

## **The “U” in Information Security**

**Raymond T. Albert**  
**Professor of Computer Science**  
**University of Maine at Fort Kent**  
**23 University Drive**  
**Fort Kent, ME, 04743**  
**(207) 834-7696**  
[ralbert@maine.edu](mailto:ralbert@maine.edu)

### **Abstract**

Information security continues to rise in importance at all levels and across all domains. Academic and administrative technology innovations often over emphasize the non-human elements of information security. Our educational computing environments are uniquely and ideally positioned to significantly contribute to the best preparation of future information workers and leaders through the advancement of safe and sensible educational computing practices. This advancement can be achieved through better education and most importantly by personal involvement, for you are the “U” in information security.

### **Introduction**

The information age has elevated the importance of information security across the globe. Advances in academic and administrative technology have contributed to improvements in information security, but often do not adequately address the human side of the equation. End users are often their own worst enemies when it comes to information security failures. Numerous organizations, including the government and various news media are reporting an increase in the number of information security failures. Often, the impact of one information security failure cascades into a collection of damages and costly knee-jerk reactions. Consider for example the following reports and scenario that relate data breaches, identity theft and the approaches for dealing with consequential damages.

The Identity Theft Resource Center (ITRC, 2008) recently reported an increase of 47% between 2007 and 2008 in the incidence of data breaches. The term data breach is commonly defined as unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information. One example of the damage that can result from data breaches is identity theft.

The number of identity theft complaints increased by 5% to 259,266 for 2007 and by another 21% to 313,982 for 2008, according to the most recently released Federal Trade Commission ID Theft Clearinghouse report (FTC, 2009, p. 5). Identity theft is ranked in the report as the top consumer fraud complaint category for the ninth year in a row.

The increase in incidence of identity theft has greatly fortified the growth of the identity protection service sector despite the very real challenges that sector faces. For example, Richard Todd Davis, CEO of LifeLock Inc., continues to advertise his social security number and a challenge to anyone to steal his

## ***2009 ASCUE Proceedings***

identity, despite the fact his own identity was compromised (Celizic, M., 2008). According to a recent press release by Hagens Berman Sobol Shapiro LLP, the company has also been named in 13 consolidated lawsuits related to an initial class-action lawsuit that alleges the company defrauds its customers by offering services it cannot legally perform, and by touting a \$1 million guarantee that the suit alleges is wildly misleading (Firmani, M., 2009).

Perhaps as a mild form of vigilantism, some are beginning to advocate a much more aggressive approach for dealing with the increasing frequency of data breaches and resulting identity theft stemming from failures of those organizations that have been entrusted with personal information. One such approach, advocated by Matthew D. Sarrel (2009), is to "... hit them where it hurts, in the bottom line" (p. 1) by encouraging victims of identity theft to cancel or transfer their accounts from those entities that have allowed the data breach to occur.

This simple collection of reports and scenario exemplify the significance of the problem at hand. The problem has continued to grow even after it was made clear in the National Strategy to Secure Cyberspace report that "healthy functioning of cyberspace is essential to our economy and our national security. ... users need to know the simple things that they can do to help to prevent intrusions, cyber attacks, or other security breaches. All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace" (DHS, 2003, p. vii). The report contains an outline of "... an initial framework for organizing and prioritizing efforts" (p. vii) to address the securing of cyberspace. Among these efforts is the acknowledgement that "education and outreach play an important role in making users and operators of cyberspace sensitive to security needs" (p. 38). Education, and in turn, educational institutions are viewed therefore as instrumental to bolstering information security for the benefit of the individual and in turn the government and global community.

One of the most efficient and commonly employed methods for bolstering information security in the community at large is through user education that is primarily targeted at raising awareness. According to Jeffrey R. Young (2008) who recently compiled a top-10 list of campus computer-security risks, "user awareness is growing in importance when it comes to computer security" (p. 1). It is therefore essential to raise awareness about information security risks and threats, how best to think and act sensibly when responding to them, and ultimately how to contribute as an educational community member toward the improvement of information security through better education and modeling of appropriate practices. Every member of the community can and must contribute.

## **The Challenge**

Threats to information security exist at very different levels and they will always exist. Charles W. Flink II (2002) captures nicely what has been suggested by so many, namely "... the root cause for 30+ years of failure in the Information System Security market derives from a failure to appreciate one of the most basic principles of security: no security solution is ultimately stronger than its weakest link" (Flink II, C., 2002, p. 1). That is, the greatest threat to information security is usually where knowledge and application of sound risk mitigation practices are weakest. The focus thus changes from the information security experts to the end users who, often unknowingly, engage in practices that exacerbate risk.

## *2009 ASCUE Proceedings*

The challenge therefore is to mitigate information security risks and threats through proper user education in the many forms that may entail. Sometimes the best way to raise awareness and appreciation of something is through the sharing of good counter-examples. Raising awareness of and modeling appropriate practices while contrasting them against inappropriate practices can often expedite the education process.

While many are somewhat knowledgeable of sound information security practices, they may not be as familiar with the many pitfalls and security mistakes that information security professionals regularly witness and are often charged to rectify. The following counter-example lists may be beneficial to such a population:

“The five worst security mistakes end users make”, according to the SysAdmin, Audit, Network, and Security (SANS) Institute (2005):

1. Failing to install anti-virus [software], keep its signatures up to date, and apply it to all files.
2. Opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources.
3. Failing to install security patches-especially for Microsoft Office, Microsoft Internet Explorer, Firefox, and Netscape.
4. Not making and testing backups.
5. Being connected to more than one network such as wireless and a physical Ethernet or using a modem while connected through a local area network. (SANS Institute, 2005)

“The ten dumbest things people do to mess up their computer”, according to Wyman, Reichert, York, Rietveld, and Paller (2008):

1. Plug into the wall without surge protection ...
2. Surf the Internet without a hardware firewall and a software firewall  
...
3. Turn off the antivirus because it slows down your system ...
4. Install and uninstall lots of programs, especially freeware ...
5. Keep your hard drive full and fragmented ...
6. Open all email attachments ...
7. Click on everything ...
8. Believe that Macs don't get viruses ...
9. Use easy quick passwords ...
10. Don't bother with backups. (Wyman, Reichert, York, Rietveld, & Paller, 2008, pp. 1-10)

“10 common security mistakes that should never be made”, according to Chad Perrin (2008) of TechRepublic.com:

1. Sending sensitive data in unencrypted email ...
2. Using “security” questions whose answers are easily discovered ...
3. Imposing password restrictions that are too strict ...
4. Letting vendors define “good security” ...
5. Underestimating required security expertise ...

## ***2009 ASCUE Proceedings***

6. Underestimating the importance of review ...
7. Overestimating the importance of secrecy ...
8. Requiring easily forged identification ...
9. Unnecessarily reinventing the wheel ...
10. Giving up the means of your security in exchange for a feeling of security ... (Perrin, C., 2008)

Lenny Zeltzer has prepared a cheat sheet entitled “How to Suck at Information Security” that provides a compendium of information security mistakes in an easy to share and publicize format (Zeltzer, L., 2008).

These counter-examples are useful not only as educational aids, but also for clarifying the challenge involved in raising awareness in and better educating the user population about proper information security practices. Sometimes, the risks and threats to information security are not as easily understood or are so clouded in hype that it becomes very challenging to users to discern the most appropriate course of action. What is also needed is a way for users to think and act in a sensible way about choices related to information security.

### **Thinking and Acting Sensibly**

Maintenance of the confidentiality, integrity, and availability of information is the primary goal of information security. It is achieved through protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The allocation of resources to the achievement of this goal most often involves the process of risk assessment and management, of considering information security not as absolute, but as something involving trade-offs.

Bruce Schneier (2003) reminds us in his book *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* that “there’s no such thing as absolute security” (p. 17) and that the degree of security we seek is dependent upon what we are willing to give-up or trade-off to achieve it. Convenience is often the factor that most often is exchanged for increase information security. Shutting down or logging off from a computer whenever you step away from it is inconvenient, but it greatly reduces many risks to information security.

Schneier presents a five-step process to demystify and make explicit the choices and trade-offs being considered when addressing security issues. It is not a solution, but instead a methodology for helping one to make choices about all forms of security including information security. The five-step process is actually a collection of questions one should answer in order to avail themselves to sensible choices and tradeoffs. The introduction of this paper posed the data breach as an example of a failure in information security that can cascade into numerous damaging consequences. That scenario will be used to help elucidate the meaning of Schneier’s questions:

Step 1. “What assets are you trying to protect?” (p. 14) The asset of concern in a data breach can be presumed in most cases to be identification information for a collection of individuals. Identification information is therefore the asset that should be protected.

Step 2. “What are the risks to these assets?” (p. 14) The risks to the asset consists primarily of loss of confidentiality through access by unauthorized individuals who can in turn use the information for the purpose of identity theft to commit one or more forms of fraud (e.g., credit fraud).

### *2009 ASCUE Proceedings*

Step 3. “How well does the security solution mitigate those risks?” (p. 14) The given scenario is non-specific in this situation, but clues about how well security solutions mitigate these risks are contained in the ITRC report “... only 2.4% of all breaches had encryption or other strong protection methods in use. Only 8.5% of reported breaches had password protection. It is obvious that the bulk of breached data was unprotected by either encryption or even passwords.” (ITRC, 2008, p. 1) The ITRC does not consider in its reports of data exposure those records that have been encrypted but does include those records that are password protected. This is probably due to the fact that data is not actually exposed until it has been decrypted. One may therefore presume that encryption or other strong protection methods are more effective in mitigating the above identified risks when compared with password protection alone. One should also remember that even the strongest of protection methods are insufficient in completely mitigating all risks.

Step 4. “What other risks does the security solution cause?” (p. 14) Again, the given scenario is non-specific in this situation, but by focusing on password protection as a candidate security solution one can conjecture as to the additional risks this solution imposes. As Schneier points out, “this question addresses what might be called the problem of unintended consequences” (p. 14) and it may therefore be difficult at first to appreciate how the use of passwords imposes some additional risk. Consider for example the relation between the often misguided belief that simply having a password will ensure protection and the effects of poor password management and use practices. Users who are required to utilize passwords may actually decrease their vigilance over information security by presuming the use of a password will guarantee information security. The reduction in vigilance may impose risk above and beyond the level that which exists when passwords are not required.

Step 5. “What costs and trade-offs does the security solution impose?” (p. 15) Continuing with the given non-specific scenario and the focus on password protection as a security solution it is possible to explore the concomitant costs and trade-offs. One cost associated with password protection is the inconvenience to access imposed upon users. It would be much more convenient for users to granted access unimpeded by passwords. Additional costs are present in the form of users’ time and energy in properly managing their passwords by, for example, changing them often and remembering them. These costs are being exchanged for improvements to information security through the reduction of the risks associated with the loss of confidentiality of identification information for a collection of individuals.

Despite the appropriateness and practicality of Schneier’s five-step process he reminds all that “good security uses technology, but centers around people” (p. 145). The human element is crucial to the maintenance of information security. Thus, users and their awareness and knowledge of sound information security practices are once again at the core. For this reason, the academic and administrative leadership communities in education are ideally positioned to best prepare the future information workers and leaders.

The ingredients to improving information security include, raising awareness of the risks, threats, and possible damages resulting from failures in information security, raising awareness of proper information security practices through modeling and sharing of effective examples and counter-examples, and personally contributing to the creation of a climate and culture of sound information security practices

## 2009 ASCUE Proceedings

within our educational environments. The overall aim is to best improve information security through proper education and the advancement of safe and sensible educational computing practices.

### A Call to Action

Knowledge of what needs to be accomplished is only as valuable as the knowledge of how it will be accomplished. One does not have to be an information security professional to contribute to the solution. Similarly no organization or community should allow itself to rely solely on such individuals to maintain information security. The solution lies in community involvement and contributions that can be made at all levels and through all styles of learning. Numerous resources have been created since the first national call to action and they are readily available for immediate use or implementation.

The educational resources and tools listed in Table 1 are only a small sampling of what is currently available for information security. They have been selected because they represent the breadth of what is available and because of the variability in demands placed upon the individual who can best use or implement. For example, the website models are best utilized by individuals within the educational organization who have web site development knowledge, skills and access. Awareness videos, on the other hand, can be utilized by virtually any individual within the organization.

Category	Educational Resource/Tool
Videos	Award winning videos to improve information security awareness (EDUCAUSE/Internet2 Computer and Network Security Task Force and the National Cyber Security Alliance) available at <a href="http://www.researchchannel.org/securityvideo2007/">http://www.researchchannel.org/securityvideo2007/</a>
Games	Cyber Ciege (Naval Postgraduate School and Rivermind, Inc.) available at <a href="http://cizr.nps.navy.mil/cyberciege/">http://cizr.nps.navy.mil/cyberciege/</a>  Cyber safety games (OnGuard Online) available at <a href="http://www.onguardonline.gov/games/overview.aspx">http://www.onguardonline.gov/games/overview.aspx</a>  Privacy Playground: The First Adventure of the Three CyberPigs (Media Awareness Network) available at <a href="http://www.media-awareness.ca/english/games/privacy_playground/">http://www.media-awareness.ca/english/games/privacy_playground/</a>
Website Model	Five elements for a Successful Security Website (EDUCAUSE/Internet2 Computer and Network Security Task Force) available at <a href="https://wiki.internet2.edu/confluence/display/secguide/Operations+Security#OperationsSecurity-5elements">https://wiki.internet2.edu/confluence/display/secguide/Operations+Security#OperationsSecurity-5elements</a>

## 2009 ASCUE Proceedings

Community/User Awareness Models	<p>Resources for Community Awareness through K-12 Schools (Purdue University Center for Education and Research in Information Assurance and Security (CERIAS)) available at <a href="http://www.cerias.purdue.edu/education/k-12/community_awareness/">http://www.cerias.purdue.edu/education/k-12/community_awareness/</a></p> <p>Model user awareness programs and materials (EDUCAUSE/Internet2 Computer and Network Security Task Force) available at <a href="http://www.educause.edu/HigherEducationResources/8767">http://www.educause.edu/HigherEducationResources/8767</a></p>
Currency Practice	<p>National Cyber Alert System Bulletins &amp; Alerts (US-CERT) available at <a href="http://www.us-cert.gov/cas/index.html">http://www.us-cert.gov/cas/index.html</a></p> <p>Security Awareness Tips (The SANS Institute) available at <a href="http://www.sans.org/tip_of_the_day.php?utm_source=web-sans&amp;utm_medium=ImageReplace&amp;utm_content=TipofDay_BigExPoint&amp;utm_campaign=HomePage&amp;ref=3626">http://www.sans.org/tip_of_the_day.php?utm_source=web-sans&amp;utm_medium=ImageReplace&amp;utm_content=TipofDay_BigExPoint&amp;utm_campaign=HomePage&amp;ref=3626</a></p>
Utilities	<p>Password Safe (SourceForge.net) available at <a href="http://passwordsafe.sourceforge.net/">http://passwordsafe.sourceforge.net/</a></p> <p>Gnu Privacy Guard (GnuPG) OpenPGP implementation (Gnu Project, Free Software Foundation, Inc.) available at <a href="http://www.gnupg.org/">http://www.gnupg.org/</a></p>

**Table 1:** A small sample of educational resources and tools for promoting information security awareness and appropriate practices.

No matter which of these resources or tools a user elects to implement or utilize to improve their own information security, they will also be fostering in their colleagues a culture of improved information security through heightened awareness and modeling of appropriate information security practices. Active acceptance and promotion of such efforts by the academic and administrative leadership greatly advances this process.

### Conclusion

Information security continues to grow in importance across the globe and it is viewed by our nation as a key aspect of the healthy functioning of cyberspace which is, in turn, viewed as essential to our economy and national security. Innovations in academic and administrative technology aimed at improving information security require concomitant advances in the awareness and education of the user population in order to achieve maximum effectiveness. Allowing oneself to be the “weakest link” is becoming more intolerable by the community at large in our increasing information age society. Social norms and expectations regarding information security are continuing to evolve. As these change over time, modifications to the legal system will also evolve to help reinforce them. Through community involvement, appropriate information security practices will supplant those that are inappropriate and society will be better for it.

## ***2009 ASCUE Proceedings***

Information security is not absolute but instead relative. It requires one to consider and make trade-offs. Convenience is often the factor that most often is exchanged for increase information security. Bruce Schneier's five-step process may be used to demystify and make explicit the choices and trade-offs being considered when addressing security issues. It is not a solution, but instead a methodology for helping one to make choices about all forms of security including information security.

Educational computing environments are ideally positioned to foster and promote improved information security through better education and modeling of appropriate practices in all users. Those who serve in academic and administrative leadership positions within these environments can and must contribute to the creation of a climate and culture of sound information security practices within our educational environments. Every individual, no matter their role in the educational organization, can contribute in their own way. The contribution can be as small as simply raising one's own awareness and refraining from engaging in inappropriate information security practices. Remember, improvements to information security are needed and made possible through better education and most importantly by personal involvement, for you are the "U" in information security.

## **References**

Celizic, M. (2008). ID theft CEO who had identity stolen defends service. *TodayShow.com*. Retrieved May 5, 2009 from <http://today.msnbc.msn.com/id/24790921/>

Firmani, M. (2009). *United States District Judge Assigned Consolidated LifeLock Lawsuits*, Appoints HBSS as Lead Counsel. Retrieved May 5, 2009 from [http://www.hbsslaw.com/lifelock\\_appointment](http://www.hbsslaw.com/lifelock_appointment)

Flink II, C. W. (2002). Weakest Link in Information System Security. *Workshop for Application of Engineering Principles to System Security Design (WAEPSSD) Proceedings*. Retrieved May 5, 2009 from <http://www.acsac.org/waepssd/papers/01-flink.pdf>

Identity Theft Resource Center (ITRC) (2008). *Security Breaches 2008*. Retrieved May 5, 2009 from [http://www.idtheftcenter.org/artman2/publish/lib\\_survey/Breaches\\_2008.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml)

Perrin, C. (2008, August 15). 10 Common Security Mistakes that Should Never Be Made. Message posted to <http://blogs.techrepublic.com.com/security/?p=542>

SANS Institute (2005), *Mistakes People Make that Lead to Security Breaches*. Retrieved May 5, 2009 from <http://sans.org/resources/mistakes.php?ref=3816>

Sarrel, M. D. (2009). Identity theft is out of your hands. *PC Magazine*. Retrieved May 5, 2009 from <http://www.pcmag.com/article2/0,2817,2340785,00.asp>

Schneier, B (2003). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, 2003. New York: Copernicus Books.

## ***2009 ASCUE Proceedings***

United States Department of Homeland Security (DHS) (2003). *The National Strategy to Secure Cyberspace*. Retrieved May 5, 2009 from [http://www.dhs.gov/xlibrary/assets/National\\_Cyberspace\\_Strategy.pdf](http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf)

United States Federal Trade Commission (FTC) (2009). *Consumer Sentinel Network Data Book*. Retrieved May 5, 2009 from <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>

Wyman, B., Reichert, A., York, J., Rietveld, B. & Paller, A. (2008). The Ten Dumbest Things People Do to Mess Up Their Computer. *SANS OUCH!*, 5/12. Retrieved May 5, 2009 from <http://www.sans.org/newsletters/ouch/issue/20081210.php>

Young, J. R. (2008). Top 10 Threats to Computer Systems Include Professors and Students. *Chronicle of Higher Education*, 55/17. Retrieved May 5, 2009 from <http://chronicle.com/free/v55/i17/17a00901.htm>

Zeltzer, L. (2009). *How to Suck at Information Security*. Retrieved May 5, 2009 from <http://www.zeltser.com/security-management/suck-at-security-cheat-sheet.html>

### **Acknowledgements**

Special thanks to Rachel, Alexandra and Samuel for their patience and support and to all those cited above for their contributions to and promotion of information security.