>No scheduled events</td>
<td></td>
</tr>
<tr>
<td>JULY</td>
<td>No scheduled events</td>
<td></td>
</tr>
<tr>
<td>AUGUST</td>
<td>No scheduled events</td>
<td></td>
</tr>
</tbody>
</table>
Certification Corner

Internal Auditor Magazine

Earn 3 CPE credits by reading Internal Auditor (Ia) magazine articles and answering questions about them here.

Other CPE Opportunities

Individuals can also earn CPE credits by giving presentations, writing exam questions, and more. Visit your individual CPE certification page (above) for details or see the administrative directive.

Member Spotlight

The IIA Spokane Chapter will be spotlighting various chapter members each month to find out why the member chose their profession, what they do for fun (besides audit), and what has made them successful.

Member: Nikki Russell
Position: Senior Auditor
Company: Global Credit Union
Certifications: Certified Operations Officer

Q: How did you become an internal auditor?
   In 1997 after 24 years in branch banking I decided I needed to do something different and the opportunity came available with Sterling Bank.

Q: What do you enjoy the most in your current position?
   Working with the people.

Q: What are some of the challenges you face in your current position?
   Staying current with all Regulations.

Q: If you were not an auditor, what would you be doing?
   Dental Hygienist.

Q: Any special skills or experiences you are proud of as an internal auditor?
   17 years as a bank auditor, over 40 years in the banking industry.

Q: What are your passions or hobbies outside of internal audit?
   Fly fishing.

Q: Any word of advice to fellow internal auditors?
   Hang in there and have fun.
The IIA’s CIA Learning System®

Prepare to pass the CIA exam with the experts! The IIA’s CIA Learning System was created by a team of CIA-certified industry experts to be the most relevant, comprehensive, and effective CIA review program available.

This interactive self-study program combines reading materials with online study tools to teach and reinforce the entire global CIA exam syllabus in a flexible, on-demand format. Looking for more structure, guidance and motivation? Facilitator-led courses are also available around the globe in traditional classroom, online and virtual formats.

Prepare to pass the CIA exam and arm yourself with critical tools and knowledge to excel in your internal audit career. Get started today!

Six Steps to Certification

1. Decide Which Certification is Right for You
The IIA’s Certified Internal Auditor® (CIA®) certification is the only globally accepted designation for internal auditors. The IIA also offers four specialty certifications.

2. Determine Your Eligibility and Skill Level
Each of The IIA certification programs has unique and specific education eligibility requirements that a candidate must meet to take the exam. In addition, you may want to assess your skill level by taking a practice test using the sample questions on the website. Although your score on a practice test will not necessarily indicate what your score would be on a certification exam, a practice test may assess your readiness and lets you know in what areas you need improvement.

3. Register for the Exam
The IIA’s certification exams are now offered year-round through computer-based testing at more than 500 locations worldwide.

   Apply and Register Online

4. Prepare for the Exam
You determine the method(s) in which you need to prepare for the exam. A variety of independent third-party providers offer exam review courses. In addition, consider joining one of the exam-related social media groups to connect with others preparing for the exam. Each exam has its own LinkedIn group and there is a Facebook page dedicated to preparing for the CIA exam.

5. Take the Exam
With the transition to computer-based testing, The IIA’s certification exams are administered through the worldwide network of Pearson VUE Testing Centers. The Pearson VUE network enables candidates to take exams at over 500 sites. The Certification Candidate Handbook provides more information on the testing experience.

6. Receive Your Certificate
Once you pass the exam and meet all other program requirements, you will be eligible to receive your certificate. To order your certificate, you must log into your candidate record in CCMS and complete the certificate order form. The certificate will be shipped directly to you using a standard postal service method at no charge. Expedited shipping is also available at an additional cost.
Back to Basics

Sometimes it’s good to get back to the basics of something we do every day. In this section of the newsletter we will review some of the basic skills and practices that internal auditors use on a daily basis.

This month’s article comes from a December, 2014 Internal Auditor article.

Five Personal Investments for Career Success
By: Richard Chambers

In my nearly 40 years in internal audit, I have worked for diverse organizations with immensely talented individuals from all corners of the globe. The experiences gained during those years taught me many valuable lessons about the profession and those we serve. Fortunately, I discovered early on how vital it is to make investments in my own career future. Warren Buffett said it best: “Investing in yourself is the best thing you can do.”

In my professional journey, I found that investing in personal growth can be grouped into five areas, and I encourage all internal auditors to consider these strategic investments in their own career.

1. Pursue Excellence
Don’t settle for being good. Pursue greatness in everything you do.

The internal audit profession is constantly evolving and adapting to the needs of a dynamic business environment focused on emerging risks and economic challenges. In this climate, internal auditors have an obligation to their stakeholders not to settle for just being good. The needs and challenges they face demand greatness from professionals who must identify emerging risks and align with the changing goals of the board and senior management.

Throughout my career, I was never willing to settle for good. I determined that whatever the challenge, whatever the requirements, whatever the goals set before me, I wouldn’t just meet them. I would do whatever it took to exceed them. It’s this mind-set — an unyielding personal mandate — that can propel people to great success.

As the business world evolves, internal auditors must pursue new skills and attributes. Beyond developing technical skills required by the rise and impact of new technologies, they also must nurture a broad range of nontechnical qualities. Nontechnical skills that will serve internal auditors well are effective communication, excellent business relationships, and shrewd negotiating for partnering with audit clients to reach reasonable and effective solutions to emerging risks.

2. Invest in Continuous Learning
Without a passion for continuous learning, internal auditors are less likely to be effective in their jobs. They should become a sponge for knowledge and supplement the training they receive at work with some of their own dollars.

3. Make Your Own Breaks
Internal auditors should look for opportunities to broaden their footprint in their career field. Opportunity often arises from personal investment in career growth. As 17th century philosopher Francis Bacon asserted: “A wise man will make more opportunities than he finds.”

I am a big believer in making your own breaks. Throughout my career many of the opportunities presented to me came as the result of my own efforts. I didn’t knowingly cause these opportunities to present themselves, but my pursuit of excellence got the attention of the people who offered those opportunities to me.
Internal auditors should recognize the potential they possess to create new opportunities beyond the specific job they were hired to do. They can find ways to increase their visibility in the audit profession by actively providing voluntary service to others.

4. Be Relevant to Those You Serve
Internal auditors should continually look for ways to increase their value to their leaders. They should challenge themselves to find creative ways to gain the leaders’ support, especially those they believe do not really value internal audit’s work. Become the team member they just can’t get along without.

5. Develop Courage in the Face of Adversity
Rising above the fear of failure can be the greatest motivator for success. We have all heard the story of the incredible fortitude and tenacity of Cynthia Cooper and her audit team in the face of the enormous adversity they confronted to expose the fraud at WorldCom. Most internal auditors may never come up against adversity of that magnitude, but most will encounter adversity that demands inner strength and tenacity. There may be times when audit engagements turn contentious. There may be times when an emerging risk threatens the solvency of an organization, and management will likely turn to the internal audit team for analysis and strategies to resolve the issues. Determine now to stand courageously in the face of such obstacles and pressures.

There have been several times during my career when I needed that kind of courage. One stands out in my mind above others. During the time I served as director of Internal Review for the Army at the Pentagon, I encountered what I later came to view as “the audit wars.” The auditor general for the Army wanted to expand the scope of his operations to directly oversee internal review. But I shared the view of other Army leaders — that allowing internal review offices around the world to report directly to commanders, the equivalent of their CEOs, made for a stronger model.

Although it was a stressful time for me, I proposed a period during which his audit team and those that I oversaw would run identical tests to determine what success each team could achieve. At the end of the agreed-upon test period, the supremacy of the existing model was readily obvious. Had those on our side of the debate not been courageous enough to stand for a test to prove the efficiency and skill of our team, it’s likely that the Army would have eliminated a valuable resource used by military leaders around the world.

The Road to Success
The time is now for internal auditors to make investments in their own career that will successfully equip them to become more relevant and valuable to their organization. Greatness for today’s internal auditors will be defined by the skill set and technical sophistication they possess to adapt to the needs and expectations of their stakeholders. While internal auditing’s fundamental principles and standards will always be the foundation of an internal auditor’s career, it is passion for remaining focused on the needs of stakeholders that will lead the way to success.
### 2014 – 2015 IIA Spokane Chapter Officers

*Spokane IIA Chapter Officers elected for the 2014-2015 Chapter Year:*

<table>
<thead>
<tr>
<th>Title</th>
<th>Officer</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter President</td>
<td>David Gifford</td>
<td>AmericanWest Bank</td>
</tr>
<tr>
<td>VP Membership &amp; Programs</td>
<td>Melanie Shanks</td>
<td>Spokane Teacher's Credit Union</td>
</tr>
<tr>
<td>VP Communications</td>
<td>Stephen Hunt</td>
<td>AmericanWest Bank</td>
</tr>
<tr>
<td>Treasurer</td>
<td>Terra Kile</td>
<td>DeCoria Maichel and Teague P.S.</td>
</tr>
<tr>
<td>Secretary</td>
<td>Vanessa Scarpelli</td>
<td>Umpqua Bank</td>
</tr>
</tbody>
</table>

### 2014 – 2015 IIA Spokane Chapter Board of Governors

*Spokane IIA Chapter Board of Governors for the 2014-2015 Chapter Year:*

<table>
<thead>
<tr>
<th>Governor</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penny Brown</td>
<td>AmericanWest Bank</td>
</tr>
<tr>
<td>Debra Peterson</td>
<td>Washington Trust Bank</td>
</tr>
<tr>
<td>Cathy Cook</td>
<td>Washington Trust Bank</td>
</tr>
<tr>
<td>Colleen Warner</td>
<td>Global Credit Union</td>
</tr>
</tbody>
</table>

[Click here to opt-out of future communications from the IIA Spokane Chapter.]